



How to Determine the Safety Integrity Level (SIL) of a Safety System

Michel Spellemaeker, Fixed Products Director, Industrial Scientific Oldham, Z.I. Est - B.P. 417, 62027 Arras Cedex, France, Tel: +33 3 21 60 81 30, Fax: +33 3 21 60 80 00, Email: Lionel.Witrant@eu.indsci.com, Website: www.oldhamgas.com

Lionel Witrant, E.M.E.A Engineering Director, Industrial Scientific Oldham, Z.I. Est - B.P. 417, 62027 Arras Cedex, France Tel: +33 3 21 60 80 82, Fax: +33 3 21 60 80 07, Email: Michel.Spellemaeker@eu.indsci.com, Website: www.oldhamgas.com



The Challenge of Safety Systems

Electronic systems that carry out safety functions, such as gas detection systems, are becoming more complex, making it impossible in practice to determine every failure mode or improbable to test all possible behaviours. It is difficult to predict the safety performance, although testing is still essential because some dangerous failures can be only detected through periodic maintenance.

The challenge for system engineers is to design a system in such a way as to prevent dangerous failures or to control them when they arise.

For a Gas Detection System, dangerous failures may arise from any of the following:

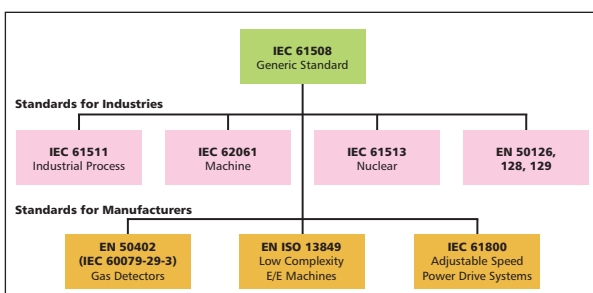
- Incorrect specifications of the system, including omissions in the safety requirement specifications (e.g. operation in unexpected poisoning gases, release of gases that cannot be detected, or lack of sensitivity to trigger the alarms)
- Random failures of hardware (reliability of electronic components) and systematic failures of hardware and software (e.g. wrong design, software bugs, etc.)
- Common root cause failures (power outage)
- Environmental influences (e.g. temperature, humidity, presence of interference gases, etc.)
- Human error

IEC 61508 contains requirements to minimize these failures in E/E/PE (electrical/ electronic/ programmable electronic) safety-related systems.

IEC 61508 – a Generic Standard

The IEC 61508 standard was published in 1998 and falls under a global approach of safety which could be compared with the ISO9001 system for quality or with the ISO14000 system for the environment.

The standard is generic in that it applies to the safety systems irrespective of their application. It provides a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants, medical or rail) or product standards (e.g. gas detection).



SIL – a Unit for Functional Safety

Functional safety is part of the overall safety that depends on a Safety Instrumented System (SIS), made up of equipment such as Fire & Gas Detection Systems that execute Safety Instrumented Functions (SIF). A safety function is designed to ensure or maintain a safety state of the SIS when a dangerous event occurs.

Each safety function has a safety integrity level (SIL). The safety integrity level is the probability for the system to execute the safety functions required in all specified input conditions within a specified time interval.

The 61508 standard details the requirements necessary to achieve each safety integrity level.

Obtaining the Safety Integrity Level (SIL) is done by:

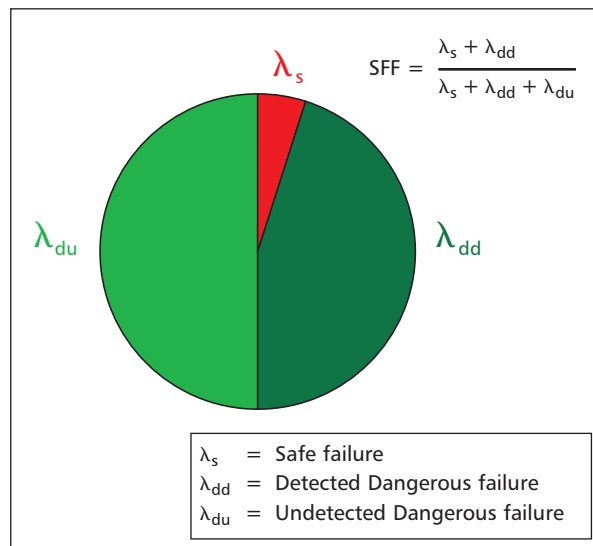
- Guaranteeing the integrity of the cycle of development of the system in the fields of specification, design and testing, with the goal of avoiding and eliminating systematic failures.
- Guaranteeing the robustness of the design by measurements allowing the systematic fault tolerances (diagnostics, access control, environment, etc.).
- Respecting the constraints on the equipment architecture for the rate of diagnostic coverage to determine the Safe Failure Fraction (SFF).
- By guaranteeing a probability of failures on demand (PFD), as a function of the failure rate and the test interval, or as failure rate per hour (PFH).
- If software is included, by guaranteeing the integrity and robustness of the design concerning only systematic failures.

