CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648145

Top-5 Things to Improve Safety without Using a Calculator

Russell Cockman*[a], Sven Lohmann[b]

[a]Emerson Process Management, Leicester, UK
[b]Emerson Process Management, Haan, Germany
russel.cockman@emerson.com

Process operators face competing demands to maintain process safety, while at the same time meeting production targets. Since June 2015 the Seveso III directive replaces Seveso II with stricter standards for inspections by notified bodies and more effective enforcement of the rules for managing safety.
Inspectors look for evidence of good practice in process safety, with reference to IEC 61511 as the benchmark. Many experienced operators of hazardous process plants already manage safety to some extent. However, IEC 61511 calls for structure and planning, to ensure that nothing goes un-checked. Records should show that plans were followed and any resulting corrective actions completed. Producing documents to show functional safety is well-managed can be challenging, when the inspector calls.
Five key areas are investigated, and opportunities for improvement are explored. Three of these topics relate to the *operational phase* of the safety lifecycle, which is applicable to all plants, regardless of age, or of safety instrumented system (SIS) technology in use:

1. Safety Requirements Specification (SRS)
2. Technology Selection
3. Management of Safety System assets
4. Planning for Proof Test and Inspection
5. Management of overrides

Suggestions for improvements are made and thought-provoking impulses are given for each of the key areas resulting in a set of recommended best practices that are likely to improve safety at any plant without causing the need of major investments.

1. Introduction

Process operators face competing demands to maintain process safety, while at the same time meeting production targets. By June of 2015 all European Union Member States must have implemented the Seveso III directive into their national laws; changes from Seveso II are stricter standards for inspections by government agencies and more effective enforcement of the rules for managing safety.
Many believe *safety integrity* is all about component failure rates and complex calculations of probability of failure on demand. However, there are many ways to improve process safety and the protection offered by your Safety Instrumented Systems.
International safety standards, IEC 61508 and IEC 61511, were developed as a direct result of several industrial process accidents. Applying the safety lifecycle approach described in IEC 61511 significantly reduces the likelihood of safety system failure because the procedures described in the standard enforce due diligence.
Inspectors look for evidence of good practice in safety systems, with reference to IEC 61511 as the benchmark. Many experienced operators of hazardous process plants already manage safety to some extent. However, IEC 61511 calls for structure and planning, to ensure that nothing goes un-checked, and records should show that plans were followed and any resulting corrective actions completed. Producing documents to show functional safety is well-managed can be challenging, when the inspector calls.

Please cite this article as: Lohmann S., Cockman R., 2016, Top-5 things to improve safety without using a calculator, Chemical Engineering Transactions, 48, 865-870 DOI:10.3303/CET1648145

2. Key Areas for Safety Improvement

The safety system itself represents a capital investment, the functional safety lifecycle is complex, and the requirements for compliance are becoming stricter. Hence, to focus on the most *effective activities* for improvement is only prudent to keep costs at bay and the safety process manageable. Such activities can be found in key areas of functional safety. Five of them, are in our opinion the “low-hanging fruits”, in other words those activities that yield the highest effectivity. The activities are safety requirements specification (SRS), technology selection, management of safety system assets, planning for proof test and inspection, and management of maintenance overrides to the SIS. They are discussed in the following.

2.1 Safety Requirements Specification

The first main section of the IEC 61511 safety lifecycle is the *analysis phase*, where we identify all of the potential hazards in our process and the degree of risk reduction required of our safety instrumented system. The HAZOP (Hazard and Operability study) is only the beginning of the process. The key deliverable from the analysis phase is the *safety requirements specification* (SRS), which should consolidate vital information from the hazard analysis, as a reference for future work. By consolidating all safety requirements in a single place, future activities and decisions can be made with a full knowledge of the original design intent.

Every safety function within the SIS is associated with a specific hazard; each SIF has performance and integrity requirements. The SRS must identify all safety functions, providing information relevant to the design and operation of the SIS. IEC 61511 lists 27 points that must be addressed by the SRS, plus additional requirements specific to SIS software. Failure to consider any of these points may lead to misunderstanding, incorrect assumptions or key facts being missed in the work that follows to design, build, operate and maintain the SIS.

For the operator of an existing process, writing an SRS is the ideal opportunity to really understand and document what you THINK you have and why you have it. It is a chance to really dig into the process safety requirements, considering important questions such as:

- How can the hazard occur?
- What other measures are in place to reduce risk?
- What are the minimum requirements to achieve a safe state of the process?

It is common practice to refer to the cause and effect charts when addressing safety functions, however the real “safety” function can be hidden amongst many “shutdown” functions required for reasons not directly associated with safety. Figure 1 shows the system boundary around a safety loop comprising the safety PLC and their final elements. Other elements can be excluded because they do not have a purpose directly relating to safety. The scope of a safety function is to detect a pre-hazardous situation and take the process to a predefined safe state, nothing more. In this example, the safety logic looks like this: if the pressure exceeds a certain threshold, then the shutoff valve is closed to prevent further inflow into the vessel.

