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

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

1978-1988 **DuPont** Canada. Project Eng, Process Eng, Product Development, Maintenance Eng, Project Manager
1988-1992 **Bayer** Canada, Supervisor LPE
1992-2001 **Westlake** Group, Principle PS Eng.
2001-2010 **FMC**. Global Safety & Sec. Mgr
2010-date **Honeywell PMT** Global PS Advisor

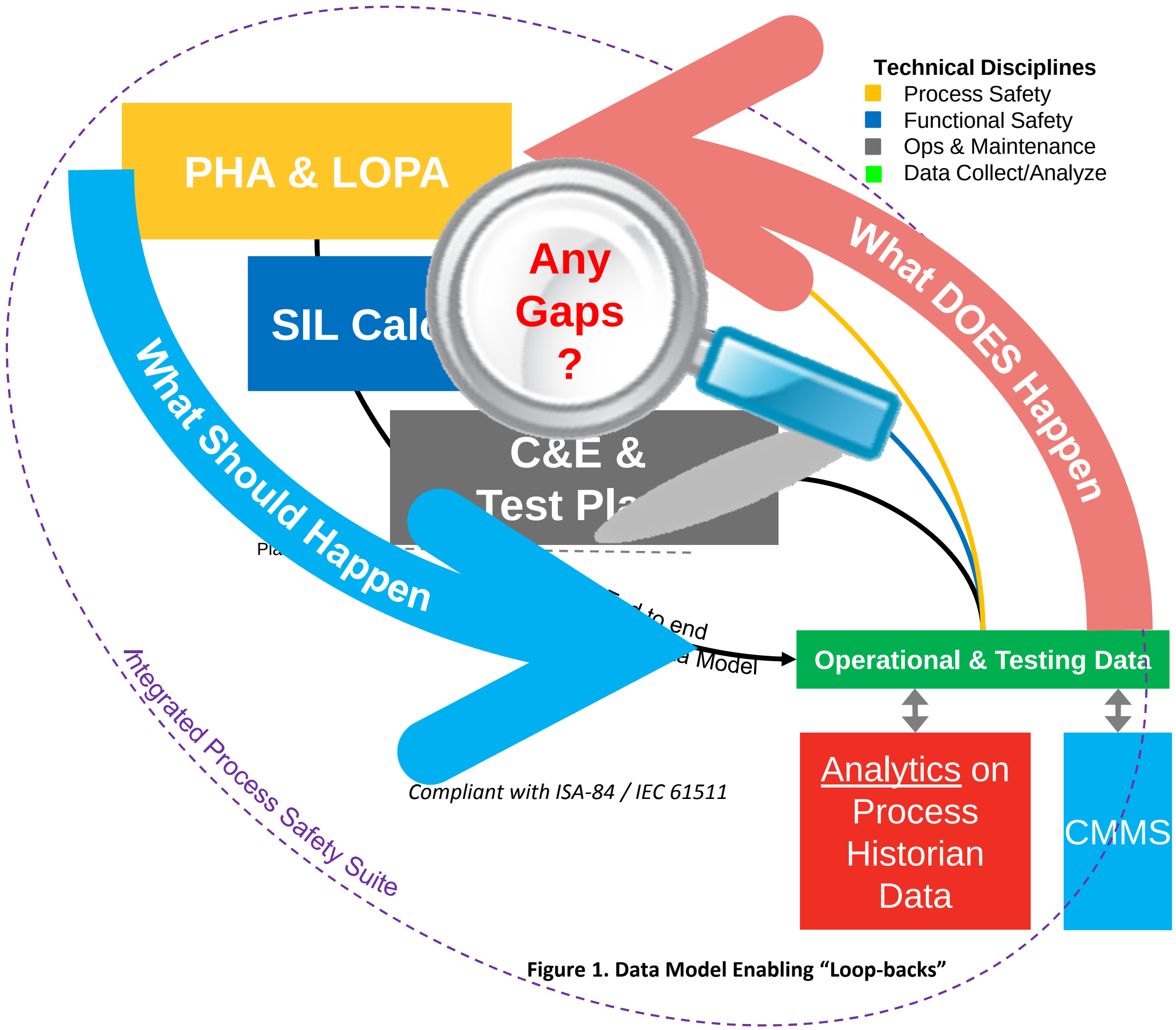
- Led over 100 PHAs
- Did first LOPA in 1999
- Led over 100 Incident Investigations
- Launched 4 Risk Reduction programs

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

"Everything I know about Process Safety, I learned in an investigation"

