MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Using Process Historian Data to Understand and Assure Barriers

A.M. (Tony) Downes*, Prasad Goteti
Honeywell Performance Materials & Technologies
115 Tabor Rd, Morris Plains NJ 07950 USA
*Presenter Email: Anthony.Downes@Honeywell.com

Keywords: American Petroleum Industry (API), Computerized Maintenance Management System (CMMS), Key Performance Indicators (KPI), Loss Of Primary Containment (LOPC), International Electrotechnical Commissions (IEC), International Society of Automation (ISA), Independent Protection Layer (IPL), Layers Of Protection Analysis (LOPA), Occupational Safety and Health Administration (OSHA), Process Hazard Analysis (PHA), Performance Materials and Technology (PMT), Safety Instrumented Function (SIF), Safety Integrity Level (SIL), Safety Instrumented Systems (SIS), Safe Operating Limits Table (SOLT)

Abstract

Like many companies, Honeywell estimates the probability of control system problems and safeguard layer faults using the available reliability data. Probably like others, we have wondered how accurate these "standard numbers" are in our services. In our Advanced Materials division, we have been collecting real-world data on initiating events, Safety Instrumented Functions (SIFs) and other Independent Protection Layers (IPLs) in the data historians at two of our new low-global-warming Hydro Fluoro Olefin (HFO) units. Recently, we began using analysis tools to "mine" this data to see what it could tell us about our actual Initiating Event Frequencies and the Risk Reduction Factors being achieved. In essence, we are comparing the actual performance of our critical safety Layers of Protection with the performance that was intended by the PHA team.
In this paper we will describe the results of the Operation and Maintenance phase of the Safety Life Cycle and how we are using the resulting data in several important ways: to indicate the real-time health of active IPLs - watching for events like IPL degrading, and bypassing; to integrate the learnings as Key Performance Indicators (KPIs) to leadership and as inputs to our PHA/LOPA revalidations.

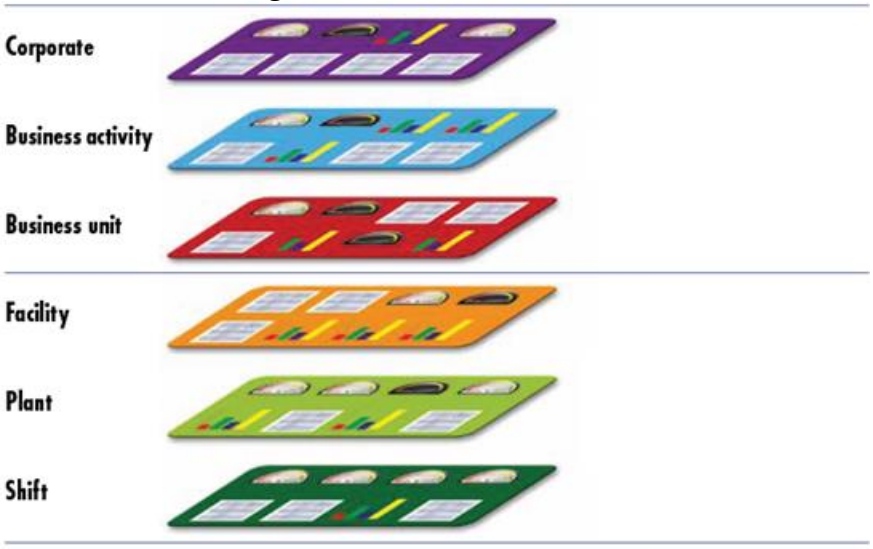
INTRODUCTION

Over the past 20+ years, improved understanding of process safety risk and decreasing risk tolerance has led to many more safety interlocks, particularly Safety Integrity Level (SIL) rated interlocks, being installed in process industry facilities. These have substantially reduced the probability and thus the risk of catastrophic incidents – generally by one or two orders of magnitude, possibly more. On the other hand, they have increased the number of trip activations – both real and spurious. And without a doubt they have increased the effort required to test and maintain these safeguards.

Standards like IEC 61511 / ISA 84.00.01*(ref 1)* and Recommended Practices like API RP 754 *(ref 2)* call for methods to identify and inform appropriate personnel at various levels in an organization on "Key Performance Indicators" (KPI) which could be either a leading indicator (before any incident or action occurs) or lagging indicator (after the incident or action). IEC61511 calls for Functional Safety Assessment of an installed Safety Instrumented System (SIS) after a few years of operation to make a judgement call based on such KPIs if the SIS is doing what it was supposed to.
Such KPI's are a useful measure to *(ref 3)*:

1. **Prevent major incidents** –KPIs released by an individual site to the company headquarters and later nationwide, the company (and other companies in the similar business) can analyze and learn what led to the Process Safety Incident, the root cause and how this can be avoided in the future.
2. **Improve Reliability –** Steps taken by a company to reduce major Process Safety Incidents help improve Reliability of Process Operations.[5]
3. **Avoid Complacency** – KPI's provide a measure of asset integrity. Just because there has been no major incident for a long time does not mean everything is fine. Leading KPI's could provide valuable information on the health of assets and indicate that it is time for maintenance on the asset.
4. **Communicate Performance –**KPI's could provide to the company and State / Country how the individual site is performing while **or** could asses performance internal to the individual site

Identifying key leading and lagging indicators at various levels in an organization and monitoring them on a continuous basis could give an indication of Process Safety performance at a site. These indicators, expressed as KPIs, are different at various levels in an organization. As an example, a major gas leak above the tolerable limits set by the local jurisdiction would be a lagging indicator and would be a KPI at the Corporate level while a demand on an SIS would be a leading indicator KPI for the Plant Manager and Shift Engineer indicating they should take a closer look at the process as to why a SIS Loop had to trigger on demand. See Figure 1 below.



KPIs at various levels in an organization will be different.

Figure 1 (*ref 3*)

COMPANY LEADERSHIP CONCERNS

Is enough being done?

It's natural to focus our attention on identifying and tracking the individual risk scenarios that have the potential to lead to catastrophic outcomes. We need to find these, then identify solutions, budget for them and eventually design and install them. While our leaders will initially be looking at achieving the risk targets, they'll eventually ask whether these solutions are giving the intended level of safety – especially if an incident occurs. Have you gone digging in a PHA report to see what it said after something went wrong? We certainly have.

