Seamlessly Connecting the Process Safety Lifecycle Inside One System

Americas HUG

PROCESS SAFETY SUITE WORKSHOP
Seamlessly Connecting the Process Safety Lifecycle Inside One System
Americas HUG

Tony Downes/Prasad Goteti
June 11, 2019

REVEAL YOUR BEST
Introduction

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 HAZOPs
• 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”
Agenda

• PSS digitizes & links all lifecycle steps.
  – Links Functional Safety to Process Safety, Operations and Maintenance → Sustainability
  – Ease assessments, engineering execution & manage real time risks
  – The risk assessment & SIL Design becomes your Digital Twin for Safety

• ISA/IEC61511 compliance in O&M phase is hard. But it doesn’t have to be.
  – “Investigation of each demand”
  – Periodic FSA

• Close the loop by returning failure – and success - data from your Historian and CMMS back to the Model
Traditionally, the process safety lifecycle is inefficient

Process Safety


SIS Design

ROLES INTEGRAL TO THE PROCESS SAFETY LIFECYCLE
- Management
- Process Safety Engineers
- Functional Safety Engineers
- Instrument & Controls
- Automation and O&M

5-7 Work Groups
Average number of teams from PHA to logic, internal staff, consultants and EPCs

INFORMATION GATHERING, DELIVERABLES, REPORTS, AND TOOLS
- PHA & LOPA Reports
- SIL Verification
- Safety Requirements Specification
- SIS Cause & Effects
- Functional Test Plans

5+ Data Sources
Disparate reports and tools supporting safety lifecycle

© 2019 by Honeywell International Inc. All rights reserved.
Finally, we have THE solution…


Honeywell | Process Safety Suite

Process Safety

SIS Design

Operate Maintain

Reduce Project delays
Reduce Human errors

Drive Consistency
Drive Consolidation
Drive Safety transparency

Ensure Compliance
Ensure Bad actor identification
Ensure Risk elimination

5-7 Work Groups
Average number of teams from PHA to logic, internal staff, consultants and EPCs

5+ Data Sources
Disparate reports and tools supporting safety lifecycle
Process Safety Suite

Today the key information in the Process Safety Lifecycle is handled through many manual and disconnected steps.

Honeywell’s Process Safety Suite automates this lifecycle helping to reduce errors, lower costs, continuously monitor operations for hazard conditions and provide safety alerts in a timely fashion.

Seamlessly Connecting the ENTIRE Safety Lifecycle Inside One System
Leverage Process Safety Suite to Unlock Project Savings

Typical Capital Project

$10 Billion
Typical investment to build a competitive production facility

2000 SIFs
Conservative count of Safety Instrumented Functions (SIFs) to support a similar-sized facility

20 Hours
Conservative estimate per SIF to design and comply with IEC 61511/ISA-84

65%
Typical copy factor between equipment and SIFs

$ 2.7 Million
Savings in functional safety engineering services alone

Lifecyle Enabled
Data generated in design is ready to be used in operations to validate assumptions and make risk-based business decisions

Reduce

Drive

Ensure
Also flagged a system with high trip rate (spurious). Reduction in spurious trips saved $1M+ each time due to operational down-time. Initially 12 times per year reduced to less than 1 per year.
SWITCH TO DEMO
Actual Case Study: Vessel Protection

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 continued

As Designed

How is it working in reality?
Case Study 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

---

**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
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

Analytics compares Actual Performance against Intended Design
ISA/IEC-61511 give guidance but don’t say HOW

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.”

16.2.9 “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.

“It is very important that ALL discrepancies between expected behaviour and actual behaviour are analysed.”

How are you doing this today? Could you prove it?
Process Safety Analyzer

Shutdown Analyzer

Final Element Scout

SIL Reporting
PSA - Shutdown Analyzer

• Verifies that SIFs performed as expected by tracking SIF inputs and outputs against the C&E Matrix
• Analysis is done automatically. Highlights problems so:
  - Engineers can save time and focus on Solving any Problems
  - Operators know that valves reached the safe state. **Speeds safe Restart after trip**
  - Maintenance can focus on valves that had problems (Stuck or Slow)

All together, as a Structured data element
Shutdown Analyzer Outputs

- SingleEvent view for Operators
- Engineer view (e.g. with more equipment information, etc.)
- Blowdown view
PSA – Safety Element Scout

- Configurable to suit user requirements. Examples of information provided includes:
  - OK operations => command and response received within maximum travel time limit, including calculation of actual travel time
  - Operations with long travel time or travel time exceeding a warning limit
  - Failed operations (e.g. operations with no command or no response)
  - Trending of travel time
  - Alerts to an AMS (e.g. Asset Sentinel)
  - Long travel time
  - Travel time warning

