

# **An Introduction to Functional Safety and Safety Integrity Levels**

**By Sean Clarke, Principal Consultant, Exveritas Limited**

## **Introduction**

Whenever something is being built (be it equipment or plant) that may introduce a hazard to people, safety standards or even legislation will probably be involved!

If any reasonably foreseeable action or inaction leads to hazards with an intolerable risk arising from the equipment or plant, then safety functions are necessary to achieve or maintain a safe mode of operation. These safety functions are carried out by one or more safety-related systems.

Initially, significant consideration should be given to the elimination of the hazards. This could be, for example, by the application of inherent safety principles or the application of good engineering practice. It is likely however that in many cases this will not be possible (or cost will be prohibitive) and some residual risk will remain.

It is at this stage that we must analyse the risk and take appropriate action. One of the more common forms of appropriate action (and a defined and published methodology) is the application of functional safety and safety integrity levels.

## **Functional Safety**

There are two distinct aspects to functional safety, the 'safety function' requirement (what the safety function is) and 'safety integrity' requirement (the likelihood of the safety function performing correctly when called upon to do so).

The safety function requirements are derived from the 'hazard analyses' (i.e. Process Hazard Analysis, Failure Mode Analysis) and the safety integrity requirements are derived from a 'risk assessment' (i.e. Consequence Analysis). In order to ensure that safety is achieved, both hazard analysis and risk assessment is necessary.

The hazard analysis identifies the hazards associated with the process or operation, the risk assessment determines the performance requirements of the safety function. The aim is to ensure that the safety integrity of the safety function is sufficient to ensure the risk associated with this hazardous event is lowered to a level considered to be acceptable.

## **Example of functional safety**

To reinforce the definitions given, we will consider a machine tool, containing a guillotine blade, which is protected by a sliding guard to prevent access to the shearing element of the blade. The guillotine blade is accessed for routine maintenance by sliding the guard open. The guard is interlocked so that whenever it is opened an electrical circuit de-energises the machine tool. Therefore, the operation of the guillotine blade is stopped before the operator can access it and the possibility of shearing injury is prevented. In order to ensure that safety is achieved, both hazard analysis and risk assessment is necessary.

a) The hazard analysis identifies the hazard associated with the routine maintenance of the guillotine blade. For this machine tool it might show that it should not be possible to open the guard without the machine tool being de-energised. This describes the safety function.

b) The risk assessment determines the performance requirements of the safety function. The aim is to ensure that the safety integrity of the safety function is sufficient to ensure that no one is exposed to an unacceptable risk associated with this hazardous event.

The harm resulting from a failure of the safety function could be shearing amputation of parts of the operator’s limbs. The risk also depends on how frequently the guard has to be opened. The level of safety integrity required increases with the severity of injury and the frequency of exposure (how often the guard is opened) to the hazard.

### Safety Integrity Levels

Process and Machinery safety is often achieved by the use of Safety Instrumented Systems (SIS) to provide safe control functions for processes; this would include functions such as emergency shutdown, gas or fire detection, explosion mitigation and dangerous level/pressure control.

Safety Instrumented Systems are typically composed of some form of sensors (e.g. motion, pressure, temperature etc.), analyzers/processors (e.g. relay logic, PLC) and control elements (e.g. actuation, alarm). The integrity of each of these elements are collated to produce a ‘system’ safety integrity level, so the individual potential failure rate and mode of each part must be known to gauge the integrity of the system.

### Safety Integrity Level related to Probability of Failure on Demand (Figure 1)

SIL	PFD	Risk Reduction Factor (1/PFD)
4	$10^{-5}$ to $10^{-4}$	100,000 to 10,000
3	$10^{-4}$ to $10^{-3}$	10,000 to 1,000
2	$10^{-3}$ to $10^{-2}$	1,000 to 100
1	$10^{-2}$ to $10^{-1}$	100 to 10

