Perry's Handbook of Chemical Engineering, Edition Fall 2007
Safety Instrumented Systems

Angela E. Summers, Ph.D., President, SIS-TECH Solutions, LP, Member American Institute of Chemical Engineers, Member Instrumentation Systems and Automation Society

Table of Contents

References: *Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, NY, (exp pub 2006); ISA TR84.00.04, *Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511)*, Instrumentation, Systems, and Automation Society, NC (ex pub 2005); ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, Instrumentation, Systems, and Automation Society, NC, (2004); IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* International Electrotechnical Commission, Geneva, Switzerland, (2003).

General References: *Guidelines for Hazard Evaluation Procedures*, *Second Edition with Worked Examples*, American Institute of Chemical Engineers, NY, (1992); *Layer of Protection Analysis: A Simplified Risk Assessment Approach*, American Institute of Chemical Engineers, NY, (2001); ISA TR84.00.02, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*, Instrumentation, Systems, and Automation Society, NC (2002).

Introduction

The chemical processing industry relies on many types of instrumented systems, e.g., the basic process control systems (BPCS) and safety instrumented system (SIS). The BPCS controls the process on a continuous basis to maintain it within prescribed control limits. Operators supervise the process and, when necessary, take action on the process through the BPCS. The SIS detects the existence of unacceptable process conditions and takes action on the process to bring it to a safe state. In the past, these systems have also been called emergency shutdown systems, safety interlock systems, and safety critical systems.

In 1993, the Center for Chemical Process Safety (CCPS) published "*Guidelines for Safe Automation of Chemical Processes"* (referred to as *Safe Automation*). *Safe Automation* provides guidelines for the application of automation systems used to control and shutdown processes. The popularity of one of the risk analysis methods presented in Safe Automation led to the publication of 2001 Concept Series book from CCPS, "*Layer of Protection Analysis: A Simplified Risk Assessment Approach*." This method identifies those barriers to process incidents that meet specific attributes considered essential for them to be classified as independent protection layers.

The Instrumentation, Systems and Automation Society (ISA) published the standard ANSI/ISA 84.01-1996, documenting the good engineering practice for the design, operation, maintenance, and testing of SIS. The standard establishes a numerical benchmark for the SIS performance known as the safety integrity level (SIL) and provides requirements on how to design and manage the SIS to achieve the target SIL.

Safe Automation and ANSI/ISA 84.01-1996 served as significant technical references for the first international standard, IEC 61511, issued by the International Electrotechnical Commission (IEC). In the United States, IEC 61511 was accepted by ISA as ISA 84.00.01-2004, replacing the 1996 standard. In 2004, the European Committee for Electrotechnical Standardization (CENELEC) and the American National Standards Institute (ANSI) recognized IEC 61511 as a consensus standard for the process industry. IEC 61511 covers the complete process safety management lifecycle. With its adoption, this standard serves as the primary driving force behind the work processes followed to achieve and maintain safe operation using safety instrumented systems.

It is important that personnel understand how to achieve safe operation, but not at the exclusion of other important considerations, such as reliability, operability and maintainability. The chemical industry has also found significant benefit to plant productivity and operability when SIS work processes are used to address other instrumented protective systems (IPS), such as those mitigating potential economic and business losses. The CCPS book (2007), "Guidelines for Safe and Reliable Instrumented Protective Systems," discusses the activities and quality control measures necessary to achieve safe and reliable operation throughout the IPS lifecycle.

Hazard & Risk Analysis

Consideration should be given to identifying process hazards as early as possible in the process equipment design, so that measures can be taken to reduce or eliminate the hazards. Inherently safer design strategies, such as minimize, substitute, moderate, and simplify, should be implemented. For example, the process risk is reduced if a less toxic or less flammable material is used. Or, a simple change in a pump specification may eliminate a potential overpressure scenario.

When it is no longer practical to reduce the risk further by process design modification, independent protection layers (IPLs) are used to mitigate the remaining process risk. IPLs meet the necessary rigor associated with seven core attributes: independence, functionality, integrity, reliability, auditability, access security, and management of change. There are two critical activities to be completed during the risk assessment phase. First, the safety functions (i.e., those functions that detect and respond to process hazards) are identified using an accepted risk analysis methodology. Second, each safety function is allocated to an IPL that is designed and managed to achieve the required risk reduction.