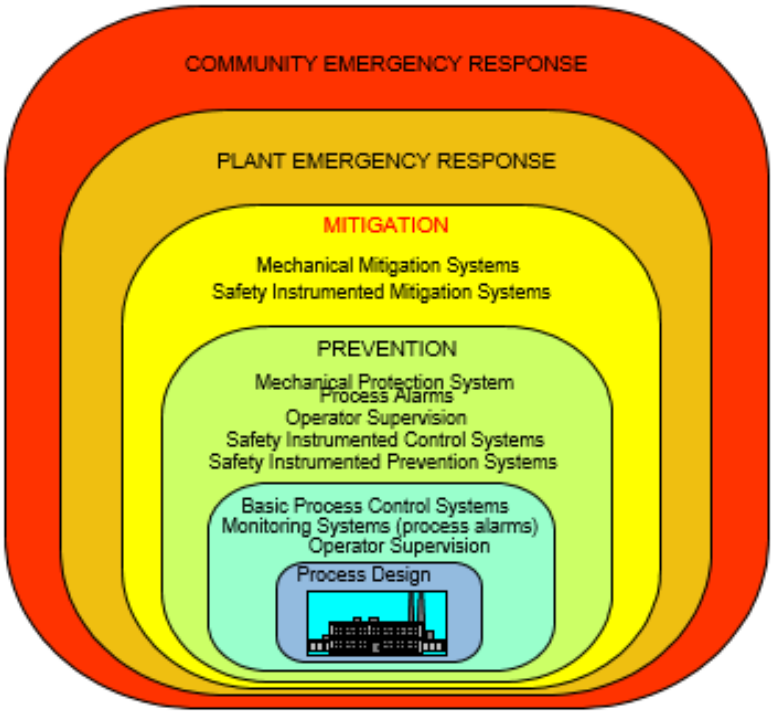


Figure 1 *(ref 1)* - The Layer of Protection Model, showing all layers

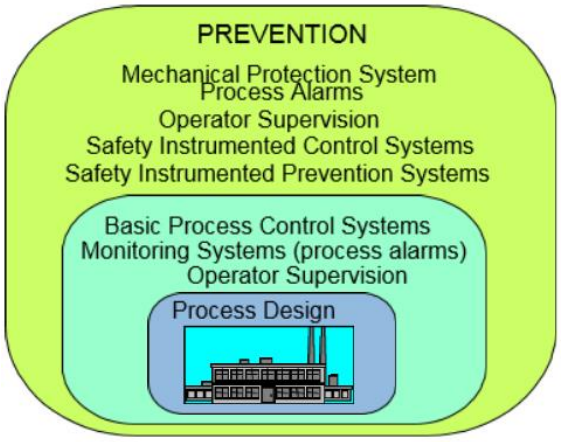


Figure 3 - Focus of this Paper

Are we doing the right things? Could we be doing too much?

For process safety staff, this is a tricky discussion. We have a tendency to think that there's no such thing as too much safety. But there are always multiple demands for capital and it's prudent to take a broader view. Certainly our leaders do. They recognize that reducing the risk of 10 scenarios by 1 order of magnitude (a factor of 10) is more effective[1] assuming ALL other factors are the same, than reducing 5 of them by 2 orders of magnitude (a factor of 100) and leaving the other 5 for later. Ignoring units for a moment, mathematically it looks like this:

Scenario 1, Mitigated Risk = 10 * 0.1 = 1

Scenario 2, Mitigated Risk = 5 *0.01 + 5 = 5.05

It's also why savvy leaders are looking for some proof that the investments they are making in process safety are paying off in reduced incidents.

1 There are enough caveats to this statement to fill another paper.

Moving from Rules-based Criteria to Data-based

Rules are important. They help the PHA teams obtain consistent results, and prevent most arguments. And we advocate for following the PHA rules in the vast majority of cases. But most operating companies allow their expert risk analysts to select partial credits for very well-understood and well controlled situations. If we are looking for optimal solutions, we need more accurate, "specific-to-our-application" data. In the past, we've looked solely to the Reliability Engineers to give us this, based on their testing data. It's still a good idea to include Reliability, but we can now provide ourselves with another source of raw data.

Is this system getting better than average Reliability? Or Worse?

Available industry standard failure rate data, such as CCPS's Process Equipment Reliability Database, has a wide range of values. In some cases more than 2 orders of magnitude from the lower values to the upper values. This makes sense given the wide variation in "quality" of something like a ball valve. Good ones tend to last longer. And, of course, services vary widely. High quality ball valves last even longer if they aren't in acidic mud ("severe") service. And the converse is true.

Most Layers of Protection Analysis (LOPA) teams struggle with these issues. If they choose to degrade the reliability from one of the "standard" values, they'll do it by a factor of 10. That may make sense, or it may be conservative. Or the actual performance may be even worse. You may have inspection results, or repair history, but it's time-consuming for maintenance to report this in great detail in their Computerized Maintenance Management System (CMMS), and it rarely gets down to the tag number of the particular instrument or valve involved. Even in the old days when paper records were kept, it was possible – though difficult – to extract reliability/availability information.

As a practical matter, you are depending on the opinion of the maintenance representative. Generally these folks remember the really bad actors IF they're close enough to the day-to-day work to know when a particular transmitter or valve required frequent repair because it failed in a "revealed" way. Only in rare cases do we get input about whether a particular valve had repeatedly failed in proof-testing even though it happens more frequently. So generally we are not getting up-to-date information in our Process Hazard Analysis (PHA) even though the information lies in our plant site's data systems.

EXAMPLES FROM A HONEYWELL PROCESS PLANT

The Problem

Honeywell's Performance Materials and Technologies (PMT) operating plants have been working on all the above issues, too. We've made it a requirement that our sites investigate each activation of a "PHA-Credited" Safeguard as a Near Miss. And IEC 61511 now asks the Functional Safety Engineers at the site to confirm the interlock worked properly as part of that investigation. Most of our SIS loops work reliably on demand once we install them. The demands on these SIS loops are also not frequent – especially as most are designed for "low demand mode". But in a business like ours, we want assurance both that the IEF is as low as we predicted and that the safeguards / protection layers are working at least as well as we predicted when we did the PHA. Here are a couple of examples – one good, and one not so good.

Example1

Pressure control loop on a distillation tower

This example considers a group of typical distillation columns. They have a Reboiler to provide heat and to boil up the liquid in the bottom. This is the most significant potential source of overpressure. Each column's vapor pressure is controlled by a simple overhead pressure control loop. A fault in that loop

could cause the column pressure to rise. Each column has a pressure safety relief valve (PSV) set to protect it by venting the contents of the column to a scrubber in case the control and alarm safety systems fail to prevent such an overpressure. In the past this might have been sufficient, but this system alone does not achieve Honeywell's current target risk level, so a High-High Pressure interlock[2] was added to shut off the reboiler heat source. This design met the risk target as designed.
Like a number of other companies, several years ago Honeywell adopted the leading practice of adding a Control Plan to its operating procedures. There is no "official" title for these. Some other companies use the term "Safe Operating Limits Table (SOLT)" and at least one company refers to this as an "Integrity Operating Window Table". See example Table 1 below.