Honeywell
THE POWER OF CONNECTED

Three available data sets: HazOp/LOPA + Process Historian + CMMS



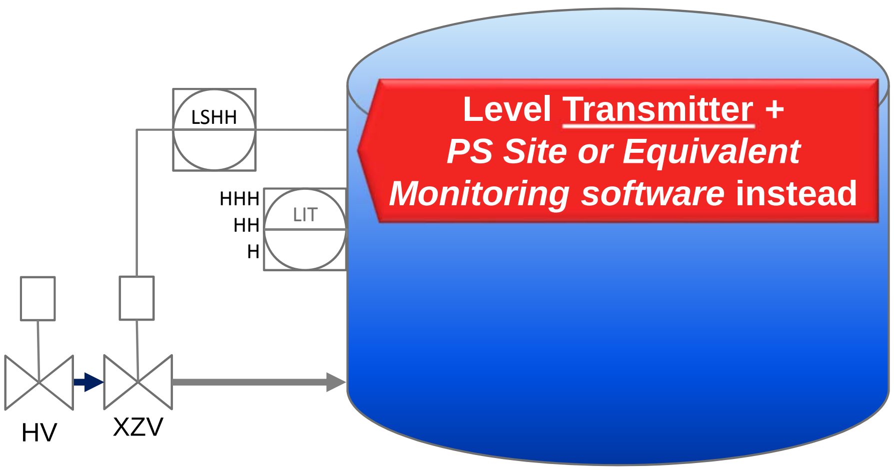
Honeywell
THE POWER OF CONNECTED

Case Study 1: What happens if/when the Layers/Barriers don't work?

Example: Gasoline Tank Overflow→ Fire

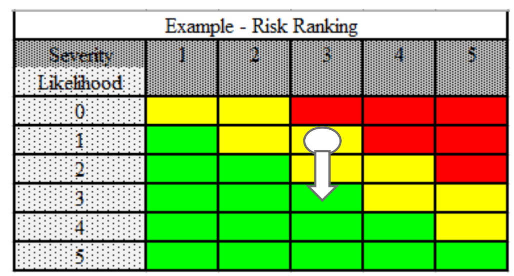
- Initiating Event: LIT Error. IEF ~1/10 years[1]
- Safety Interlock: LSHH→XZV   SIL2[2]
- Conditional Modifier: Prob. Of Ignition ~0.99[3]
- Combined Probability of Fire ~ 0.001/year

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



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*



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

Turn your Process Historian data into Safety Insights

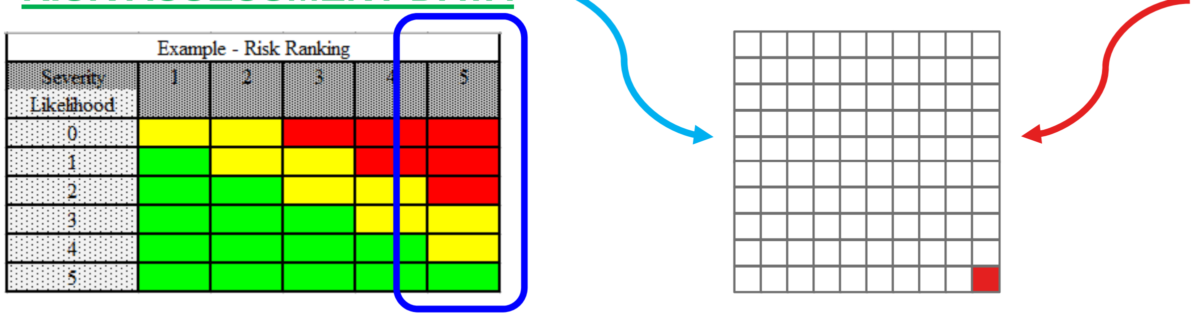
Refresher

Calculating & Summing Risks

$$Risk from\ Scenario = Consequence\ x\ Likelihood$$

$$Likelihood = (IEF\ x\ PFD_1\ x\ PFD_2\ etc)$$

RISK ASSESSMENT DATA



ANALYTICS from HISTORIAN

100 x 0.01 = 1

99 x 0.01 +1 = **1.99**

10% not unusual

90 x 0.01 + 10 = **10.99**

$$Total\ Corporate\ Risk = \sum_{1}^{\#\ Sites} Site\ k \sum_{1}^{\#\ Units\ at\ site} Unit\ j \sum_{1}^{\#\ Hazards} Consequence\ \ i * Likelihood\ i$$

