by Mike Boudreaux

A Primer on SIS

Understanding Process Safety Systems Design

***Mike Boudreaux** is the DeltaV SIS product manager at Emerson Process Management in Austin, Texas. Prior to joining Emerson, he previously filled various engineering, sales and marketing roles at AkzoNobel and Alcoa. While at AkzoNobel, Mr. Boudreaux gained his experience specifying, designing and implementing safety instrumented systems. He earned a bachelor's degree in Chemical Engineering from the University of Houston and an MBA from the Kellogg School of Management at Northwestern University. He is a member of the ISA 84 functional safety standards committee and he is a co-chair for ISA 99 Working Group 7 on safety and security. Mr. Boudreaux can be reached at Mike.Boudreaux@emerson.com or 512 832-3547.*

Q: How did the concept of safety instrumented systems come to be? How has SIS design strategy evolved since its inception to where it stands now?

A: Industry incidents, such as those that have occurred in Flixborough, England, Seveso, Italy, Bhopal, India, and Pasadena, Texas, as well as others, have led to an increased interest in process safety. Much of the focus has been to reduce process risk through inherently safe design and independent layers of protection (IPL). Safety instrumented systems are one of the many layers of protection that are used to deliver increased process safety.

Modern safety instrumented systems are based on functional safety design concepts that are provided by IEC 61508 and IEC 61511. Over the past 25 years, SIS design concepts have mirrored process control system developments. Control systems have evolved from pneumatics and hardwired panel boards to centralized DCSs to digital plant architectures. Similarly, SISs have progressed from relays and switches to PLCs with redundant architectures to logic solvers with advanced diagnostics capabilities. SIS design has evolved from using rules of thumb and prescriptive requirements to designing safety loops based on the functional safety requirements of the process.

Q: From a general process safety perspective, why are safety instrumented systems important? What capabilities do SISs generally offer the end-user for process safety improvement?

A: When a process cannot practically be designed to be inherently safe, an SIS can be used to reduce risks to an acceptable level. An SIS can be designed to deliver a specified safety integrity level (SIL) of risk reduction. IEC 61508 defines SIL 1 through SIL 4, with each SIL designating a relative level of risk reduction provided by a safety instrumented function (SIF) by an additional order of magnitude.

Q: What role do standards play in the world of SIS? What should end-users know about standards related to SIS?

A: The modern concept for SIS in the process industries is based on IEC 61508 and IEC 61511. IEC 61508 is a generic functional safety standard that can be applied across all industries. IEC 61511 is a functional safety standard that applies specifically to the process industry sector. ISA (*www.isa.org*) has adopted IEC 61511 as ANSI/ISA 84.00.01-2004 (ISA 84), with the addition of a grandfather clause. Other industry sectors have standards based on IEC 61508, such as IEC 62061 for machinery safety and IEC 61513 for the nuclear power industry.

In the United States, OSHA (*www.osha.gov*) has stated that ISA 84 is recognized and generally accepted as good engineering practice for SIS. This means that if a process manufacturer uses ISA 84 as a basis for SIS design, this manufacturer will be considered in compliance with OSHA PSM requirements for SIS. IEC 61511 has similar recognition as a best practice under the SEVESO II Directive in the European Union. Some other countries have similar regulations that recognize IEC 61511.

Q: What are some of the common pitfalls end-users need to be aware of when devising their SIS design and implementation strategies?

A: During the analysis and implementation phases of the safety lifecycle, there are two major activities that can have a significant effect on the performance of the SIS. When developing a safety requirements specification (SRS), process manufacturers sometimes go overboard and make the SRS too complex to be practical, or they go in the opposite direction and don't provide a consistent set of documentation where the safety requirements are clearly specified. Clause 10 of IEC 61511 contains an itemized list of information that should be included in a SRS, but at the most basic level, the SRS should provide a functional description and the integrity requirements for each SIF. The SRS is the document against which all of the safety lifecycle activities are verified and validated. As such, it is important that this documentation be simple to use and maintain.

Other activities that can have a significant impact on the performance of the SIS are SIF design and SIL verification. This task requires significant engineering knowledge, training, and experience. The basic PFD_{avg} calculations can be automated via safety lifecycle tools, such as exSILentia. Knowing which devices to use, selecting the appropriate hardware fault tolerance, correctly applying prior-use data, and designing the most economical SIF to minimize capital and operating costs while maximizing availability, can be a difficult task. End-users should make sure the people performing this work are competent in the area of process safety systems design and, more specifically, SIF design and SIL verification.

Q: What are some key steps end-users should take to ensure they are employing SIS in a way that will provide the most benefit in terms of process safety?

