CONTROL

January 2013

ESSENTIALS OF SAFETY INSTRUMENTED SYSTEMS

A Control Essentials Guide by the editors of Control

About the Control Essentials Series

The mission of the Control Essentials series is to provide process industry professionals with an up-to-date, top-level understanding of a range of key process automation topics. Our intent is to present essential engineering concepts in a practical, non-commercial fashion, together with a review of the latest technology and marketplace drivers—all in a form factor well suited for onscreen consumption. We hope you find this first edition on Safety Instrumented Systems useful. Check in at ControlGlobal.com/Essentials for other installments in the weeks to come.

—The Control Editorial Team

EXECUTIVE SUMMARY

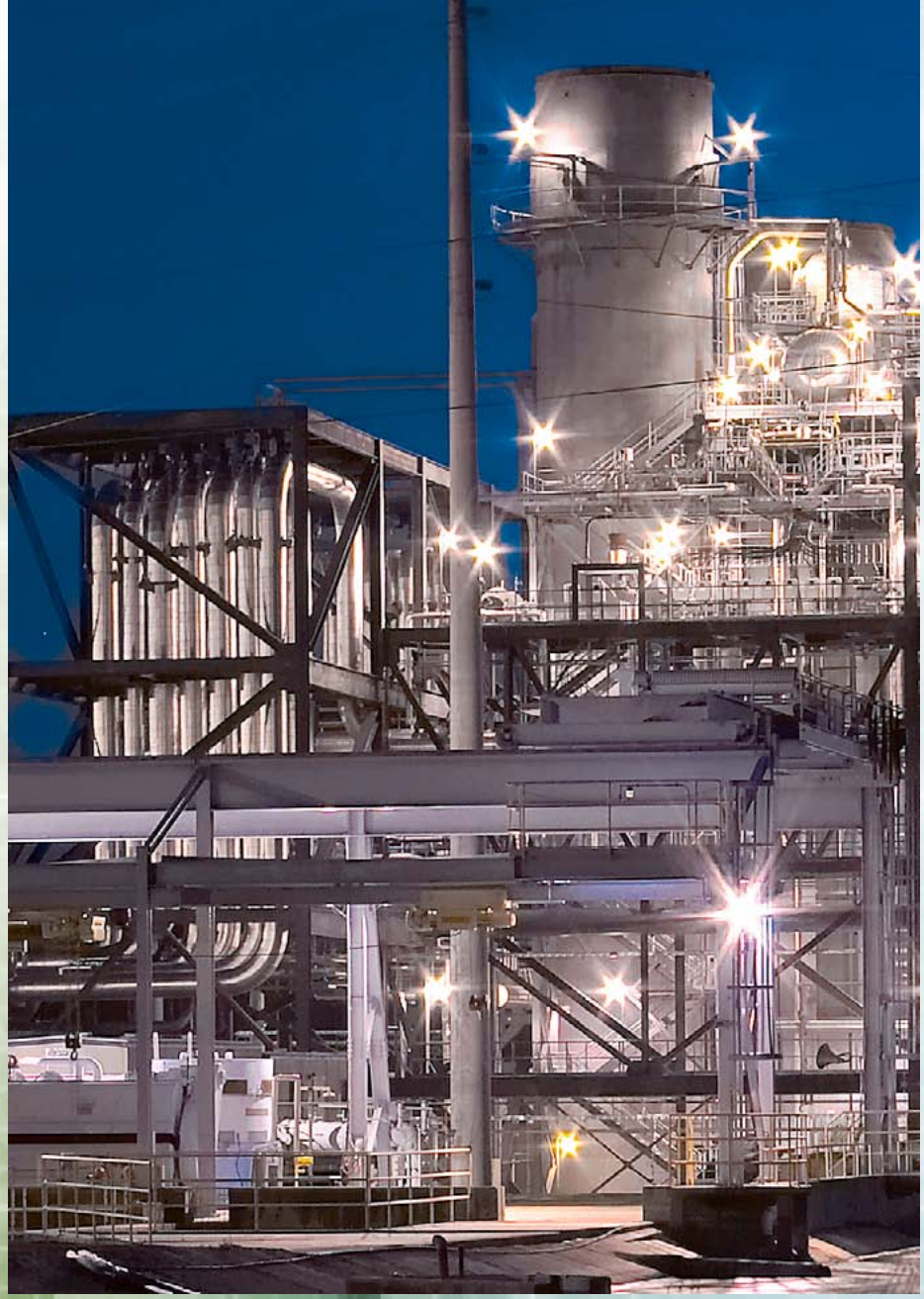
Throughout the global process and energy industries, the safety instrumented system (SIS) plays an essential role in protecting workers and equipment as well as nearby communities and the environment from harm. Much has changed in the several decades since the first programmable systems for safety protection were developed and deployed, and today the discipline continues to evolve and advance in terms of both methodology and technology.

