Risk Topics

Functional Safety – Safety Instrumented Systems in Process Industries
August 2015

Process industries handling hazardous substances need reliable protection systems. The standardization of the specification, design, installation, operation and maintenance of such systems, defined as Safety Instrumented Systems, has gained importance. To this effect, the standard IEC 61511 is a reference guidance widely applied in the process industries. Risk Engineers should have a basic understanding of this standard and be able to recognize whether the safety systems in the process plants are properly managed and will provide the required level of protection.

Introduction

The intent of this publication is to summarize the basic concepts and general management practices depicted in the standards IEC 61511*/61508**. These standards are a powerful tool to maintain acceptable risk levels during the operational lifetime of a facility, also known as Functional Safety.

The approach described in the standards includes several aspects, from the technical requirements to the managerial activities, all of them clearly placed in the “Safety Life-Cycle” process which includes stages as specification, design, installation, operation and maintenance, modification and decommissioning of Safety Instrumented Systems.

This publication is not addressed to experienced people who are familiar with the application of the standard, but to those who need a basic understanding of Functional Safety and its related subjects.

Once the concepts and requirements of the Safety Life-Cycle phases are understood it should be easier to identify potential deviations to the correct implementation of the standards.

* IEC 61511: Functional safety - Safety instrumented systems for the process industry sector

** IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
Discussion

Risk reduction systems used in continuous process facilities such as those performed in refineries, chemical and petro-chemical sites are designed according to the following graph (from IEC standard), known as the onion representation – superimposed “layers” of protection.

![Diagram of onion representation of layers of protection](image)

*Fig. 1 - Onion representation of the layers of protection*

Functional Safety concepts are applicable to the Safety Instrumented Systems included in the “Prevention” layer of the onion above.

The IEC 61508/61511 standards deal with the management of safety instrumented systems (SIS), which are based on the use of electrical/electronic/programmable electronic technology. A safety instrumented system includes all of the components and subsystems that are necessary to carry out the safety instrumented function from sensor(s) to final element(s) as illustrated below:
It is critical that all three elements achieve certain performance levels in order to provide the desired level of protection.

The main definitions needed to understand the basics of Functional Safety are as follows:

- **Functional Safety (FS):** This is the part of the overall safety objective for an item of plant that is achieved by active systems such as a Safety Instrumented System (SIS). The illustration on the previous page (a sensor activating a shut-off valve when a certain parameter is exceeded) is an example of Functional Safety. Functional Safety relies on **active systems** (other examples: smoke detectors activating suppression systems; high level switch(es) on a flammable storage tank that will shut down a pump to prevent overflowing). Safety achieved by measures that rely on **passive systems** are not a part of Functional Safety.

- **Safety Instrumented System (SIS):** Are instrumented systems used to implement one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final elements(s). These can include either safety instrumented control functions (continuous mode) or safety instrumented protection functions, or both.

- **Safety Instrumented Function (SIF):** Is a function to be implemented by a SIS that is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event. Another, perhaps clearer definition of SIF is an identified safety function that provides a defined level of risk reduction (or safety integrity level - SIL) for a specific hazard by automatic action using instrumentation. A SIF is made up of sensors, logic solver, and final elements that act together to detect a hazard and bring the process to a safe state. An example of a SIF is the high temperature in a furnace that could cause a tube rupture (hazard), but is avoided by installation of a temperature gauge (sensor) that actuates an emergency shutdown valve (final element) to trip the fuel gas, once the pre-set high temperature level in the furnace is exceeded (logic solver - PLC). By definition each SIF must have a specified Safety Integrity Level (SIL), necessary to achieve the desired Functional Safety (i.e. the reduction of the risk to an acceptable level). A SIF can be either a safety instrumented protection function (i.e. operating in the demand mode) or a safety instrumented control function (i.e. operating in continuous mode).

- **Safety Integrity:** Is the average probability of a SIS to perform the required SIF under all the stated conditions in a period of time. For dormant systems (non-continuous mode) the probability of failure on demand (PFD)*** increases with time, and the average can be calculated for a given period.

***Note:

The calculation of the Probability of Failure on Demand (PFD) of a dormant (i.e. remaining idle until required) SIF depends on several aspects: the architecture (voting sensors, hardware fault tolerance, redundant final elements), the failure frequency of the components (failure mode analysis to estimate the dangerous undetected failure frequency), the common cause of failures (for example: transmitters connected on same piping exposed to freezing upon tracing failure, or clogging; redundant transmitters of same type subject to common failure modes), testing period, availability during test, partial tests performed, diagnostics, etc. The analysis of the calculation of the PFD is not included in the scope of this Risk Topic.

