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/CET1648104

Safety Instrumented System- Requirements for Successful Operation and Maintenance

Rafal P. Selega

ABB, Safety Lead Competency Centre, Howard Road, Eaton Socon, St Neots Cambridgeshire, PE19 8EU
rafal.selega@pl.abb.com

In today's world, personal risk posed by hazardous explosive or flammable industry processes depends on the correct functioning of both Safety Instrumented and other technology protection systems. They must be properly designed, operated, maintained and managed in order to achieve a tolerable level of risk on site. IEC 61508 and IEC 61511 standards constitute good engineering practice for safety instrumented systems (SIS) in this area. Based on these standards, this paper will attempt to explore the requirements constituting good practice for operation and maintenance of SIS for the process industry.
Good practice for operations and maintenance comprises essentially a number of legs for successful SIS operation:

1. Operation – The SIS is correctly operated within its specified limits for a specified operating time interval.
2. Maintenance – The routine recurring work implemented to keep a SIS in its designed capacity and at optimum efficiency.
3. Management – The coordination of the efforts of people to achieve safety. This comprises planning, organizing, competent staffing, leading and controlling.

For each of these three legs a number of key activities have been explored. The following list summarizes those topics which are to be addressed within the following sections of this paper:

- Essential SIS documentation
- Action to be taken on detection of SIS fault and SIF bypass
- SIF device life time
- SIS security
- Corrective, preventive and reliability centered maintenance
- SIF proof test, inspections,
- Test results analysis and spare parts
- Organization, planning and staff competency
- Assessment, auditing and management of change

1. Introduction

The key requirement for an organization responsible for operation and maintenance of the SIS is to maintain the designed functionality and safety integrity of the SIS during the whole operation and maintenance phase. The ideal scenario for this is that during the SIS design and engineering SIL classified devices are precisely selected, purchased and installed. All of them are new, reliable and perfectly functioning. The SIS application program is tested during Factory and Site Acceptance Tests. The operating plant is then commissioned and started up with the SIS fully available and it all works really great. We feel that we are safe.
So how long this ideal scenario last? Will it be one month, one year, ten years? We simply do not know. But one thing is certain, the SIS will eventually fail. The SIS is usually static e.g. a process unit feed line on-off valve can stay in normal process working condition (valve open) for years and be demanded to close on hazardous process demand which may come once per five or ten years. If the SIS is not inspected maintained and managed correctly, then when it fails this would not be detected by the responsible people and systems. Additionally it will not be repaired in a timely manner which further leads to the SIS not being able to respond when a real demand occurs.

Please cite this article as: Selega R., 2016, Safety instrumented system- requirements for successful operation and maintenance, Chemical Engineering Transactions, 48, 619-624 DOI:10.3303/CET1648104

SIS reliability can be underpinned by the three key principles of proper operation, proper maintenance and proper management. All three requirements are now explored in the following sections:

2. SIS operation

The SIS shall be operated within its specified limits for a specified operating time interval in order to be reliable. We also need to define what we mean be reliable operation. What is classified as satisfactory performance and which is not? SIS reliability includes five important aspects that need to be addressed during the SIS operation phase.

1. The system's "intended function" must be known. We shall know what the SIS does and what the SIS will not do regarding the designed functionality. Example: If the SIS is used for protection of compressors the target SIL of the Safety Instrumented Function (SIF) has been selected assuming certain personnel occupancy in this area. So if the SIL 2 has been selected for compressor overtemperature protection, assuming in LOPA personnel occupancy of 30 minutes per shift, then the field operator should be aware that when they spend more than 30 minutes within the compressor area the risk is higher than tolerable.
2. Regarding safety functionality, "when the system is required to function" must be identified. Usually it will start when the Basic Process Control System fails, but the SIS is required to know what is an exact measured process variable trip point activating one or more SIFs.
3. "Satisfactory performance" must be determined. Example: If 'valve A' actually closes within 10 seconds it will be treated as unsatisfactory performance because it will not protect a compressor separator from overfilling. The defined safety requirements call for the valve to be closed within 1 second so as not to exceed the maximum liquid level in the separator.
4. The "specified design limits" must be known. Note that all claims for device safety performance (failure rates) can be valid only if they are supported where the device is operated within its environment limits and for the specific process medium. Example: Reliable operation of the PT100 sensor for temperature measurement used for a SIF can only be guaranteed for process temperatures operating below 500 ^{O}C.
5. "Device design lifetime". As operating time interval increases, it becomes less likely that the device will achieve a successful outcome. We know it will eventually fail. However it should be known when to remove the device from operation when the manufacturer's recommended design and operating lifetime has elapsed.

