Honeywell | Connected Industrial

PROCESS SAFETY VALIDATION, VERIFICATION AND DOCUMENTATION

How to Reduce the Hidden Costs of Achieving and Proving Process Safety

White Paper

Abstract

There are significant hidden costs in most of the current practices for validating, verifying and documenting that Safety Instrumented Systems and control systems as installed are functioning as designed. One key reason is that until now, there has been no automated mechanisms to support this critical activity. There are no standard ways in the industry to achieve this validation, verification and documentation.

The hidden costs come from the effort to validate, verify and document using manual processes and disconnected information sources. Even more significant are the opportunity costs from longer planned and more frequent unplanned shutdowns that reduce the total revenue opportunity.

In this whitepaper, we outline here the principles and approaches of a new capability to perform this function in an automated way. This results in structured information and shared knowledge, provable safety state and benefits from lower costs and higher revenue opportunity.

Table of Contents

Automated Approach to Process Safety Validation, Verification and Documentation

With automated validation and reporting, process facilities can achieve more, quickly perform safety tests, be more aware of issues and reduce down time.

Introduction

The process of validating and verifying the good function of installed process safety systems and equipment is driven as a mandatory effort, governed by company and regulatory stipulations, across the process industry.

At stake is the protection of people – whether employees, contractors, visitors or the general public – as well as the environment, property and equipment and the benefits of preventing unscheduled downtime and lost production. The importance of this validation and verification is to ensure that, if an equipment is demanded to go to safe state, that expectation of good function, on such demand, is established.

With much needed attention given to the initial design of all related mechanisms to have the basic expectation of safe state on demand, the industry has established well-accepted tools using statistics and documented Probability of Failure on Demand to set design practices that define measurable mitigated risks. As a result, the required Safety Integrity Levels (SIL) of safety instrumented functions are then established and incorporated into Safety Instrumented Systems (SIS). These take into account the safe state responses from process control systems, emergency shutdown systems as well fire and gas protection systems.

After installation of such systems in process plant facilities, the expectation is that the actual function, i.e. the response to a demand to safe state, is checked and documented on a regular cycle. The cycle may be driven by statutory regulations, company rules, equipment cycle-driven timings (such as on planned major equipment downtime / shutdowns), or ad-hoc tests if safely achievable.

A Continuous and Efficient Validation, Verification and Documentation

While the requirements for timeliness and documentation of the completed validation and verification effort are generally expected, the actual mechanism to perform this effort are not stipulated. Authorities are not prescriptive on how to perform this task. With the proliferation of different systems, different generations of technology installed at sites, there has been general adoption of home-grown tools, requiring time-consuming manual inspection of results from tests that, themselves, are manpower-intensive.

Due to the regular cycle of validation and verification requirements and the intensive manual work, there is in fact a hidden cost to follow these efforts, whether they are necessary or not. For example, if a process safety equipment has demonstrated proper operation on actual process demand, the test interval timer on it can be reset, leading to a reduction of the otherwise fixed test interval. Yet we cannot capture this benefit without the necessary structured documentation of proven good function.

The general result from these in-house approaches is a wide variety of tools, with little consistency across the industry. The actual manual effort to review results is itself subject to variations from person to person, leading to possible variability in the quality of the analysis itself. Due to the drudgery of observing long lists of events from logs, sequence of event recorders, safety historian functionality of SIS / ESD systems or even of consolidated process and safety event journals, the task of such review has often been handed to more junior engineers. This may result in less experienced or less critical eyes for the review of event journals.

A structured approach to this task can provide significant savings by a better targeting of the validation and verification efforts. This can result in cost avoidance and cost reduction. By reducing the work load during planned shutdowns, the duration of these shutdowns is potentially shorter in those cases where this verification is an immediate pre-start-up, critical path activity. A significant benefit of this is shorter downtime, with reduced deferred or lost production.

How It Happens

When an unplanned shutdown occurs in a process area, it is urgent to understand the cause to quickly see if the cause can reoccur. If it is momentary (high or low value to process variation reaching a critical point) or a latched failure (equipment repair needed), engineers need to conclude on the prospects or the timing of a restart, whether immediately following confirmed observations and engineering conclusions or after additional time due to other process area effects and verifying safe starting point.

The question then becomes, do we know what the root cause was and did everything happen as it should with the expected effects at the expected timing?

Manual checking of sequence of events or other related event logs may then take place manually. Such checking may not identify what is not in the log, such as missing events, unless the engineer has expert knowledge of the specific sequences. In addition, related causes, logical relationships to other effects or sub-shutdown levels may not show up in a manual analysis or at least take considerable time to discover and may require expert eyes.

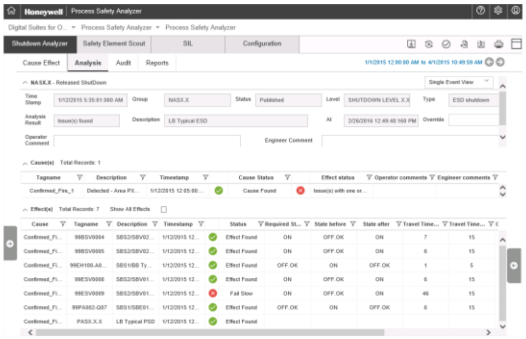
Having the ability to receive an automated analysis of how the shutdown occurred and whether all consequent elements performed as expected can provide some critical time savings and relief to detailed searches across multiple systems. Such an automated validation, verification and documentation can support the process safety management function in a direct way.

