SIL and functional safety in rotating equipment

Unravelling the terminology and meaning of safety integrity level and functional safety in rotating equipment

Oliver Franz
Prognost Systems

SIL (safety integrity level) is a very important safety indicator that has been extensively discussed, described and often misunderstood within the industry over the past years. The purpose of this article is to provide operators, reliability engineers, instrumentation engineers and department managers with a practical overview of the areas where SIL and functional safety are important in their daily business life. Note that, in the light of the International Electrotechnical Commission (IEC) and most other safety relevant standards, risk is strictly defined as "harm to health safety environment" (HSE).

Potential economic losses resulting from process downtime are often one of the justifications for the realisation of process improvements. However, there are concerns in the industry that the implementation of additional and SIL certified machinery protection may add to the nuisance trip rate. This is discussed at the end of this article.

Most safety responsible staff members have gone through a HAZOP (hazard and operability study), evaluating imposed process weaknesses, potential risks and even working out ways to improve process safety. This very systematic approach has brought huge improvements to process industry safety and is still one of the key tools. It involves going through a process, step by step, looking left and right at what can go wrong under certain, even rare, circumstances. However, accidents are not entirely avoidable and in all cases some kind of risk remains and severe accidents still do happen. This is where IEC 61511, initially released in 1998, steps in with yet another systematic evaluation based on those imposed risks found out through the HAZOP.

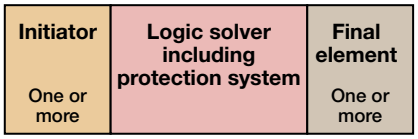

Figure 1 Safety instrumented system

IEC 61511 offers guidance to the process equipment operator, defining the SIL requirements necessary to be met by the machinery protection system of choice (also often called a safety instrumented system, or SIS, see **Figure 1**). It is important to note that the end user/operator is finally responsible for this evaluation as well as for the reduction of the remaining process risks to an acceptable damage level (HSE related). IEC 61511 requirements are mandatory and to be followed by operators. In the US, ANSI/ISA84.00.01-2004 was issued in September 2004 and it primarily mirrors IEC 61511. The European standards body CENELEC has adopted the standard as EN 61511 (see **Figure 2**).

LOPA, risk graph and risk assessments

Commonly, detailed risk assessments applying IEC 61511 criteria on the process hazard analysis (PHA) results are performed by expert consulting companies. An often seen approach is called layers