This activity will re-acquaint you with the original design intent and probably raise some very important issues to be addressed. Using an independent consultant to help with SRS preparation is a good opportunity to challenge and question the work that has gone before, making sure that the safety requirements are clearly understood by all involved.

If you work on a hazardous process, do you know where the Safety Requirement Specification is stored? Has the SRS been updated to reflect any process modifications? Are the key points within IEC 61511 all addressed?

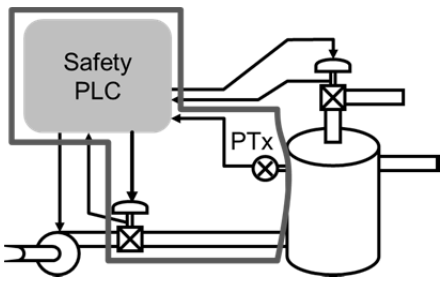

Figure 1: Example for identifying a safety function in a process chart.

2.2 Technology Selection

When selecting components of the SIS, a great deal of emphasis is placed on certificates which provide those all-important reliability figures. Theoretical reliability figures make assumptions about the device service and environmental conditions. In practice we should look carefully at our maintenance records to decide whether theoretical performance can be expected in practice.

Instrumentation must of course be suitable for the application. A valve designed to regulate flow may not be the most appropriate device to shut off a process stream. Regulating valves which move continually may be prone to mechanical wear whereas a shutdown valve which rarely moves might stick, failing to close when needed. Digital valve positioners can automate partial stroke testing of SIS valves and provide useful diagnostic data to analyse any valve movements.

Analogue sensors are preferable to on-off digital inputs. The constant variations of an analogue value show that the device is still working, particularly if measurements can be correlated with other process variables. A digital input which only changes state when the hazard is present is prone to un-detected failure. Smart transmitters may provide additional diagnostics, provided the logic solver enables access to this data.

For each safety-related device, ask yourself:

- Are you experiencing higher than expected failure rates during testing or during operation?
- Does the device provide the information and protection I need?
- Does the device meet the design intent which you have established by writing an SRS?

Whatever technology you are using you will need to verify the probability of failure of all the components in the SIF against the required SIL target. Having manufacturers' data which is approved by the certifying authority seems like the right starting point but this can be misleading. There are different opinions on how this data is produced and this can lead to vastly different results. Table 1 shows two examples of failure rate data relating to almost identical valve assemblies and a third example based on industry gathered statistics. With a factor of around 180 times between the two sets of certified data which one represents the type of failure rate you might experience? What is clear is that a calculation using over optimistic predictions is not in anyone's interest.

Table 1: Examples of failure rate data.

Valve assembly	DU failures, FITs	Certified by
ASCO 327 - Biffi Algas - Cameron BT	**8.26** (0.46+3.1+4.7)	TÜV
ASCO 327 - Bettis G - Cameron T31	**1473** (180+633+652)	Exida
Generic	**2565** (585+1980)	(Exida)

2.3 Management of Safety System assets

SIS components installed in various locations throughout the process area should be clearly identifiable amongst similar equipment used for the basic process control system (BPCS). The standards require us to make sure that competent people with the correct training and experience work on the safety instrumented system, and that no changes are made without proper planning and authorization. Therefore it seems clear that maintenance technicians or field operatives need to know if a particular device is part of the SIS, or not.

Running a calibration check on a transmitter used within a flow control loop requires completely different precautions to running the same check on a similar transmitter used in a Safety Instrumented Function. The flow controller will freeze its output, keeping the flow constant whilst the transmitter is out of service, allowing operator adjustments. The SIF can no longer protect against its identified hazard; the disabled measurement may lead to a process shutdown, or worse the process might continue to operate without the protection you think is there.

IEC 61511 includes requirements for configuration management, in which all parts of the SIS should be clearly identified, managed and traceable. By clearly identifying all component parts of the SIS, and training all personnel that SIS devices are subject to special controls, the risk of a change leading to a process safety incident is greatly reduced.

The management of the safety system assets is key to ensuring integrity over the entire operational phase of the safety lifecycle which is usually many years. In fact, "incorrect SIL is rarely a direct cause of incidents" as HSE pointed out at a meeting of the ICHEME in 2015, most root causes stem from deficiencies and negligence in the operational phase. A properly written SRS leads you to identify the most important SIS

assets and effective asset management will ensure that you have the right equipment configured and maintained to perform the required function.

