Safety Instrumented Systems

Angela E. Summers, SIS-TECH Solutions, LP

Chemical processing involves many different unit operations that must perform within defined boundaries to yield the desired production and quality. Unit operations are controlled using a combination of human, electrical, and mechanical systems. Each control system has failure mechanisms that can result in the process deviating from planned operation with potentially hazardous consequences. Various approaches can be taken to address process hazards. The most fundamental approach uses inherently safer design practices (1) to eliminate or minimize the potential for process hazards to the degree possible. Other approaches involve the implementation of engineered and administrative safeguards that act to achieve or maintain a safe state of the process based on specified conditions.

One of the most common engineered safeguards is a safety instrumented system (SIS). It uses instrumentation to detect process excursions and takes action on the process to prevent further propagation. Over the years, many terms have been used to describe types of SISs. Often, terms are used which facilitate more rapid understanding of the system's specific purpose, such as safety critical systems, high integrity protective systems, emergency shutdown systems and safety interlocks. Because they have a wide variety of functions and applications, SISs are generally designed to address specific process hazards.

An international standard, IEC 61511 (2) provides an extensive set of requirements covering the SIS lifecycle. Some specialized functions are also covered by industry practices that dictate unique requirements for specific applications. IEC 61511 relies on a quality control process to ensure that the SIS achieves the performance necessary to adequately reduce potential risk in the operating environment. The performance target for this quality process is defined in the standard as the safety integrity level (SIL), which is related to the SIS's average probability of failure on demand (PFD_{AVG}). The standard establishes four discrete ranges for benchmarking the performance of each function in the SIS, where SIL 4 is the highest and SIL 1 is the lowest (Table 1):

Table 1: Safety Integrity Level Related to SIS Risk Reduction and Average Probability of Failure on Demand

Safety Integrity Level (SIL)	Target Risk Reduction	Target Average Probability of Failure on Demand (PFD_{AVG})
4	>10,000 to ≤100,000	$<10^{-4}$ to $\geq 10^{-5}$
3	>1,000 to ≤10,000	$<10^{-3}$ to $\geq 10^{-4}$
2	>100 to ≤1,000	$<10^{-2}$ to $\geq 10^{-3}$
1	>10 to ≤100	$<10^{-1}$ to $\geq 10^{-2}$

SIS-TECH

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

Achieving these performance ranges requires that the SIS be rigorously designed and managed. An effective management system uses a systematic approach to manage the risk throughout the process equipment life. With early consideration of process hazards, the risk reduction strategy can be tailored to meet operating, maintainability and reliability goals. A strong, sustainable strategy ensures that the process design, SIS design, and operation and maintenance procedures are successfully integrated to achieve high integrity and reliability. A proactive approach monitors for behaviors, errors, and failures that are leading indicators for potential releases of highly hazardous chemicals. Finally, the management strategy should incorporate periodic assessments of existing equipment performance to identify opportunities for further reduction of risk, thus yielding safer operation.

Lifecycle Approach

IEC 61511 covers a wide range of chemical process operations. Due to its broad scope, the standard has many general requirements addressing the complete lifecycle of the SIS, starting with the identification of SIS requirements in the risk assessment and ending when the SIS is decommissioned. While there are many different ways of representing the lifecycle, a simple four step approach can be followed:

1. Define a risk-management strategy - establish a facility management system for how SISs are identified, designed, inspected, maintained, tested, and operated to achieve safe operation and perform a hazard and risk analysis to identify where SISs are needed and their target SIL

2. Implement the strategy - develop a design basis to achieve the target SIL and execute the detailed design to meet the requirements

3. Validate, start-up, operate and maintain the strategy - implement the SIS following the design basis and detailed design documentation and define what is required of operation and maintenance personnel to sustain the SIL

4. Manage changes to the strategy - ensure the SIS meets the target SIL by monitoring operation, inspection, test, and maintenance records and making changes as necessary to improve its performance

The lifecycle approach can be used to address any risk, whether safety, environmental, asset or business related. Many governments require the use of recognized good engineering practices in the design and management of the instrumented systems that maintain safe operation in the process industry. Local regulations, applicable codes, or insurance practices may require the use of specific good engineering practices. Consequently, the management strategy should incorporate current good engineering practices and continuous improvement activities to provide a comprehensive program.