CONTROL POINT	PROCESS VARIABLE	CONTROL METHOD	OPERATING LIMITS/ALARM SETTINGS		SAFEGUARDS	CONSEQUENCES of DEVIATION	OPERATOR ACTIONS / INTERACTION
PIC-101	Column Pressure		MAWP	450		Damage/Loss of Containment	
		Automatic: PSV calibrated	Never to Exceed	400	PSV-103	Will relieve pressure through RVs, causing release through relief scrubbers.	Ensure column is venting to LPS. Isolate column from any higher sources of pressure. Stop reboiler steam flow manually and increase condenser water flow to max.
		Automatic: Pre-programmed and cannot be altered without a MOC approval process	High High Interlock	350	SIS, At High High Pressure, PZIT-102 closes XZV-102 to stop heat to the Reboiler	Approaching pressure that will require relief through RVs.	Ensure XV-201 has opened and HIC-401 is allowing pressure to vent. Confirm XZV-102 has closed. Increase condenser water flow.
		Automatic: Operator inputs desired pressure setpoint. BPCS adjusts setpoint of flow control FIC-102 in a cascade loop	High Alarm	240	BPCS	May reduce flow from reactor or cause upset.	Check pressure in downstream column. Check reboiler and condenser are normal.
			Target	215-240 Typical: 230			Set pressure based on what gives good column performance and recovery of recycle material.
			Low	200		Can stop feeding forward to next column.	Ensure column is not venting to LPS. Check reboiler and condenser are normal.
			Low Low	--		Quality	
			Never to Exceed	--		None	

Table 1 : Example of Safe Operating Limits Table (SOLT)

[2] Where practical, Honeywell uses the Inherently Safer approach of selecting the MAWP of distillation columns such that the maximum potential pressure from the heat source would not challenge the vessel integrity.

The principle behind the table is to show important process parameters with the instrument loop which controls that parameter, as well as its normal set point and (often) some range in which the operator might vary the set-point or operate the system in manual - say, during startup or shutdown.

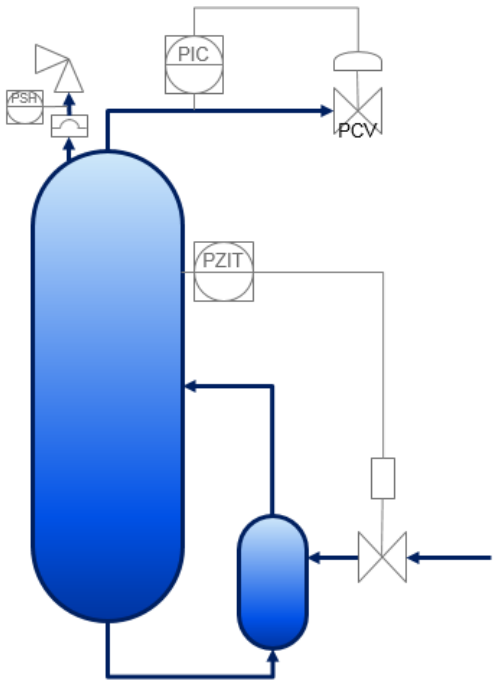


Figure 4. Typical Distillation Column with Safeguards

These fit well with Layers of Protection Analyses (LOPA) and provide direct mapping for the analyst checking the system performance.

Any Interlock activation (eg. PZIT102) needs to be “Validated” per IEC61511 (2015, Clause 5.2.5.3), and should be reported as a “Near Miss” per API754. It’s also a “Demand” of the Safety interlock also referred to as Safety Instrumented Functions (SIF), so it should be counted to compare these with the target frequency assumed in the PHA/LOPA.

So how well is it working in practice? Is the plant operating “in the Green”? This and nine other similar columns were checked. Only one fault was found anywhere in the control loops in more than three and a half years of operation. There’s a good chance that fault was due to an installation problem as it happened very shortly after start-up. Nevertheless that failure was counted as part of “all causes”. Thus the unit experienced 1 fault with 10 x 3.5 years of experience, so the failure rate was 1/35 or 0.029 faults/year. This is about 10x better than the standard LOPA assumed rate for similar cases. This is not a statistically large enough sample to consider changing the LOPA guidance for Initiating Event Frequency (IEF), but it is reassuring that the LOPA team assumption has not been found to be aggressive.

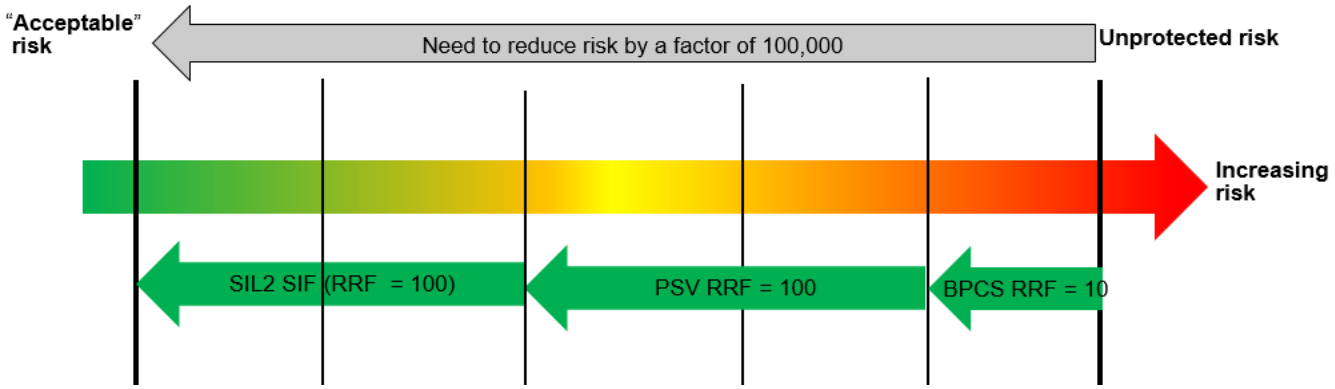


Figure 5. IPLs in a LOPA to reduce Risk

The Reliability and Availability of the SIFs were also checked. Based on the LOPA, the SIFs were designed to be SIL2 which would be a Reliability of 99% (refer Table 3 and Figure 5) in our scenario. To understand how Reliable they really are, the test records and the historian data were checked. The test records have shown all subsystems of the loops were functional at the end of each test interval. Thus it can be inferred that the interlocks were functional all the time they were in service since installation and would have operated Reliably on demand. This conforms to "more than 99%" reliability for which the SIFs had initially been designed.