- **Safety Integrity Level (SIL):** Is a measure of safety system performance, more precisely the relative level of risk-reduction provided by a SIF. There are four discrete integrity levels (1 to 4) associated for SIL, for specifying the safety integrity requirements of the SIF to be allocated to the SIS. The higher the SIL, the
higher the probability that the required SIF will be carried out successfully, in other words the lower the probability of failure on demand for the safety system.

The following table (from IEC standard) shows the relationship between SIL and PFD:

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Target average probability of failure on demand</th>
<th>Target risk reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(10^{-5} \text{ to } 10^{-4})</td>
<td>(&gt;10,000 \text{ to } \leq 100,000)</td>
</tr>
<tr>
<td>3</td>
<td>(10^{-4} \text{ to } 10^{-3})</td>
<td>(&gt;1000 \text{ to } \leq 10,000)</td>
</tr>
<tr>
<td>2</td>
<td>(10^{-3} \text{ to } 10^{-2})</td>
<td>(&gt;100 \text{ to } \leq 1000)</td>
</tr>
<tr>
<td>1</td>
<td>(10^{-2} \text{ to } 10^{-1})</td>
<td>(&gt;10 \text{ to } \leq 100)</td>
</tr>
</tbody>
</table>

Fig. 2 – PFD – SIL correspondence

The SIFs, part of the SIS, are dormant systems, since they only actuate when the first layer (control system) fails to maintain the process within the operating window of the selected variables (temperature, pressure, flow, level, composition, etc.). That is why the most critical thing is to define what is the “dangerous failure frequency” which is associated with the failure modes that give no evidence of the unavailability of the safety function to perform in case of a real demand of the system.

And what is the purpose of all this theory?

**Reduce the risk of the installation**

Proceeding: Consider the following scheme (from IEC 61511 standard):

Fig. 3 – Risk reduction: general concepts – 61511-3 © IEC 2003€
A risk assessment is essential to define if Functional Safety is necessary. It should be performed to identify the hazards, their causes, the potential consequences and the required protection layers, which must be independent from each other to be considered effective barriers. It is considered that each protection layer will reduce the frequency of occurrence of the consequences. Hence, in the graph shown previously the “risk line” is analogue to “frequency” of occurrence of the estimated consequences. A protection layer must be specific, independent, effective, and auditable.

A HAZOP is normally used in the process industry to identify deviations leading to severe consequences that will require a more detailed semi-quantitative assessment such as LOPA (quantitative in terms of frequency; qualitative in terms of consequences).

LOPA (Layers of Protection Analysis) is a powerful analytical tool for assessing the adequacy of protection layers used to mitigate process risk. LOPA will determine the required PFD of the SIF which will protect the installation from an identified hazard, in order to maintain the scenario below the tolerable risk boundary. Knowing the PFD, the SIL required by the SIF is then easily obtained.

Other methods recommended by the IEC standard are the semi-quantitative method (combination of fault tree and event tree), the safety layer matrix method, the Calibrated risk graph, and the Risk graph.

As part of the risk assessment, it is necessary to define the “Risk Tolerance Boundary”, i.e. the acceptable frequency (probability of occurrence) for the expected consequence (severity) of the scenario. This can be defined by each specific location. As low As Reasonably Practical “ALARP” criteria may also be applicable for specific cases where risk reduction is a trade-off, as illustrated on the next page:

![Fig. 4 - ALARP criterion (As Low As Reasonable Practicable)](image-url)
The following scheme (from IEC) shows the concept of layers using an event tree analysis:

![Event Tree Analysis Diagram]

To illustrate this concept consider the following example:

A process vessel could be subject to overpressure caused by, for instance, a failure of the BPCS (Basic Process Control System) or an external fire. The frequency of overpressurization (in terms of times per year) is estimated or calculated by means of a fault tree. From left to right there are columns representing each protection layer which could prevent the release to the environment of the hazardous substance. Each layer has a PFD (Probability of Failure on Demand) ranging from 0 to 1. Each branch of the “tree” represents the success or failure of the protection layer on its function.

On the right end of the scheme the outcomes of the tree represent the final events with their associated frequencies which are calculated utilizing the PFDs of the protection layers (fconseq=fin.event x ΠPFDbarrier i). For the case of a release to the environment further analysis could be performed to define the actual consequences (i.e. pool fire, jet fire, VCE, flash fire, etc.) and their related frequency and severity considering a number of additional factors. For a quantitative approach also a statistic distribution of the release hole sizes can be considered. At this stage it is acceptable to consider the severity of the worst case.