2.4 Planning for Proof Test and Inspection

Because process control systems continually regulate, failures are quickly identified when instruments or valves do not function as expected. Process safety systems only act when things go wrong, so failures could go un-noticed in normal operation. Safety Instrumented Systems use increasingly frequent diagnostics to detect as many dangerous failure modes as possible. However, some failure modes can only be diagnosed by regular proof testing. At the point where a device is fully tested the probability of failure is close to zero and hence the average probability over time is reduced.

The diagnostic data is transmitted via the HART (Highway Addressable Remote Transducer) protocol in modern safety instrumented systems. Please refer to Rezabek (2009) for a concise overview for HART 7.

The failure rate is used in conjunction with the test interval (TI) term to calculate the PFD. It is this test interval that accounts for the length of time before a covert fault is discovered through testing.

Lengthening the interval between tests directly impacts on the PFD value in a linear manner (if you double the interval between tests, you double the PFD and make it twice as difficult for the system to meet the target SIL). Figure 2 shows the development of PVD over time (dashed line). The solid saw-tooth shaped line shows the relation for a test interval of one year. A complete coverage is assumed. The dotted line shows the contribution to PFD by an automated partial test, such as partial stroke test (PST).

In the past, plant turnarounds were scheduled every two to three years. However, with increased system reliability and more inclusive preventive maintenance programmes, plant turnarounds now are being scheduled to occur every five to six years. Although extended periods between turnarounds improve economic returns by increasing production, they also mean that safety system final control elements are tested less frequently. This has a dramatic impact on the PFD of the system, which often prevents it from meeting the target SIL.

In an attempt to avoid this problem, many companies have devised methods for testing SIS valves online so they do not have to shut down the process. The typical approach is to install a bypass around each safety valve. Although bypassing the safety valve during testing is done to improve the PFD, not all of this testing approach goes to that benefit. The fraction of time that the system remains in bypass must be taken into account in the PFD calculation. For long bypass periods or frequent testing, the negative impact on PFD can be significant to where it could negate much of the benefit obtained by the testing.

Safety engineers recognise that the most likely failure mode of a discrete shutoff valve is that it remains stuck in its normal standby position. Testing for this type of failure requires stroking the valve only a small amount to verify that the valve is not stuck. This partial-stroke technique can detect a large percentage of covert valve failures. Furthermore, performing this type of test online without shutting down the process could improve the PFD without a loss of production.

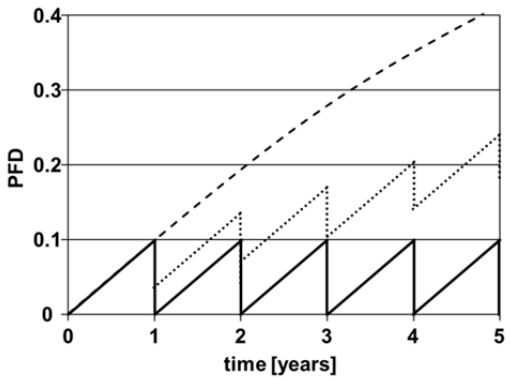

Figure 2: Sketch of the principal relation between testing and PFD.

Over the years, a variety of partial testing methods have been developed. While all of them have a definite risk of spurious shutdown trips, limiting valve travel using a mechanical device seems to be the most popular. Mechanical limiting methods may involve a pin, a valve stem collar, a valve handjack, or some other apparatus that restricts valve travel to 15% or less of full stroke.

While these mechanical limiting devices themselves are inexpensive, the pneumatic test panels used to conduct the test are complex and costly. The testing process must be manually initiated in the field, and the

tests themselves are manpower-intensive and subject to error. In addition, a major drawback is that the safety shutdown function is not available during the test period. Likewise, there is always the possibility that the safety valve will be left inadvertently in a mechanically-limited condition. Worse yet, this situation cannot always be determined by a casual inspection. This means that the valve potentially could be out of service for an extended period of time with the operators being unaware of the situation.

So-called “smart” positioners have become established. These are microprocessor-based, current-to-pneumatic digital valve controllers that are communicating instruments with internal logic capability. In addition to the traditional function of converting a current signal to a pressure signal to operate the valve, these smart positioners use the HART communications protocol to give easy access to information that is critical to process operation.

In addition to this, the smart positioner receives feedback about valve travel position plus existing supply and actuator pneumatic pressures, which allows it to diagnose not only itself, but also the valve and actuator to which it is mounted. Including a smart positioner as part of the final control element facilitates on-line, partial-stroke testing without the need for special mechanical limiting devices or other special test apparatus. Because the positioner communicates via HART protocol, the PST can be initiated from a HART hand-held communicator, from a personal computer running the positioner companion software, or from a panel-mounted pushbutton hardwired to the positioner terminals. Since the testing sequence is completely automatic, it eliminates errors and possible nuisance trips. For safety reasons, the operator is required to initiate the test sequence.