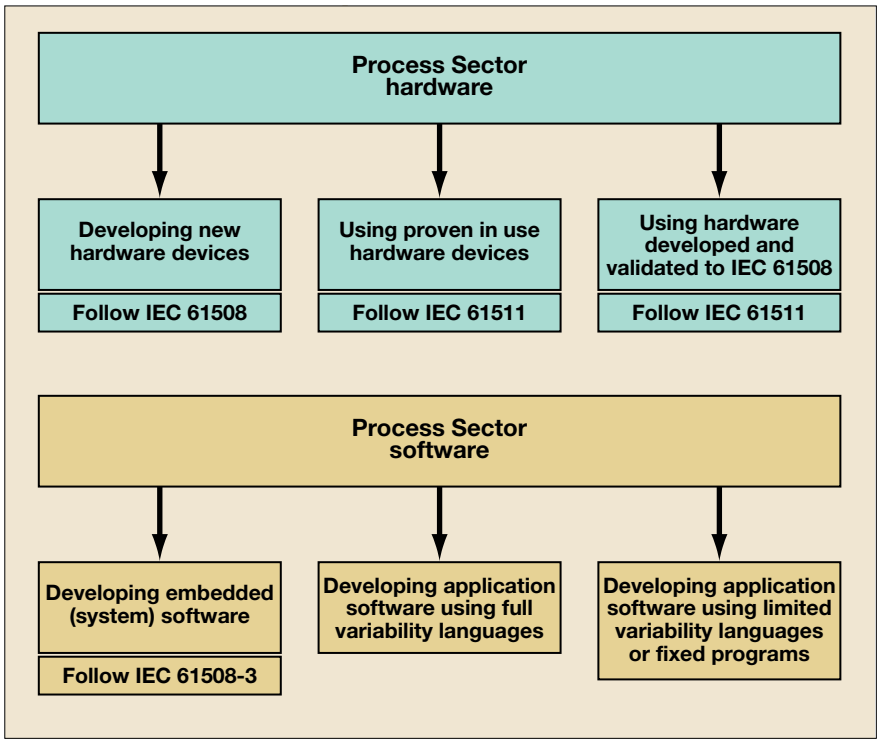

Figure 2 Standards for SIL requirements in machinery protection systems

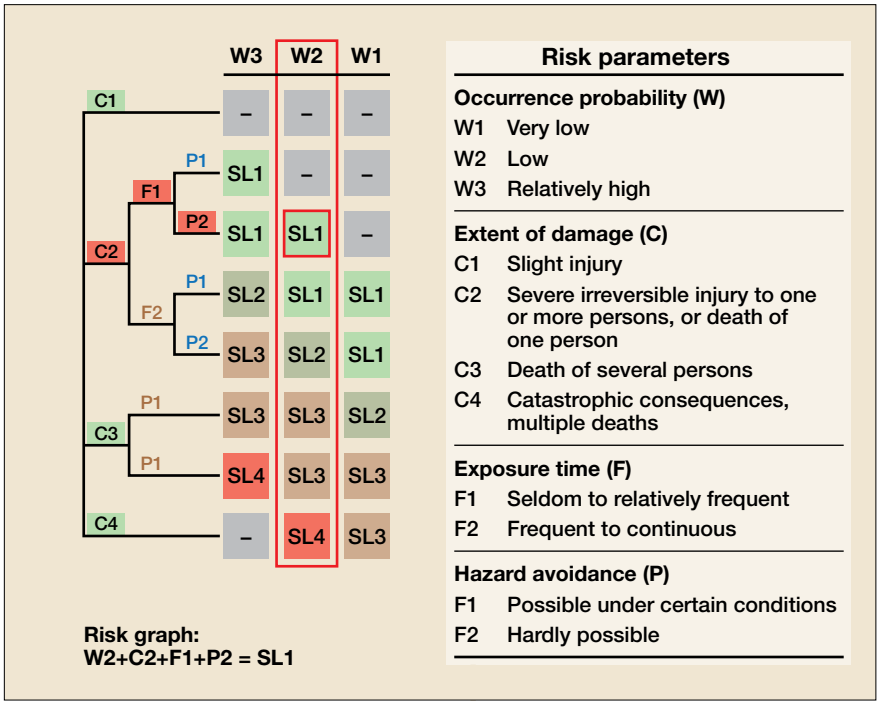

Figure 3 Risk graph

of protection analysis (LOPA) assessment. The SIL of a SIS is derived by taking into account the required risk reduction to be provided by that function. IEC 61511 notes that this is best accomplished as part of a process hazards and risk analysis (PHA) to benefit from possible synergies and the information developed. Another way to obtain an overview of the appropriate SIL is the risk graph (see **Figure 3**). By following the path characterised through the four different risk parameters (occurrence probability, extent of damage, exposure time and hazard avoidance [once damage occurs]) the appropriate SIL1 to SIL4 will result (with 4 being the highest, most stringent SIL). The example within the risk graph indicates that even under rather dramatic circumstances (unexpected death of one person) a SIL1 machinery protection system would meet the IEC 61511 requirements in this respect.

The author wants to be very clear that the SIS is employed to prevent a severe HSE event and that severe harm or even the death of a person are not acceptable in any way. Every effort and technical advancement should be employed to prevent harm and HSE in general.

If a SIS is chosen to reduce the imposed process risks to the acceptable level it must meet the SIL requirement just evaluated.

IEC 61508, PFD and PTI

Vendors of SIS have to follow the guidance given under IEC 61508 when developing, testing and having them SIL certified. Stringent availability criteria must be met by each individual component employed inside a SIS. Also every single embedded algorithm is tested, improved if needed and finally approved by a certifying body such as TÜV or Exida with the appropriate SIL certificate. During the certification process as well as during the implementation phase, the probability of failure on demand (PFD) is one of the guiding values (see **Figure 4**). This is calculated by adding up the PFD for all individual components within each loop (demand = dangerous event occurs and component should perform as it is supposed to).

One very important factor with a linear impact on the PFD calculation is the proof test interval (PTI). The shorter the chosen PTI, the lower the PFD. Modern machinery protection systems offer the convenience of a two to three year PTI along with a SIL2 certificate, reducing the testing and documentation effort to an acceptable level.

Figure 4 shows the correlation of SIL and PFD values to be met per loop to meet the requirements. In order to meet SIL2, a PFD value of 10^{-2}–10^{-3} (per hour; low demand mode) is required. The inverted value results in a theoretical systems availability of 99-99.90%.

It is important to note that the PFD evaluation must be done per each individual safety relevant loop, and must include all elements involved, from the sensing element down to the acting relay finally stopping the process/machine at acute risk, potentially resulting in HSE harm. It is not sufficient for one individual sensor, card or relay to be SIL certified and meet the appropriate PFD criteria – the entire loop must meet the PFD hence SIL requirement. Which sensors and characteristic sensors should be incorporated into a safety strategy depends heavily on the application and type of process equipment.

		SIL	Required availability	Probability of failure on demand (PFD)	$^1/_{PFD}$
IEC 61511	ISA 584	4	>99.99%	E-005 to E-004	100,000 to 10,000
		3	99.90-99.99%	E-004 to E-003	10,000 to 1000
		2	99.00-99.90%	E-003 to E-002	1000 to 100
		1	90.00-99.00%	E-002 to E-001	100 to 10

Figure 4 Correlation of SIL and PFD values

Boundary conditions when installing and planning a protection system

The two biggest fears related to machinery protection systems covering critical machinery are false trips, resulting in economic losses and sometimes dangerous process

situations, and missed detects, which are simply dangerous.

On many safety critical applications it is mandatory to use sensor redundancy and voting logic to ensure proper system function and availability even when a single end device has failed and can often not be replaced while the process is operational.

