

The 'SIL Concept' in the process industry

International standards IEC 61508/ 61511

Chris M. Pietersen MSc
Safety Solutions Consultants BV (SSC)
Director
pietersen@safety-sc.com

11th Urea Symposium
19-22 May 2008, Noordwijk Netherlands

Introduction

The safety provisions of a process plant need to be related to the risk level. Until a few years ago, no adequate standard did exist for the determination of the necessity and assessment of the required reliability of the safety provisions. How safe is safe enough?

With the introduction of the IEC 61508 standard [1] and the related process industry related IEC 61511 standard [2] this gap has been filled. A risk based approach is given, resulting in a Safety Integrity level (SIL). The standards are prescribing the requirements for Safety Instrumented Systems, depending on the SIL level (1-4). These international standards also indicate the requirements for a management system to ensure that these are maintained through all lifecycle phases.

The IEC standards are increasingly used worldwide. All major companies are complying with this SIL concept. It means that the safety approach for the plant designs are fully in line with the international best practice based on the IEC 61508 standard.

The SIL concept has a number of important benefits for plant safety:

- A systematic, transparent and verifiable way of risk reduction to an acceptable level.
- An optimum cost benefit situation: 'fit-for-purpose' safety and minimum nuisance shut downs or disturbances in the plant.
- The design of Safety Instrumented Systems (SIS) is based on the SIL requirements. This includes redundancy requirements as well the test interval.
- A worldwide harmonised approach.

This paper describes the essence of the SIL approach and its benefits.

Two large accidents in 2005

The importance of the safety through a systematic approach of safety provisions can best be illustrated in showing accident causation processes of two recent large accidents in the process industry in which the lack of the implementation of the SIL concept have contributed to the causation of the accidents. Two accidents in 2005 are briefly described below. The direct cause of both accidents was overfilling of a vessel/ column with hazards, flammable/ explosive material. The resulting explosions and fires were devastating.

1. *Texas City (USA) Refinery Explosion, 23 March 2005*

Fifteen people died, more than 170 people were injured. This accident has been thoroughly investigated by different independent parties [3]. Safety management was not adequate, resulting (a.o) in an inadequate hazard identification (HAZOP) and insufficient safety instrumentation for overfill prevention.

2. *Buncefield Depot (UK), 11 December 2005*

Over 40 people were injured; fortunately there were no fatalities. A devastating explosion occurred and the resulting fire burned for several days, destroying most of the site. The investigations [4] showed that both the Tank level gauging system (monitoring the level) as well as the (automatic) overfill protection (switch) system failed.

The investigation of the accidents resulted in a number of important lessons about Safety management. In the framework of this paper: the reports show important evidence of the lack of implementation of the international IEC 61511 standard principles:

- Lack of systematic hazard identification resulting in a thorough overview of the need for safety instrumentation
- Lack of a proper assessment of the risk levels, resulting in the required SIL level for the automatic safety systems.
- Lack of proper implementation in the IEC described safety Management system. In particular: the lack of proper testing and maintenance as required for a certain SIL.

The impact in the industry of both accidents is large. It is noted that even more companies started to implement the IEC SIL principles as the way to deal with safety. Regulatory bodies also requires this increasingly.

The IEC 61508 standard

How safe is safe enough? How many protection systems of which type do you need and how reliable do they need to be? What is really determining the safety of the plant and how do we continuously, over all activities of the lifecycle act accordingly? This paper focuses at the integrated approach for lifecycle safety as introduced in the international standards in relation to Lifecycle Safety of process installations: IEC 61508 (overall) and the IEC 61511 (same principles for the process industries).

It describes the necessary reliability of Safety Instrumented Systems (SIS) in relation to the required risk reduction of the plant. It is clear that for that purpose you need to know:

- The risk of the plant
- The non- SIS related risk reduction (e.g. relief/check valves)
- The acceptable risk level
- The reliability of the safety system and its influence on the availability of the installation for production

The standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/ programmable electronic systems (E/E/PESs)) that are used to perform safety functions. In most situations, safety is achieved by a number of protective systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while the standard is mainly concerned with electrical/electronic/programmable electronic (E/E/PE) safety-related systems, it also provides a framework within which safety-related systems based on other technologies need to be considered. No further distinction is therefore being made below between the different technologies.

