

Find Your Product:

**MY ACCOUNT LOG IN**

[If you don't have a login, click here to register](#)  
[Forgot your password?](#)

## SIS - Safety Instrumented Systems - A practical view - Part 1

[Tweet](#) [G+](#) [Share](#)



César Cassiolato

**Marketing, Quality, Project and Services Engineering Director**  
**SMAR Industrial Automation**  
[cesarcass@smar.com.br](mailto: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 will start with a Safety Life Cycle and Risk Analysis.

## Safety Life Cycle

Definition: "It is an engineering process with the specific purpose of reaching and ensuring that a SIS is effective and allowing the reduction of risk levels at an effective cost during the entire system life".

In other words, the cycle is intended to be a risk evaluation guide during the entire system life, since the project conception to the daily maintenance.

Why the Safety Life Cycle?

- Accidents may happen and, therefore, it is necessary to minimize them in frequency and severity.
- Safety Instrumented Systems and Safety Life Cycles are designed to minimize risks.

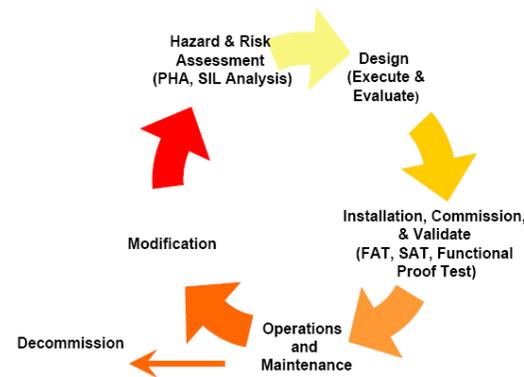


Figure 1 - Typical example of a Safety Life Cycle

The Safety Life Cycle involves the probability analysis so as to ensure the safety project integrity. In addition, it allows, by the calculations, reducing the risk at an effective cost. Keeping a SIS integrity during the plant life cycle is extremely important for the safety management. An effective management program should include strict controls and procedures ensuring that:

- The identification of critical points, concepts and choice of sensors, technology, logic solver and final equipment and elements and the redundancy need comply with the safety levels and calculated risks reduction. Once the technology and the architecture are chosen, there is an analysis plan and periodic review of them, reassessing the overall safety.
- The tests of each phase (project, installation, operation, modification/maintenance) are conducted in compliance with the safety requirements, safety procedures and standards.
- The SIS goes back to its normal operation after a maintenance.
- The system integrity is not compromised by non-authorized access to set up, trip or bypasses points.
- Procedures of change management are always followed to any system change.

- The changes quality is verified and the system is revalidated before returning to operation.

The Safety Life Cycle should be part of a PSM (Process Safety Management System). In this way, it will be conveniently adopted and applied in a conscious way and involving employees in all its stages and company levels.

## Risk Analysis

The more risks a system has, the more difficult is to meet the requirements of a safe system. Basically, the risk is the sum of the probability of something undesirable happening as a consequence of such occurrence.

The risk of a process may be defined as the product of the frequency of occurrence of a specific event (F) and the consequence resulting from the event occurrence (C).

$$\text{Risk} = F \times C.$$

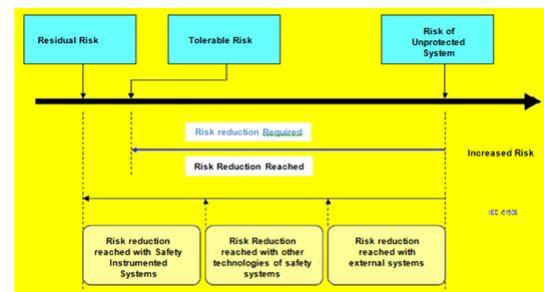


Figure 2 - Risk considerations according to IEC 61508.

In the safety systems, the search is for minimizing the risks at acceptable levels and the SIL level for control may be determined by the analysis and identification of process risks. The verification of the SIL level may be conducted by the probability of failure on demand (PFD).

The IEC 61508 defines requirements for a system operation and integrity. The requirements for operation are based on the process and for integrity; they are based on reliability, which is defined as the Safety Integrity Level (SIL). There are 4 discreet levels which have 3 important properties:

1. Applicable to the overall safety function;
2. The highest the SIL level, the stricter are requirements;
3. Applicable to technical and non-technical requirements