SIL	**Risk Assessment**	**Protection Layers**	**Performance**
Safety Integrity Level	Risk Reduction Factor (RRF)	Probability of Failure on Demand (PFD)	Reliability (1 - PFD)
1	10 to 100	0.1 to 0.01	.9 to .99
2	100 to 1,000	0.01 to 0.001	.99 to .999
3	1,000 to10,000	0.001 to 0.0001	.999 to .9999
4	>10,000	0.0001 to 0.00001	.9999 to .99999

Table 3. SIL in relation with other parameters

The Historian information was then checked for the amount of time the SIFs were in "Bypass mode". This was about 24 hours over the same period, so >99.9% of the period, the SIFs were Available to operate on demand. Figure 6 below shows Availability over a period of 60 minutes as snapshot.

At about 9:35 am, the Operator put the SIF input (100PZI4001) on "bypass" and at that instant onwards the input parameter shows "zero". All actions and events on the SIS are attributed with a "Risk index" number which is configurable based on user input. In this case, putting the Input value on Bypass is associated with a Risk index of "One" which means the process is running on a High risk because the SIF input is not being measured.

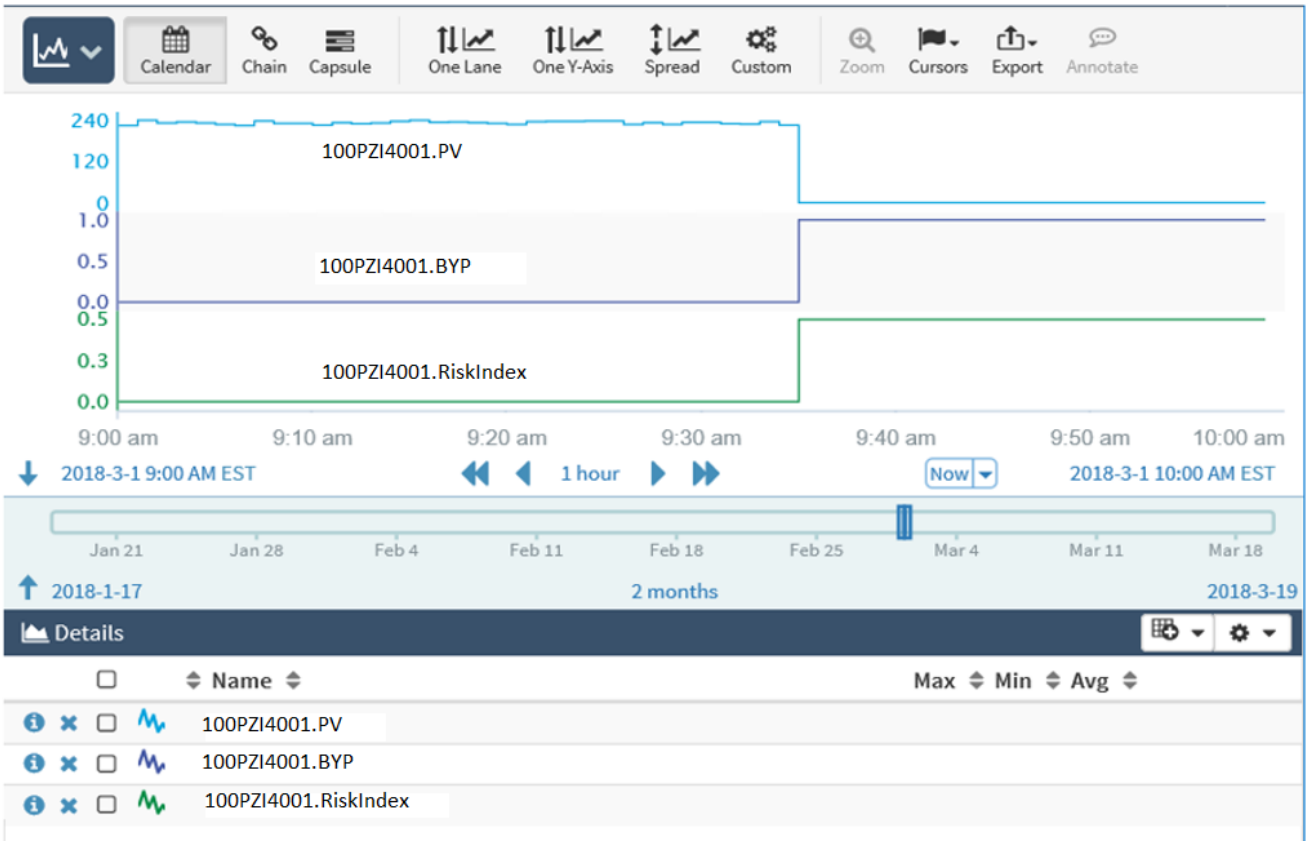


Figure 6. Safety interlock Availability over a 60 minute snapshot showing a change

Thus the analysis has validated that the LOPA target is being met for this scenario both in terms of Reliability and Availability

Other parameters that could affect Reliability or Availability of Independent Protection Layers (IPL) can also be monitored. Examples:

1. Safety Interlock in degrade mode due to failure of Input Transmitter signal (0 mADC) to the Logic Solver which could affect Reliability (See Figure 7). At about 9:35 am, the transmitter (100PZI4002) signal drops to 0 mADC and from there on the process value reads zero. The Risk index is configured to “0.5”, which means there is a redundant transmitter available for the SIF to function