The key reference methodology that has emerged for managing safety instrumented systems over their entire lifecycle—from risk assessment through design, operations and maintenance—are the IEC's 61508 and 61511 international standards. The standards originally were developed by industry for industry as technical standards. But in some arenas, compliance with the standards already carries the force of law. And even in areas where they are not legislated, the standards' growing acceptance as descriptors of best practices means that non-compliance may have very real liability implications if something does go wrong.

The standards themselves are purposely performance-based: they allow engineers the flexibility to meet industry and society's safety expectations in more than one way. Indeed, from a technology perspective, today's digital SIS options increasingly leverage integration and diagnostics to boost safety, availability and productivity even while reducing cost and complexity for end users. But the extent to which safety and control should be integrated or remain separate without compromising safety remains a subject of heated discussion. For their part, many independent consultants take the side of the standards and the math: integration doesn't necessarily compromise safety protections, but suppliers and their users need to adequately demonstrate that is indeed the case.

Further complicating the SIS landscape is the fact that many of industry's installations predate current standards, and verifying that older systems perform—and continue to perform—to standard is a significant undertaking. Indeed, many first and second generation installations are at or beyond the end of their serviceable lives and need to be migrated to more current technology.

Bottom line, the engineering of safety instrumented systems remains a complex and subtle task. And once commissioned, both proactive work processes and ongoing corporate commitment are needed to assure that SIS protections do not degrade over time.



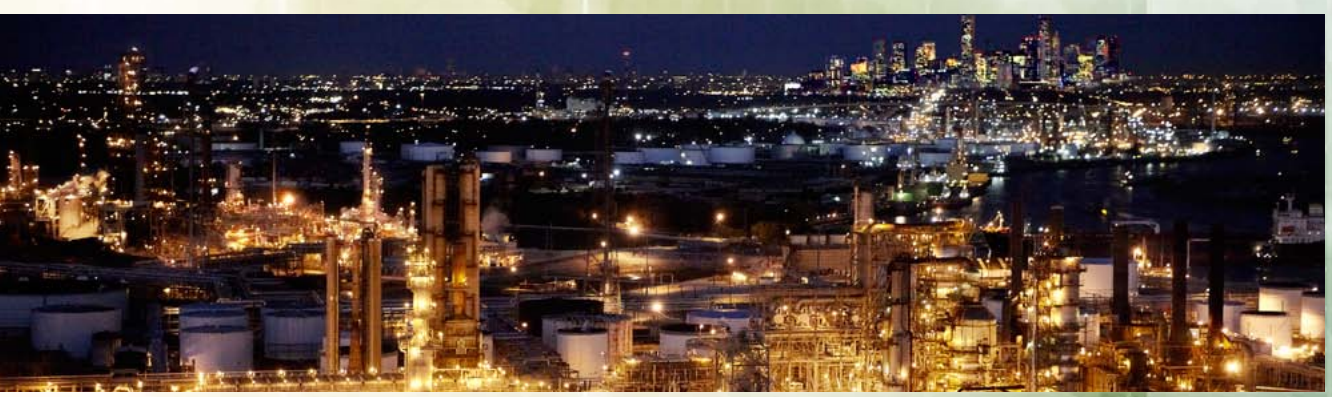
SIS IN A PROCESS SAFETY CONTEXT

Safety is at its core an exercise in risk management. And safety instrumented systems provide but one layer in a holistic, multi-layered approach designed to reduce risk not to an ideal but unachievable zero, but to a level deemed "as low as reasonably practicable" (ALARP).

