Trust, but Verify:
The case for placing the entire safety lifecycle in one accessible place

Presenter
A.M. (Tony) Downes
Global Process Safety Advisor

1988-1992 Bayer Canada, Supervisor LPE
2001-2010 FMC. Global Safety & Sec. Mgr
2010-date Honeywell PMT Global PS Advisor

• Led over 100 PHAs
• Did first LOPA in 1999
• Led over 100 Incident Investigations
• Launched 4 Risk Reduction programs

• CCPS Tech Steering and Planning Cmtes
• CCPS Certified Process Safety Engineer

“Everything I know about Process Safety, I learned in an investigation”
Three available data sets: HazOp/LOPA + Process Historian + CMMS
Case Study 1: What happens if/when the Layers/Barriers don’t work?

Example: Gasoline Tank Overflow → Fire
- Initiating Event: LIT Error. IEF ~1/10 years\(^1\)
- Safety Interlock: LSHH→XZV  SIL\(^2\)
- Conditional Modifier: Prob. Of Ignition ~0.99\(^3\)
- Combined Probability of Fire ~ 0.001/year

---

Some potential problems
- Process measuring device faults (sticking)
- XZV fails to shut
- XZV closes, but slowly (degraded)
- LSHH Fail-dangerous unrevealed
- LSHH left in bypass after proof-test

---

Level Transmitter + PS Site or Equivalent Monitoring software instead

---

Most LSHH faults can’t be diagnosed remotely. Only a proof-test will do.

---

Turn your Process Historian data into Safety Insights
Calculating & Summing Risks

Risk from Scenario = Consequence \times Likelihood

Likelihood = (IEF \times PFD_1 \times PFD_2 \text{ etc})

**Example - Risk Ranking**

**Total Corporate Risk** = \sum_{1}^{\#\text{Sites}} \sum_{1}^{\#\text{Units at site}} \sum_{1}^{\#\text{Hazard}} \text{Consequence}_i \times \text{Likelihood}_i
Case Study 2: Vessel Rupture Hazard

Safe Operating Limits – High Level

Level High High: 507” – SIF-1 Trips
Inlet Flow Shutoff Valves

Level High: 348” – LSH-102
Separate Safety Rated Alarm with Operator Action

Normal Level High: 327”

LIC-100 BPCS Level Controller

Normal Level Low: 302”

Design meets criteria

How can we assure we are “in the Green” year after year?
Case Study 2 continued

As Designed

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SCENARIO:
High high high level leads to rupture – single fatality. Assumed low Occupancy

Cause Frequencies: 0.1 / yr – 0.01 / yr
PSV: PFD = .01
Alarm: PFD = 0.1
SIF: RRF Target - ~20 (SIL 1)

How is it working in reality?
Case Study 2 continued - From the Analytics System

- **Initiating Event Frequency**
  - Level in Vessel versus SOLTs
    - Level > 327” – 9 times 2017; 17 times 2018
    - Level > 348” – 9 times 2017; 17 times 2018
    - Level > 507” – 0 times

- **Time in Bypass for IPLs**
  - 0 hrs operated with SIF in bypass

- **IPL proof testing**
  - SIFs – 365 day Proof Test Interval (PTI) req’d
    - Actual PTI days = 365, 600, 337, 312, 473
  - Safety Rated Alarm – 36 month PTI req’d
    - Actual PTI = *Never Tested*

- **IPL failures**
  - SIFs – 2 failures

---

After 5 years of time in service, how does actual operations compare to the project assumptions?

The following data impacts the actual mitigated event likelihood:

**SCENARIO:**
High high high level leads to rupture – multiple fatality.

- **IEF:** >>0.1/yr
- **Alarm:** ?
- **SIF:** < 10RRF

- **Time in Bypass for IPLs**
- **IPL proof testing**
- **IPL failures**
Conclusions

1. HAZOP/LOPA contains the Intended Risk situation
2. Analytics using data historians shows risk gaps (opportunities to improve)
3. The issues and opportunities were not apparent at first.

Having the HAZOP, LOPA, Cause & Effect Matrix and Historian Analytics in a Safety ‘Digital Twin’ enables sustainable analytics
Digital Twin for Process Safety enables...

Identify Bad Actors. Real-time Risk Management

System Behavior from LOPA / SOL

Expected SIF Behavior from Cause & Effects Matrix

DCS/SIS Process Data, & Event Log

Device information

Cloud Analytics

Cloud Data Consolidation

Track SIF overrides, bypasses across units and sites

Provide Demand Rate and SIL/RRF estimates to PHA

Capture proven-in-use data for SIF elements, and more...

Identify Bad Actors. Real-time Risk Management
Honeywell is building a smarter, safer, and more sustainable world

THAT’S THE POWER OF CONNECTED
THAT’S THE POWER OF HONEYWELL

Connected Aircraft · Connected Automobile · Connected Home · Connected Building
Connected Plant · Connected Supply Chain · Connected Worker

Honeywell
THE POWER OF CONNECTED