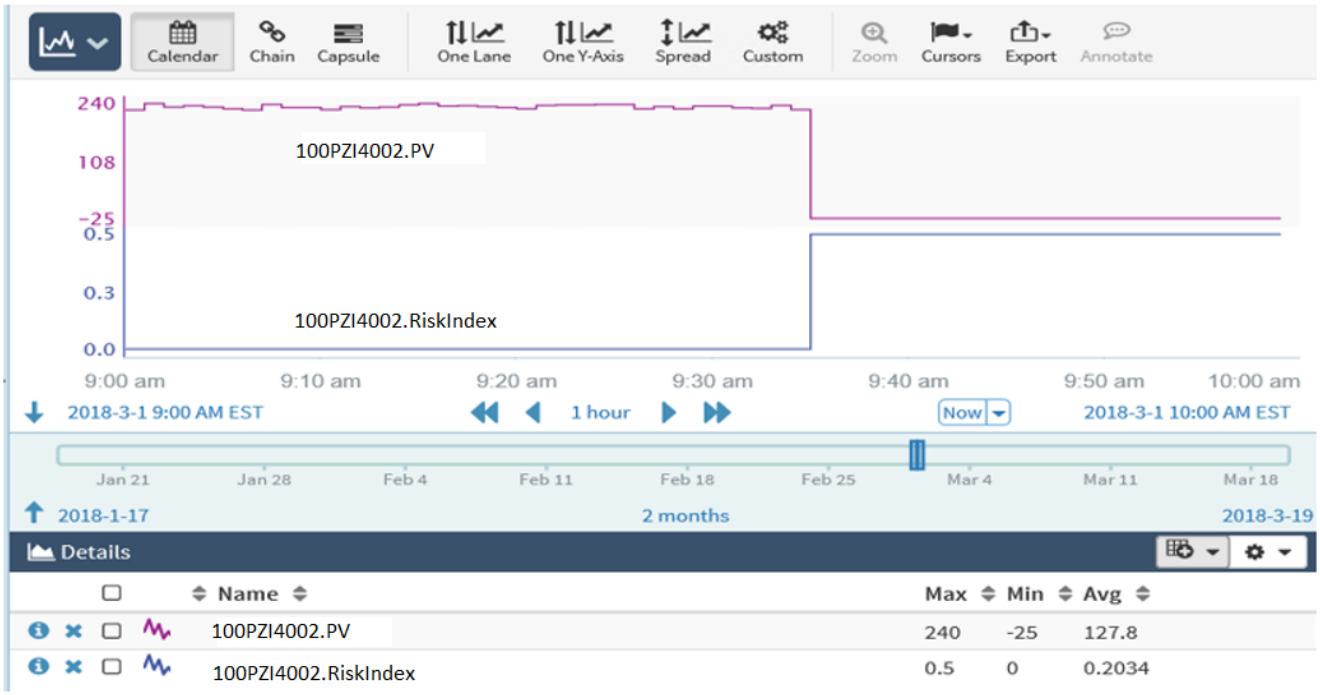


Figure 7. Safety interlock transition to Degrade mode due to transmitter failure over a 60 minute snapshot

2. Safety Interlock in degrade mode due to “frozen” Input Transmitter signal to the Logic Solver which could affect Reliability. The example below indicates two transmitters in a redundant configuration and one of the transmitters (100AZI4001A) is essentially “frozen” for the most part reading a process value of 200. The Risk index is configured to “0.5”, because there is a redundant transmitter available as part of the SIF input

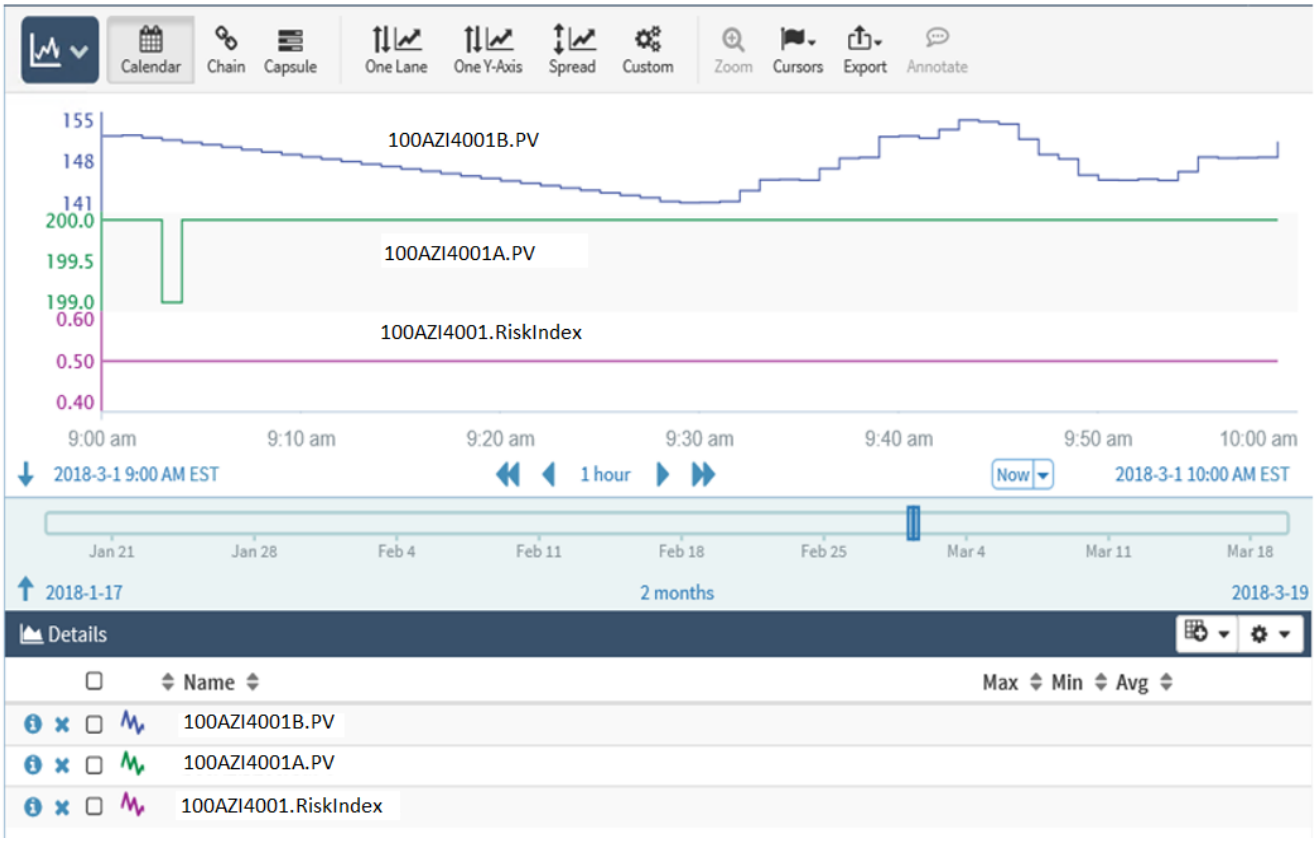


Figure 8. Safety interlock transition to Degrade mode due to transmitter signal “frozen” over a 60 minute snapshot

3. BPCS control loop in Degrade mode due to it being in “Manual” instead of “Auto” for a long time which could affect Reliability. In Figure 9, 100PIC4003 mode is changed to Manual at 9:41am. The controller output is manually changed to 100% and the process value starts increasing and saturates at 350 engineering units. The Risk index is configured to be “One” in this state.

