SIS - Safety Instrumented Systems - A practical view - Part 4

César Cassiolato
Marketing, Quality, Project and Services Engineering Director
SMAR Industrial Automation
cesarcass@smar.com.br

Introduction

The Safety Instrumented Systems are used to monitor the condition of values and parameters of a plant within the operational limits and, when risk conditions occur, they must trigger alarms and place the plant in a safe condition or even at the shutdown condition.

The safety conditions should be always followed and adopted by plants and the best operating and installation practices are a duty of employers and employees. It is important to remember that the first concept regarding the safety law is to ensure that all systems are installed and operated in a safe way and the second one is that instruments and alarms involved with safety are operated with reliability and efficiency.

The Safety Instrumented Systems (SIS) are the systems responsible for the operating safety and ensuring the emergency stop within the limits considered as safe, whenever the operation exceeds such limits. The main objective is to avoid accidents inside and outside plants, such as fires, explosions, equipment damages, protection of production and property and, more than that, avoiding life risk or personal health damages and catastrophic impacts to community. It should be clear that no system is completely immune to failures and, even in case of failure; it should provide a safe condition.

For several years, the safety systems were designed according to the German standards (DIN V VDE 0801 and DIN V 19250), which were well accepted for years by the global safety community and which caused the efforts to create a global standard, IEC 61508, which now works as a basis for all operational safety regarding electric, electronic systems and programmable devices for any kind of industry. Such standard covers all safety systems with electronic nature.

Products certified according to IEC 61508 should basically cover 3 types of failures:

- Random hardware failures
- Systematic failures
- Common causes failures

IEC 61508 is divided in 7 parts, where the first 4 are mandatory and the other 3 act as guidelines:

- Part 1: General requirements

- Part 2: Requirements for E/E/PE safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

Such standard systematically covers all activities of a SIS (Safety Instrumented System) life cycle and is focused on the performance required from a system, that is, once the desired SIL level (safety integrity level) is reached, the redundancy level and the test interval are at the discretion of who specified the system.

IEC61508 aims at potentializing the improvements of PES (Programmable Electronic Safety, where the PLCs, microprocessed systems, distributed control systems, sensors, and intelligent actuators, etc. are included) so as to standardize the concepts involved.

Recently, several standards on the SIS development, project and maintenance were prepared, as IEC 61508 (overall industries) already mentioned, and is also important to mention IEC 61511, focused on industries with ongoing, liquid, and gas process.

In practice, in several applications it has been seen the specification of equipment with SIL certification to be used in control systems, without safety function. It is also believed that there is a disinformation market, leading to the purchase of more expensive pieces of equipment developed for safety functions where, in practice, they will be used in process control functions, where the SIL certification does not bring the expected benefits, making difficult, inclusive, the use and operation of equipment.

In addition, such disinformation makes users to believe that they have a certified safe control system, but what they have is a controller with certified safety functions.

With the increase of usage and applications with digital equipment and instruments, it is extremely important that professionals involved on projects or daily instrumentation are qualified and have the knowledge on how to determine the performance required by the safety systems, who have domain on calculations tools and risk rates within the acceptable limits.

In addition, it is necessary to:

- Understand the common mode failures, know which types of safe and non-safe failures are possible in a specific system, how to prevent them and, also, when, how, where and which redundancy level is more appropriate for each case.
- Define the preventive maintenance level appropriate for each application.

The simple use of modern, sophisticated or even certified equipment does not absolutely ensure any improvement on reliability and safety of operation, when compared with traditional technologies, except when the system is deployed with criteria and knowledge of advantages and limitations inherent to each type of technology available. In addition, the entire SIS life cycle should be in mind.

Commonly we see accidents related to safety devices bypassed by operation or during maintenance. Certainly it is very difficult to avoid, in the project stage, that one of such devices are bypassed in the future, but by a solid project that better satisfies the operational needs of the safety system user, it is possible to considerably eliminate or reduce the number of non-authorized bypass.

By using and applying techniques with determined or programmable logic circuits, failure-tolerant and/or safe failure, microcomputers and software concepts, today is possible to project efficient and safe systems with costs suitable for such function.

The SIS complexity level depends a lot on the process considered. Heaters, reactors, cracking columns, boilers, and stoves are typical examples of equipment requiring safety interlock system carefully designed and implemented.