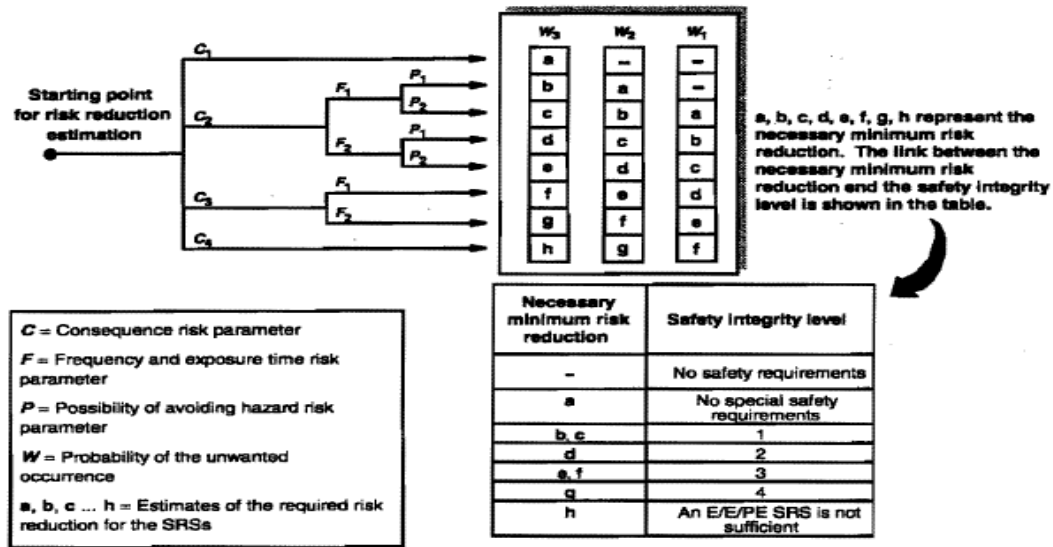
A Safety Integrity Level (SIL) is a simple numerical representation of the reliability of Safety Instrumented Systems (SIS) correlated to the probability of failure of demand (PFD), this is expressed as the unavailability of a system at the time of a defined unwanted event such as a process failure that could potentially injure people.

**Safety Integrity Level related to probable injury levels (figure 2)**

SIL	Qualitative Terms
4	Potential for fatalities in the community or large scale on site facilities
3	Potential for multiple fatalities
2	Potential for major on site injuries or single fatality
1	Potential for minor on site injuries

The level of SIL required for a system will be determined by analyzing the frequency of the event, the likelihood of detecting or avoiding the event and the consequence of the event. SIL therefore defines the level of protection required to lower the risk of an undesirable event to an acceptable level.

**Determining the SIL Level in accordance with IEC61508 (Figure 3)**



IEC 1 657/98

Although the table for determining SIL given in IEC 61508 (Figure 3) is relatively simplistic, the assignment of Target SILs must involve people with relevant expertise and experience in the systems, processes and hazards under consideration. IEC 61508 specifically states, "All persons involved in any overall safety life cycle activity, including management activities, should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform."

Appropriate Hazard Analysis tools should be used (e.g. HAZOP, Fault tree analysis) and as with all Hazard Analysis, all considerations and decisions should be documented. Once a

SIL is established (through the risk assessment and analysis process) the SIS design, operation and maintenance choices must then be conducted and checked against the target SIL Standards requirements.

One of the primary international standards for Safety Integrity is IEC 61508, 'Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.' IEC 61508 has defined four categories of safety referred to as SIL 1,2,3 and 4. (In North America under ANSI/ISA-S84.01 there are only three categories defined, SIL 1, 2 and 3). In simple terms, the higher the SIL is, the more reliable or effective the system is (and the more difficult it will be to achieve)

### **Applying the IEC 61508 series of Standards.**

The IEC 61508 series of Standards works under the common title of 'Functional safety of electrical/electronic/programmable electronic safety-related systems' and consists of the following parts;

- Part 0: Functional safety and IEC 61508
- Part 1: General requirements;
- Part 2: Requirements for E/E/PES 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;
- Part 7: Overview of measures and techniques.

There is a great deal of information contained within these standards (approaching 1000 pages) and it may seem a daunting task to approach and understand SIL via the Standards. It is recommended that if you are new to the Standards (and/or the subject of SIL) that you begin by reading the following sections.