1. Define a risk-management strategy

A chemical process operator has cradle-to-grave responsibility for a facility's safe operation. Risk derived from the operation of chemical processes can be successfully and cost effectively managed throughout the life of the process. The earlier a risk-management strategy is defined, the better it will work and the less it will cost. Identify process

hazards early in the project planning and process design, so measures can be implemented to reduce or eliminate hazards through inherently safer design (3).

Once process design is complete, the remaining risk will need to be managed for the life of the process equipment. Although inherently safer design may increase the initial capital cost, it substantially reduces long-term risks and their associated costs. Safety systems should only be applied when inherently safer design becomes impractical, because safety equipment requires long-term investment in administrative, operating and maintenance activities.

To develop the risk-management strategy, start with a process hazards analysis (PHA) and review the process design and its control, operation and maintenance practices. Select a multidisciplinary team with expertise in these areas, and use an accepted hazard-evaluation procedure (3), such as a hazard and operability (HAZOP), what-if, or checklist analysis, to determine how process deviations from intended operation lead to process hazards.

Identify the causes or conditions that lead to deviations. For example, low flow can be caused by the failure of the flow control loop. Events can be caused by a single failure or by multiple failures. Ensure that the identified causes are the minimum that will lead to the process deviation. The most common initiating causes are related to control system failures, which can happen multiple times over the life of the process. If the consequence is significant, safety systems are generally required to address identified process hazard.

Estimate the severity of the consequence, taking into account likely event conditions. Occupancy during an abnormal event is typically not the same as during normal operation. If abnormal operation occurs, what are the responsibilities of the field operators or maintenance crew? If a safety alarm goes off, is the field operator expected to respond locally? The slower the event, the more likely there will be field response and higher occupancy, possibly including supervisory, operations and maintenance personnel.

The process risk of a particular event is related to how often the event could occur and the severity of the consequences if it does. Compare the process risk to facility risk criteria (4) to determine if the risk is tolerable or whether additional protection is required to reduce it below the defined criteria. Residual risk represents a likelihood that an unacceptable consequence could occur, so drive it as low as reasonably practicable.

To lower risk, implement a defense-in-depth strategy in which one or more independent protection layers (IPLs) act to interrupt the event sequence. IPLs can be implemented using a variety of systems, such as safety alarms, pressure relief devices, and SISs. Independence is achieved when the IPL operation is not affected by the occurrence of the initiating event or by the failure of other IPLs. Verify during the PHA that identified IPLs are designed to detect and respond to the hazardous event in a timely manner. Seven core attributes of an IPL must be managed rigorously throughout the life of the process: independence, functionality, integrity, reliability, auditability, access security, and management of change.

In addition to addressing the risk arising from identified process deviations the risk-reduction strategy should also address secondary consequences associated with the operation of the IPLs, such as reduced production, shutdown, and flaring. Secondary consequences can be thought of as the side effects of the risk-reduction strategy — each time an IPL takes action, there is an effect on the process. Determine

the cost of the spurious operation of IPLs to establish the maximum acceptable spurious activation rate. The final risk-reduction strategy should ensure that the side effects are acceptable or properly managed.

2. Implement the strategy

Document the SIS design basis and maintain it under revision control as process safety information for the life of the system. All SISs are unique in that each is designed to address a specific hazardous event. Two SISs may be similar, but no two are exactly the same. The SIS design basis should address the following:

- Detection of and response to potential hazardous events
- Selection of equipment based on prior history
- Fault detection, such as diagnostics and proof testing
- Fault tolerance against dangerous failures
- Procedures for maintenance and test, including the use of bypasses
- Operation and maintenance procedures required when SIS equipment is out of service
- Emergency shutdown capability if the SIS fails to take action as expected
- Start-up and shutdown of the process equipment

The SIS design basis is covered by IEC 61511 (Clauses 10 through 12). ISA Technical Report TR84.00.04 (6) gives extensive guidance on design requirements for the hardware and software used to implement SISs. It is possible to develop uniform facility practices for similar applications to promote consistency in SIS implementation, as well as to reduce training costs and the potential for human error.