Once the severity is estimated and the frequency of the consequence calculated, the assessment is performed, utilizing the risk matrix. If for the given severity, the calculated frequency is acceptable, then no further action is needed. If it is not acceptable, then a higher SIL will be required to the SIF (s), hence a lower PFD.

The determination of the SIL required to each SIF, to maintain the process within a tolerable risk level boundary, is one of the stages of the Safety Life-Cycle. The Safety Life-Cycle is a set of guidelines (engineering process) covering safety-related systems over their lifetime, i.e. from cradle (risk analysis) to grave (decommissioning).
The Safety life-cycle as presented in the Standard 61511 is reported in Appendix A.

The management of the Functional Safety includes several aspects: Hazard identification, risk assessment, and the SIL allocation.

Another relevant factor is the Safety Requirement Specification (SRS), containing all the requirements of the SIF that have to be performed by the safety instrumented systems. The SRS shall specify all requirements of safety instrumented systems needed for detailed engineering and process safety information purposes. For instance, in respect of Operation and Maintenance, the test intervals and techniques are defined in order to maintain the required SILs during the lifetime of the facility.

If a SIL analysis is to be conducted for an existing facility, a gap analysis should be performed in order to assess the current SIL level, and the required SIL that will attain a tolerable risk level. The calculation of the SIL of existing SIFs often has challenges, due to the lack of information regarding the components of the installed SIFs.

**Guidance**

The objective of this Risk Topic is to provide basic information that could be helpful during an on-site survey. It is generally observed that the documentation about these topics is not readily available on-site during the surveys, letting the risk engineer use judgment (on the proper management of the functional safety) based on the knowledge and involvement of the personnel being interviewed.

It should be mentioned that SIL rating does not apply to processes or facilities, but only to individual SIFs. The high SIL rated SIFs should be known by the safety, instrument and operations engineers, as well as by the site management since they are knowledgeable with the most relevant hazards of the plant.

SIL assessment studies are generally performed during the design phase of new facilities, in conjunction, or after the HAZOPs studies. The SISs are developed using the risk assessment as input. The Safety Requirement Specifications (SRSs) need to be defined for every SIF. However, this may not be sufficient to maintain the required integrity levels during the lifetime of the facility. The SIL management, over time, is critical including any modifications performed on the SIS, using a proper Management of Change protocol.
• During a site survey some aspects related to the operation and maintenance practices on SILs can be verified as follows:

• Proof-test intervals defined by the SIL determination and procedures to reveal dangerous undetected failures

• Mitigation measures during testing or maintenance of critical SIFs (impairment/degradation due to by-pass)

• Registers of systems failures and demand rates on the SIS, causes and actions taken, spurious trips

• Audits performed, maintenance instruments calibration

• Procedures to follow upon faults or failures of the SIS (faults diagnostics, repairs, revalidation, failures reporting, bad actors etc.)

• Inspections registers (to verify for missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation)

• Identification in the maintenance program system as Safety Critical Element (SCE) with no backlog

Additional, more in-depth criteria for assessing the implementation of Functional Safety and Safety Instrumented Systems are provided in the Appendix B.

SIL4 rated SIFs are only used in specific industries, such as nuclear power plants. SIL3 rated SIFs are generally avoided due to the architectural restrictions and the testing frequency required maintaining its average PFD: additional layers of protection are placed instead.

As a rule of thumb the SIL rating distribution of SIFs in a plant are as follows: SIL 1 ~95%, SIL 2 ~5%, SIL 3 ~<1% (high risk associated, off-shore, nuclear), SIL 4 highest risk (nuclear industry).

A SIL3 rated safety PLC means that it can be used in applications up to SIL3, that is all. It does not guarantee that any SIF (sensors/ logic solver-PLC/ final element) will attain that integrity level. The sensors (i.e. temperature, pressure transmitters etc.) and final elements (i.e. relays, shutdown valves, and solenoid valves) have much higher failure frequencies than the logic solvers.

When there is no Functional Safety management at the facility, the first step is to allocate resources for this task. This is not a specific project but a continuous process. The training of the personnel involved and the definition of the program is of paramount importance. The hazards identification step would be the kick-off of the process.

Some companies may have a good process safety management, in terms of hazards identification and continuous improvement, state of the art control and protections systems, as well as qualified personnel in maintenance and operation, but lack the implementation of a Safety Lifecycle concept. In this case the introduction of Safety Lifecycle could provide excellent benefits with little investment.
Conclusion

The information presented in this Risk Topic is aimed at providing a basic understanding of the identification of the potential deviations from the internationally recognized standards IEC 61511/61508 on Functional Safety. This should help the Risk Engineer in the field assessment of a continuous processing plant, and to provide proper advice or to recommend the adequate measures for the implementation of a SIS management system.