The IEC 61508 standard:

- *adopts a risk-based approach for the determination of the safety integrity level requirements. See figure 1 and 2.*
- *uses Safety Integrity Levels (SIL) for specifying the target level of safety integrity for the safety functions to be implemented by the safety-related systems. See figure 2.*
- *sets numerical target failure measures for safety-related systems which are linked to the safety integrity levels (see table 1).*

According to the IEC concept, all steps need to be verified, documented, auditable and embedded in a proper (safety) management system.

SIL Classification: Risk analysis/ reduction

The target levels for the safety integrity (probability of failure) of the safety instrumented systems are determined with a systematic risk analysis. The IEC standard covers personnel safety. However, the practice in the industry shows that also classification schemes are used for environmental risks and/or economic damage (see below). The necessary risk reduction is indicated in figure 2 in a general way.

Figure 2 presents the most frequently used risk analysis method, called the 'Riskgraph'. It leads to the required Safety Integrity Levels (SIL). These levels depend on the risk parameters indicated in the figure 2.

The risk graph requires as input:

- The frequency of occurrence of the accident scenario (without SIS); shown as W1, W2, and W3
- The potential extent of human injury in case the SIS fails on demand (shown as C- factor).

- Exposure duration in the hazard zone (shown as F-factor).
- Possibility to avoid the hazard (shown as the P factor).

The transparent, verifiable documented choices of the parameters above will lead to the numbers shown in the figure: SIL a, SIL 1-4, SIL b. The IEC 61508 standard only give requirements for SIL 1-4. SIL a (no specific requirements, can be implemented in the control system and SIL b (normally redesign is required) however are used in practice.

Economic SIL considerations

If the SIS fails on demand the following related costs can occur:

Process failure

- Lost production or "downtime"
- Additional emergency maintenance
- Replacement power
- Catastrophic failure
- Major damage to capital equipment which leads to major capital expense
- Injury to plant personnel

These costs need to be balanced against the lifecycle cost of a SIS:

Life cycle cost of a SIS consists of all the costs of owning and operating a safety instrumented system (SIS). Components of life cycle cost include:

Design, specification, and procurement

- * Installation
- * Training
- * Operation & maintenance

The economic SIL level shows that it will be economical to invest in the Life Cycle Cost of a SIS to reduce the frequency of the SIS failure.

SIL verification

Once the requirement of the SIL levels has been determined, the Safety Instrumented System (SIS) which will perform the safety function need to be designed accordingly. The system normally comprises of initiating devices (sensors, transmitters), a logic solver (trip amplifiers, safety interlocks, fail safe output) and final elements (e.g. valves).

Probabilistic requirements

The complete SIS need to comply with the requirements for the Probability of Failure on Demand (PFD) depending on the SIL, as shown in table 1 below.

In the IEC standard, different PFD assessment methods for assessing the SIL level of a certain SIS are described. Two of the more common techniques described are Reliability Block Diagrams and Markov models. The modelling needs failure rates of all components used in the SIS, test intervals, the percentage of diagnostic coverage, repair times etc.

Table 1 — Safety integrity levels (SIL)

Safety integrity level (SIL)	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Architectural requirements

Depending on the type of components used and the 'Safe Failure Fraction', components need redundancy. This is also described as Hardware Fault Tolerance (HWFT). For details, see [1] and [2].

Conclusions

- The international standards IEC 61508 and the related IEC 61511 are increasingly used worldwide as the 'best practice' for a systematic approach for design/ operation of Safety Instrumented Systems (SIS).
- Accident data shows the need for a systematic approach in design, operation and maintenance of Safety Instrumented systems. This approach is available with the IEC 61508/ 61511 standards. The use is increasingly stimulated by the regulators.
- The SIL concept provides a means of systematic risk reduction to a level that is acceptably low. It answers the question: how safe is safe enough in a transparent and verifiable way
- The target SIL sets design requirements for the SIS: probabilistic requirements (Probability of Failure on Demand) and architectural (redundancy) requirements.