SIL Safety Integrity Level (per IEC 61508)	Safety Availability	PDF Probability of Failure on Demand 1 – Availability	RRF Risk Reduction Factor 1 / PDF
4	> 99.99%	< 0.0001 (1E <sup>-4</sup> )	> 10,000
3	99.9 – 99.99%	0.001 – 0.0001 (1E <sup>-3</sup> to 1E <sup>-4</sup> )	1,000 – 10,000
2	99 – 99.9%	0.01 – 0.001 (1E <sup>-2</sup> to 1E <sup>-3</sup> )	100 – 1,000
1	90 – 99%	0.1 – 0.01 (1E <sup>-1</sup> to 1E <sup>-2</sup> )	10 – 100
0	Basic Process Control		

Table 1 - SIL Levels

How to interpret the SIL levels? As we have seen, the SIL level is an integrity measure of a SIS and we can interpret it in two ways:

1) Taking into consideration the risk reduction and table 1:

- SIL1: risk reduction  $\geq 10$  and  $\leq 100$
- SIL2: risk reduction  $\geq 100$  and  $\leq 1000$
- SIL3: risk reduction  $\geq 10000$  and  $\leq 100000$
- SIL4: risk reduction  $\geq 100000$  and  $\leq 1000000$

2) By interpreting table 2, where, for example, SIL 1 means that the risk of accident or something undesirable is low and that a SIS has 90% availability, or even a 10% chance of failure.

Safety Failure Fraction (SFF)	Hardware Fault Tolerance (HFT) for Type B Device		
	0	1	2
< 60%	Not Allowed	SIL 1	SIL 2
$\geq 60\%$	SIL 1	SIL 2	SIL 3
$\geq 90\%$	SIL 2	SIL 3	
$\geq 99\%$	Special requirements apply (see IEC 61508)		

Table 2 - Levels of SIL and SFF according to the tolerance to hardware failure

The SIL evaluation has grown in the last few years, mainly in chemical and petrochemical applications. We can even express the need for SIL due to the likely impact on the plant and community:

- “4”- Catastrophic impact for the community.
- “3”- Protection of employees and community.
- “2”- Protection of production and property. Possible damages to employees.
- “1”- Slight impact on the property and protection of production.

SIL Safety Integrity Level (IEC 61508)	Availability	PFDF Probability of Failure on Demand (1-Availability)	Risk Reduction Factor (1/PFD)
4... Catastrophic impact for community	> 99.99%	< 0.0001 ( $e^{-4}$ )	> 10000
3 Protection of employees and community	99.9 – 99.99%	0.001 – 0.0001 ( $e^{-3}$ - $e^{-4}$ )	1000 - 10000
2... Protection of production and property, Possible damage to employees	99 – 99.9%	0.01 – 0.001 ( $e^{-2}$ - $e^{-3}$ )	100 – 1000
1 Slight impact to property and protection of production	90 – 99%	0.1 – 0.01 ( $e^{-1}$ - $e^{-2}$ )	10 – 100
0	Basic Process Control System (BPCS)		

Figure 3 - SIL due to the likely impact on the plant and community

Such analysis is not satisfactory as it is hard to classify what is a slight and big impact.

There are several methods of risks identification:

- HAZOP technique (Hazard and Operability Study): where risks are identified and when higher SIL levels are required;
- Check Lists technique;
- FMEA technique (Failure Modes and its Effects), when the failure of each equipment and component is analyzed at the control screening.

In terms of SIL levels, the higher the required level, the higher the cost due to more complex and stricter specifications for hardware and software. Usually, the SIL choice of each safety function is associated with the staff experience, but one may choose the HAZOP matrix analysis or the Layers of Protection Analysis (LOPA), where the policy, procedures, safety strategies and instrumentation are included.

Follows below some stages and details of Risk Analysis:

1. Identification of potential risks
  - a. Starts with HAZOP (Hazard and Operational Issues Study)
  - b. The company should have a group of experts in the process and in its risks
  - c. Several methodologies may be applied, such as PHA (Process Hazard Analysis), HAZOP for risks identification, modified HAZOP, accident consequences, Risks Matrix, Risks Diagram or Quantitative Analysis for identification of the safety level to be reached.
  - d. The standards suggest methodologies for the SIL identification
  - e. The available methods are qualitative, quantitative or semiquantitative
  - f. Determine the SIL appropriate for the SIS, where the risk inherent to the process should be equal to or lower to the acceptable risk, ensuring the necessary safety for the plant operation.
2. Evaluate the probability of a potential risk related to
  - a. Equipment failure
  - b. Human errors

3. Evaluate the potential risks and consequences of the event impacts

<b>Frequency</b>	<b>4</b>	<b>SIL 2</b>	<b>SIL 3</b>	<b>SIL 4</b>	<b>SIL 4</b>
	<b>3</b>	<b>SIL 2</b>	<b>SIL 3</b>	<b>SIL 3</b>	<b>SIL 4</b>
	<b>2</b>	<b>SIL 1</b>	<b>SIL 2</b>	<b>SIL 3</b>	<b>SIL 3</b>
	<b>1</b>	<b>SIL 1</b>	<b>SIL 1</b>	<b>SIL 2</b>	<b>SIL 2</b>
<b>Consequence Severity</b>		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>

