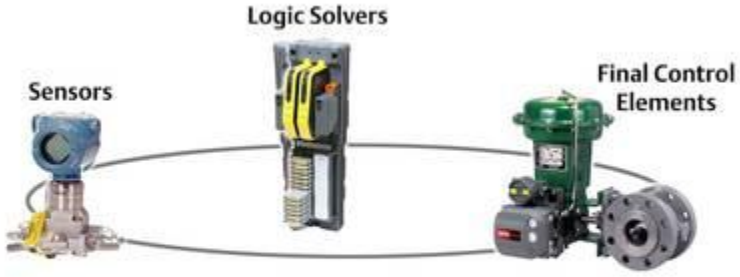
Understanding SIS industry standards

Process safety standards and practices are spreading from oil and gas and other energy-related industries to broader process industry applications. Here's basic advice on how to make more sense of the numbers and acronyms.

Robert I. Williams, PE
05/14/2013

Safety instrumented system (SIS) applications grew primarily out of the oil and gas industries, where they are used to mitigate safety hazards related to many dangerous feedstocks, products, and processes. When applied appropriately, the fundamental concepts of SIS applications are integrated within the total lifecycle of the overall safety system. Understanding these systems involves unraveling the sometimes arcane language of safety engineers with standards numbers and many acronyms.



An SIS provides an integrated approach to complete safety loops, as shown in Figure 1. Such a loop includes a sensor, logic solver, and final control element. The SIS system shuts down a process plant or part of a plant when needed for safety, but keeps the plant running safely when devices fail.

What is a safety function?

Safety instrumented functions (SIFs) are actions taken by a SIS to shut down the process plant safely. Each identified SIF consists of a set of actions to protect against a specific hazard. A process plant SIS therefore consists of a number of SIFs which are listed in the process hazard analysis (PHA) report.

Part of the design process is considering many what-if scenarios that examine what happens if various components fail. A safety integrity level (SIL) is a performance measure which tries to quantify the probability of a specific SIF failing to perform its required function when called upon, known as the probability of failure on demand (PFD). Whereas a DCS is performing process control functions continually while the plant is running, the SIS is dormant by design until required to perform a safe shutdown function. Table 1 lists four SIL levels and their related PFDs as defined by IEC 61508 and IEC 61511. All standards are not necessarily the same. For example, ANSI/ISA-S84.01-1996 recognizes only three SILs.

Table 1: Safety Integrity Levels

SIL	PFD_{avg}	RRF
1	10^{-1} to 10^{-2}	10 to 100
2	10^{-2} to 10^{-3}	100 to 1,000
3	10^{-3} to 10^{-4}	1,000 to 10,000
4	10^{-4} to 10^{-5}	10,000 to 100,000

Techniques to establish the required SIL for a SIF in a SIS are defined in the relevant industry standards. (Some are listed in the online resources for this article.) SIL 4 is the highest level of safety integrity while SIL 1 is the lowest.

The risk reduction factor (RRF) for a SIF is the mathematical inverse of the PFD_{avg} for that SIF. It represents a number corresponding to the factor that the SIF reduces the likelihood of the hazardous event that the SIF intended to prevent.