How can we achieve this? Such automated analysis must be performed considering reference cause and effect matrices, with all relevant event signatures, timings and relationships, acts as the documented, as-expected base. Events captured from Level 2 control or safety system event journals form the basis of the as-is case to be validated. The automated analysis then carries out the sequential comparison between the set of stored logical relationships and the event signatures with those observed from the captured event journals.

Features Highlights

An automated analysis of the logical relationships and timed flow of events in a shutdown and safety operations provide observations and conclusions automatically. This is based on the set of cause and effect diagrams, event signatures and expected timings of the effects. The events are flagged automatically as to whether they are OK, already in safe state, failed, missing, or as no response from command, too long in execution or otherwise needing attention.

- *Comments*: Enter comments, on individual events or overall shutdown comments.
- *View raw event log*: View the cause and effect diagrams and the raw event log.
- *View any shutdown, recent or history*: View any shutdown on any part of a configured plant, over historical span selected. This gives a structured history of all shutdown activity, easily available for navigation by plant area, unit, etc.
- *Easily distinguish between demands*: View the differences between SIS demands, process demands or test demands.
- *Approval cycle*: Enable review / approval / lock-down cycle on shutdown results.
- *Demand cause correction*: Correct test demands.
- *Observe function of individual final safety elements*: Analyze full history of elements operations, for example safety valves and breakers, from individual events, that may be months apart.
- *Report on vessel or line blowdown*: Validate that final target pressures are achieved within a specified time.



NASX.X - Released ShutDown

Time Stamp	1/12/2015 5:35:01:000 AM	Group	NASX.X	Status	Published	Level	SHUTDOWN LEVEL X.X	Type	ESD shutdown
Analysis Result	Issue(s) found	Description	LB Typical ESD			At	2/26/2016 12:49:48:160 PM	Override	
Operator Comment				Engineer Comment					

Cause(s) Total Records: 1

Tagname	Description	Timestamp		Cause Status		Effect status	Operator comments	Engineer comments
Confirmed_Fire_1	Detected - Area PX...	1/12/2015 12:05:00:...	✓	Cause Found	✗	Issue(s) with one or...		

Effect(s) Total Records: 7 Show All Effects □

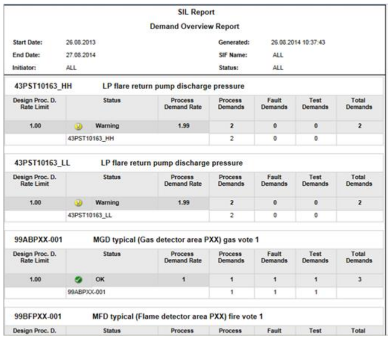
Cause	Tagname	Description	Timestamp		Status	Required St...	State before	State after	Travel Time...	Travel Time...
Confirmed_Fi...	99BSV0004	SBS2/SBV02...	1/12/2015 12...	✓	Effect Found	ON	OFF.OK	ON	7	15
Confirmed_Fi...	99BSV0005	SBS2/SBV02...	1/12/2015 12...	✓	Effect Found	ON	OFF.OK	ON	6	15
Confirmed_Fi...	99EH100-A0...	SBS1/BB Ty...	1/12/2015 12...	✓	Effect Found	OFF.OK	ON	OFF.OK	1	5
Confirmed_Fi...	99ESV0008	SBS2/SBV01...	1/12/2015 12...	✓	Effect Found	ON	OFF.OK	ON	6	15
Confirmed_Fi...	99ESV0009	SBS2/SBV01...	1/12/2015 12...	✗	Fail Slow	ON	OFF.OK	ON	46	15
Confirmed_Fi...	99PA002-Q07	SBS1/SBE01...	1/12/2015 12...	✓	Effect Found	OFF.OK	ON	OFF.OK	6	15
Confirmed_Fi...	PASX.X.X	LB Typical PSD	1/12/2015 12...	✓	Effect Found					

Online detailed view of an Analyzed Shutdown

The following reports and statistics are provided:

- Test interval report provides a view of remaining time to next test date / time expected, based on standard times and providing a reset on achievement of good function. This is a report showing the available time to next inspection, as well as timers counting down, showing upcoming inspections due and any overdue inspections.
- Demand history by individual element,
- Demand overview,
- Failure rate,
- Final element verification,
- Valve stroke report and

Data from all the reports can be exported into read-only PDF files or extracted to spreadsheets to be combined with other information.