So where do we find the requirements for reliable operation? It is not untypical that requirements for successful plant operation can usually be found within the following documentation:-

- Operation and maintenance manuals are the first and most important documents. They are typically prepared by plant designers and reviewed before plant start-up by the O&M team in order to evaluate the feasibility of safety requirements and the required operating conditions at the facility
- The Safety Requirements Specification (SRS). This is the key document for the Safety Instrumented System and which provides both functional and safety integrity requirements for each SIF designed for the project.
- Application program safety requirements specification (if not part of the SRS). Where all software requirements to achieve functional safety for the SIS application program are collected.
- List of safety critical elements along with the necessary procedures for how to handle them. It refers to the list of devices (SIS and Other Technologies) for which credit has been given during allocation of risk reduction for protection layers. For example: critical alarms or relief valves, which shall be regularly tested.
- Safety manuals for SIS devices. Here we can find the device manufacturer's requirements for safe use, maintenance, repair and modification of the SIS devices.

The below section 2.1 to 2.4 further explores the key requirements for SIS operation.

2.1 Action to be taken on detection of a fault

Are your operating teams confident of what to do if one of the SIF devices fails whilst the process plant is running? In this instance shall we trip the process unit protected by this SIF as the SIF is no longer available, or we shall keep the process unit running to avoid production losses?

Here IEC 61511-1 (2015) states that:

When a dangerous fault in an SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation. If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken. The specified action (fault reaction) required to achieve or maintain a safe state of the process should be specified in the SRS and shall be available for plant operator

So have you specified any compensating measures? If so do they meet Human Factor requirements in as much that the operating teams, the supporting operating procedures and the ability to monitor other mitigation systems can achieve the necessary level of the risk reduction now lost by the faulty SIF? Are you certain this

level of operator activity can be maintained over many hours whilst the SIF is being repaired? And what happens if the outputs to the final elements are overridden under MTTR? Are you certain they have been removed after re-instatement of the SIF?

2.2 Device life time – a "Bathtub" curve

Each device has its own useful life time after which it will eventually wear out and fail. After a defined period of time, the device failure rate increases considerably. The probabilistic model used for PFDavg calculation assumes a constant failure rate so we should know based on this calculation when to remove the device from service.
Process severity, environmental conditions and the company approach to inspection and maintenance typically impact on how long the device is to be kept in service (e.g. after some time, the maintenance costs to service the device to restore it to an 'as new condition' is very high and usually triggers the decision to replace it with a new one). All of these factors influence 'real' device life time. Based on the documented device operating field experience under defined operating conditions, the useful life time for the device can be assessed and modified by maintenance team. Maintenance should have this 'proven in use' data available to decide about exactly when the device is to be replaced / renewed.

2.3 Cybersecurity

It should be noted that ISA99 WG7 TG1 (2015) in cooperation with IEC TC65 is responsible for developing cybersecurity standards and related products. There are some reasons identified by ISA99 for why we need to integrate safety and security into industrial automation control systems:
Throughout the debate on control system security, there are a number of industry expert concerns arising that propose that overly strong alignment and integration can lead to ineffective or conflicting controls. The underlying premise here is that the means to implement, operate, and maintain system security should not compromise the performance of the safety instrumented systems (SIS). To this end, SIS installations should be designed and maintained using the foundation requirements found in IEC 61511 and ANSI/ISA-84.00.01-2004, and in the ISA/IEC 62443 series.
Recognizing the importance of SIS, and the rapidly emerging vendor solutions that offer varying degrees of integration with control networks, note that the LOGIIC group ("Linking the Oil and Gas Industry to Improve Cybersecurity") conducted a project assignment which consisted of the security evaluation and study of several SIS architectures. From this evaluation, the general conclusions where:-

- Greater integration may introduce greater risk
- Default configurations are not secure
- Defense in depth reduces risk
- Clear guidance is needed

2.4 Physical security

Physical security must be addressed by the asset owner and system integrator in their overall comprehensive security program. All SIS parts shall be protected against unauthorized or inadvertent modification of any of the SIS functions or devices.
If technical means are not possible to be applied than administrative procedures should be implemented.
Such systems and procedures and the parts of the SIS to be addressed should include:

- Cut off valves on transmitter impulse lines
- Transmitter manifold valves
- Transmitter (HART access disabled)
- Cabinets holding logic solver part with isolators interposing relays IO termination boards and so on
- Manipulating elements on valve(e.g. hand wheel)
- Clear identification of SIS devices via distinctively colored labels
- Physical separation of SIS and BPCS equipment (making it easier to secure the associated enclosures with key-locks)

3. Maintenance

By proper SIS maintenance, this means the routine recurring work provided to keep a SIS in its original or designed capacity and efficiency. In this paper, three basic types of maintenance are further reviewed:

- Corrective maintenance (initiated after the failure): Unscheduled maintenance which involves fixing any sort of failures
- Preventive maintenance (initiated before the failure): Performed in an attempt to avoid failures, unnecessary production loss and safety violations

622
- Reliability centered maintenance: Based on probabilistic performance based design. A series of activities based on device specific FMEDA and SIF specific reliability calculations

Each of the above maintenance activities including the links to inspection and proof testing are further explored below.

