Comparative Analysis of Hazard and Operability Study (HAZOP) and Systems Theoretic Process Analysis (STPA)

Faisal Jamal
Manager - Corporate HSE & TS, Fatima Fertilizer Company Limited, Pakistan

Dr. John P. Thomas
Scientist - Department of Aeronautics and Astronautics, MIT, USA
Preamble

• Fatima Fertilizer Company Limited (FFL) - Fatima Group’s flagship manufacturing facility. Annual fertilizer production 1.3 MT.


• An endeavor to establish a comparison between STPA and current and established risk assessment techniques in the process industry - HAZOP.

• Looked at past 30 years’ incidents in Ammonia plants using published info.

• Selected the complex CO₂ Removal System - includes human, machine and software interactions.

• This system’s HAZOP was conducted by an experienced and qualified team maintaining high quality as per HAZOP methodology.

• An incident occurred on this HAZOP-ed system due to a missing control logic - not identified during HAZOP.
CO₂ Removal System Process Flow

Synthesis Gas to Methanator

Absorber

Stripper

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)
CO₂ Removal System Process Flow

Synthesis Gas
(H₂, N₂, Ar, CH₄, H₂O, CO₂ & CO in ppm)

HV-25

(CO₂, H₂, H₂O)

Semi-lean Solution

Absorber

Raw Synthesis Gas
(H₂, N₂, Ar, CH₄, H₂O, CO₂)

Lean Solution

To Cold Box

Synthesis Gas
(H₂, N₂, Ar, CH₄, H₂O)

Seal Gas to Expander

Heat Input

Methanator

Regenerator

Lean Solution

Semi-lean Solution
Incident Description

- Foaming in CataCarb solution observed causing excessive and repeated carryover of solution to Methanator.
- Methanator temperature increased to 960°F (515°C) and the Methanator inlet valve HV-25 closed immediately as per control logic.
- However, this also cut the downstream seal gas flow towards the Cold box expander.
- Cold box expander process gas broke through from HP drain to oil console causing console over pressurization and consequently hydrogen fire.
Incident Description

Synthesis Gas
(H₂, N₂, Ar, CH₄, H₂O, CO₂ & CO in ppm)

HV-25
(CO₂, H₂, H₂O)

Methanator
To Cold Box
Synthesis Gas (H₂, N₂, Ar, CH₄, H₂O)

Regenerator
Heat Input

Absorber
Semi-lean Solution
Raw Synthesis Gas (H₂, N₂, Ar, CH₄, H₂O, CO₂)
Lean Solution

Seal Gas to Expander
Methanator and Expander

Methanator Selector Switches & Discontinuation of Seal Gas flow caused cold process gas ingress to sour oil return towards oil console
Corrective Actions

1. Control logic modified to automatically trip Cold box expander on:
   - Methanator inlet valve HV-25 closure
   - Differential Pressure across seal gas and HP seal oil < 0.2 kg/cm$^2$
   - Differential Pressure across seal gas and expander casing drops below 0.1 kg/cm$^2$

2. Installed a degasifying tank at sour oil HP drain line to avoid oil console over pressurization and consequent fire due to higher seal gas venting.

Safe and smooth plant operation after trip logic and other relevant modifications
Remarks

• The experienced team did everything as required by the HAZOP methodology, but the requirement was missed.

• Petrochemical/refining processes are complex in nature and there is always a possibility of missing out any critical logic due to nodes/guidewords analyses.
Let’s try STPA!
STPA: Hazard Analysis

1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios

Identify Losses, Hazards
Define System boundary

Environment

System

Losses to prevent
Model
Behavior to prevent
How could behavior occur

(Leveson and Thomas, 2018)
CO₂ Removal System Process Flow

- CO₂ Analyzer DCS
- Lean Pump
- Level Indicator to DCS
- PDI to DCS
- TI to DCS
- CO₂ Analyzer DCS
- Lean solution on top bed
- Semi lean solution
- Rich solution
- CO₂ to Urea Plant
- Manual valve and local indicator
- Synthesis Gas to Methanator
- HV-25
- Gas IN
- Reboiler
- Manual valve
- CO₂ Removal System Process Flow