A: The IEC 61511 safety lifecycle is the best model for designing, implementing, and operating an SIS. The safety lifecycle activities are often grouped into three basic phases: analysis, implementation, and operation. During the analysis phase, it is important that end-users first try to design their processes to be inherently safe. Some ways to do this are to implement simpler process designs and to carry out PHAs early in the design to allow for inherent safety in the design process. If this is not practical, then non-SIS layers of protection should be applied to reduce risk to an acceptable level. An SIS should be implemented only after this has been done, and not by default.

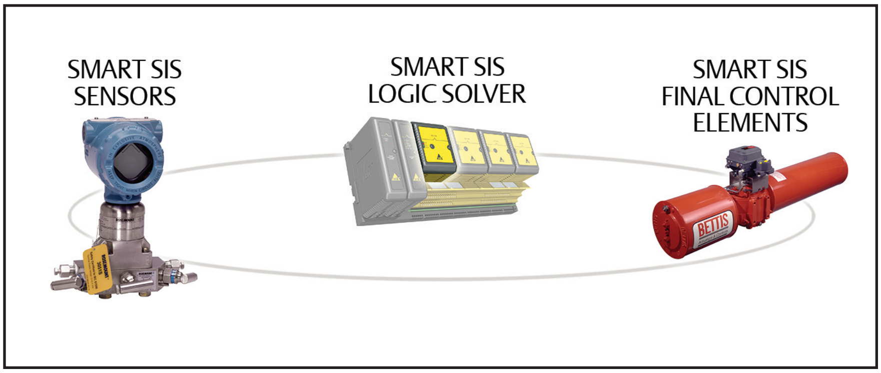
Many end-users try to avoid SIL 3 SIFs altogether. In cases where SIL 3 integrity is required, end-users should make a second attempt to go back and reduce the process risk in other ways before implementing an SIL 3 specified SIF.

During implementation and operation, it is important to have a good safety management system (SMS) in place to ensure that the SIS is delivering the functional and integrity requirements specified in the SRS. A good SMS will provide competency tracking for safety lifecycle roles, well documented design, operating and maintenance procedures, and routine function safety assessment and auditing. A well-run SMS will prevent systematic failures from undermining SIS performance.

Q: What are some of the technology application environments that typically benefit from SIS? Please explain how each application benefits from SIS in some detail.

A: There are many types of SIS applications, including emergency shutdown systems (ESD), fire and gas systems (FGS), burner management systems (BMS), and others. An SIS that is used as an ESD is the last line of defense to prevent a hazardous event from being initiated. In this kind of application, an SIS will bring the process to a safe state when an abnormal situation is detected. An FGS is another type of SIS, but these systems typically alert personnel or initiate actions in order to mitigate the consequences of a hazardous event. A BMS is a safety solution for control and monitoring of burner units that employs sequencing and interlocks to allow the burner unit to go safely through all the relevant states: from start-up, to operation, to shutdown.

IEC 61511 is replacing many of the older, prescriptive application standards. However, IEC 61511 doesn't map perfectly to FGS and BMS applications for a variety of reasons. Work is being done by the ISA 84 committee to provide better guidance to process manufacturers so they can more easily apply IEC 61511 to these applications. This will continue into the future, with the aim of IEC 61511 ultimately eliminating the need for many of the existing FGS and BMS standards.



DeltaV SIS is part of Emerson's smart SIS solution, which is an extension of the PlantWeb digital plant architecture, providing an integrated approach to complete safety loops. As illustrated here, the DeltaV SIS platform includes SIS soltions from sensor to logic solver to final control element.

Q: How do you envision SIS evolving going forward? How will the SIS of tomorrow be better than the SIS of today?

A: Process manufacturers are realizing the benefits of an integrated control and safety system (ICSS). Existing single-vendor ICSS platforms have shown that an integrated system can meet the IEC 61511 requirements for independence, diversity, physical separation, and common-cause failures between protection layers. New technologies will continue to challenge the existing conceptions about how to deliver both separation and integration of BPCS and SIS. Business needs for lower engineering and lifecycle costs, reduced training and maintenance expenses, and improved asset and event management will continue to drive the trend of ICSS adoption as the preferred solution for process manufacturers.

Improved device diagnostics is being driven by technology advancements in microprocessors and device design. Diagnostics reduces the dangerous undetected failure rates for devices. Automated online proof testing and device diagnostics will deliver safer systems, because failures will be detected whenever they occur. For the diagnosed failures in field devices, digital communications will send device status information to the logic solver so that the process can continue running safely while the device is repaired. For manual tasks that require maintenance personnel, automated workflow will be integrated with the SIS and asset management systems. Automation of the diagnostics and proof tests will make it economically feasible to perform them frequently; it will ensure that the tasks are completed correctly; and it will provide electronic documentation to ensure completion.

www.emersonprocess.com