Safety Corner

What is Safety Integrity Level (SIL)?

Engineers have learned to accept that the safety is not binary (either safe or unsafe) but there is a continuum between absolute safety and catastrophe measured by a scale called risk. While risk can be characterised by probability distributions to register the likelihood and consequence of undesired outcomes, one simple way to represent a known spectrum of risk is to use predetermined intervals in terms of risk classes or risk levels.

The concept of safety integrity levels (SILs) follows just that idea by specifying the safety requirements of components or systems into levels of risk reduction capability. Typically, four levels of SIL are used, as in the international standard IEC 61508 (*Functional safety of electrical/ electronic/ programmable electronic safety-related systems*). However, ANSI/ISA-S84.01 (*Application of safety instrumented systems for the process industries)* uses only 3 SILs. The higher the SIL is, the more effective or reliable a safety-critical component is in risk reduction, with SIL 4 being the most demanding and SIL1 being the least. To achieve a given SIL, a safety-critical component must satisfy the following requirements in probability of failure: 10^{-2} to 10^{-1} for SIL 1, 10^{-3} to 10^{-2} for SIL 2, 10^{-4} to 10^{-3} for SIL 3, and 10^{-5} to 10^{-4} for SIL 4.

The specification of SIL is subjective and design-specific. A SIL specified for a component may be tolerable in one system design but may be unacceptable for the same component in another application. In specifying SIL, engineers must determine the risk acceptance level based on the safety specifications, risk control philosophy, budget, and a variety of other factors because costs increase considerably to achieve higher SIL. Typically in the process industry, engineers would accept safety system designs up to SIL 2. However, in railway and other industries with high safety demand, specifying SIL 4 safety-critical components is not uncommon.

To demonstrate a component or a system has achieved its specified SIL rating, engineers would use system safety techniques to evaluate the likelihood of a demand, the complexity of the system, and types of risk control mechanism used. Field test data and operating history would be needed to validate the system safety analyses in supporting the SIL specification.

==========

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho.hkarms@gmail.com