SFF – Safe Failure Fraction

The Safe Failure Fraction, as mentioned previously, is one parameter that is necessary to assess the SIL capability of SIF functions.

The SFF is the percentage of safe failures, e.g. those that are safe or detected.

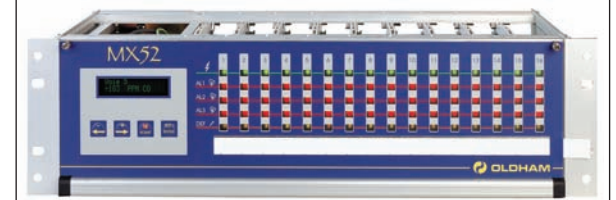
The calculation is based on the architecture of each Safety Instrumented Function and on a functional analysis by carrying out a FEMDA, Failure Mode Effect and Diagnostic Analysis.



Example: SFF of 94% means that 6% of the failures are dangerous and undetected

The following table taken from IEC 61508-1 gives the SIL levels, in relation to the Safe Failure Fraction (SFF) and the tolerance for hardware fault.

SFF Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% - ≤ 90%	SIL 1	SIL 2	SIL 3
90% - ≤ 99%	SIL 2*	SIL 3†	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4



*Industrial Scientific - Oldham control unit MX52 SIL2



† Industrial Scientific - Oldham control unit MX62 SIL3, full redundant system with double processors

Example: To be SIL2, a simple non-redundant control unit that will not ensure the safety function in the event of 1 hardware fault, must have a Safe Failure Fraction between 90% and 99% (i.e. the percentage of undetected dangerous failures shall not be greater than 10 %).

Probability of Failures on Demand (PFD) & Probability of Failures per Hour (PFH)

The qualitative parameter SFF is not enough. As such undetected dangerous failures exist, their probability to occur during the testing interval should be determined.

IEC 61508 describes two modes of operation for a safety function: 1) low demand mode of operation and, 2) high demand or continuous mode of operation. A safety function operating in demand mode is only performed when required (i.e. on demand) in order to transfer the Equipment Under Control (EUC) into a specified state. The safety-related system that performs the safety function has no influence on the EUC until there is a demand for the safety function to be performed. This type of system can be as simplistic as a gas detection system in a boiler room that cuts the gas supply in the event of gas leakage.

A safety function operating in continuous mode operates to retain the EUC within its normal safe state. That is, the safety-related system continuously controls the EUC, and a dangerous failure of the safety-related equipment will lead to a hazard. A simple example is a gas concentration measurement by gas detector system associated with control ventilation and heating to regulate the concentration of gas in a tank.

Depending of the timing between the demand and the test proof, IEC 61508 defines:

- Low demand mode is where the frequency of demand for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
- High demand or continuous mode is where the frequency of demand for operation made on a safety-related system is greater than once per year or greater than twice the proof test frequency. In the context of this definition, continuous is regarded as very high demand.

In relation with these two modes of operation, IEC 61508 relates the safety integrity level of a safety function to:

- The PFD, the average Probability of Failure to perform its design function on Demand, in the case of low demand mode or,
- The PFH, the Probability of a dangerous Failure per Hour, in the case of high demand or continuous mode. The probability of a dangerous failure per hour is sometimes referred to as the dangerous failure rate (i.e. dangerous failures per hour).

