

SAFETY INTEGRITY LEVEL (SIL) - IEC 61508/61511

Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In (somewhat) simple terms, SIL is a measurement of performance or probability of failure on demand (PFD) required for a Safety Instrumented Function (SIF) within a Safety Instrumented System (SIS) based on the ANSI/ISA 84, IEC 61508, and IEC 61511 standards.

All organisational and technical risk reduction measures act as a counterweight to the risk potential. The values SIL 1 to SIL 4 (SIL = Safety Integrity Level) are derived from the risk analysis. The greater the risk, the more reliable risk reduction measures must be implemented and, consequently, the greater the reliability the components used must exhibit. Typically, as the SIL level increases, the cost and complexity of the hardware/system also increase. The four SIL levels are defined, with SIL4 being the most dependable and SIL1 being the least. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management. The requirements for a given SIL are not consistent among all of the functional safety standards.

SIL Determination

The determination of the safety integrity level (SIL) for each Safety Instrumented Function (SIF) in a Safety Instrumented System (SIS) is dependent on the following factors:

1. The Corporate Standard for the tolerable risk after applying all the layers of protection. This tolerable risk may be a function of the cost of reducing the residual risk. The IEC 61508-5 Standard – Example of methods for the determination of safety integrity levels, discusses the general concept of risk and safety integrity in Annex A and the concepts of ALARP and tolerable risk in Annex B of the Standard outline.
2. The overall risk from the unprotected hazards that can occur. The Layers of Protection Analysis (LOPA) provides a methodology for determining the overall risk from data determined in a Hazard and Risk Analysis (HAZOP). The LOPA methodology is discussed in Answer #C of the Standard outline.
3. The risk reduction provided by all of the non-SIS protection layers. LOPA also provides a methodology for analyzing the risk reduction from various non-SIS protection layers.

The residual risk remaining can be computed from the unprotected risk and the risk reduction provided by the non-SIS protection layers. If the residual risk is greater than the tolerable risk, a SIS is required to provide the final required risk reduction. The average probability of failure on demand of each safety instrumented protection function, PFD_{avg} , is equal to the necessary risk reduction the protection function must provide. The necessary risk reduction is computed by dividing the tolerable risk by the residual risk remaining before the application of the safety instrumented function. The SIL for each safety function can be determined from Table 2 in IEC 61508-1 by use of the required PFD_{avg} . Annex C in IEC 61508-5 discusses this method of determining the required safety integrity level and includes example calculations.

Annexes D and E in IEC 61508-5 describe two qualitative methods for determining the SIL. Annex D outlines the risk graph method, and Annex E describes a hazardous event severity matrix method. It should be noted that the PFD_{avg} and the corresponding SIL must be computed for all safety functions required within the Safety Instrumented System.

con't...

SIS Selection

The user should determine the appropriate safety standard to be used to develop their guidelines. The IEC 61511 standard requires all components and subsystems necessary to achieve a safety instrumented function to be designed in accordance with IEC 61508 or to meet the requirements for a component to be proven-in-use. Clause 11.5.3 in the IEC 61511-1 specifies the requirements for proven-in-use. Clause 11.5.3 requires many years of operational experience with a component or device, so the random hardware failure rates can be determined to a single sided lower confidence limit of at least 70%. Most users will probably purchase logic solvers from manufacturers that have developed logic solvers designed in accordance with IEC 61508 and certified by an independent certification body like TÜV.

The guidelines for selection of the logic solver required to implement a complete SIS that performs many safety instrumented functions should consider the following factors:

1. The IEC 61511 standard requires manufacturers and suppliers of devices for safety instrumented systems to conform to the IEC 61508 standard. Hence the manufacturer of the logic solver should follow the IEC 61508 standard.
2. The logic solver portion of the SIS should be suitable for implementing the SIF requiring the highest SIL.
3. The logic solver manufacturer should provide a safety manual that details all restrictions and operating requirements for the logic solver and its associated tools that are appropriate for the SIL required. The IEC 61511 standard requires a safety manual for the logic solver.
4. If the user or the user's system integrator selects a logic solver that was not designed in accordance with IEC 61508, the logic solver must meet the requirements for proven-in-use.
5. The hardware fault tolerance requirements in Clause 11.4 in IEC 61511-1 must be followed when selecting the logic solver.
6. The spurious trip rate of the logic solver, $MTTF_{spurious}$, should also be considered since a spurious trip can disrupt production and result in significant lost production costs.

Since very few sensors and final elements have been designed to be in accordance with IEC 61508, most users will be required to select sensors and final elements that have been proven-in-use.

The guidelines for selection of the sensors and final elements required to implement safety instrumented functions should consider the following factors:

1. The sensor and final element process interfaces should be included when determining the failure rates and failure modes of the subsystem.
2. The sensor and final element subsystem redundancy required to implement the various safety instrumented functions should be determined by calculation of the PFD_{avg} for each subsystem.
3. The sensor and final element hardware common cause should be included in the calculation of PFD_{avg} .
4. The hardware fault tolerance requirements in Clause 11.4 in IEC 61511-1 must be followed when selecting the sensor and final element redundancy.

con't...

IEC 61508 and IEC 61511

The international 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. To achieve a given SIL, the device must have less than the specified probability of dangerous failure and have greater than the specified safe failure fraction. These failure probabilities are calculated by performing a Failure Modes and Effects Analysis (FMEA). 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 Failure on Demand) and RRF (Risk Reduction Factor) for SIL Levels as defined in IEC61508 are as follows:

SIL Level	PFD	RRF
1	0.1-0.01	10-100
2	0.01-0.001	100-1000
3	0.001-0.0001	1000-10,000
4	0.0001-0.00001	10,000-100,000

The SIL requirements for systematic safety integrity define a set of techniques and measures required to prevent systematic failures (bugs) from being designed into the device or system. These requirements can either be met 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 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.

Useful Links

IEC Functional safety zone -- <http://www.iec.ch/functionalsafety>

Functional Safety and IEC 61508: A basic guide -- http://www.iec.ch/zone/fsafety/pdf_safe/hld.pdf

Safety Users Group - Functional Safety-Information Resources -- <http://www.safetyusersgroup.com>

Inside Functional Safety - Technical magazine focusing on functional safety -- <http://www.insidefunctionalsafety.com>

61508.org The 61508 Association -- <http://www.61508.org>