SISs operate best when they are based on simple logic. For example: “When the high-pressure alarm initiates, open the pressure control vent,” or “when high temperature occurs, close the feed valve.” This logic is simple enough that it can be implemented in a hard-wired system. Programmable logic controllers (PLCs) are complex systems with the potential for large numbers of unidentified random and systematic failures. Because of the unknown and unpredicted failures associated with PLCs, IEC 61511 (Clause 11.5) requires the PLC to be safety-configured for SIS applications. It also requires that an SIS be designed to be separate and independent from the basic process control system to provide protection against postulated control system malfunctions. Safety configuration addresses the widely known failure modes of the inputs, main processors, communications, utilities (e.g., power, instrument air) and outputs. This requires additional diagnostics and fault-tolerance capabilities that are generally not provided for control systems, but are implemented in systems designed specifically for safety applications.

IEC 61511 (Clause 11.5) requires implementation of a user approval process to ensure that field equipment has an established history of performance in a similar operating environment and that its failure mechanisms are understood and accounted for in the design, operation and mechanical integrity practices. An SIS must be sufficiently robust to withstand environmental stresses and provide the required integrity and reliability. For each installation, define the operating environment conditions that impact SIS equipment selection, such as:

- process composition, e.g., solids, salts, or corrosives
- process operating conditions, e.g., extremes in temperature, pressure, or vibration
- external conditions, e.g., winterization needs or hazardous area classification

The SIS must be capable of detecting the process hazard and responding in time to prevent the hazardous event. How much time the SIS has to respond depends on the process dynamics and the conditions initiating its actions. When multiple engineered safeguards are implemented to address an event, they are often designed to operate in a preferred sequence. The available process safety time for any given safeguard starts when it is required to take action and ends at the point where the event can no longer be prevented. In many applications, it is desirable that each safeguard be capable of completing its action prior to the initiation of the next in the sequence; the goal being to achieve or maintain a safe state with the safeguard that causes the least disruption. Regardless, the need to allocate a limited process safety time to multiple safeguards leads to less time being available for safeguards operating later in the sequence.

The SIS begins protective action at a defined process condition or setpoint. The SIS's response speed is limited by the sensor dynamics and overall instrument loop response time, which can be significantly affected by the process design itself. The shutdown lag can be long (seconds to minutes), particularly in applications where there is significant retained mass or energy that must be removed. It can also be short (milliseconds), such as stopping a motor. Given the degree of uncertainty in the process safety time, the SIS should be capable of completing its action within one-half of its allocated process safety time.

Assess potential common causes in the process support systems, such as power, communications, instrument air, cooling water and hydraulic power. Ensure that SIS support systems are designed to take the affected equipment to a specified safe state as necessary to achieve the required integrity. Approval of non-fail-safe design should consider the impact on the risk-reduction strategy assumptions, the type of SIS, the support system integrity, and alternative means to achieve a safe state. Human and cyber access to any SIS should be sufficiently restricted using administrative procedures and physical means to ensure that changes to the SIS are approved through a change management process.

IEC 61511 Clause 11.9 also requires that the SIS integrity be verified quantitatively. Ensure that the selected equipment is fit for use in the operating environment, that the subsystems meet minimum fault-tolerance requirements and that the system achieves the required functionality and integrity. SIS equipment should be included in a mechanical integrity program that seeks to maintain the SIS in the "as good as new" condition. Mechanical integrity includes a variety of activities, such as inspection, maintenance, calibration, repair/replacement, and proof testing. An equipment list should be maintained that identifies SIS equipment by a unique designation and includes the required inspection and proof-test interval necessary to ensure the equipment remains fit for service.

The initial proof-test interval is determined based on offline test opportunities, relevant regulations, equipment history in similar operating environments, manufacturer's recommendations, and integrity requirements. When proof-testing is required more frequently than scheduled outages, online proof-test and repair facilities will be necessary.