SIL Report

Demand Overview Report

Start Date:	26.08.2013	Generated:	26.08.2014 10:37:43
End Date:	27.08.2014	SIF Name:	ALL
Initiator:	ALL	Status:	ALL

43PST10163_HH LP flare return pump discharge pressure

Design Proc. D. Rate Limit	Status	Process Demand Rate	Process Demands	Fault Demands	Test Demands	Total Demands
1.00	⚠ Warning	1.99	2	0	0	2
	43PST10163_HH		2	0	0	

43PST10163_LL LP flare return pump discharge pressure

Design Proc. D. Rate Limit	Status	Process Demand Rate	Process Demands	Fault Demands	Test Demands	Total Demands
1.00	⚠ Warning	1.99	2	0	0	2
	43PST10163_LL		2	0	0	

99ABPXX-001 MGD typical (Gas detector area PXX) gas vote 1

Design Proc. D. Rate Limit	Status	Process Demand Rate	Process Demands	Fault Demands	Test Demands	Total Demands
1.00	✓ OK	1	1	1	1	3
	99ABPXX-001		1	1	1	

99BFPXX-001 MFD typical (Flame detector area PXX) fire vote 1

Design Proc. D.	Status	Process	Process	Fault	Test	Total

Easily validate actual SIF demand rates vs. design limits using Demand Overview Report.

Benefits in Use

Quick and complete review of automated analysis: All of the system facilities / functionalities for an automated validation, verification and documentation support an engineer to quickly view the resulting analysis, saving time in the process.

Consistency of conclusions – no dependence on single individual's observation capability: Having the analysis done automatically ensures consistency and a structured approach to the validation, verification and documentation process.

Retrievable, sharable information on how shutdowns occurred: Having all the related information stored in a structured way makes it easily retrievable, usable also by maintenance crews as a visible set of priorities for available ad hoc testing.

No dependency on large number of manually maintained tags: One observation of this approach and application capability – it does not depend on any large-scale access to process data. It is event data (from event logs) that drive this function, with only few needed actual process values, used in some safety logic. As such, the event logs are often pre-fetched by existing Level 2/3 systems, meaning that there is no need to separately make demands on process control or process safety systems to obtain the event logs. This capability does not impose any additional bandwidth load on control or safety systems.

Benefits to the Business

Additional benefits to the business provided by an automated validation are as follows:

Possible shorter downtime following shutdowns due to quicker analyzed results pointing to any offending elements or conversely establishing good function and resetting the test interval clock – following approval.

Possible shorter downtime in planned shutdowns due to lower, focused workload for only the required test inspections. We can call this exception-based safety inspection – leading to less wasted time on unneeded tests / inspections – and therefore to lower maintenance costs. This also leads to earlier start-up if process safety test / inspections are critical path elements (as when they are mandatory as immediate pre-start up activities).

Use during shutdowns as automatic recording for valve travel times leading to less time to do multiple tests and fewer unneeded tests.

Use for capturing results of valve stroke tests in historical event database, leading to decreased use of private spreadsheets and making information visible to wider organization.

Requiring fewer travelling personnel: for remote facilities, low manned or offshore locations, fewer personnel needing to travel to site or facility.

Higher reliability and process safety, due to better and earlier discovery of any issues with shutdowns and structured statistics directly from the system.

Better overall organizational learning due to wider visibility of shutdown performance information; share easily across multiple sites and with a centralized safety function.

Better provable or demonstrable safety performance, for example to authorities.

Early fault detection, leading to higher overall up time.

Lower insurance rates may be possible due to the structured documentation available on shutdown performance and test interval visibility, as this is an auditable, provable performance of shutdowns and safety final elements.

More accurate information on actual demand rates based on captured information on failures of specific equipment, leading to more cumulative knowledge for safety professionals to use in later designs and for comparing performance of specific vendor equipment in various services.

Less time searching for process safety related information, since all stored in a structured database (e.g. ask only for shutdowns on a certain plant area over a given date range).

Conclusion

Industry has generally accepted as given the assumed and hidden costs of process safety equipment and shutdown systems' validation, verification and documentation. An opportunity exists to better support the workflows, reducing the overall quantity of work needed to achieve validated, verified and documented process safety. More importantly, reducing downtime due to shutdown occurrences and reducing downtime during planned shutdowns both result in higher overall production – and therefore revenue enhancement.

The combination of cost avoidance, cost reductions and revenue enhancements make this a compelling value proposition. The actual benefits can be opportunistic and stochastic, but they are real. Honeywell's Process Safety Analyzer (PSA) provides the functionality, in its Shutdown Analyzer and Safety Elements Scout as well as SIL Reporting modules, and the technology means by which to achieve these benefits.

About Process Safety Analyzer

Honeywell's Process Safety Analyzer is a solution designed to support work processes towards safer processes and remote operations goals via the continuous and efficient validation of shutdown systems and safety elements in order to protect people, environment and assets.

Process Safety Analyzer is part of Honeywell's Digital Suites. Honeywell is the expert, global source of consultancy, applications and solutions that can be tailored to the specific needs of each client. With more than 30 years of experience across oil and gas and other industries, clients choose Honeywell to improve safety and performance.

For More Information

Learn more about how Honeywell's Process Safety Analyzer can improve safety, visit honeywellprocess.com or contact your Honeywell Account Manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com

WP-16-02-ENG
November 2016