When applying automatic PSTs it must be considered that not all undetected failures are accounted for. Hence, the PFD rises even if the same test interval is chosen as for the complete proof test. Additionally, the manual proof test can uncover random faults that automatic tests cannot. PSTs are not to replace the manual proof test entirely; they are a recommendable measure to stretch the time between complete proof tests.

Many process operators do test safety devices periodically; however the planning and recording of those tests may not meet the specific requirements of the safety standards, when the inspector asks to see proof test records. Proof tests should be compatible with requirements in the SRS and with assumptions during SIL Verification. Proof test coverage and proof test frequency both impact the average probability of failure on demand calculation. Proper proof test plans will ensure that the design intent is met consistently, failures logged for future evaluation and records kept to allow proper auditing. Comprehensive long term records of proof tests will allow the failure rate assumptions and design intent to be validated.

It should be noted that HART is not a safety-rated platform. You should never substitute HART signals for hardwired signals when the hardwired signal is being used to detect a hazardous condition with a SIL rating. For example, valve position is a HART parameter in the Rosemount DVC6200 series positioner. If valve position is being used to detect a hazardous condition with a SIL rating, the valve position must be read using limit switches or position transmitters. However, if valve position is a diagnostic used to determine the status and health of the valve, then the HART parameter can be used. HART should only be used for diagnostic purposes.

2.5 Management of overrides

Maintenance overrides may be needed to enable proof testing whilst the process is in operation, or perhaps if a SIS device has failed and the process must continue operating whilst the repair is made. Operational overrides may be required to enable the process to be started or taken from one operating condition to another. Facilities to override sensors are fairly common, and in some cases overrides are also possible on final elements. Overrides must be used with caution; an overridden safety function will certainly fail on demand!

For this reason, IEC 61511 requires operating procedures for control and authorization of Maintenance Overrides, and checks to see that overrides are removed as soon as possible. Overrides should be reviewed at shift change, with automatic alarms to remind operators.

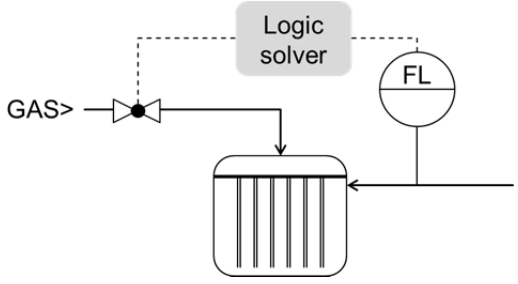

Figure 3: Example of a safety loop.

Any override applied for longer than the mean time to repair should be challenged. Systems which offer software tools to control and monitor overrides may support operational procedures. It is increasingly common for system designers to ask the question “why do you need that override?” If you don’t have an override it doesn’t require management! Where operational overrides are required consideration should be given to how they are removed, an automated process is always preferred. In a recent example (Figure 3) a manual override was specified on a low flow trip of liquid to a continuous reactor. This was manually removed when flow was established and before the hazardous gas was introduced. Operator error could leave the override in place and the process unprotected. By integrating the “not closed” signal from the gas valve into the SIF the override would be automatically removed and the correct protection in place whenever the hazard was present. The possibility of human error removed.

3. Conclusions

The strain on process operators and safety practitioners is continuously rising. On the one hand the legislative demands are becoming stricter, on the other hand the competition in all markets of the processing industries is growing tighter. To be successful commercially it is becoming critical to jointly fulfil safety requirements and operation targets. In everyday scenarios the responsible engineers get overwhelmed by a plethora of requirements from diverse sources. In order to come to grips with safety without getting lost in the tangle of demands, it is vital to focus on the “low-hanging-fruits”; those activities that yield the highest effectivity. Often, “functional safety” and “SIL” is subconsciously attributed with “calculations of probability on demand” or “SIL certified field devices” and other profound-sounding buzz words, so that the sight of the crucial matters becomes blurred.

This contribution is resetting the focus and narrowing the perspective to those activities that matter substantially. Five key areas were investigated and the cloud of buzz around functional safety was lifted to result in a set of recommendations that point at the core of the safety of plants in the processing industry.

Adhering to the recommendations given will not only improve the operating time of your plant but also the degree of safety of the daily operations. The five key areas constitute the foundation of a firm and solid safety concept that stretches over the entire safety life cycle of the plant, and therefore improves operations not only today but also for the future.

Reference

Cockman R., 2014, Customers and Safety, Emerson-User-Exchange, Stuttgart, Germany.

Riyaz A., LeRoy J., 2003, Q1, Smart positioners in safety instrumented systems, eptq.com.

Rezabek J., 2009, New HART for an old standard – has HART 7 given this old standby a new lease on life?, CONTROL Magazine, controlglobal.com.