The appropriate operation of a SIS requires better performance and diagnosis conditions compared to the conventional systems. The safe operation in a SIS is composed by sensors, logic programmers, processors and final elements designed with the purpose of causing a stop whenever safe limits are exceeded (for example, process variables such as pressure and temperature over the very high alarm limits) or event preventing the operation under unfavorable conditions to the safe operation conditions.

Typical examples of safety systems:

- Emergency Shutdown System
- Safety Shutdown System
- Safety Interlock System
- Fire and Gas System

We have seen in the previous article, in the third part, some details on the models of fault trees analysis, Markov model and some calculations.

In the forth part, we will see some points about the SIF Verification Process.

SIF Verification Process (Safety Instrumented Function)

A Safety Instrumented System (SIS) is a critical layer for the accident prevention. A SIS performs several SIFs (Safety Instrumented Function) and is typically composed by sensors, logic analyzers and final elements of control. Acceptable probability of failure on demand (SIL - Safety Integrity Level) for each SIF need to be determined for the project and subsequent verification.

The safety analysis is made over the SIFs risks levels.

A Pressure transmitter and a Positioner are part of the SIF, for example;

There are several methods to identify the SILs required to SIFs. One of them is the Layer of Protection Analysis, LOPA, a technique of risk analysis which is applied following the use of a qualitative technique for hazard identification, such as, HAZOP (Hazard and Operational Study). Derived from a risk quantitative analysis tool, the frequency analysis by an event tree, LOPA may be described as a semiquantitative technique, as it provides a risk estimative.

The control systems are projected to keep the process within the specific process parameters considered as acceptable for the normal and safe operation of the plant. When the process exceeds the normal operation limit, it may present potential risk to human life, environment, and assets. In the evaluation stage, the risks are identified together with its consequences and the ways to prevent their occurrence are defined.

The risk identified will have its probability reduced according to capacity of the system providing preventive layers. The risk reduction establishes three criteria:

- The equipment should be approved for the environmental conditions where it will be installed;
- The subsystems should have tolerance to failures required due to the dangerous failures presented by the process;
- The Probability of Failure on Demand (PFD) of SIF should be appropriate to the risks acceptable by the company.

The user should have domain of information on the equipment, so it is possible to conduct a good analysis of SIF performance. The constructive techniques with a tolerance view concerning the component failures prevent that a single failure causes a device failure. Finally, the performance calculation determines if the SIS keeps the project expectations regarding the desired integrity level. The SIS reliability is defined by some parameters:

- Mean Time Between Failures (MTBF)
- Voting Architecture
- Diagnosis coverage (DC)
- Test interval (TI)
- Mean Time to Repair (MTTR)
- Common failure mode

For each SIF, at least the following information should be analyzed:

- Hazard and its consequences
- The hazard frequency
- Definition of the process safe state
- SIF description
- Description of the process measurements and its trip points
- Relation between inputs and outputs, including logics, mathematical functions, operation modes, etc.
- Required SIL

- Proof test period
- Maximum trip rate allowed
- Maximum response time for SIF
- Requirements for SIF activation
- Requirements for SIF reset
- SIF response in case of diagnosis failure
- Human interface requirement, that is, what needs to be shown in Displays, supervision, etc.
- Maintenance requirement
- MTTR estimation after trip
- Expected environmental conditions in several situations: normal and emergency operation.

Equipment Selection

It is necessary to take care of the choice of equipment working in safety systems. Certified pieces of equipment should be specified according to IEC61508 or complying with the "prior use" criteria according to IEC61511.

Proven in Use (PIU) is a characteristic defined by IEC61511 (clause 11.4.4) in which if a equipment has already been successfully used in safety applications and meets some requirements (see below, then the HTF (hardware tolerance fault) can be reduced and, with that, use it in safe applications with lower costs:

- The supplier quality system should be considered
- Equipment hardware and software version
- The performance and application in safety systems documents
- The equipment can not be programmed and should allow, for example, setting up the operation range
- The equipment need a write protection or Jumper command
- In such case, the SIF is SIL 3 or lower.

The major advantage is that it is possible to standardize Equipment for use in control and Equipment for safety with a much lower cost.