Even at this early stage, a necessary level of subjectivity enters into safety calculations, as risk analysis must first endeavor to quantify the consequences of all potential risks as well as their likelihood of occurrence. Multiplying the severity of consequence by frequency of occurrence (in absence of any protective measures) in turn allows one to quantify potential risks so each can be appropriately addressed. Depending on the level of risk and complexity of operations involved, this often entails a rigorous hazards and operability (HAZOP) study involving a multi-disciplinary team of process, electrical, mechanical, instrumentation and safety professionals.

Measures of first resort for reducing risk include changes to the process and the equipment itself—for example, through using a solvent that is less toxic or a vessel with a higher pressure rating. For a given process design, then, protective layers may be needed to further address any gap between identified process risk and a level deemed acceptable. These protective measures are generally grouped into preventive layers, such as operator actions and automated emergency shutdown procedures, and mitigation layers such as pressure relief valves and emergency response procedures (**Figure 1**).

In a simplified methodology appropriately referred to as layers-of-protection analysis (LOPA), the risk-reduction contribution of each of these often overlapping layers of protection can be calculated, including the contribution of a safety instrumented system if employed.



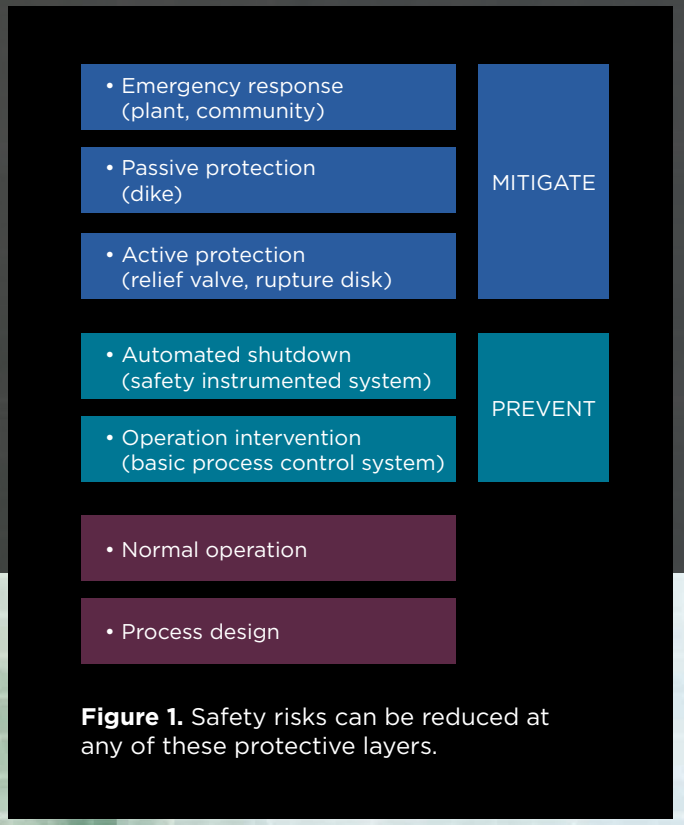


Figure 1. Safety risks can be reduced at any of these protective layers.

FUNDAMENTAL CONCEPTS

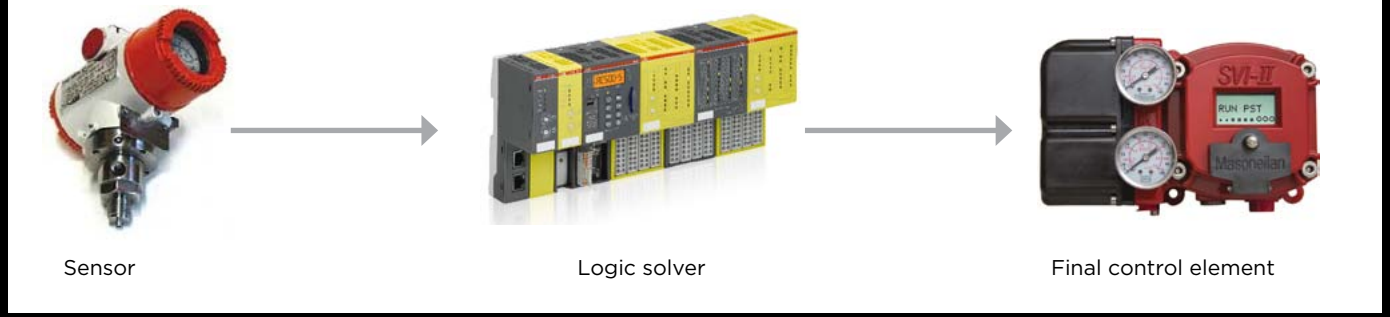
In the context of most process industry applications, safety instrumented systems are there just in case— just in case the human operators and the basic process control system fail to maintain process conditions within a safe operating envelope.