SIL	PFD: Low Demand Mode (<1 year and <2 demands between each test/maintenance)	PFH: High Demand or Continuous Mode (>1 year or ≥ 2 demands between each test/maintenance)	Risk Reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	10000-100000
3	$\geq 10^{-4}$ to $< 10^{-3**}$	$\geq 10^{-8}$ to $< 10^{-7}$	1000-10000
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	100-1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	10-100

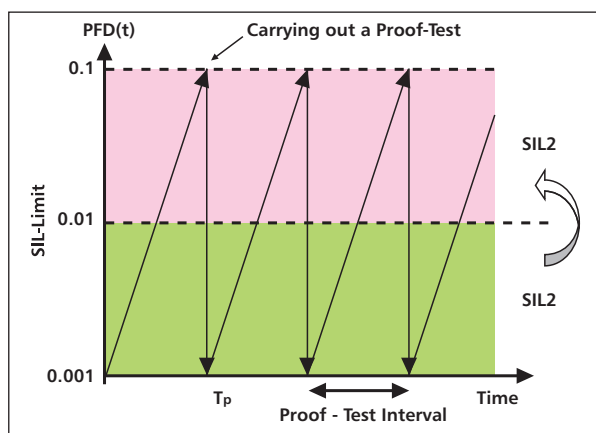


**Industrial Scientific Oldham control unit MX62
SIL3: PFD = 4.3710^{-4}

SIL and Field Test Interval

There is a link between the safety integrity and the test done in the field to verify that the safety function operates as intended. Over time components drift and the probability to have failures increases. To keep the SIL level at the initial value, it is mandatory to perform a proof test to check the availability of the safety function. For example, detectors based on chemical sensors which may have reduced sensitivity to gas due to environmental conditions will need to be tested periodically. The following figure shows that the probability of failure PFD increases versus time, leading to reduction of the SIL level, from SIL2 to SIL 1 in this example. Carrying out a proof test leads to return to the normal situation.

There is a link between the average PFD, λ_{du} the probability of failures per hour PFH, the test interval T_p and the mean time to repair.



For a simple safety system -

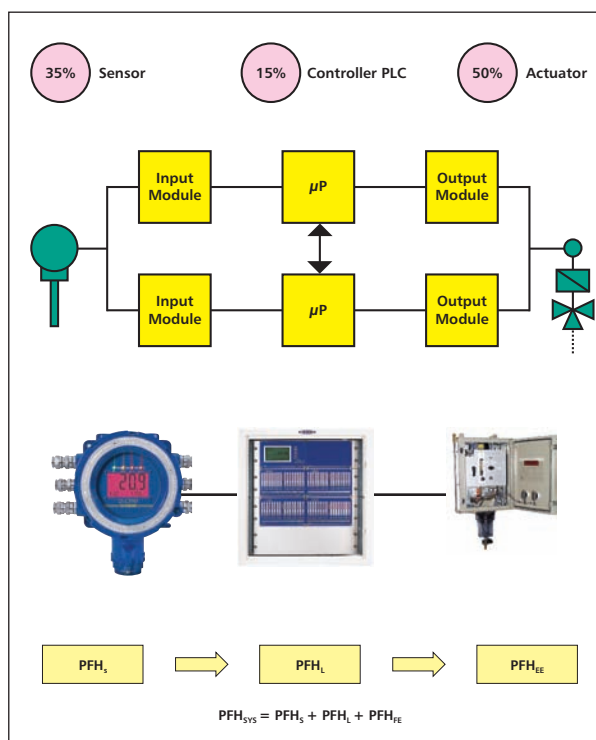
$$PFD_{AV} = \frac{1}{2} \lambda_{du} \cdot (T_p + MTTR)$$

This means that statistically, a dangerous failure will remain undetected during half of the proof test interval T_p .

SIL Capability and Safety System

Each component of a Safety Instrumented System involved in the safety function has a SIL level. The overall SIL of a safety function is determined by calculation based on the failure rate probability of each component. Each component contributes its part to the final SIL level. The weakest link of the chain reflects the maximum achievable SIL level. It is useless to request a SIL3 controller if the sensor is only SIL1 and the actuator has no SIL capability.

The figure below shows that the weakest component is often the actuator.



The New Standard for Gas Detection: EN 50402 / IEC 60079-29-3 (draft)

The 61508 standard is a generic standard for Electronic Devices. It has generic requirements and not dedicated requirements for gas detectors which comprise electronic

components like chemical, electro-optical sensitive elements with special modes of failures that cannot be found in books.

