IRSE
Institution of Railway Signal Engineers

Back to basics: SIL explained

Paul Darlington and Ian Mitchell

Safety Integrity Level (SIL) is an indicator of the relative risk-reduction provided by a safety function in a device. A SIL number between 1 and 4 (SIL 1 being the lowest level of safety protection and SIL 4 the highest) is used to describe the degree of safety protection required and the safety reliability of a system which is needed to achieve that protection. It should be noted that safety reliability is not the same as performance reliability, as this back-to-basics article will explain.

For traditional hardware-based systems, safety is typically specified and demonstrated in terms of Mean Time Between Wrong Side Failure (MTBWSF), which can be calculated from the observed random failure rates of the individual components. When programmable systems began to be used in safety critical applications, duplicated or triplicated system architectures were adopted to give very high MTBWSF as a result of random hardware failures. But what about failure of the software embedded in these systems? Software failures may appear to be random, but in fact they are always systematic; if the circumstances are repeated the result will be the same. This means that any attempt to predict safety from observed failure rates of the system is futile – a small change in operating circumstances can reveal or hide a latent defect in the software.

The solution is to recognise that the hazardous failure rate as a result of these 'systematic failures' cannot be quantified, and instead it is necessary to demonstrate safety by means of the rigour of the design and validation process for the system and the software. This is inevitably a qualitative (as opposed to a quantitative) approach and the SIL system provides an internationally recognised approach to managing this issue for safety critical systems.

The concept of SIL originated in the International Electrotechnical Committee standard IEC 61508: Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems. IEC 61508 is not railway specific and applies to all safety engineering disciplines. For the rail industry CENELEC (European Committee for Electrotechnical Standardisation) derived the following standards from IEC 61508 to meet railway specific requirements.

- EN 50126: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
- EN 50128: Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.
- EN 50129: Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.

Safety Integrity Levels can be assigned to virtually any function presenting a safety risk. Typical examples of SIL functions for rail are: SIL 1 light metro train speed monitoring and display, SIL 2 monitoring of axle box bearing temperature, SIL 3 depot protection, SIL 4 interlocking of points and signals. The allocation of SIL

Safety integrity level	Tolerable Functional Failure Rate per hour
SIL 1	10^{-5} to 10^{-6}
SIL 2	10^{-6} to 10^{-7}
SIL 3	10^{-7} to 10^{-8}
SIL 4	10^{-8} to 10^{-9}

What the SIL levels mean in terms of tolerable failure rates.

takes into account the frequency and severity of the risk that is being managed, and whether there are other systems or manual processes that can mitigate the effect of a hazardous system failure.

When developing systems to a required SIL, techniques are selected from a list of recommended or mandatory techniques dependent upon the level of SIL. For example, when creating the software requirements specification for a SIL 4 system the techniques include: formal methods, modelling, structured methodology, and decision tables.

A common misconception is that individual products or components have SIL ratings. But simply buying a SIL suitable component (if possible) does not ensure a SIL system. Rather, products and components may be suitable for use within a given SIL system, but they are not individually SIL rated.