There are different strategies available today to reduce the nuisance trip level of modern SIS to almost zero, while in parallel ensuring severe events are detected timely and the machinery is safely shut down with minimum consequential damage.

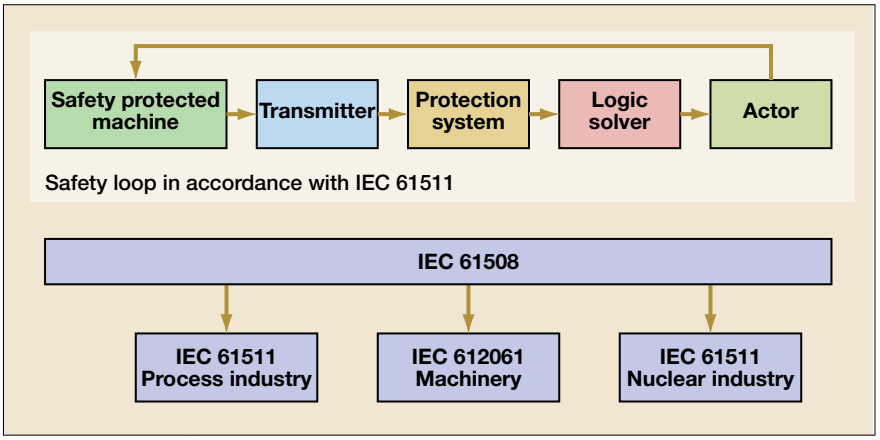

Figure 5 Scope of IEC 61508 for safety protected machinery

Sensor redundancy and voting

One frequently chosen strategy is the application of sensor redundancy. Voting schemes include 1-out-of-n voting, n-out-of-n voting and n-out-of-m voting (2oo3 or 2oo4). The n-out-of-m voting involves a higher number of sensors being installed, but offers a feasible way of reducing both spurious and missed trip rates.

Alternatively, modern systems also offer an interesting alternative using diagnostic coverage (DC) in a 1oo1D sensor architecture, employing a single sensor per location and closely monitoring its proper function at all times (DC>99%) and thereby achieving a higher SIL.

Here are two brief examples. If, on a given turbine application, the axial thrust analysis based on a proximity signal is the only safety relevant shutdown parameter, sensor redundancy should certainly be involved, ensuring sufficient machinery protection system availability even if a single sensor fails.

Looking at another example, on a four-throw reciprocating compressor, we often find up to 10 different sensors employed for machinery protection (four for crosshead acceleration, two for frame velocity and four for dynamic rod positions). In this case a 1oo1D architecture employed by a modern machinery protection system does not only meet SIL2 criteria at an affordable level, but also achieves a virtually zero false trip rate through sophisticated diagnostic coverage, by ensuring proper function of all loops at all times.

An interesting approach, bringing the legal IEC obligations potentially in line with economic interest, reducing loss of production and potential machinery damages, is the determination of acceptable damage/loss per process. Referring back to the second example above, most users would rate a failed suction valve on a reciprocating compressor as acceptable damage, not needing a machinery shutdown by a SIS. In contrast, events involving a broken piston rod, seized wrist pin or loose piston require immediate attention to reduce consequential damage, which in HSE and economical respect makes perfect sense.

A low PFD value (which equals a high SIL level) does not mean a system protects effectively; it only means that the system is available when it needs to be, regardless of how often it trips, and even how often it false trips. It is all about HSE: functional safety considers the safest process to be no process.

Conclusion

It is important to understand what SIL certification means, and what it does not mean. SIL ratings were established to define a metric for evaluating a system's level of operational reliability with regard to safety, as defined by IEC 61508 (see **Figure 5**). As it applies to machine monitoring systems, a SIL rating refers to the PFD of the protection system. A key point to remember is that SIL ratings have nothing to do with monitoring precision, which is represented by false trips and missed detects. Keep in mind that, before a SIL rated safety system comes into play, operators have to determine the appropriate SIL rating for the machinery that has to be safety protected. In other words, IEC 61508 is a risk based standard and, in order to apply it, criteria for the tolerability of risks must be established for the machine. For instance, a HAZOP study must be carried out.

Some marketing phrasing such as "SIL ready" or "Equates to SIL" can be puzzling. However, there are two ways to clarify the confusion. Firstly, look for a monitoring system from vendors who provide genuine SIL certificates issued by recognised certification institutions.

The SIL rating must cover not only the safety system itself, but also the inherent components in the safety loop, from sensors to the emergency shutdown device (ESD). Secondly, be aware that SIL ratings should not only be high, but relevant to your application. For instance, SIL certification for monitoring over-speed protection is of no significance to a reciprocating compressor user, but a rating for a safety system that performs segmented RMS vibration analyses may be significant for your machine. You can expect a protection system with specialised capabilities for reciprocating machinery to be rated as high as SIL2.

Oliver Franz is a Product Manager with Prognost Systems. He is an active member of API 670 5th edition task force and graduated from the University of Paderborn with a diploma in chemical engineering.