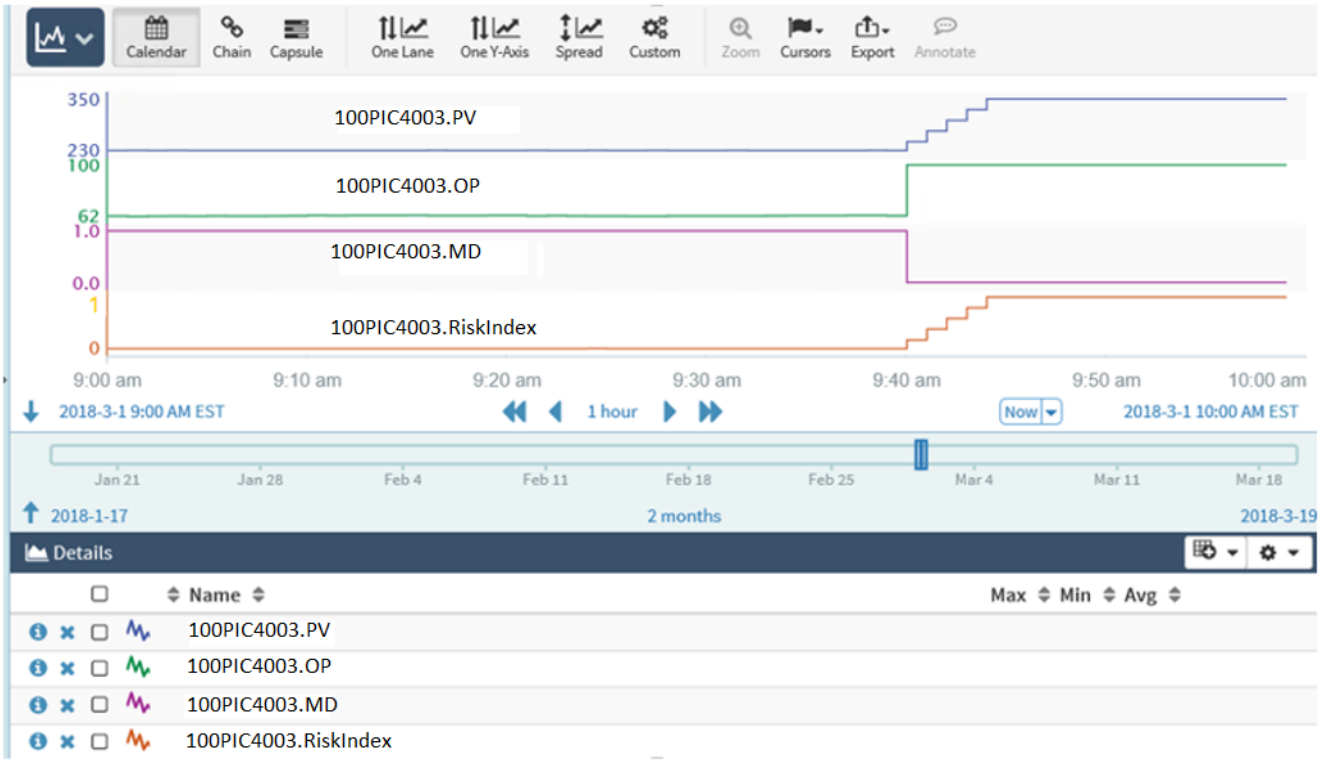


Figure 9. BPCS Control loop from “Auto” to “Manual” mode over a 60 minute snapshot

Example 2

Redundant Analyzers as inputs to SIF

If a heat exchanger in process service experiences a tube leak, it may put a hazardous material into the heat transfer fluid. It may be possible to detect the leak using analyzers such as for pH, Conductivity, depending on the properties of the process and heat transfer fluids. This is a useful capability, though analyzers tend to be relatively complicated systems with a number of potential fault modes and thus are generally considered to have relatively lower reliability/availability.

Here's an example of a "problem" set of Analyzers. The team estimated the IEF based on the LOPA table. They determined a safeguard should also be applied, so they added dual analyzers in a 1oo2 configuration. As it turned out, the tubes were more reliable than estimated and substantially more reliable than the analyzers that were meant to find any leaks. In one 5 week period, six of the analyzers had activated a total of 30 times, an average of once per week (Table 1). In fact, there had not been *any* leaks – as demonstrated by test and/or inspections after each activation. Thus all analyzer-triggered trips have been spurious. This High Spurious Trip Rate meant the Technology and PHA teams had to come back to the issue and find suitable alternates. There were two problems to be solved: the analyzers weren't reliable enough in this particular application to be part of a SIF and the spurious trip rate was causing significant business interruption.

.

Week Number	100AZIT1774A	100AZIT1774B	100AZIT1790A	100AZIT1790B	100AZIT1791A	100AZIT1791B	Grand Total
40	3	3					6
41	2						2
44			1	1	10	8	20
45	1						1
46	1						1
Grand Total	**7**	**3**	**1**	**1**	**10**	**8**	**30**