Process alarms should first alert the operator to an escalating temperature or pressure, but if the operator is unable to address the problem, the SIS takes over, automatically shutting things down before an out-of-control process becomes an unsafe one. At its simplest, a dedicated safety instrument senses a potentially unsafe condition, communicates with a safety logic solver which then activates a dedicated final control element (normally a valve) to effect a safe process shutdown (Figure 2.) In a refinery or other complex process facility, SIS loops can run into the dozens or hundreds.

By design, then, safety instrumented systems spend most of their time idling about in stand-by mode—so how can one be sure that when they're called on to do their job they will react in a timely and effective manner? And on the other side of the ledger, how do you ensure that a safety system doesn't trip when a shutdown isn't really needed? While not unsafe, spurious trips can put a substantial dent in process availability and ultimately company profitability. These essential and often contradictory demands on SIS performance explain why their design and upkeep remains a demanding yet critical task.

Like most engineering specialties, the safety system vernacular is rife with useful terminology and shorthand that nevertheless can quickly intimidate the uninitiated. Two of the most useful concepts to understand are those of the safety instrumented function (SIF) and the safety integrity level (SIL). It's easiest to think of a SIF as simply the action of the simple safety loop described above, abstracted from implementation details. Safety integrity levels, in turn, describe the risk reduction achieved by a particular SIF or required by a particular application.

SILs are assigned integer values from 1 to 4, with each level representing another order of magnitude increase in required risk reduction or decrease in probability of failure on demand, or PFD. SIL 1 describes an application with a risk reduction of 10 to 100, which translates to 90-99% SIF availability. At the other end of the scale, SIL 4 entails a required risk reduction of 10,000 to 100,000, or a SIF availability of 99.99% to 99.999%. Translation: SIL 1, mildly hazardous. SIL 4, extremely dangerous.



Sensor Logic solver Final control element

Figure 2. At its simplest, a safety instrumented system consists of a sensor, a logic solver (controller) and final control element.

FAULTS & COUNTER STRATEGIES

To ensure that safety systems continue to deliver their intended risk reduction while not eroding uptime, SIS designers have developed a variety of approaches over the years, including redundancy, diversity, diagnostics and testing/inspection. All of these strategies are intended to cope with a range of random, systematic and common cause faults that could result in an SIS not tripping when it's needed—or tripping when it's not.

In the course of designing a new safety system—or evaluating an existing one—each type of fault for every system component (together with the risk reduction strategies employed) must be classified according to its effect on safety system performance.

Broadly speaking, faults are classified as safe or dangerous, and may be overt (apparent in normal operation), detected (as through diagnostics) or revealed (as through proof tests or periodic inspections). For detected and revealed faults, procedures must be in place to ensure that detected or revealed faults are indeed addressed in a timely fashion. The time between proof tests and manual inspections as well as the time needed to execute a repair also affect the overall SIS performance calculations.

Key Types of Faults...

- Random faults include the unpredictable failure of a system component, such as an electronics board.
- Systematic faults are when a combination of conditions results in a reproducible failure of the system and are most often attributable to software issues in programmable safety systems.
- Common cause faults are when a single external influence causes more than one system component or layer of protection to fail.

... and Strategies for Coping

- Redundancy refers to the use of multiple parallel system components configured to back each other up if a failure in one component occurs. Redundancy often is used in conjunction with voting schemes and diagnostics to help verify which between two or among several components is operating correctly in the event of a fault.
- Diagnostics help improve safety system performance by identifying the presence of current or imminent faults in system components and in turn communicating that information back to operations and maintenance personnel before SIS performance is compromised.
- Diversity is most often cited as a means to counter common cause and systematic failures and can refer to redundant functionality within the SIS itself and/or with respect to the basic process control system. Diversity can be applied to sensor technologies, I/O technologies, control and software platforms and even product development teams.
- Testing and inspection of safety system components can be performed manually or in an automated fashion to detect—and importantly, correct—current or imminent faults.