<table>
<thead>
<tr>
<th>Nomenclature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCS:</td>
<td>Distributed Control System (Human + Software)</td>
</tr>
<tr>
<td>Ti:</td>
<td>Temperature Indicator</td>
</tr>
<tr>
<td>PI:</td>
<td>Pressure Indicator</td>
</tr>
<tr>
<td>LI:</td>
<td>Level Indicator</td>
</tr>
<tr>
<td>LAL:</td>
<td>Level Alarm Low</td>
</tr>
<tr>
<td>LAH:</td>
<td>Level Alarm High</td>
</tr>
<tr>
<td>GLG:</td>
<td>Glass Level Gauge</td>
</tr>
<tr>
<td>FIC:</td>
<td>Flow Indicator and Controller</td>
</tr>
<tr>
<td>HPDA:</td>
<td>High Pressure Differential Alarm</td>
</tr>
<tr>
<td>PDI:</td>
<td>Pressure Differential Indicator</td>
</tr>
<tr>
<td>I:</td>
<td>Interlock (Software for safe shutdown)</td>
</tr>
<tr>
<td>Manual valve</td>
<td>Manual valve</td>
</tr>
<tr>
<td>Level Indicator DCS</td>
<td>Level Indicator to DCS</td>
</tr>
<tr>
<td>Lean solution</td>
<td>Lean solution</td>
</tr>
<tr>
<td>Lean exchanger</td>
<td>Lean exchanger</td>
</tr>
<tr>
<td>Sem lean Pump</td>
<td>Semi lean Pump</td>
</tr>
<tr>
<td>Hydraulic turbine</td>
<td>Hydraulic turbine</td>
</tr>
<tr>
<td>Rich Sol to stripper</td>
<td>Rich Sol to Stripper</td>
</tr>
<tr>
<td>Synthesis Gas to Methanator</td>
<td>Synthesis Gas to Methanator</td>
</tr>
<tr>
<td>Reboiler</td>
<td>Reboiler</td>
</tr>
<tr>
<td>Manual valve</td>
<td>Manual valve</td>
</tr>
<tr>
<td>Level Indicator DCS</td>
<td>Level Indicator to DCS</td>
</tr>
<tr>
<td>Lean solution</td>
<td>Lean solution</td>
</tr>
<tr>
<td>Lean exchanger</td>
<td>Lean exchanger</td>
</tr>
<tr>
<td>CO₂ Analyzer DCS</td>
<td>CO₂ Analyzer DCS</td>
</tr>
<tr>
<td>Lean Pump</td>
<td>Lean Pump</td>
</tr>
<tr>
<td>Level Indicator DCS</td>
<td>Level Indicator to DCS</td>
</tr>
<tr>
<td>Gas IN</td>
<td>Gas IN</td>
</tr>
<tr>
<td>Rich solution</td>
<td>Rich solution</td>
</tr>
<tr>
<td>CO₂ to Urea Plant</td>
<td>CO₂ to Urea Plant</td>
</tr>
</tbody>
</table>

DCS: Distributed Control System (Human + Software)
Ti: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)
Nomenclature

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAH: Level Alarm High
LAL: Level Alarm Low
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)
**DCS/PLC Controls**

**Human Controls**

- Synthesis Gas to Methanator
- CO₂ to Urea Plant
- Lean solution on top bed
- Semi lean solution
- Reboiler
- Absorber
- Stripper
- Manual valve
- Lean Pump
- Semi Lean Draws Off
- Lean exchanger
- Rich solution
- Lean solution
- Manual valves
- Local TI

**Nomenclature**

- **DCS**: Distributed Control System (Human + Software)
- **TI**: Temperature Indicator
- **PI**: Pressure Indicator
- **LI**: Level Indicator
- **LAL**: Level Alarm Low
- **LAH**: Level Alarm High
- **GLG**: Glass Level Gauge
- **FIC**: Flow Indicator and Controller
- **HPDA**: High Pressure Differential Alarm
- **PDI**: Pressure Differential Indicator
- **I**: Interlock (Software for safe shutdown)
- **Manual valve and local indicator (Human dependent)**

**Flowchart Details**

- Synthesis Gas to Methanator
  - CO₂ Analyzer DCS
- Lean exchanger
- Semi Lean Pump
- Level Indicator to DCS
- PDI to DCS
- TI to DCS
- CO₂ to Urea Plant
- Manual valve
- Lean Pump
- Semi Lean Draws Off
Hydraulic turbine
P-4
Lean exchanger
Semi lean Pump
Level Indicator to DCS
PDI to DCS
TI to DCS
CO₂ to Urea Plant

DCS/PLC Controls
Human Controls
Feedback

Nomenclature
DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)
STPA Control Structure Model (Quick sketch)

Human Operator

Open/Close HV-25

PLC (Programmable Logic Controller)

Close (Expander Inlet Valve)

Open, Close

Valve (HV-25)

Valve 1-PDV-030A

Methanator Bed High Temp

Level low

Level Alarm Low (LAL)

Sensor

1-TT-025 A/B/C/D (TAH)

Level Alarm High (LAH)

1-LI-048 /1-LI-049 (LAH)

Controlled Processes
(E.g. Absorber, Stripper, Methanator, Cold box, Expander)

Incomplete, for demonstration purposes only
STPA Control Structure Model (Quick sketch)