Table 3 - Example of Risk Matrix

Frequency Range	Qualitative Criteria
4	(> 1/100 year): Failures in simple pieces of equipment or valves, failures in pipes or a simple error in routine activities
3	(1/100 – 1/1000 year): Failures in double equipment or valves, ruptures in pipes, leakage or human error
2	(1/1000 – 1/10000 year): Combination of failures in instruments and human errors or failures in small process lines
1	(> 1/10000 year): Multiple failures in instruments and human errors or spontaneous failures in tanks and process vessels

Table 4 - Frequency Range - Qualitative Criteria

Consequence Range	Qualitative Criteria
4	Individual: Multiple critical injuries or fatalities Public: Potential for critical injuries or fatalities Environment: Release of unconfined with high environmental impact Property: Loss > US\$100M
3	Individual: Potential for serious injuries or small fatalities Public: Potential for serious injuries or small fatalities Environment: Release of unconfined with medium environmental impact Property: Loss between US\$10M and US\$100M
2	Individual: Serious injuries requiring medical emergency Public: Potential for serious injuries requiring medical emergency Environment: Release of unconfined with low environmental impact Property: Loss between US\$1M and US\$10M
1	Individual: Injuries require first-aid Public: Smell, noise/ disturbance, no direct impact Environment: Release of unconfined with located impact Property: Loss between US\$100k and US\$1M

Table 5 - Consequence Range - Qualitative Criteria

### Some terms and concepts involved in safety systems

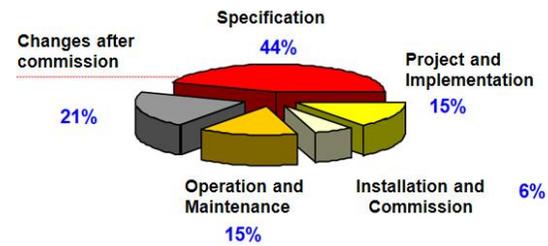
- Demand: Every condition or event generating requiring a safety system to operate

- PFD (Probability of Failure on Demand): Indicator of reliability appropriate for the safety systems.
- The MTBF is a basic measure of the reliability in repairable items of a piece of equipment. It may be expressed in hours or years. It is commonly used in systems reliability and sustainability analysis.
- MTBF: can be calculated by the following formula:
- $MTBF = MTTR + MTTF$   
Where:
- $MTTR = \text{Mean Time to Repair}$
- $MTTF = \text{Mean Time to Failure} = \text{the inverse of the sum of all failures rates}$
- $SFF = \text{Safe Failure Fraction}$ , is the fraction of all failure rates of a equipment resulting in a safe or unsafe failure, but duly diagnosed.

$$SFF = \frac{[\lambda^S + \lambda^{DD}]}{[\lambda^S + \lambda^{DD} + \lambda^{DU}]}$$

- Types of Failures analyzed in a FMDEA (Failure Modes, Effects, and Diagnostic Analysis):
  - 1) Dangerous Detected (DD): Detectable failure and may take to an error over 2% in the output.
  - 2) Dangerous Undetected (DU): Undetectable failure and may take to an error over 2% in the output.
  - 3) Safe Detected (SD): Detectable failure and does not affect the measured variable, but places the output current to a safe value and notifies the user
  - 4) Safe Undetected (SU): In this case, there is a problem with the equipment, but it is not possible to detect it, but the output operates with success within a limit of 2% of safety tolerance. If such safety tolerance is used as a project parameter, such type of failure may be ignored.
  - 5) Diagnostic Annunciation Failure (AU): a failure with no immediate impact, but that a second occurrence may place the equipment under a risk condition.
  - 6) The following failures may also be characterized:
    - Random failures: A spontaneous failure of a component (hardware). The random failures may be permanent (they exist until they are eliminated) or intermittent (occur under some circumstances and disappear in the following moment).
    - Systemic failures: A failure hidden within a project or assembling (hardware or typically software) or failures due to errors (including mistakes and omissions) in the safety activities cycle which cause the SIS to fail in some circumstances, under specific combinations of input or under a specific environmental condition.
    - Failure in a common mode: The result of a defect in common mode.
    - Defect in a common mode: A single cause may cause failures in several elements of the system. May be internal or external to the system.

## Curiosity



*"Out of Control: Why Control Systems go Wrong and How to Prevent Failure," U.K.: Sheffield, Heath and Safety Executive, 1995*

Figure 4 - Study on the causes of accidents involving control systems

## 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, Marcelo; 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