THE SAFETY LIFECYCLE

While other industry-specific codes and standards apply to industrial safety systems, the IEC's 61508 and 61511 international standards are the key documents relevant to safety instrumented systems developed and deployed for use within the global process industries.. The standards originally were developed by industry for industry as technical standards. But in some arenas, compliance already carries the force of law. And even in areas where they are not legislated, the standards' growing acceptance as descriptors of best practices means that non-compliance may have very real liability implications if something does go wrong.

In addition to the functional safety concept, the IEC standards outline a holistic methodology for managing every stage of a safety system's lifecycle—from risk analysis and design engineering through operations, management of change and decommissioning (Figure 3).

Included within the scope of the standards are such topics as alternative methods for gauging the reliability of system components through third-party certifications or actual historical data. And, much like the more familiar ISO 9000 series of quality standards, they strongly emphasize the importance of documentation at all lifecycle stages, such as the need to develop and maintain a clear and unambiguous safety requirements specification.

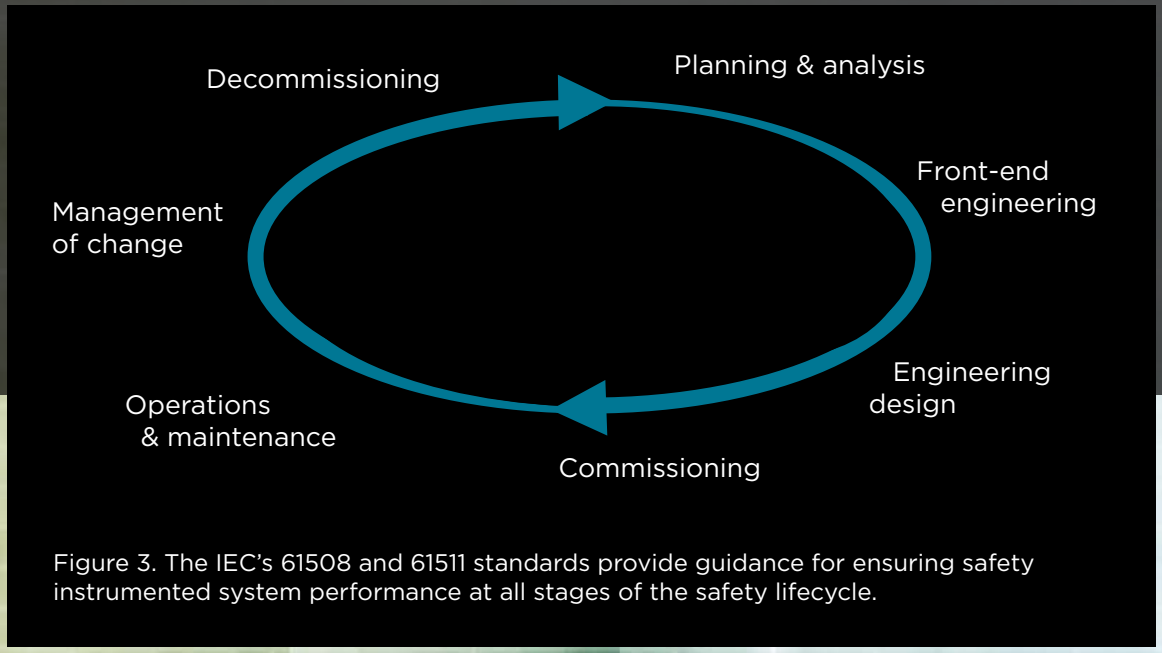


Figure 3. The IEC's 61508 and 61511 standards provide guidance for ensuring safety instrumented system performance at all stages of the safety lifecycle.

INTEGRATED SAFETY

One the most contentious areas in the SIS community today is at the intersection of diversity and integration. Some voices advocate for the continued complete physical separation of safety and control systems—preferably purchased from and developed by different supplier organizations. Others argue that given today's technology and other risk reduction strategies, that logical or functional separation can reduce risk just as effectively as physical separation.