This gap has been the reason for gas detection experts to work on a product standard in the frame of the CENELEC committee. The result of this collaborative effort is the standard EN50402, voted by CENELEC country members in June 2005. The title of EN5042 is, "Requirements on the functional safety of fixed gas detection systems for the detection and measurement of combustible or toxic gases or vapours or of oxygen." This standard includes the main requirements of IEC 61508 and defined specific requirements for each sub-component of the safety chain, including diffusion mode, sampling system, sensor, signals transmission, central processing unit, and outputs such as relays.

EN50402 has been the base of international standardization work for gas detector functional safety and is currently on draft at the IEC level, under IEC 60079-29-3. Many of Industrial Scientific-Oldham products have been evaluated according to EN50402, such as the SIL3 MX62 control unit and sensors series OLC 20/40/50 (certificate INERIS 01ATEX0004/0006/0027X).

Do SIL Levels Solve All Safety Issues?

Using products proven for use in SIL 3 systems is not the magic key to a safer facility. Consideration must be taken for the overall system (gas detectors, controllers and actuators). SIL 3 certificates alone do not allow one to determine whether that the overall system will meet the desired level of risk reduction because a chain is only as strong as its weakest link.

Other factors to keep in mind are maintenance routines. When your Safety Instrumented System is SIL approved, you have to maintain this system in order to keep it at this level. That is the reason why it is so important to ask for the average, the SFF and the maintenance interval.

The number of detectors and their placement is probably more important than the safety-related function itself. The impact of field devices (sensors and final elements) typically has a dominating impact on safety instrumented system performance. Detector coverage has a major influence on fire and gas system performance and may prevent most systems from meeting SIL 1 performance levels if sensors are not placed in areas that will detect a hazardous leak. Remember, if the detector doesn't see gas, it does not respond. Placing sensors in areas that are potential release points is good practice. Once the detector coverage is better understood and addressed, then focusing on the SIL rating of the hardware will be more meaningful.

Sources:

This text contains extracts from the IEC Functional Safety Zone (<http://www.iec.ch/functionalsafety>).

All such extracts are copyright of International Electrotechnical Commission® 2005, IEC, Geneva, Switzerland. All rights reserved.

- Article from Paul Gruhn, ICS Triplex: "SIL Ratings for Fire & Gas system hardware"
- ISA Guide



Reliable Respiratory Protection Upon Demand

Respiratory protection is essential for the long term preservation of good health for employees working within industrial environments, where hazardous substances pose a threat. Health complaints can result from exposure to contaminants such as toxic gases, dusts, spores, fumes and mists, often resulting in lack of oxygen and contributing to possible fatalities.

Whilst the Health and Safety at Work Act, COSHH and other recognised international regulations have raised awareness of these dangers and successfully promoted employers to take measures for their employees, there are still many instances in which the necessity for self contained breathing apparatus is overlooked.

Where, for maintenance reasons, workers are required to perform tasks for which they are exposed to contaminants for only short duration's the risk may appear insignificant and the use of breathing apparatus unnecessary. Continuous or regular performance within these conditions, without protection, will pose a serious health risk.

Much self-contained breathing apparatus is purchased for only occasional use. A good example of this is the need for the merchant marine to carry self-contained breathing apparatus on many classes of vessel; other than for training the hope is that this apparatus will never be used.

The specifications for compliance breathing apparatus are often different from those for the professional user who may well use the SCBA on a very regular basis. Recognising this difference, Scott Health and Safety (UK) offer Sigma II, a positive pressure self-contained breathing apparatus, specifically targeted at the marine and compliance industrial markets. "Traditionally SCBA for the compliance market has simply been manufactured to a price," said Tony Picket, Product Manager for Scott Breathing Apparatus, "but in Sigma II, we have not compromised the level of performance in order to achieve a cost effective price." Sigma II is a high performance self contained breathing apparatus, which is easy to operate with low through life costs and is ideally suited for shipboard fire fighting and confined space working. It features a lightweight, ergonomically shaped backplate for optimised load distribution to maximise wearer comfort, plus an instant positive pressure demand valve which is very simple to operate and provides the user with maximum protection. Sigma II accepts a wide range of 200/300 bar cylinders.