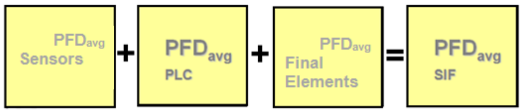
By hardware analysis, called FMEDA (Failure Modes Effects and Diagnostics Analysis) it is also possible to determine the failure rates and the instrument modes. Such analysis type is an extension of the known FMEA method, the methodology of Failure Mode and Effect Analysis. In that case, the FMEDA identifies and calculates the failure rates in the following categories: Detectable safe, non-detectable safe, detectable dangerous and non-detectable dangerous. Such failure rates are used to calculate the safety coverage factor and the risk factor

Once the safety integrity level and its requirements are calculated, then the equipment, redundancy levels and tests are to be chosen, according to the SIF demand. After that, with the information of each equipment and device, it is calculated by equations, tree analysis, Markov model and other techniques if the equipment chosen meet the safety requirements.

How to determine the architecture?

- A SIF architecture is decided by the failure tolerance of its components.
- It may reach a SIL higher level using redundancy.
- The number of pieces of equipment will depend on the reliability of each component defined in its FMEDA (Failure Modes, Effects and Diagnostic Analysis).
- The three commonest architectures are:
- Simplex or voting 1oo1 (1 out of 1)
- Duplex or voting 1oo2 or 2oo2
- Triplex or voting 2oo3

Figure 1 shows the most common examples of architecture for safety systems, where several techniques are used according to the voting system and desired SIL:



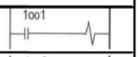
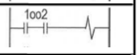
Voting	(PFD_{avg})	Architecture
1oo1	$\lambda_{du} * T/2$	
1oo2	$\frac{(\lambda_{du})^2 * T^2}{3}$	
2oo2	$\lambda_{du} * T$	
2oo3	$(\lambda_{du})^2 * T^2$	

Figure 1 - Typical examples of architecture for safety systems

For SIFs, the failure probability may be interpreted as the transition of a device from the operation state to the state where it is no longer playing the role to which it was specified.

When the device is tested, the PFD (t) is reduced to the initial value. That involves two implicit assumptions:

- Every device failure is detected by the inspection and by the proof test.
- The device is repaired and returned to service as new. The proof test effect is shown by the form of the saw tooth shown on figure 2.

As the result, the test interval is a imperative factor to determine the reached SIL classification.

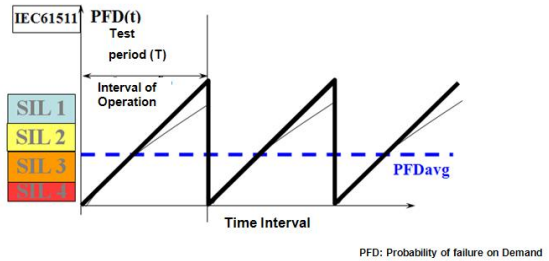


Figure 2 - Transition and PFD states

Establishing Functional Tests Interval

- The time period is a parameter significantly affecting the PFD and, therefore, the SIL
- It is common to increase the frequency of tests and, then, decreasing the the failures probabilities (example: valve tests, partial strokes)
- Suppose a SIL supports SIL 2, but the test interval is long, and it can support SIL 1.
- In the same way, if you have 2 pieces of equipment SIL 2 in voting and the interval is short, SIL 3 can be supported.

Conclusion

In practical terms, the aim is the reduction of failures and, consequently, the reduction of shutdowns and operational risks. The purpose is to increase the operational availability and also, in terms of processes, the minimization of variability with direct consequence to the profitability increase.

References

- IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems.
- IEC 61511-1, clause 11, " Functional safety - Safety instrumented systems for the process industry sector - Part 1:Framework, definitions, system, hardware and software requirements", 2003-01
- ESTEVES, Marcello; RODRIGUEZ, João Aurélio V.; MACIEL, Marcos.Sistema de intertravamento de segurança, 2003.
- William M. Goble, Harry Cheddie, "Safety Instrumented Systems Verification: Practical Probabilistic Calculation"
- Sistemas Instrumentados de Segurança - César Cassiolato
- "Confiabilidade nos Sistemas de Medições e Sistemas Instrumentados de Segurança" - César Cassiolato
- Manual LD400-SIS
- Sistemas Instrumentados de Segurança – Uma visão prática – Parte 1, César Cassiolato
- Researches on internet