Integration, or at least "interfacing," of safety systems with basic process control systems is in fact not a new practice. Indeed, the standards' non-prescriptive language doesn't rule out even the physical integration of control and safety in the same box or on the same network. Rather, the standards assert that functional safety cannot be compromised by a failure or by maintenance activities associated with the basic process control system. Diagnostics technology, meanwhile, has advanced in its ability to intercept faults, and some of today's integrated safety alternatives feature embedded diversity that reaches all the way back to separate development teams.

Suppliers' commercial interests also are at play. A supplier of historically stand-alone safety systems might argue (understandably) that complete independence provides the greatest assurance of safe operation—and that they have the track record to prove it. Meanwhile, a supplier of both safety and control systems will (understandably) promote comparable safety along with the cost and productivity benefits to be gained by an integrated approach. These systems, too, have a significant and growing installed base that can be referenced. For their part, third-party consultants tend to come down on the side of mathematics: the standards provide a way to quantify and document the risk reduction capability of either approach, and should be the ultimate arbiter from a safety perspective.

Bottom line, risks can be reduced in more than one way, and safe operations do not necessarily come at the expense of increased productivity and reduced complexity offered by integration. Third-party certifications and the existence of "proven in use" data from other similar installations can help make decision-making easier.

ACRONYMS & DEFINITIONS

- **As low as reasonably practicable (ALARP)** sets the bar for the level to which risk is to be reduced to using protective measures.
- **Basic process control system (BPCS)** is the system routinely used by operators to control and interact with the process.
- **Dual modular redundant (DMR)** is a voting scheme based on two redundant safety system components.
- **Equipment under control (EUC)** refers simply to the process equipment in question.
- **Failures modes, effects and diagnostic analysis (FMEDA)** is a detailed methodology used to determine a particular application's safety integrity level.
- **Functional safety** describes the logical separation of safety protections, or functions, from the systems that provide them.
- **Functional safety management system (FSMS)** describes the work processes and systems in place that are designed to maintain safety system protections over time.
- **Hardware fault tolerance (HFT)** refers to the ability of a functional unit to continue to perform its required function in the presence of faults or errors.
- **Hazards and operability study (HAZOPS)** is a detailed methodology for identifying and quantifying risks presented by a manufacturing process.
- **Independent protection layers (IPL)** are layers of risk reduction that operate independently of one another.
- **Layers of protection analysis (LOPA)** is a simplified risk assessment methodology that attributes risk-reduction contribution to various independent prevention and mitigation measures.
- **Probability of failure on demand (PFD)** quantifies the probability that a safety system failure will cause the system to not respond as needed.
- **Process hazards analysis (PHA)** is the overarching methodology for qualifying and quantifying risks presented by a manufacturing or other industrial process.
- **Programmable electronic system (PES)** refers to any microprocessor-based safety or control system.
- **Quad modular redundant (QMR)** is a voting scheme that features two pairs of redundant safety system components.

- **Safety integrity level (SIL)** refers to the level of risk reduction provided by a given safety instrument function, or required by a given application.
- **Safe failure fraction (SFF)** is the portion of safety system failures that do not result in a loss of protective function.
- **Safety instrumented function (SIF)** is the risk-reducing action, or function, of a safety instrumented system loop, divorced from implementation details.
- **Safety instrumented systems (SIS)** are the hardware and software that perform safety instrument functions.
- **Safety requirements specifications (SRS)** spell out in detail the characteristics of various safety instrumented functions required by a given application.
- **Triple modular redundant (TMR)** is a voting scheme based on three redundant safety system components.

MADE POSSIBLE BY ABB

This Control Essentials guide on Safety Instrumented Systems was made possible by ABB, which over the past 30 years has successfully delivered and installed safety systems in more than 55 countries worldwide. With operations on all continents and dedicated safety system teams around the world, ABB provides not only highly-qualified technical resources during project delivery, but also ensures competent local support and service in operation. ABB works hard with end-users to maintain and evolve existing installations, thereby maximizing customer value and ensuring safe plant operation.

Learn more about ABB's safety offering.