3.1 Corrective maintenance

A repair work order can be generated as a result of shift daily field rounds, scheduled inspections, execution of proof testing, on-line diagnostics or spurious process unit trips. Repair work should be performed in a timely manner (should be done as soon as it can be scheduled and safely executed). As faults are found and corrected, the repair information should be recorded for later review as part of the company continuous improvement processes. Compensating measure should be taken to maintain safe operation, or if not possible a specified action to achieve or maintain safe state of the process shall be taken (Refer back to section 2.1).

3.2 Preventive maintenance

Preventive maintenance is often required to extend the useful life of the equipment when some device part(s) have a shorter life (such as soft goods in sealing service). It is usually performed as based on the manufacturer recommendations and user experience with the equipment in similar operating environments. This ensures that equipment reliability is maintained when certain items are proactively repaired or overhauled.
Today's SISs employ a great deal of diagnostics which support preventive maintenance management as based on the device observed condition.

3.3 Reliability centered maintenance

This type of maintenance is similar to preventive maintenance but further allows SIS reliability and plant availability increases by the implementation of probabilistic performance based design. By quantifying the target risk reduction for the SIF, knowing the failure rates of safety devices used and assessing the effectiveness of testing (which device failures are detected by a specific test), it is possible to calculate how frequently the function or a device shall be tested and what exactly shall be addressed during the test.
It includes performing periodic proof testing at calculated frequencies which keep the device safety integrity within tolerable limits. Additional factors which differentiate this type of maintenance from conventional preventive maintenance are: functional safety assessment, analysis of frequency of process hazardous demands, device failure rates and controlling human errors for maintenance activities.

3.4 Inspection

IEC 61511-1 (2003) requires that each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g. missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, missing insulation, etc.
A periodic inspection shall be performed to identify and correct incipient issues and degraded conditions; this is often called 'proactive or condition-based maintenance'. Some inspections can be conducted externally during operation but others require more-rigorous internal inspection, such as looking at a valve seat or de-energizing circuits for pulling wires to see if they're loose. A report of an inspection should be prepared and maintained.

3.5 Proof test

Proof testing is a periodic test performed to detect dangerous hidden failures/faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition. Hidden Failure means the device(s) failure which is hidden from the operator during normal operation or not detected by any of the SIS automatic diagnostics or such failures which are not detected during routine inspection. The proof test should address both random and systematic failures. It should be noted that detection isn't the primary goal of proof testing. Its main purpose is finding weaknesses in maintenance strategy and root-cause identification with subsequent changes in the specification, design, installation or strategy.
Any failure found in a proof test should be considered as a serious problem, requiring immediate investigation to prevent future failures. Many incident investigations point out that companies have found and repeatedly corrected failures prior to an incident; but didn't prevent the failure from re-occurring by determining and addressing the root cause. The proof test only validates maintenance integrity, which depends upon inspection and preventive maintenance. IEC 61511-1 (2003) requires that:

- Periodic proof tests shall be conducted using a written procedure.
- The schedule shall be according to the Safety Requirements Specification.

- The whole SIS must be proof tested.(It can be performed in parts)
- Any deficiencies found shall be repaired in a safe and timely manner.
- Proof test shall also address the diagnostic failures.

It is not practicable to test all the SIS diagnostics during operations and maintenance. That said, some diagnostic tests are practicable e.g. checking that out of range is detected and annunciated. If high levels of diagnostics (>95%) are claimed when calculating the PFDavg and the diagnostics are not tested during proof testing then the calculated value could be misleading. If the diagnostics are not tested at the proof test itself, then the probability of the diagnostics being in a failed state will increase with time. Unfortunately in most cases, you don't know whether the vendor diagnostics are even working because there are no means to test them.