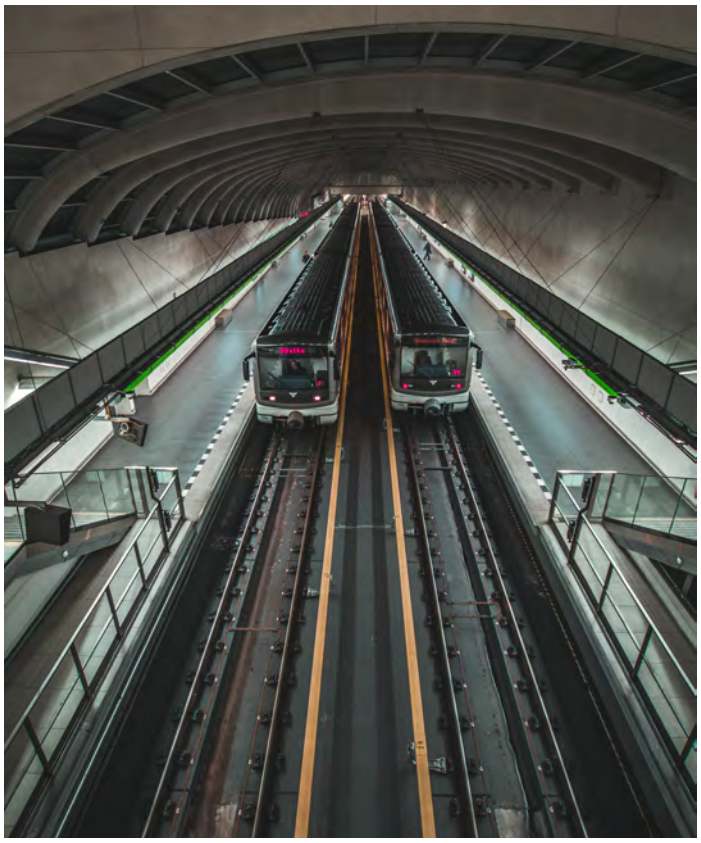
SIL levels apply to safety functions and safety systems, and products and components are only suitable for use in specific SIL applications if the end user can ensure that the overall safety system is implemented correctly. The equipment or system must also be operated and used in the way it was designed in order to achieve the required safety risk reduction level.

The owner/operator must determine the acceptable level of risk, based on standards or other factors such as ALARP and society acceptance of the risk. A risk level that one owner determines is tolerable may be unacceptable to another. Unfortunately, the requirements for a given SIL are not consistent among all of the functional safety standards across different industries, which does cause some confusion.

Some asset owners and project managers may be tempted to specify a high SIL simply for availability reasons, and SIL is sometimes mistakenly used to imply that a product has better quality and higher reliability, but this is incorrect. Some products may be described as 'SIL rated', suggesting that they are suitable for use in safety systems, but this depends on many other aspects of the overall system design. Even when a product genuinely complies with SIL requirements, this only provides assurance that it is capable of performing a specific role within a safety system. Its safety reliability may be high, but its general reliability may not be.

An item is highly available if it does not fail very often and, when it does, it can be quickly returned to service. A system is considered to be safe if it is reliably performing its safety function. However, the system may fail much more frequently in ways that are considered not to be dangerous (fail safe). Therefore, a safety system may be less reliable overall (i.e. with a lower mean time between failures) than a non-safety system performing a similar function.

Selecting the appropriate SIL level must be done carefully. Whole life costs are generally considerably higher in order to achieve higher SIL levels. This is because designing, testing and maintaining systems to meet high levels of safety integrity



A complex railway system will typically employ systems with different SIL levels. Interlocking, train absence detection and automatic train protection for example may be SIL 4 systems, whilst the automatic train operation and control centre systems may be configured to meet the failure rates of SIL 2.
Photo Pixabay/Jan Hloušek.

is complicated, time-consuming and expensive, and can lead to lower levels of overall system performance reliability which has cost implications. It can also be an obstacle to future enhancements of the system to meet new requirements and operational circumstances.

For example, some industries outside of rail with a lower safety risk requirement (for example factory production) companies will typically accept designs up to SIL 2. If an assessment indicates a requirement for a higher SIL, owners will usually require the redesign of the process to lower the intrinsic process risk, rather than design the system to achieve SIL 3.

In modern railway signalling systems the use of SIL 4 is usually restricted to those parts of the signalling which are safety critical, for example the interlocking. Other parts of the signalling system, such as the control panel or workstation, are usually of a lower SIL value (typically SIL 0 to SIL 2). Network Rail in the UK has recently reviewed its standards to determine where the SIL 4 interlocking could be simplified by deploying lower SIL functions in another part of the system.

Further reading

- Understanding Safety Integrity Levels (SIL) International Technical Committee (ITC) IRSE News October 2015. **irse.info/yahut**
- The Use and Misuse of SILs (2009) Roger Short IRSE News February 2009. **irse.info/0s8vc**
- Understanding the Use, Misuse and Abuse of Safety Integrity Levels (2000). Felix Redmill Proceedings of the Eighth Safety-critical Systems Symposium, Southampton, UK, February 2000. **irse.info/1jsow**