Hazard analysis involves a review of the process design and its control, operation, and maintenance practices. The review is conducted by a multi-disciplinary team with expertise in the design and operation of the process unit. The team uses a systematic screening process to determine how deviations from normal operation lead to process hazards. The risk analysis identifies areas where the process risk is too high, requiring the implementation of safety functions to mitigate the risk. The team's objective is to reduce below the owner/operator's risk criteria.

Process risk is defined by the frequency of the occurrence and the potential consequence severity of the process hazard. To define the frequency, the initiating events (e.g., single causes or multiple causes/conditions) are identified for each process hazard, and their frequency of occurrence is estimated. The consequence severity is the logical conclusion to the propagation of the process hazard if no protection layers are implemented as barriers to the event.

The gap between the process risk and the owner/operator's risk criteria establishes the requirements for risk reduction. The risk gap can be managed by a single safety function or by multiple functions allocated to protection layers. The team defines the risk reduction that must be provided by each safety function and allocates the safety function to a protection layer that is designed and managed to achieve the allocated risk reduction.

When the safety function is allocated to the SIS, it is a safety instrumented function (SIF). The risk reduction allocated to the SIF defines its target safety integrity level (SIL). This target is related to the SIF probability of failure on demand (PFD), e.g., SIL 1 (PFD range: 0.01 to 0.1), SIL 2 (PFD range: 0.001 to 0.01), SIL 3 (PFD range: 0.0001 to 0.001), and SIL 4 (PFD range: 0.00001 to 0.0001).

The identification of safety functions continues until the process risk is reduced to meet the risk criteria. When there is insufficient risk reduction provided by the current or planned design, the team makes recommendations for process design changes (e.g., inherently safer design), improvement to existing functions, or the design and implementation of new functions. These recommendations are generally

prioritized based on the magnitude of the gap between the mitigated process risk (i.e., risk considering the presence of existing functions) and the risk criteria.

Design Basis

In the design phase, the project team works together to create an SIS design basis that achieves the risk reduction strategy outlined in the risk assessment findings. This strategy relies, in part, on the implementation of SIFs to reduce specific process risk. The SIF uses dedicated devices, including processsensors that detect the process hazard, a logic solver that decides what to do, and final elements that take action on the process. Often, a single logic solver implements multiple SIFs, so the potential for common cause failures between SIFs should be considered during design.

The SIS is normally designed to fail-safe on loss of power and takes action only when the process demands that it do so. These demands often occur when safe operating limits are exceeded due to BPCS failures. Therefore, the SIS is designed and managed to be independent of the BPCS in terms of its hardware and software and its user interfaces, such as operator, maintenance, and engineering interfaces.

Systematic errors can occur anywhere in the design and implementation process or during the operational life of an SIS device. These errors put the SIS on the path to failure in spite of the design elements incorporated to achieve robust hardware and software systems. Systematic errors are minimized using work processes that address potential human errors in the SIS design and management (e.g., programming errors or hardware specification errors).

Random hardware failure can occur throughout the device life as components age in the environmental conditions of the process unit. These failures can cause a device to fail dangerously, i.e., it cannot perform as required. These failures are estimated by examining the dangerous failure modes of each device and their frequency of occurrence. The resulting failure rate is used to estimate the PFD of the SIS considering its specific devices, redundancy, diagnostics, common cause failure potential, and function test interval. The PFD is then compared to the target SIL assigned during the H&RA phase to determine whether the design is adequate.

The design basis includes the process requirements specification and the safety requirements specification. The process requirements specification is typically developed by process engineering, with input from operations personnel. The process requirements are provided to the instrumentation, electrical, or controls systems personnel to develop the safety requirements specification with input from operations and maintenance personnel.

Process Requirements Specification

Process engineering uses the H&RA findings, process design information, and operations input to:

- Define safe state, including safety-related and non-safety-related actions.
- Define reliability requirements necessary to achieve desired process unit uptime performance.

- Define operability requirements for modes of operation, such as start-up, reduced rates, maintenance modes, shutdown, etc.
- Identify windows of opportunity for SIS testing.
- Define process-related parameters.
- Define human-related parameters.

Guidance can be found in the CCPS book (2007) "*Guidelines for Safe and Reliable Instrumented Protective Systems*" related to the development of the process requirements specification.