4. SIS management

Angel Casal (2011) noted that out of 35 major incidents 1987 to 2012 at least 90% were due to multiple systematic failures rather than due simply to random failures of equipment. So Industry should take note and focus equally as well on managerial problems and not only on the technical issues. The objective of SIS management requirements is to identify the management activities that are necessary to ensure the functional safety objectives for the plant are met. Responsibility for safety at the operational level is shared between multidisciplinary groups of people working as teams. It is therefore vital that communication between these groups is effective. The key SIS management requirements are further explored below:

4.1 Organization

IEC 61511-1 (2003) requires that *"The policy and strategy for achieving safety shall be identified together with the means for evaluating its achievement and shall be communicated within the organization"*. Responsibilities shall be assigned to persons and they shall be informed of these responsibilities*. It shall be documented who is responsible for what.*

4.2 Planning

Appropriate plan of all required activities for SIS operation and maintenance must be prepared and it should address the following:

- Routine and abnormal operation activities
- Inspection, proof testing, preventive, breakdown maintenance activities and functional safety audit performed by an independent person at a defined frequency.
- When these activities shall take place and who is responsible
- A SIS maintenance plan

Procedures should be implemented to ensure prompt follow-up and satisfactory resolution of all O&M recommendations. Unfortunately a common occurrence within lean operating facilities is when the personnel performing the activities are pressurized to rush through the proof test / inspection procedure for quickly restoring the process conditions. It is important to make sure to set aside adequate time for safety related activities and ensure the personnel are aware of the importance of their activities.

4.3 Staff competence

IEC 61508 (2010) and its process sector standards are performance based standards (as distinct from prescriptive standards) which require competent persons to properly understand and implement functional safety requirements. Competence is the ability of an individual to do a job properly. It is a combination of knowledge, skills, training and behavior. Competence shall be relevant to the specific responsibilities the person have been assigned for and can be underpinned specialized training and it is gained by experience under supervision. Sometimes engineers know the theory but not the installed system; the operators know a little about the system but not the process theory. Often personnel are trained not for dealing with failure/abnormal conditions, but for normal operating / ideal running conditions.

4.4 Assessment, auditing and control

SIS that have been installed and operating for a number of years are subject to modification and different kind of environmental changes. It is expected that such installed systems are subject to 'Periodic Functional Safety Assessments' to ensure that the SIS continues to provide the correct level of risk reduction via appropriate maintenance, operation and modification controls, including supporting procedures and safe systems of work.
This functional assessment shall be carried out by independent personnel to make sure the hazards arising from a process and its associated equipment are properly controlled. Note also that it is designed to assess and to identify that all procedures are in place for change management and that they are understood by personnel and followed. Experience suggests some management procedures are not tailored for the

personnel who have to use them (and invariably lie on a shelf somewhere and never actually be used by the O&M staff they were intended for).

4.5 Test results analysis and spare parts

Discrepancies between expected behavior and actual behavior of the SIS shall be analyzed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- the demand rate on each SIF and the cause of the demand.
- the actions taken following a demand on the system;
- the failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing or demand on a SIF;
- the cause and frequency of spurious trips;
- the failure of equipment forming part of any compensating measures and if compensating measures functions as planned.

All needed SIS spare parts should be identified and be available in order to minimize the bypass duration. A lack of spare parts can cause unnecessary plant shutdown when the MTTR cannot be achieved.

4.6 Management of change

Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification (Often overlooked is the impact of the change on other safety-related systems.). Modification activity shall not begin until an impact assessment and gap analysis is completed and after proper authorization. For larger change requirements – the requirements need to be managed as a real project.

5. Conclusions

As noted by UK HSE (2003) inadequate operation, maintenance and modification contribute to 35% of all primary causes of incidents in the process industry. This underpins the importance of O&M management in terms of failure avoidance. Operation phase typically last 20-30 years. This is long period where SIS reliability shall withstand different stresses such as: device wear out process, the SIS hardware and software improper operation and maintenance. The SIS reliability could be impaired by a poor company policy and strategy for achieving safety e.g. management process with no or little planning, not assigning persons to activities or not enough staff competency leading to wrong decisions and actions. The SIS never stays unchanged for years. Different requests for modification arise in time which needs to properly managed. The impact of the change on SIS performance, and process plant, update of all calculations and documentation must be done. All of the above factors are addressed by IEC61508 and IEC 61511 which constitute good practice guidance and are accepted worldwide. This paper aims to raise general awareness of good practice expectations and lists the key requirements for SIS which are today the major contributor in achieving process safety.

Acknowledgement

The constructive comments and editorial guidance by John Walkington from the ABB Safety Lead Competency Centre are gratefully acknowledged.

Reference

Angel Casal. 2011, ‘SIS Pitfalls, Major Accidents and Lessons Learned’, paper presented at the IDC Technologies Safety Control & Instrumentation Systems Conference, Perth, 20th September 2011.

IEC 61511-1 Functional safety –Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements First edition 2003

IEC 61511-1 Functional safety –Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements edition 2 FDIS version 2015

IEC 61508-1-7 Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 1 to 7 Edition 2 2010

ISA99 WG7 TG1 Recommendations to align safety and security for industrial automation control systems 2015

UK HSE, Publication, ‘Why control systems go wrong and how to prevent failure - Out of control’ 2003