The correct specification, design, installation, operation and maintenance, and modifications’ management of the Safety Instrumented Systems is critical to maintain the plant risks as low as reasonable practicable.

References


“The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards IEC 61511-1 ed.1.0 (2003) and IEC 61511-3 ed.1.0 (2003).

All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein”

IEC 61511-1 ed.1.0 “Copyright © 2003 IEC Geneva, Switzerland. www.iec.ch”

IEC 61511-3 ed.1.0 “Copyright © 2003 IEC Geneva, Switzerland. www.iec.ch”

ANSI/ISA-84.00.01 – Adopting IEC 61511.

DIN V 19250 - Fundamental safety aspects for measurements and control equipment
Appendix A

Safety life-cycle (Standard 61511)
Appendix B

**Assessment criteria for standard 61511**

Functional Safety and Safety Instrumented Systems is a complicated subject and it would be easy for field engineers to lose focus in the depth of technical information presented. To better gauge the extent and maturity of 61511 implementation by a company during a site survey field engineers may complement the list presented on page 8 with following issues:

On the basis of all scenarios generated with the hazard identification step, is there a process in place for screening the process hazards that will require a SIL assessment. The remaining ones, i.e. those process hazards that are adequately controlled by the basic process control system and operating procedures, will not require a SIL rated SIS.

- Has the site been able to SIL screen a large number of hazards scenarios such as by risk graphs
- Does the site use LOPA where a SIL 1 or above requirement has been identified from screening
- Are there management endorsed residual risk criteria that have been sensibly used to set an overall tolerable residual risk criterion for use with LOPA that could be applied to an individual hazard scenario where one of the layers of protection is a SIS.
- calibrate screening risk graphs
- Have residual risk criteria also been established to cover financial (property) and environmental losses, in addition to people harm. While people safety usually determines the necessary integrity levels, occasionally either financial or environmental considerations will increase the integrity level needed.
- How is the quality of SIL assessment practice ensured – training, in house procedures, use of external experts
- Are SIL assessment and safety requirements allocation records of good standard, auditable and detailed?
- Is a safety plan produced to define and monitor the safety lifecycle activities?
- Does the site understand and implement the broader 61511 safety life cycle. How do they ensure that the original functional safety requirement and allocation to SIL rated SIF/SIFs remains uncorrupted by potential systematic/human error at each stage of the project life cycle? Is there a process of verifying that all the necessary inputs were available and necessary steps done at each stage and then validating that the output of that stage will result in the required level of functional safety being maintained (on-going functional safety assessment)? I.e. how do you make sure the SIS designer correctly interprets the SIL and functional safety requirements, how do you make sure the SIS is produced and installed as intended by the designer, how do the commissioning team validate correct functioning of the SIS etc.?
Real example of a systematic/human error creeping into the safety life cycle

A SIL 2 reactor dump system failed its first annual proof test – one of the redundant dump valves didn’t open. The investigation showed that this wasn’t due to random premature component failure, it was a systematic error by the installation team. The discharge ports of the solenoid valves had been orientated upwards and condensation from within the reactor house had fallen into the solenoid and corroded the internals. All solenoid valves had to be replaced and installed with the correct orientation of the discharge ports.
The information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Group Ltd. or any of its subsidiaries (hereinafter ‘Zurich’) as to their accuracy or completeness.

Some of the information contained herein may be time sensitive. Thus, you should consult the most recent referenced material.

Information in this document relates to risk engineering / risk services and is intended as a general description of certain types of services available to qualified customers. It is not intended as, and does not give, an overview of insurance coverages, services or programs and it does not revise or amend any existing insurance contract, offer, quote or other documentation.

Zurich and its employees do not assume any liability of any kind whatsoever, resulting from the use, or reliance upon any information, material or procedure contained herein. Zurich and its employees do not guarantee particular outcomes and there may be conditions on your premises or within your organization which may not be apparent to us. You are in the best position to understand your business and your organization and to take steps to minimize risk, and we wish to assist you by providing the information and tools to assess your changing risk environment.

In the United States of America, risk services are available to qualified customers through Zurich Services Corporation and in Canada through Zurich Risk Services as also in other countries worldwide, risk engineering services are provided by different legal entities affiliated with the Zurich Insurance Group as per the respective country authorization and licensing requirements.

©2014/2015 Zurich Insurance Group Ltd.