If the online activity requires bypassing, document the measures or safeguards put in place to compensate for the loss of SIS capability during the out of service period. Assess bypass activities and potential hazards to define the compensating measures and the maximum allowable repair time. Implement bypass alarms when practical, and ensure operating procedures adequately communicate bypass activity

across operator shift changes, e.g., re-initiate bypass and safety alarms across shifts. Ensure that operators know the state of SIS equipment and what to do if abnormal operation occurs.

3. Validate, start-up, operate and maintain the strategy

Validation has traditionally been referred to as a site acceptance test (SAT) because its successful completion results in the formal acceptance of the SIS by the plant operations staff. The equipment is proven to work as required, and from this point forward, changes are reviewed and approved according to the plant's change management practices. Validation is performed after instrument calibration and loop checks have been completed. A validation plan is developed to ensure orderly execution and thorough documentation and resolution of any findings. IEC 61511 (Clause 15) addresses validation of SISs.

Validation demonstrates that the installed SIS operates according to the design basis and that appropriate documentation is in place to support its long-term management. An input-to-output test is used to prove that the SIS functions properly and that the SIS equipment interacts as intended with other systems, such as the BPCS and operator interface. The SAT also provides an opportunity for a first-pass validation of the operating and maintenance procedures. Validation must be completed prior to the initiation of any operating mode where a hazardous event could occur that would require the operation of a new or modified SIS. Some users require that validation be repeated after any major process outage or shutdown.

Clearly define the safe operating limits in the operating procedures, the consequences of deviating from these limits, and the proper action to take when these limits are exceeded. The operator's response to an indication, alert, alarm, or incident is dictated first by procedures and training and then by experience. Audit the operator's response to SIS diagnostic and safety alarms. IEC 61511 (Clause 16 and 17) addresses operator and maintenance procedure requirements for SISs. Procedures should include:

- a description of the hazardous events being prevented
- a description of the SIS
- the appropriate operator response to detected SIS equipment failure and provisions for operation with detected faults (i.e., compensating measures)
- coordination/communication with maintenance during any troubleshooting, repair or test activity
- conditions under which it is safe to reset an SIS
- use of start-up bypasses and the process conditions to be monitored during start-up
- the expected operator response when safety alarms are received and the setpoints for those alarms
- trip setpoints, the expected safe state when a trip is completed, and the form of trip notification (if provided)
- expected operator actions if a safe state is not achieved
- the "never exceed, never deviate" process conditions that require manual shutdown

Installed safety equipment is subject to the same operational stresses as control equipment. However, when control equipment fails, the failure can be detected because the process behaves abnormally. In contrast, safety equipment typically operates on demand only, i.e., when abnormal condition occurs, so failure may not be detected until it is required to act. Equipment often demonstrates a failure rate over time that follows a so-called bathtub curve.

Early failures are caused by manufacturing, assembly, test, installation and commissioning errors. Many early failures are the result of rough handling, improper pre-installation storage, poor installation practices, or sloppy construction practices. Rigorous inspection, commissioning and validation activities are necessary to identify and correct these failures.

The wear-out period is characterized by an increasing failure rate over time. Poor mechanical integrity practices have been cited as a primary cause of equipment failure. Preventive maintenance can extend equipment useful life and improve its reliability. Mechanical integrity records provide data that equipment is being maintained in the "as good as new" condition and justify its continued use. Consequently, maintenance personnel must be trained on the activities necessary to ensure equipment integrity.

Periodic proof-tests should be performed at a frequency sufficient to detect the transition from the useful life period to the wear-out period, so that the need for equipment replacement or upgrade can be identified and planned. Equipment failure should be investigated using root-cause analysis to reduce or eliminate failure causes. The proof-test interval should be periodically evaluated based on plant experience, hardware degradation, demonstrated software reliability, etc., and in the event of repeated failures, the interval should be shortened as necessary to ensure expedient failure detection.

