Honeywell Advanced Materials’ new Low-Global-Warming Refrigerant Plant in Geismar, LA
A little about the 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”
LOPA and the Integrity of the Layers

Focus on the Control and Safety Layers

Two key questions:

1. Is the SIS Prevention layer ready?
   - Is it Degraded in any way today?
   - How did it perform during last Demand (Real or Spurious)?
   - What is the RRF/PFDavg over the past year or so?

2. How steady is the control system (BPCS Layer)?
   - Any critical control loops “Degraded”?
   - What is the Initiating Event Frequency really?
   - “Flat-line” diagnosis

Initiating Event + SIF not ready → Serious incident
What happens if/when the Layers/barriers don’t work?

Example: Gasoline Tank Overflow → Fire
- Initiating Event: LIT Error. IEF ~1/10 years¹
- Safety Interlock: LSHH → XZV  SIL²
- Conditional Modifier: Prob. Of Ignition ~0.99³
- 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 trip test

1. Typical failure rate from CCPS LOPA Book.
2. Assumed RRF of 100 (PFD = 0.01)
3. CCPS POI Tool for heptane at 60degF: POII ~.01; PODI ~0.99; POEGI ~0.5

Level Transmitter + PSSuite 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 x Likelihood

Likelihood = (IEF x PFD1 x PFD2 etc)

Total Corporate Risk = \[ \sum_{k=1}^{\# Sites} \sum_{j=1}^{\# Units at site} \sum_{i=1}^{\# Hazards} \text{Consequence}_i \times \text{Likelihood}_i \]

Enterprise data systems support Corporate Risk Management
It’s really an “estimate” of Risk

1. PHA/LOPA teams estimate the Initiating Event Frequency (IEF)
   - Likely based on typical industry probabilities.
   - A number of good references available these days
     - New CCPS LOPA database
     - Usually OK within an order of magnitude
   - Teams have a bias towards Underestimating likelihood

2. Independent Protection Layer (IPL)/ Safety Instrumented Function (SIF) reliability.

3. Maintain: Not simple to keep SIL2 PFD better than 0.01 forever

Can we get more accurate numbers from our own facilities?
Example of a LOPA taking credits for various IPLs

Need:
- TMEL = 100,000
- PFD = 1/RRF

So PFD of:
- BPCS = 0.1
- PSV = 0.01
- SIF = 0.01

PFD = 0.1 x 0.01 x 0.01
= 0.00001
→ RRF = 100,000 ✓

Order depends on process design, etc.
New HFO Unit (Overpressure Protection)

The LOPA

• Initiating Event (IE):
  - Pressure Control loop fails →
    ▪ Overpressure & Rupture, Major Hazard
    ▪ Frequency (IEF): 1 Failure / 10 years = 0.1/yr

• Independent Protection Layers (IPL):
  1. Overpressure SIF102 closes XZV102
     ▪ PFD = 0.01
  2. Pressure Safety Valve (PSV)
     ▪ PFD = 0.01

• Mitigated Event Likelihood
  - MEL = 0.1/yr * 0.01 * 0.01 = 0.00001 = 1E^-5

✓ Design meets criteria

How can we assure we are “in the Green” year after year?
Insights from a Recent Analysis

From LOPA1: Pressure Control System

Demand rate (IEF)
- From HAZOP/LOPA:
  - Expected fault rate between 1/year – 1/10 years
  - Actual control system fault rate: 1 amongst 10 PIT loops in 3+ years
  - No reason to suspect the PIT fault was related to process application

Safeguard
- SIL affirmation
  - Target Availability SIL-2 (>99%)
  - Actual outage/unavailable time for 2 PZIT loops <48 hours in 3+ years (>99.9%) better than expected

From LOPA2: HtEx Leak Monitoring

Demand rate (IEF)
- From HAZOP/LOPA:
  - Special tubes. Special precautions. New service
  - Expected tube failure rate about 1/year
  - Actual Heat Exchanger leak-through rate: 0 amongst 10 exchangers in similar service over 3+ years

Safeguards
- SIL
  - Combination of Conductivity and pH analyzers arrayed in voting systems
  - Target RRF ~10 for each analyzer
  - ACTUAL on next few slides
Example – LOPA2 High SIF Demand Rate

• In “Low Demand Rate” designs, we assume the Safety Instrumented Function (SIF) will get a demand less than once per year

• More than once per year indicates the design needs expert diagnosis and may need to be more robust

• A few times per week???

PSS Workbench showed 2oo3 Voting System is better choice
Valve Stroke Duration Evolves Over Time

• This XZV is performing well within the required Process Safety Time, BUT

• Stroke time is trending up for both Opening and Closing.

• Will your plants notice when stroke time is getting close to Process Safety Time?

NOTE: This spreadsheet, pivot and graph originally took about 1 hour in Excel
Diagnosing a Flat-Lined Transmitter

- Transmitter signals (PV’s) generally change over time.
- If the signal is not varying in any way for a long time, like 100AZI4001A, the transmitter may have developed a fault.
- Maintenance Inspection/recalibration appropriate (once diagnosed).

Hard to do Manually. Easier with Analytic Tools.
Conclusions

• While the Design of the Safety Instrumented Functions provides the target amount of protection, the actual field performance of a few SIFs did not.

• This didn’t matter as the Initiating Event Frequency was actually much better than anticipated by the HAZOP/LOPA team.

• Analytics from field performance showed a number of opportunities to improve the system.

• The issues and opportunities were not apparent at first.

• Having the LOPA, Cause & Effect Matrix and Historian Analytics in a Single Data System simplifies analysis dramatically.
Process Safety Suite enables…

- Identify Bad Actors. Real-time Risk Management

- Expected SIF Behavior from Cause & Effects Matrix
- System Behavior from LOPA / SOL
- DCS/SIS Process Data, & Event Log
- Cloud Data Consolidation
- Cloud Analytics

- 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…

* On-premise solution if preferred

© 2015 by Honeywell International Inc. All rights reserved.
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
Consensus Standards give guidance but don’t say HOW

**IEC61511:**

16.2.2 tells us to develop “the information which needs to be maintained on system failure and demand rates on the SIS” and “the information which needs to be maintained showing results of audits and tests on the SIS” and have “procedures for analysing systematic failures.”

16.2.6 “Discrepancies between expected behaviour and actual behaviour of the SIS shall be Analysed”…

This shall include monitoring the following:

- the actions taken following a demand on the system;
- the failures of equipment forming part of the SIS established during routine testing or actual demand;
- the cause of the demands;
- the cause of false trips.

16.3.1.5 At some periodic interval (determined by the user), the frequency of testing shall be reevaluated based on various factors including historical test data, plant experience, hardware degradation, and software reliability.”