SAFETY INTEGRITY LEVELS

Do You Understand The Odds?

Angela E. Summers, Ph.D., P.E., President, SIS-TECH Solutions, LP

"Understanding Safety Integrity Levels," Control Engineering website, February 2000.

The perception of safety integrity levels (SIL), as related to ANSI/ISA 84.01-1996 and IEC 61508, currently exists somewhere between science fiction and marketing. The science fiction is bounded by the belief that the safety integrity level describes the absolute performance of the safety instrumented system (SIS) in terms of potential incidents. The marketing perception is controlled by vendors and service providers, who make claims concerning product performance. Neither perception is true.

SIL is a measure of the SIS performance related only to the devices that comprise the SIS. This measure is limited to device integrity, architecture, testing, diagnostics, and common mode faults inherent to the specific SIS design. It is not explicitly related to the cause and effect matrix, but it is instead related to the devices used to prevent a specific incident. Further, SIL is not a property of a specific device. It is a system property; input devices through logic solver to output devices. Finally, SIL is not a measure is incident frequency. It is defined as the probability (of the safety instrumented system) to fail on demand (PFD). A demand occurs whenever the process reaches the trip condition and causes the SIS to take action.

A simple explanation of the relationship between incident frequency and SIL is to consider a roulette wheel. A roulette wheel consists of a horizontal wheel containing numbered slots. The wheel is spun and a ball is tossed into the wheel. In a gaming establishment, bets are placed on a specific numbered slot. If the ball lands in the slot that the player has selected, the house pays the player.

SIS-TECH

12621 Featherwood Drive • Suite 120 • Houston, Texas 77034
Tel: (281) 922-8324 • Fax: (281) 922-4362
www.SIS-Tech.com

On an SIL roulette wheel, the SIL represents the chance of landing in a specific slot on the wheel. SIL is therefore defined by probability and the standards have created four probability categories:

SIL 1	1 in 10	to	1 in 100
SIL 2	1 in 100	to	1 in 1000
SIL 3	1 in 1000	to	1 in 10000
SIL 4	1 in 10000	to	1 in 100000

On an "SIL 1" roulette wheel, let's assume that there are 10 slots (minimum required for SIL 1). One is painted red; the other nine are painted black. The roulette wheel is spun when a process demand occurs, e.g. the level in a tank reaches the high level trip set point. The roulette wheel spins; the ball is tossed. If the ball lands in any of the black slots, the safety function works, e.g. the dump valve opens lowering the level. If the ball lands in the red slot, the safety function does not work and whatever the safety function was designed to prevent occurs, e.g. the tank overflows. How often the tank overflows is a product of the number of spins (process demand) and the ratio of red slots to black slots (PFD or SIL). Therefore, in this game, the player can control the probability of success by controlling the number of slots (SIL). The player can also reduce the incident frequency by reducing the number of spins (process demands).

How many slots are required and what actions should be taken to reduce the number of process demands is based on the perceived risk and tolerable incident frequency. The risk, as identified during the process

hazards analysis, is essentially the "bet" placed on the red slot. The bet may consist of injuries, fatalities, environmental releases, property/equipment damage, permit violations, and the plant's "license to operate." If the bet is small, e.g. high level in a tank occurring 10 times per year with the potential consequence of overflowing water into a dike, maybe 10 slots are acceptable with a resultant incident frequency of once per year. If the bet is large, e.g. high pressure in a process vessel with the potential for rupture, release of flammable gas, subsequent ignition, and multiple fatalities and catastrophic damage occurring once in 10 years, maybe 1000 slots are required with a resultant incident frequency of 1 in 10,000 years.

Unfortunately, while it is easy from a risk standpoint to understand the penalty behind the failure of a safety function to work, sometimes it is more difficult to acknowledge that the true payout is when the safety function does what it is supposed to do. After all, how many times do plant engineers get a pat on the back because a safety function worked? The plant engineers don't get a hefty check related to the successful prevention of the incident. No small bets or large bets are actually paid to anyone. Therefore, this game is difficult to play, because the game only issues penalties (the incident) for incorrect design choices.

Making matters worse is that the drive toward more production may result in the desire to ride-out upsets by temporarily disabling or bypassing trip outputs. This action results in the wheel being reduced to one slot with the operator making the ultimate bet. Will the wheel spin before he can get the process back into control?

In most of the literature, SIL is referred to as a performance criteria – the capability of the safety function to perform at the time it is needed. As explained above, the choice of the SIL is more often related to the cost of non-performance – a blurry sometimes difficult to sell concept, especially at project budget meetings. However, no matter how SIL is viewed, the concept represents an important shift in industry's attitude toward safety system design. The SIL must be chosen to reduce the incident frequency to a tolerable level. The SIL is the design basis for all engineering decisions related to the safety function. When the design is complete, it must be validated against the SIL. Therefore, SIL closes the design cycle - risk identified, requirements quantified, and design validated.