Execute proof-tests using operation and maintenance procedures that ensure the test is completed correctly, consistently and safely. Proof-tests should determine the "as-found/as-left" condition for all defined operating modes. Documentation should be traceable to the procedure, equipment, and person performing the test. Identify and assess deviations from the design basis and equipment specification, e.g., undocumented changes or accelerated degradation. Use the proof-test results and findings to train personnel and to verify procedure clarity and completeness.

Real-world risk-reduction is demonstrated by mechanical integrity data. The records associated with any SIS must show that the equipment can operate as specified during all intended operating modes. Failure tracking and analysis is essential to close the safety lifecycle. Repeated failures likely indicate that the installed equipment is not capable of meeting the performance requirements. Use root-cause analysis to determine why metrics are trending in the wrong direction, in order to implement action plans that improve the management system, equipment, procedures, and personnel training. Identify special and previously unknown failures and communicate these to personnel, ensuring that lessons learned are not hidden in mechanical integrity records.

4. Manage changes to the strategy

A successful risk-management strategy accepts that humans are involved in every aspect of an SIS's lifecycle. Therefore, the integrity claimed for any SIS is limited by the quality management system that identifies and seeks to eliminate flaws in the system. Human error must be reduced to the point where it does not significantly impact system integrity. Assurance of personnel competency is key.

Knowledge evolves over time as research and development yields operational enhancements to process facilities. Events involving abnormal operation may identify weaknesses in the risk-reduction strategy, leading to the need for more safeguards and improved performance metrics. New ideas identify ways to lower risk further.

Periodically evaluate existing SIS against current criteria and industry practices to determine whether equipment is designed, maintained, inspected, tested and operating in a manner that would hold up to public scrutiny. Use a change management process to initiate, document, review and approve changes to SISs other than replacement-in-kind. Evaluate changes to the process and its equipment to determine their potential impacts on the approved SIS design basis prior to implementing the change. Personnel need to understand when hazards analysis is required and why tracking changes is important.

Update documents to "as-built" status, incorporating changes made since the last formal drawing/document revision. Maintain documentation under revision control for the life of the equipment. Documentation should be traceable to the process hazards analysis and should be auditable.

Final thoughts

An effective process safety management system uses a systematic approach throughout the process equipment's life. With steadfast effort, the risk-management strategy can be tailored to meet operating, maintainability and reliability goals. A strong, sustainable strategy ensures that the process design, SIS design, and operation and maintenance procedures are rigorously managed to achieve high integrity and reliability with minimum opportunity for common-cause failure. Over the life of the equipment, this approach will reduce cost and improve process safety.

Literature Cited

1. Center for Chemical Process Safety (CCPS), *Inherently Safer Processes, Second Edition*, American Institute of Chemical Engineers, New York, NY (Dec. 2008).
2. International Electrotechnical Commission, IEC 61511, Geneva, Switzerland (2003).
3. Center for Chemical Process Safety (CCPS), *Guidelines for Hazard Evaluation Procedures,* Third Edition with Worked Examples, American Institute of Chemical Engineers, New York, NY (2008).
4. Center for Chemical Process Safety (CCPS), *Guidelines for Developing Quantitative Safety Risk Criteria,* American Institute of Chemical Engineers, New York, NY (2009).
5. Center for Chemical Process Safety (CCPS), *Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, New York, NY (2007).
6. International Society of Automation, *Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511)*, ISA TR84.00.04, ISA, Research Triangle Park, NC (2005).

ANGELA E. SUMMERS, PhD, is president of SIS-TECH (12621 Featherwood Dr., Suite 120, Houston, TX 77034; Phone: (281) 922-8324; E-mail: asummers@sis-tech.com; Website: www.sis-tech.com) and has 20 years of experience in safety instrumented systems (SIS), process engineering, and environmental engineering. She is a licensed professional engineer in Texas, is a member of AIChE, ISA, IEC and ANSI, and is an active participant in industrial standards committees. She has published over 50 papers, contributed chapters to engineering handbooks, and edited technical reports and books on topics related to process safety and instrumented system design. She received her PhD in chemical engineering from the Univ. of Alabama, MS in environmental engineering from Clemson Univ. and BS in chemical engineering from Mississippi State Univ.