Honeywell
THE POWER OF CONNECTED

Case Study 2: Vessel Rupture Hazard

<u>Safe Operating Limits – High Level</u>

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

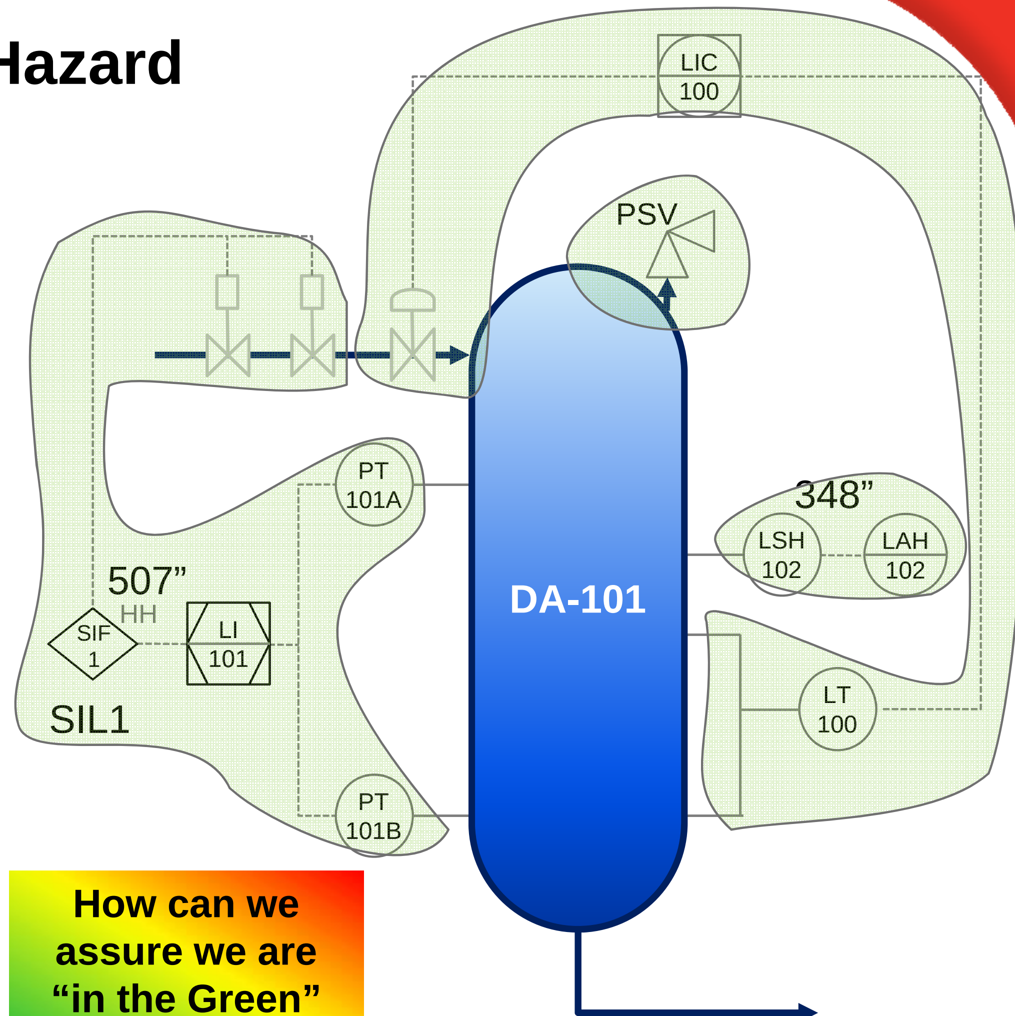
Level High: 348" – LSH-102 Separate Safety Rated Alarm with Operator Action

Normal Level High: 327"

LIC-100 BPCS Level Controller

Normal Level Low: 302"

✓ **Design meets criteria**

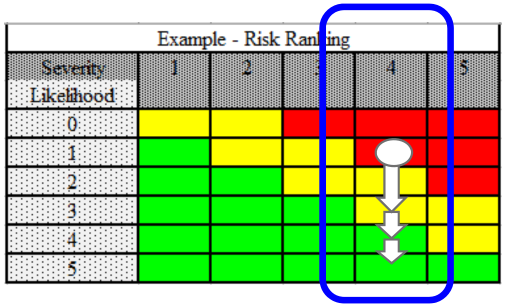


How can we assure we are "in the Green" year after year?

