PROCESS INSTRUMENT SOLUTIONS

SAFETY INTEGRITY LEVEL

WHAT IS IT?

Safety integrity level (SIL) is defined as a relative levels of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF).

The requirements for a given SIL are not consistent among all of the functional safety standards. In the functional safety standards based on the IEC 61508 standard, four SILs are defined, with SIL 4 the most dependable and SIL 1 the least. The applicable SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

ASSIGNMENT

Assignment of SIL is an exercise in risk analysis where the risk associated with a specific hazard, that is intended to be protected against by a SIF, is calculated without the beneficial risk reduction effect of the SIF. That unmitigated risk is then compared against a tolerable risk target. The difference between the unmitigated risk and the tolerable risk, if the unmitigated risk is higher than tolerable, must be addressed through risk reduction of the SIF. This amount of required risk reduction is correlated with the SIL target. In essence, each order of magnitude of risk reduction that is required correlates with an increase in one of the required SIL numbers.

There are several methods used to assign a SIL. These are normally used in combination, and may include:
- Risk matrices
- Risk graphs
- Layers of protection analysis (LOPA)

Of the methods presented above, LOPA is by far the most commonly used by large industrial facilities.

The assignment may be tested using both pragmatic and controllability approaches, applying guidance on SIL assignment published by the UK HSE.[1] SIL assignment processes that use the HSE guidance to ratify assignments developed from Risk Matrices have been certified to meet IEC EN 61508.

PROBLEMS

There are several problems inherent in the use of safety integrity levels. These can be summarized as follows:

- Poor harmonization of definition across the different standards bodies which utilize SIL
- Process-oriented metrics for derivation of SIL
- Estimation of SIL based on reliability estimates
- System complexity, particularly in software systems, making SIL estimation difficult to impossible

These lead to such erroneous statements as, “This system is a SIL N system because the process adopted during its development was the standard process for the development of a SIL N system”, or use of the SIL concept out of context such as, “This is a SIL 3 heat exchanger” or “This software is SIL 2”. According to IEC 61508, the SIL concept must be related to the dangerous failure rate of a system, not just its failure rate or the failure rate of a component part, such as the software. Definition of the dangerous failure modes by safety analysis is intrinsic to the proper determination of the failure rate.[2]

SIL is for electrical controls only and does not relate directly to the caT architecture in IEC/EN 62061. It appears to be a precursor to PL ratings that are now the new requirements which encompass hydraulic and pneumatic valves.

CERTIFICATION

The International Electrotechnical Commission's (IEC) standard IEC 61508 defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL.

The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. In order to achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum safe failure fraction. The concept of 'dangerous failure' must be rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development. The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used.

PFD (probability of dangerous failure on demand) and RRF (risk reduction factor) of low demand operation for different SILs as defined in IEC EN 61508 are as follows:

SIL	PFD	PFD (power)	RRF
1	0.1–0.01	10–1 – 10–2	10–100
2	0.01–0.001	10–2 – 10–3	100–1000
3	0.001–0.0001	10–3 – 10–4	1000–10,000
4	0.0001–0.00001	10–4 – 10–5	10,000–100,000

For continuous operation, these change to the following. (Probability of dangerous failure per hour)

SIL	PFD	PFD (power)	RRF
1	0.00001-0.000001	10–5 – 10–6	100,000–1,000,000
2	0.000001-0.0000001	10–6 – 10–7	1,000,000–10,000,000
3	0.0000001-0.00000001	10–7 – 10–8	10,000,000–100,000,000
4	0.00000001-0.000000001	10–8 – 10–9	100,000,000–1,000,000,000

Hazards of a control system must be identified then analysed through risk analysis. Mitigation of these risks continues until their overall contribution to the hazard are considered acceptable. The tolerable level of these risks is specified as a safety requirement in the form of a target 'probability of a dangerous failure' in a given period of time, stated as a discrete SIL.

Certification schemes are used to establish whether a device meets a particular SIL.[3] The requirements of these schemes can be met either by establishing a rigorous development process, or by establishing that the device has sufficient operating history to argue that it has been proven in use.

Electric and electronic devices can be certified for use in functional safety applications according to IEC 61508, providing application developers show the evidence required to demonstrate that the application including the device is also compliant. IEC 61511 is an application-specific adaptation of IEC 61508 for the Process Industry sector. This standard is used in the petrochemical and hazardous chemical industries, among others.

SAFETY STANDARDS

The following standards use SIL as a measure of reliability and/or risk reduction.

- ANSI/ISA S84 (Functional safety of safety instrumented systems for the process industry sector)
- IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety related systems)
- IEC 61511 (Safety instrumented systems for the process industry sector)
- IEC 61513 (nuclear industry)
- IEC 62061 (safety of machinery)
- EN 50128 (railway applications – software for railway control and protection)
- EN 50129 (railway applications – safety related electronic systems for signalling)
- EN 50402 (fixed gas-detection systems)
- ISO 26262 (automotive industry)
- MISRA, various (guidelines for safety analysis, modelling, and programming in automotive applications)
- Defence Standard 00-56 Issue 2 – accident consequence

The use of a SIL in specific safety standards may apply different number sequences or definitions to those in IEC EN 61508.[2]

[1] M. Charlwood, S Turner and N. Worsell, UK Health and Safety Executive Research Report 216, “A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines”, 2004. ISBN 0-7176-2832-9. [2] Redmill, Felix (2000). “Understanding the Use, Misuse, and Abuse of Safety Integrity Levels” (PDF). Retrieved 16 February 2017.