Add operator or engineer comments
PSA – SIL Reports Examples

Test Interval Report

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Service Description</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>43PST10163_HH</td>
<td>LP flare return pump discharge valve</td>
<td>PSD Full Stroke</td>
</tr>
<tr>
<td>43X3V10064</td>
<td>HP flare return pump discharge valve</td>
<td>ESD Full Stroke</td>
</tr>
<tr>
<td>43X3V10164</td>
<td>LP flare return pump discharge valve</td>
<td>PSD Full Stroke</td>
</tr>
<tr>
<td>96ABPXX-001</td>
<td>MGD typical (Gas detector area PXX) gas vote 1</td>
<td></td>
</tr>
<tr>
<td>99BFXX-001</td>
<td>MFD typical (Flame detector area PXX) fire vote 1</td>
<td></td>
</tr>
<tr>
<td>99BMPPXX-001</td>
<td>MMCA1 typical (Manual call point Aut. Area PXX)</td>
<td></td>
</tr>
<tr>
<td>99BSBPXX-001</td>
<td>MDA1 typical (Smoke detector Aut. Area PXX) fire vote 2</td>
<td></td>
</tr>
<tr>
<td>99BSV0004</td>
<td>SBS2/3BV02 Typical (Blowdown valve with 2 solenoids)</td>
<td>ESD Full Stroke</td>
</tr>
<tr>
<td>99BSV0005</td>
<td>SBS2/3BV02 Typical (Blowdown valve with 3 solenoids)</td>
<td>ESD Full Stroke</td>
</tr>
<tr>
<td>99EH100-A01-007</td>
<td>SBS1/BB Typical (Breaker with breaker feedback)</td>
<td>ESD Full Stroke</td>
</tr>
<tr>
<td>99ESV0008</td>
<td>SBS2/3BV01 PS Typical (ESV Valve 3 sol with partial stroke)</td>
<td>ESD Partial Stroke</td>
</tr>
<tr>
<td>99GMV0001</td>
<td>SBF typical (Fire Damper SM)</td>
<td></td>
</tr>
<tr>
<td>99HS9001</td>
<td>MBS typical (CAP push button) NA3 X X x initiator</td>
<td></td>
</tr>
</tbody>
</table>

Demand Overview Report

<table>
<thead>
<tr>
<th>Demand Overview Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date: 18.06.2010</td>
</tr>
<tr>
<td>End Date: 19.06.2014</td>
</tr>
<tr>
<td>SIF Name: ALL</td>
</tr>
<tr>
<td>Status: ALL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Process Demand Rate</th>
<th>Process Demands</th>
<th>Fault Demands</th>
<th>Test Demands</th>
<th>Total Demands</th>
</tr>
</thead>
<tbody>
<tr>
<td>43PST10163_HH</td>
<td>1,00</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Process Demand Rate</th>
<th>Process Demands</th>
<th>Fault Demands</th>
<th>Test Demands</th>
<th>Total Demands</th>
</tr>
</thead>
<tbody>
<tr>
<td>99BFXX-001</td>
<td>2,5</td>
<td>10</td>
<td>1</td>
<td>1</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Process Demand Rate</th>
<th>Process Demands</th>
<th>Fault Demands</th>
<th>Test Demands</th>
<th>Total Demands</th>
</tr>
</thead>
<tbody>
<tr>
<td>99BMPPXX-001</td>
<td>1,00</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

© 2019 by Honeywell International Inc. All rights reserved.
### Final Element Verification Report

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Description</th>
<th>Number of Safety Operations</th>
<th>Number of Critical Faults</th>
<th>Fault Operations</th>
<th>All Operations</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>99BSV0004</td>
<td>SBS2/SBV02 Typical</td>
<td>12</td>
<td>9</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99BSV0005</td>
<td>SBS2/SBV02 Typical</td>
<td>20</td>
<td>15</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99XY0001</td>
<td>SBS1/SBV (Shutoff Damper)</td>
<td>2</td>
<td>1</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99XY0002</td>
<td>SBS3/MA (Deluge/Mist valve)</td>
<td>2</td>
<td>1</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99PA001A</td>
<td>SBE (SM) typical (Fire Water)</td>
<td>2</td>
<td>1</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99PA002-Q07</td>
<td>SBS1/SBE01 typical (Open Fire Damper)</td>
<td>2</td>
<td>1</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99GMV0001</td>
<td>SBF typical (Fire Damper SM)</td>
<td>2</td>
<td>1</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99XY0003</td>
<td>SBS3 Typical (Foam Valve)</td>
<td>1</td>
<td>0</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99EH100-A01-01</td>
<td>SBS1/BB Typical (Breaker)</td>
<td>2</td>
<td>1</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99ESV0008</td>
<td>SBS2/SBV01 PS Typical</td>
<td>20</td>
<td>15</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99KSV0007</td>
<td>LP flare return pump</td>
<td>12</td>
<td>9</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99KSV0009</td>
<td>HP flare return pump</td>
<td>20</td>
<td>15</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>99KSV0006</td>
<td>SBS1/SBV01 PS Typical</td>
<td>12</td>
<td>9</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
</tbody>
</table>

Drill down on «bad actors»
Functional Safety Assessment during Operations Phase

“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.”

Do this during the PHA Revalidation?
THE FUTURE IS WHAT WE MAKE IT.

...and we make it Safer
What if your Instrument Inspection system was connected?

• CMMS indicates Inspection is due
• Inspection procedure sent to Inspector
• Field inspection completed.
• Today, paper goes into file drawer

• Tomorrow, the As Found/As Left data goes back to PSS
• Validate Maintenance assumptions
• Proven-in-Use
Movilizer Inspect makes it possible
Record the observed trip point and compare it to the intended trip point. If the trip point is not within the tolerable range, mark the device as a Fail and continue the test.

Lower Test Limit: 0
Upper Test Limit: 650

PT-0100  Observed High
Trip Point: 330

Process Safety Suite