Table 4 - Demands for Analyzers in 1oo2 input configuration

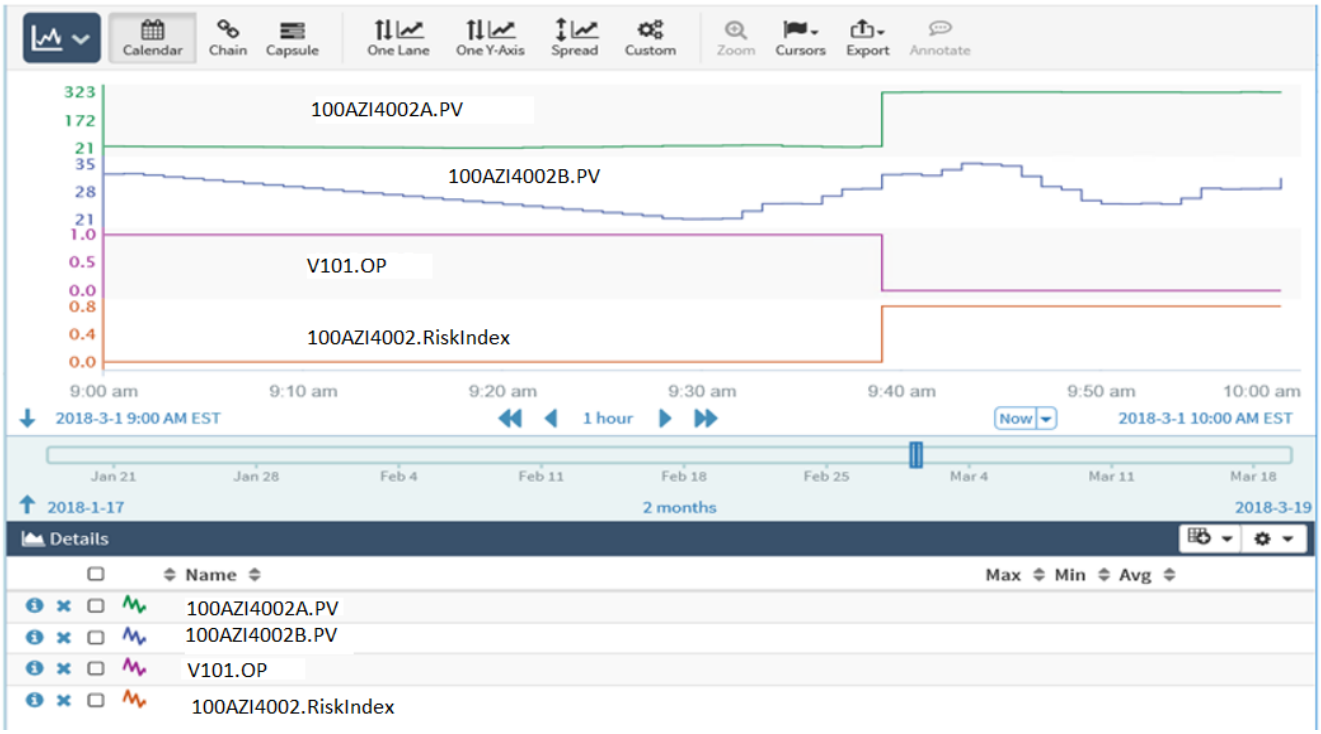


Figure 10. Spurious trip in a 1oo2 input configuration over a 60 minute snapshot

In Figure 10, at about 9:40 am, Analyzer 100AZI4002A spuriously senses the value as 323 engineering units when it is actually between 21 and 35 engineering units. Because of this reason, being in a 1oo2 input configuration with Analyzer 100AZI4002B, the output (Valve V101) trips. In this scenario, the Risk Index is configured to 0.8 as this is a Safe failure.

Emergency shutoff valves (XZVs) as Output Devices of a SIF

Emergency block valves go by many names: Emergency Shut-Down (ESD) valves, Remote Operated Shut-Off Valves (ROSOV), etc. Honeywell generally calls shutoff valves “XV’s” or “HVs”. The ISA convention is to put a Z in SIL-rated safety loops, so shutoff valves in SIL-rated service are XZV’s or HZV’s. XZV’s are generally provided with ZSO and ZSC limit switches at the “open” and “closed” end of their travel. Thus the time required for such a valve to travel from its active to its “safe” position can be measured using the data from the event historian. If a trend chart of the travel-time shows an increase, one may anticipate that eventually the travel-time will exceed the required Process Safety Time limit.

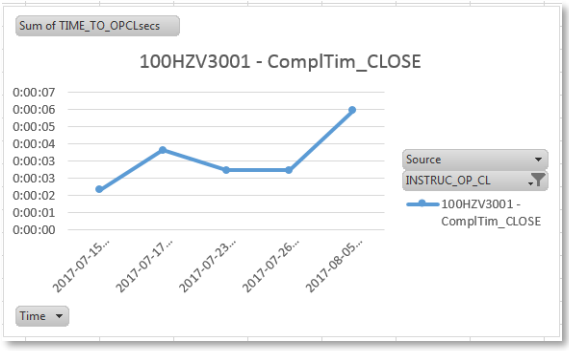


Figure 11. Travel time for an HZV to Close

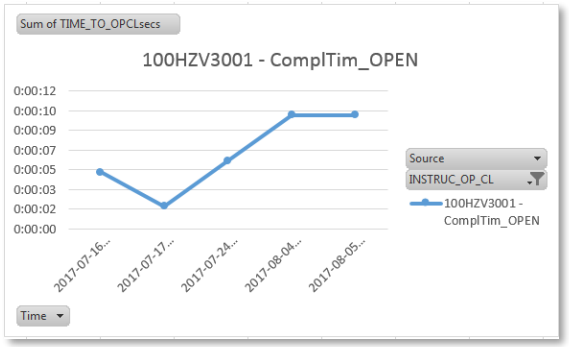


Figure 12. Travel time for the same HZV to Open

The increasing travel time may be an early warning sign of stickiness. Once it exceeds a threshold, Maintenance should take a look.

EMPOWERING PHA REVALIDATION TEAMS WITH THEIR PLANT DATA

The cases above show what can be done with historian data to either support the PHA/LOPA assumptions or to identify where non-conservative assumptions have been made. It may also reveal other opportunities like high spurious trip rates and overly conservative assumptions.
But anyone who has done this kind of analysis by hand, or using Excel, understands that it's time-consuming. In an era of financial constraints, the staff might not get to it. Fortunately, computer tools are available which can now search for and report these issues and opportunities, so the site's process safety and functional safety staff can spend their time solving problems rather that downloading data and developing pivot-tables – the techniques used for this paper. It's possible to get a report of demand rates and faults, area by area throughout the facility as input to the PHA teams.

How far can this concept be taken?

Scrutiny of the historian data enables some diagnostics to show when a degraded condition may have occurred. Honeywell is testing software that allows "degraded" situations to be diagnosed and flagged

in real time, so the controls and operations staff can see potential problems and take prompt action to fix them.

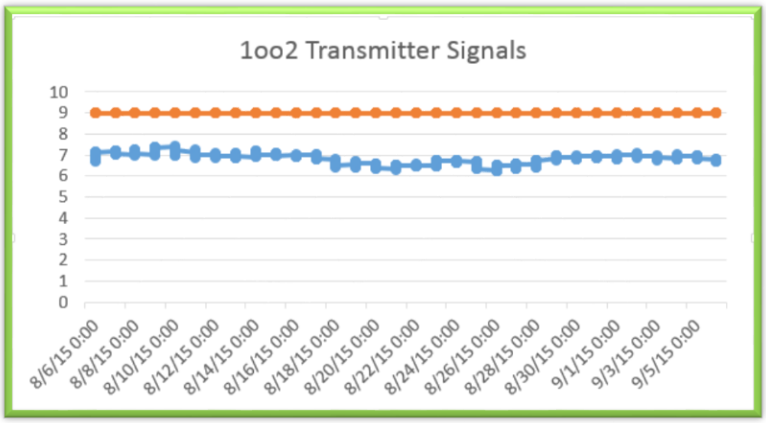


Figure 13 - Diagnosing a "flat-lined" transmitter signal

Analyzer and Transmitter signals, or Process Variables (PV's) generally change over time. If the signal is not varying in any way over a period of time, the analyzer or transmitter may have developed a fault. Maintenance Inspection/ recalibration is appropriate - once diagnosed. This is a reminder why continuous "analog" signals from transmitters are more valuable than the on/off signals from discrete switches where only a test can reveal a "covert" fault.