<b>Technical Understanding</b>	<b>Managerial Understanding</b>
Annex A of IEC 61508-5, which covers risk concepts and safety integrity in a simplified form	Figure 2 and Table 1 of IEC 61508-1, which illustrate the overall safety lifecycle and list the objectives of each lifecycle phase. The lifecycle and phase objectives provide a key to understanding the requirements of Clause 7 of IEC 61508-1.
Annex A of IEC 61508-6, which gives an overview of the requirements in IEC 61508-2 and IEC 61508-3.	Clauses 6 and 8 of IEC 61508-1, which contain requirements relating to management of functional safety and functional safety assessment.
Figure 2 and Table 1 of IEC 61508-2 and Figure 3 and Table 1 of IEC 61508-3, which provide a key to understanding the requirements IEC 61508-2 and IEC 61508-3	

If you are about to undertake your first functional safety or SIL assessment, It is highly desirable to undertake training in this field and/or partner with a company that has experience in this area if you do not have experience in this area.

### **SIL and the Machinery Directive**

BS EN 62061 is a sector standard to the seven-part standard IEC 61508, 'Functional safety of electrical/electronic/programmable electronic safety-related systems', written specifically for the machinery sector. It takes a quantitative risk-based approach similar to that found in EN 61508, which requires rather more work than the qualitative 'risk graph' that was in the former Standard EN 954-1.

In addition to the management and documenting requirements, specific technical measures are required and described. There are requirements for the specification of Safety Related Control Functions (SRCFs), and the standard explains how the functional requirements specification and safety integrity requirements for each SRCF should be compiled to create a safety requirements specification (SRS). Three safety integrity levels (SIL 1, SIL 2 and SIL 3) are specified and they require that the probability of dangerous failures per hour (PFHd) must fall between certain target values as follows:

<b>SIL</b>	<b>probability of dangerous failures per hour</b>
SIL 1	$\geq 10^{-6}$ to $< 10^{-5}$ (or 1 failure in 100,000 h)
SIL 2	$\geq 10^{-7}$ to $< 10^{-6}$ (or 1 failure in 1,000,000 h)
SIL 3	$\geq 10^{-8}$ to $< 10^{-7}$ (or 1 failure in 10,000,000 h)

There are also specific requirements for the selection or design of the safety related electrical control system (SRECS) to meet the functional and safety integrity requirements specified in the safety requirements specification (SRS). Also covered is the identification of the Probability of Dangerous failures (PFHd), estimation of Safe Failure Fractions (SSF), Common Cause Failures (CCF) and diagnostic functions.

### **SIL and the ATEX Directive**

It should be noted that there are draft standards that align ATEX with the requirements of SIL. They will cover safety related devices (for ignition prevention) and will be applied by Notified Bodies under the ATEX Directive. Under DSEAR (ATEX 137) it should be noted that if any safety devices or systems that have been added to prevent the formation of an explosive atmosphere (ventilation, dilution, gas monitoring) or mitigation of an explosion will probably require a functional safety assessment.

## About ExVeritas

ExVeritas is owned and run by team of highly respected and experienced safety specialists. The owners have over 50 years experience in the field of safety, including owning an ATEX Notified Body, explosion research, accident investigation, safety system design consultancy, testing and explosion risk assessment.

Examples of the management teams experience include:

Consultancy on gas and dust explosion safety  
Risk Assessments and Mitigation,  
HAZOP/HAZID for fire/explosion and machinery/process safety,  
Design of explosion protection systems, safety systems and SIL.

**Free SIL Calculator – On-Line or Download at [www.exveritas.com](http://www.exveritas.com)**



The screenshot shows a web browser window titled "ExVeritas - SILCal - Windows Internet Explorer". The address bar displays "http://software.exveritas.com/SILCal/default.aspx". The page header features the "ExVeritas" logo on the left and "SILCal" on the right. The main content area is divided into two sections: "INPUT" and "OUTPUT".

**INPUT**

Description of Risk: Furnace 3 Gas Leak, Room 101

Consequence: Death to several people

Frequency and Exposure to Hazard: Rare to more often exposure to the hazardous zone

Possibility of Avoidance: Possible under certain conditions

Probability of Occurrence: Very slight probability and event frequency

**OUTPUT**

Safety Integrity Level: SIL 2

Produced By ExVeritas Limited Version 1.0.0

Internet | Protected Mode: Off 100%