- **Human Operator**
  - Open/Close HV-25
  - Open, Close (Expander Inlet Valve)
  - **PLC (Programmable Logic Controller)**
    - Valve (HV-25)
    - Valve 1-PDV-030A
    - Methanator Bed High Temp
    - **Controlled Processes** (E.g. Absorber, Stripper, Methanator, Cold box, Expander)
      - 1-TT-025 A/B/C/D (TAH)
      - Level Alarm Low (LAL)
      - Level Alarm Low (LAL) Sensor
      - Level Alarm High (LAH)
      - 1-LI-048 / 1-LI-049 (LAH)

Incomplete, for demonstration purposes only
A simpler diagram

Physical Process

Absorber → HV-25 Valve → Methanator → Expander

HV-25 Close Cmd

Expander Trip Cmd
<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, Too late, Order</th>
<th>Stopped too soon, Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td><strong>UCA-1:</strong> PLC does not provide Close HV-25 Cmd when actual liquid level is high in the Absorber. [SH-2, SH-3, SH-4]</td>
<td><strong>UCA-2:</strong> PLC provides Close HV-25 Cmd when actual liquid level in absorber is normal (cause Methanator trip). [SH-4]</td>
<td><strong>UCA-4:</strong> PLC provides Close HV-25 Cmd too early when liquid level is high (trip set point) [SH-4]</td>
<td><strong>UCA-6:</strong> PLC continues providing Close HV-25 Cmd too long after liquid level is normal (will prevent startup when issue is resolved)</td>
</tr>
<tr>
<td></td>
<td><strong>UCA-3:</strong> PLC provides Close HV-25 Cmd while expander remains in service (causes low seal gas flow to expander which will eventually result in fire) [SH-1,SH-2,SH-4]</td>
<td></td>
<td><strong>UCA-5:</strong> PLC provides Close HV-25 Cmd too late when liquid level in absorber is high (causes solution carryover to Methanator causing run away of reaction which will lead to Methanator vessel failure) SH-1,SH-2,SH-4</td>
<td><strong>UCA-7:</strong> PLC stops providing Close HV-25 Cmd too soon before valve has fully closed</td>
</tr>
<tr>
<td>Open</td>
<td>[...]</td>
<td>[...]</td>
<td>[...]</td>
<td><strong>UCA-8:</strong> PLC stops providing Close HV-25 Cmd too soon before liquid level in absorber has returned to normal</td>
</tr>
</tbody>
</table>
### STPA Step 3: Operator Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, Too late, Order</th>
<th>Stopped too soon, Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td>[...]</td>
<td>[...]</td>
<td>[...]</td>
<td>[...]</td>
</tr>
<tr>
<td>Unsafe Control Action</td>
<td>Controller Requirement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCA-1: DCS does not provide Close MV-25 cmd when actual liquid level in absorber is too high</td>
<td>R-UCA1: DCS shall provide Close MV-25 cmd when actual liquid level in absorber is too high (LAH=true) [UCA-1]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCA-3: DCS provides Close MV-25 cmd too late (&gt;10 sec) after liquid level in absorber is too high</td>
<td>R-UCA3: DCS shall provide Close MV-25 cmd within &lt;10 sec of liquid level in absorber too high [UCA-3]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCA-6: DCS provides Open MV-25 cmd when liquid level in absorber is too high</td>
<td>R-UCA6: DCS must not provide Open MV-25 cmd while liquid level in absorber is too high [UCA-6]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Incomplete, for demonstration purposes only
UCA-3: PLC provides Close HV-25 Cmd while expander remains in service (causes low seal gas flow to expander which will eventually result in fire) [SH-1, SH-2, SH-4]

CA-1: Tripping expander incase of low seal gas pressure/flow as a result of HV-25 closure is not incorporated in control algorithm

R-CA.1: DCS shall provide automatic Expander Trip Cmd when HV-25 is closed
STPA Step 4: Building Accident Scenarios

**UCA-3:** Operator does not manually trip Expander C-103 when HV-25 is closed (causes low seal gas flow to expander which will eventually result in fire) [SH-1, SH-2, SH-4]

**CA-1:** Tripping expander in case of HV-25 closure not effectively learned as a procedure (missing procedure, inadequate training for this procedure, conflicts with experience, etc.)

**PM-1:** Operator busy in emergency handling and forgets to trip expander

**PM-2:** Operator believes expander is already tripped automatically

**FB-1:** Missing alert/warning indicating HV-25 closed without expander trip (fire danger)

**FB-2:** RMP signal are not visible to operator on DCS

**FB-3:** Incorrect pressure reading for seal gas
Conclusion

At the time of detailed engineering of Catacarb unit, the potential Hazard was not anticipated against the HAZOP guide word of no flow to expander. Similarly the consequence was not captured during HAZOP under Methanator upstream valve closure due to two separate nodes.

Therefore, it may be concluded that this specific and well recognized technique “HAZOP” may be limiting in capturing all the hazards even if applied as per defined methodology/guideline.

However, STPA did result in identifying the missing control logic.
Thank You