Literature

[1] Functional safety of electrical/electronic/programmable electronic safety- related systems. IEC 61508; www.iec.ch

[2] Functional safety – Safety instrumented systems for the process industry sector – IEC 61511. www.iec.ch

[3] Investigation report Refinery Explosion and fire; U.S. Chemical Safety and Hazards Investigation Board, march 2007. www.csb.org

[4] <http://www.buncefieldinvestigation.gov.uk/index.htm>

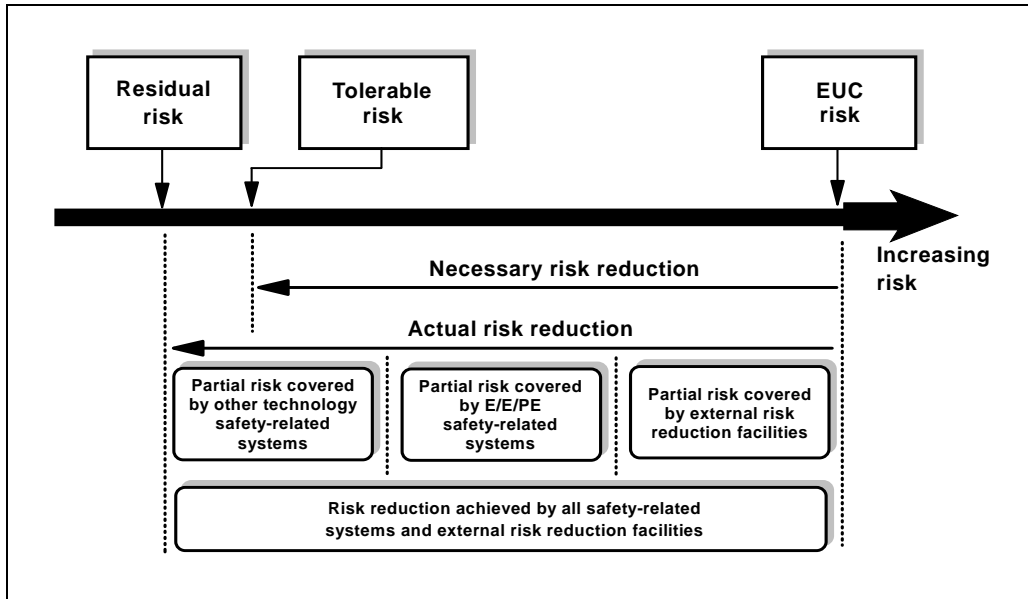


Figure 1 Risk Reduction requirements

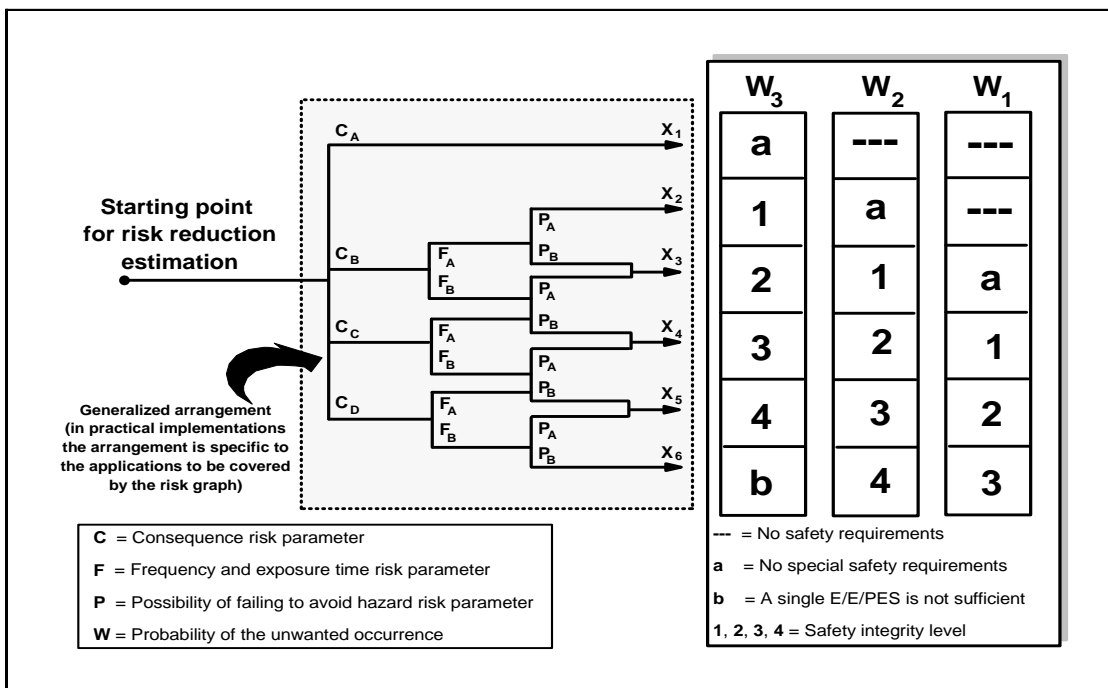


Figure 2 Determination of SIL levels