Honeywell
THE POWER OF CONNECTED

Case Study 2 continued

As Designed



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)

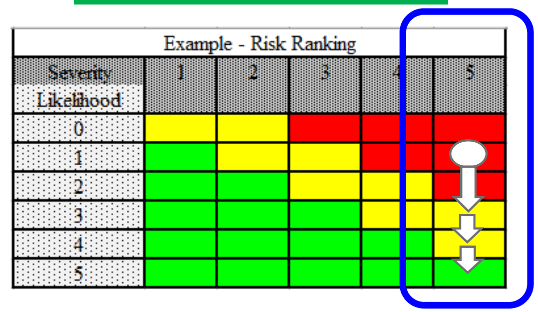
How is it working in reality?

Honeywell
THE POWER OF CONNECTED

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

During Revalidation



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

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

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:

- Cause Frequency
- Time in Bypass for IPLs
- IPL proof testing
- IPL failures

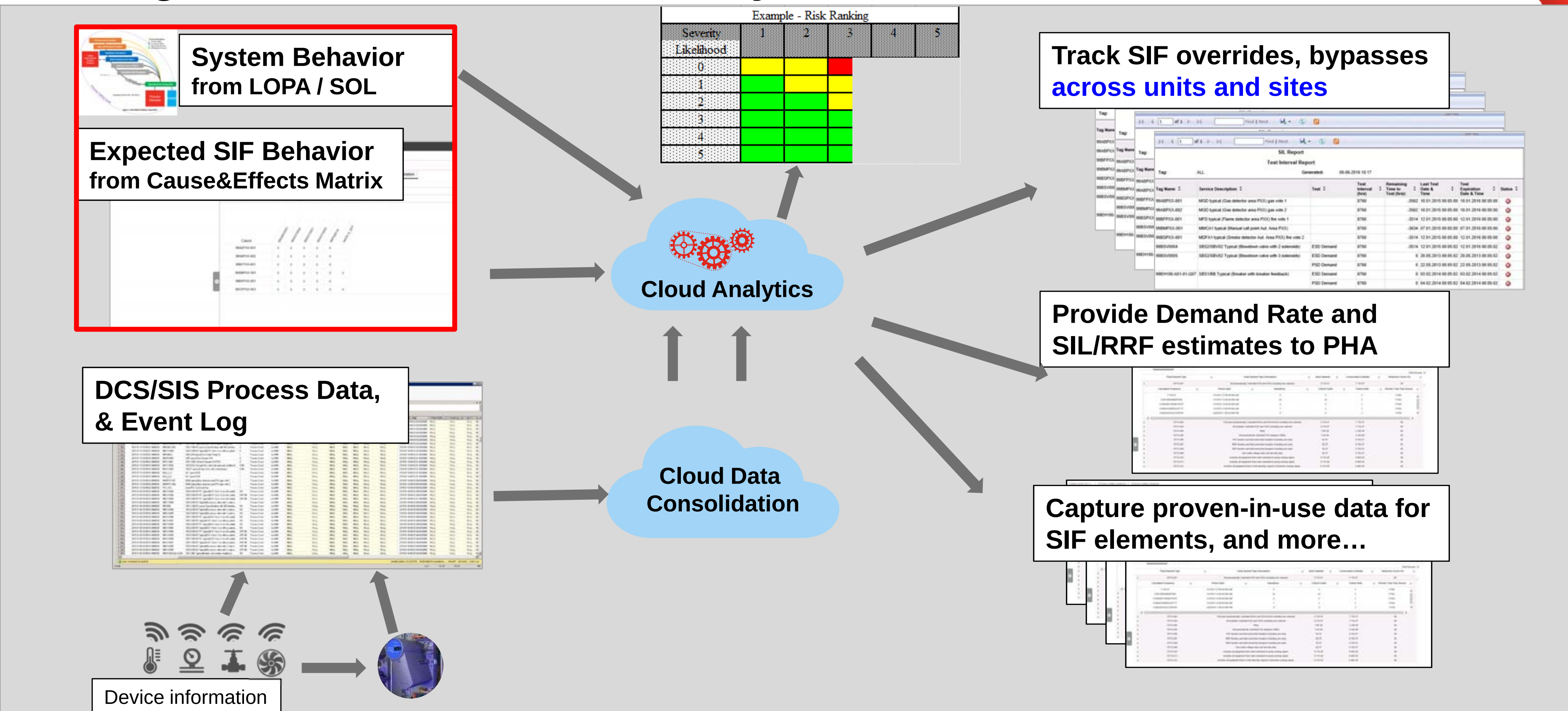
Honeywell
THE POWER OF CONNECTED

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

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**