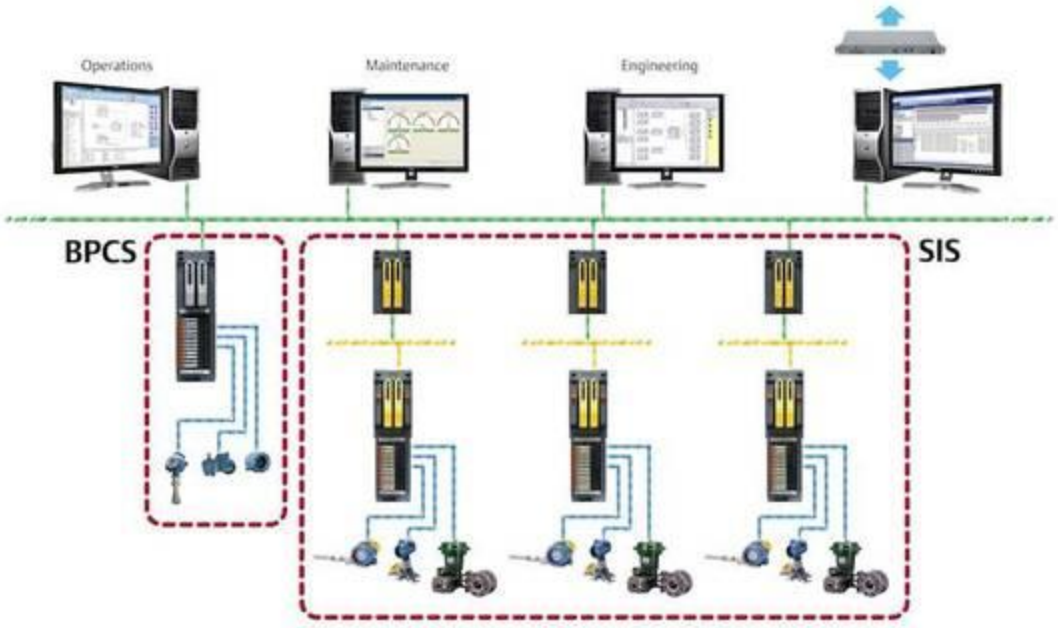
Probability of failure on demand (PFD) is the probability that a SIF designed to protect a process plant will fail to shut down the plant safely when the hazard shutdown condition occurs. In other words, the safety function fails to do its job when called upon.

Safety lifecycle

The safety lifecycle, as defined by IEC 61508 and ANSI/ISA-S84.01, structurally defines a SIS development from its initial conceptual design through to its final decommissioning, as follows:

1. Conceptual design
2. Hazard and risk analysis PHA (HAZOP)
3. Safety requirements specification
4. System architecture and detailed engineering
5. Application programming
6. System production
7. System integration
8. Factory acceptance tests (FAT)
9. System installation and commissioning
10. Safety system validation—site acceptance tests (SAT)
11. Operation and maintenance plan
12. System change management
13. Decommissioning, and
14. Information and documentation requirements.

Generally, the significant hazards for equipment and any associated control systems have to be identified by the specifier or developer via a hazard analysis. The analysis identifies whether functional safety is necessary to ensure adequate protection against each significant hazard. If so, then it has to be taken into account in an appropriate manner in the design. Functional safety is just one method of dealing with hazards, and other means for their elimination or reduction, such as inherent safety through design, are of primary importance.



IEC 61508 applies to safety-related systems when one or more of such systems incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices. It covers possible hazards caused by failure of the safety functions to be performed by the E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself. It is generically based and applicable to all E/E/PE safety-related systems irrespective of the application.

The underlying assumptions of the standards recognize that the consequences of failure could have serious economic implications. In such cases the standard could be used to specify any E/E/PE safety-related system used for the protection of equipment or product. The scope of IEC 61508-1 goes into more detail.

The range of E/E/PE safety-related systems to which IEC 61508 can be applied includes:

- Emergency shutdown systems
- Fire and gas systems
- Turbine control
- Gas burner management
- Crane automatic safe-load indicators
- Guard interlocking and emergency stopping systems for machinery

- Railway signaling systems, and
- Variable speed motor drives used to restrict speed as a means of protection.

Relevant means of implementing safety functions include electromechanical relays (electrical), nonprogrammable solid-state electronics (electronic), and programmable electronics. Programmable electronic safety-related systems typically incorporate programmable controllers, programmable logic controllers, microprocessors, application specific integrated circuits, or other programmable devices which could include smart devices such as sensors, transmitters, and actuators.

In every case, the standard applies to the entire E/E/PE safety-related system. That could encompass, for example, a sensor, through control logic and communication systems, to final actuator, including any critical actions of a human operator. For safety functions to be effectively specified and implemented, it is essential to consider the system as a whole. The physical extent of an E/E/PE safety-related system is solely determined by the safety function.

Working through the entire safety lifecycle is a major undertaking, but it is a process critical to the safety of people, property, and environment.

Robert I. Williams, PE, is instrumentation and control systems manager at Brinderson, Costa Mesa, Calif.

Key concepts:

- Understanding process safety involves potentially confusing standards and acronyms.
- Working through the overall safety lifecycle is a major project, but the process is straightforward.
- Understanding a few basic concepts can help decipher the complexities of standards language.

Source:

http://www.controleng.com/industry-news/single-article/understanding-sis-industry-standards/90db923905bf9f60271f67a82ad3592c.html