	Technical Note	20/04/2010
	IEC61508 and SIL Document Reference: GEN010	

IEC61508 and Safety Integrity Level (SIL)

Safety instrumented systems (SIS) are used to provide safe control functions for processes, e.g. emergency shutdown (ESD), and gas and fire detection alarm systems. SIS typically are composed of sensors, logic solvers and final control elements. Due to the critical nature of such systems, many process industries recognize compliance with international standards from the International Electrotechnical Commission (IEC) as good engineering practice for safety instrumented systems.

The international standard IEC 61508 "Functional Safety of electrical/electronic/ programmable electronic safety-related systems" defines four safety integrity levels (SIL). They are defined as the measure for the safety performance of electrical or electronic control equipment. The safety integrity level (SIL) defines the level of safety performance of a critical control system. SILs are ranked Levels 1-4, with a higher level indicating greater safety performance. Typically, higher SILs are achieved with more redundancy, more frequent testing, and diagnostics.

Safety Integrity Level (SIL)	Impact of the SIS Failure on plant personnel , public or community	TUV Class- Possible comparison
1.	Minor property and production protection.	AK2 or AK3
2.	Major property and production protection. Possible employee injury.	AK4
3.	Employee and community protection.	AK5 or AK6
4.	Catastrophic community impact.	AK7

In *quantitative* terms SILs are defined as:


Safety Integrity Level (SIL)	Availability	Risk of Failure
1.	0.9 to 0.99 or 90%-99%	10%
2.	0.99 to 0.999 or 99%-99.90%	1%
3.	0.999 to 0.9999 or 99.90%-99.99%	0.1%
4.	0.9999 to 0.99999 or >99.99%	0.01%

Typically, gas detection systems are required to be validated to SIL 1, SIL 2 or SIL 3 depending on application. Consider the installation of a SIL 3 SIS for a high level alarm and plant shutdown in a Petrochemical plant. The acceptance of a SIL 3 SIS means that the level of hazard or economic risk is sufficiently high that a SIS with a 0.1% chance of failure (99.90% availability) is acceptable. The availability or chance of failure of 99.90% of the control system would mean that out of every 1000 times that there is a high level alarm there would be a one predicted failure of the SIS and subsequent plant shutdown.

Some common terms relating to IEC61508 and system reliability:

- SIS: Safety Instrumented System
- SRS: Safety Related System
- E/E/PES: Electrical/Electronic/Programmable Electronic System
- PFD: Probability of Failure on Demand
- SFF: Safe Failure Fraction
- MTBF: Mean Time Between Failure
- FMEA: Failure Mode Effect Analysis

Parameters such as PFD, SFF and MTBF will usually be stated on the IEC61508 Declaration for each product. This data is used by the engineer compiling the system to assess the overall SIL rating.

	Technical Note	20/04/2010
	IEC61508 and SIL Document Reference: GEN010	

Note: it is important to understand that IEC61508 applies to the complete system (ie all components that are utilised to perform the safety function: inputs and outputs). As gas detection systems usually only form part of the safety system (provision of shut-down devices, valves etc is usually by others), gas detectors and control panels can only be termed 'compliant with the requirements of IEC61508', or 'validated to SIL2' etc. Individual products cannot be 'certified' to IEC61508 as they cannot perform the complete safety function in isolation. It is for the engineer compiling the system to select components that are validated to a sufficient 'SIL' level to achieve the overall required level for the plant.

Technischer Überwachungs- Verein Rheinland (TUV)

TUV is a third party agency that certifies safety instrumented systems (SIS). If the product is tested and meets the strict technical and performance requirements, it is approved and certified for Classes (AK) 1-8. There is no direct conversion between the AK requirement classes and SIL levels, but for example in a typical application AK 5 and AK 6 might correspond to SIL 3 depending on the quantitative assessment.

Note: the proliferation of IEC61508 in the marketplace is driven by customer demand rather than legislation. Equipment manufacturers can opt for self-certification (supported by a full product assessment and report), or contract 3rd-party agencies such as Technis or TUV (see below) for assess products on their behalf. Whether self-certification is accepted depends on the individual customer; TUV assessment carries a lot of weight, but less well known bodies such as Technis offer rigorous assessment supported by comprehensive documentation.

Related Standards

IEC 61508- "Functional safety of electrical/ electronic/ programmable electronic safety-related systems".

This 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. This unified approach has been adopted in order that a rational and consistent technical policy is developed for all electrically-based safety-related systems. A major objective is to facilitate the development of application Sector standards.


IEC 61511- "Functional safety- Safety instrumented systems for the process industry sector".

This international standard addresses the application of safety instrumented systems for the process industries. The safety instrumented system includes sensors, logic solvers and final elements. The safety instrumented system logic solvers addressed include programmable electronic safety-related technology (PES) amongst others. Where other technologies are used for logic solvers, the basic principles of this standard shall be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This standard is process industry specific within the framework of the IEC 61508. It comprises:

- Part 1: Framework, definitions, system, hardware and software requirements
- Part 2: Guidelines for the application of IEC 61511-1
- Part 3: Guidance for the determination of the required safety integrity levels

EN 50402- "Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen. Requirements on the functional safety of fixed gas detection systems".

This standard considers the safe and reliable integration of gas detection systems. It defines frameworks to ensure that the Safety Integrity Levels of the different combination of parts of the gas detection system comply with the reliability of other systems already installed in the plant. The standard illustrates the functional parts as being the outputs and inputs from/to the controls units, including the detectors, signal transmission and gas sampling.

	Technical Note	20/04/2010
	IEC61508 and SIL Document Reference: GEN010	

IEC 60079-29-3- "Explosive atmospheres - Part 29-3: Gas detectors- Requirements on the functional safety of fixed gas detection systems".

Forecast for publication in 2011, this standard is currently under development.

System Redundancy

System redundancy provides a safeguard so that if a component fails, services are retained or can be restored in the shortest time possible. Redundancy is commonly required in environments such as petrochemical plants or off-shore platforms where system failures can lead to severe risks. Redundancy is achieved by having more than one vital component in the system such as gas detectors or controllers. In these situations the system may be termed as dual or even triple redundant. If a main part of the system fails the redundant components come into operation to maintain system integrity. This technique is often used to increase the 'SIL' rating of a safety system.

IEC61508 SIL Compliant Crowcon Products

Crowcon products validated to IEC61508 (validation by Technis; declaration certificates available on request):

Gasmaster: SIL 2

Gasmonitor: SIL 2

Vortex SIL 1

Nimbus: SIL 2

Xgard Type 1 (toxic): SIL 2

Xgard Type 1 (oxygen): SIL 3

Xgard Type 1 (toxic; biased – NO, HCL, ETO, VO): SIL 1

Xgard Type 2 (toxic): SIL 2

Xgard Type 2 (oxygen): SIL 3

Xgard Type 3: SIL 1

Xgard Type 4: SIL 1

Xgard Type 5: SIL 1

Xgard Type 6: SIL 3

Xgard IR: SIL 2

IREX: SIL 2

IRmax: SIL 2