Similarly, if a control input is regularly in fault or Bypass mode while being repaired, it seems reasonable that the likelihood of an initiating event is higher than if it's controlling properly. Could this kind of data analytics, especially if continuously provided to operations, have diagnosed and escalated the issues at Buncefield ahead of time? If the high, high level sensor were a continuous signal and if the data were in the historian, and all signals were being continuously analyzed looking from a process safety perspective, then it seems possible that it could have.

While this is of particular interest to the site level staff, the division-level staff will want to ensure these problems do not persist long-term. Generally site-level needs detail to support the analysis while senior levels of the organization need enough detail to know the site–level staff is able to promptly manage any issues which are identified.

Closing the loop back to the PHA

All this data feedback takes effort. The first studies within Honeywell were all done using Excel spreadsheets and manual techniques. This was effective, but too time consuming to be sustainable in the long term without significant additional staff. The rise of analytical computer tools enables the comparisons to be done regularly and much less expensively than using automation engineers to sift through the historian data once per month looking for issues.

Still, it's not without an effort. In order for the analytic engines to find issues, they have to be configured with the expected behavior. The Cause and Effect Matrix can be used as a data entry tool once it has been created in Excel. But it has to be created, maintained and updated if anything changes. The tools to look for flat-lined transmitters have to be configured to know which transmitters are protecting against high severity scenarios and thus are important enough to monitor.

How can we convey the expected behavior of our critical control, alarm and interlock protection layers? Today we do it manually by reviewing the LOPA and "programming" the analytics tools to look how these critical systems are behaving. But a new set of tools is emerging to help set these expectations.

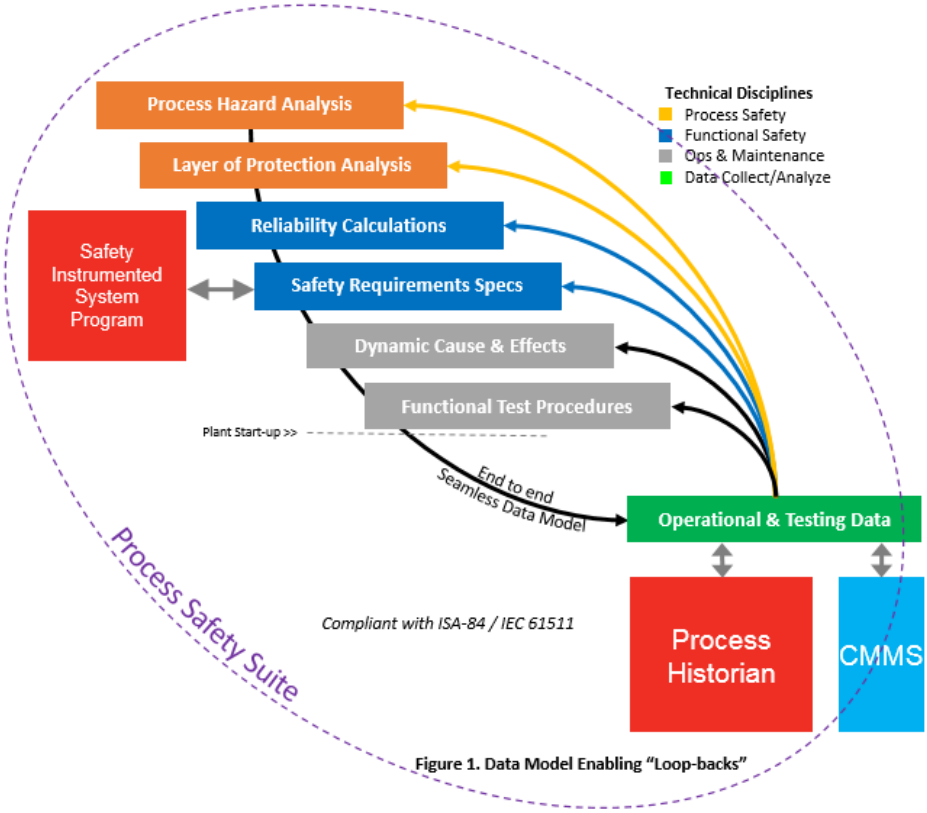


Figure 1. Data Model Enabling "Loop-backs"

The PHA and LOPA recording software can be used to manage this data. One such system is shown in the Figure above. This system is "programmed" by the PHA teams during the hazard reviews to understand the expected initiating even rate and the desired risk reduction factor for each barrier layer. The team needs to be diligent in recording control and interlock loop numbers properly so they can later be connected with the historian data, but the reward is significant. As with so many things today, bringing all this information into the digital realm enables much more to be done with it. The resulting "risk model" provides a real-time view into the actual risk on the site or at the division, regional or even the enterprise level.

CONCLUSION

The analysis shows that the data in the process and event historians can provide valuable insights into the actual safety of our operations as they stand today. Manual analysis showed that the design of the Safety Instrumented Functions looked at does provide the target amount of protection. In most cases the actual field performance of the SIFs also met target. However, a few did not. As it happened, this didn't matter as the Initiating Event Frequency was actually much better than anticipated by the

HAZOP/LOPA team. Nevertheless, analytics from field performance showed opportunities to improve the system in a few cases. The issues and opportunities were not apparent at first. Thus the analysis met it's intended purpose.

However, the manual analysis takes resources and time to complete. The addition of more advanced, and continuously-running computer analysis tools takes this into the realm of being practical to do all the time. And today's new enterprise-level integrated PHA/LOPA and SIL Calculation systems take this to the next level.

REFERENCES

1. IEC 61511 / ISA 84.00.01- Functional Safety – Safety Instrumented System for the Process sector
2. API RP 754 - Process Safety Performance Indicators for the Refining & Petrochemical Industries
3. OGP Process Safety – Recommended Practice on KPIs – Report # 456, Nov 2011
4. Occupational Safety and Health Administration (OSHA) Process Safety Management of Highly Hazardous Chemicals Regulation, 29 CFR 1910.119
5. CCPS "Guidelines for Integrating Management Systems and Metrics to Improve Process Safety" pp109