Safety Requirements Specification

The instrumentation and electrical (I&E) requirements are developed to meet the intent of any H&RA findings and the process requirements. The design documentation should establish a clear connection between each process hazard and the design of its SIFs. I&E personnel should meet with the process engineering representative responsible for the process requirements to ensure that its intent is understood.

I&E design focuses on achieving the target SIL through careful selection of the devices (e.g., user approved for safety), use of redundancy, on-line diagnostics and frequent function testing. The ISA technical report, ISA TR84.00.04, gives extensive guidance on design requirements for the hardware and software systems used to implement the SIS. Application-specific standards by organizations such as American Society of Mechanical Engineers (ASME), American Petroleum Institute (API), and the National Fire Protection Association (NFPA) may provide additional requirements and guidance.

There is often quite a bit of give and take between the process requirements and I&E requirements in the early stages of the project. For example, the ideal process measurement may not be practical in the existing installation. At all times, it should be recognized that the goal of the design is to mitigate the process hazard.

Engineering, Installation, Commissioning and Validation (EICV)

This phase involves the physical realization of the design basis, which is developed in response to process risk identified in an H&RA study. The bulk of the work in this phase is not a process engineering effort. Detailed engineering, installation and commissioning is generally an I&E function. However, this is where the assumptions and requirements developed by the process engineer are put into practice and validated.

Validation of the SIS functionality is performed as part of a Site Acceptance Test (SAT). Validation involves a full functional test that demonstrates that the SIS actually works in the real world installation. It proves the SIS devices execute the logic according to the specification and ensures the SIS and its devices interact as intended with other systems, such as the BPCS and operator interface. From a systematic error standpoint, the SAT also provides an opportunity for a first-pass validation of the procedures developed for the operating basis (see next section).

Pre-start-up Safety Review (PSSR) approval of the SIS establishes the point where the SIS design and construction is considered complete. All documentation should be formally updated to 'as-built' status, incorporating any modifications made since the last formal drawing/document revision. Any deviation from the approved design basis should be reviewed and approved by appropriate parties prior to change implementation.

Operating Basis

As the SIS engineering design nears completion, the resources and skills of plant operations should be considered. At some point, the SIS is turned over to operations and maintenance personnel, who must be trained on the new SIS and on their responsibilities. Consequently, thought should be given to the content and depth of the information that must be communicated to various personnel. This is especially important as the responsibility for the SIS transitions from the project team to operations and maintenance control.

The process engineer is responsible for defining the content of SIS operating procedures, which should cover SIS specific information (e.g., set points, SIS actions, and the hazard that is being prevented with SIS), the correct use of bypasses and resets, the operator response to SIS alarms and trips, when to execute a manual shutdown, and provisions for operation with detected faults (e.g., compensating measures). These procedures, along with analogous ones developed by maintenance/reliability engineering for maintenance activities, make up the backbone of the operating basis.

Since a device can fail at any time during its life, periodic proof tests are performed to demonstrate the operation of the SIS. Proof tests are covered by operation and maintenance procedures that ensure that the test is done correctly, consistently, and safely and that the device is returned to a fully operational state after test. Each test serves as an opportunity for personnel to see the SIS in action and to validate the procedures associated with its operation.

Proof testing is required for all SISs. It is used to demonstrate that the devices are operating as specified and are maintained in the "as good as new" condition. Failures found during testing indicate gaps in the mechanical integrity program, necessitating root cause investigation and corrective action.

Glossary

Basic Process Control System (BPCS) – System that responds to input signals from the process, its associated equipment, other programmable systems, and/or from an operator and generates output signals causing the process and its associated equipment to operate in the desired manner. The BPCS is commonly referred to as the "control system"

Compensating Measures – Planned means for managing process risk during periods of process operation with known faults or increased risk.

Core Attribute – One of seven fundamental underlying properties that describe a protection layer. The core attributes are: independence, functionality, integrity, reliability, auditability, management of change, and access security.

Protection Layer – Mechanism to reduce process risk, which may be automated or initiated by human action. A protection layer is a device, system, or action that is capable of preventing a hazard scenario from proceeding to the undesired consequence severity regardless of the initiating event occurrence (or its consequences) or the failure of any other protection layer.

Safety Instrumented Function (SIF) – A protective function allocated to the safety instrumented system layer with a safety integrity level (SIL) necessary to achieve the desired risk reduction for a specified hazard scenario. The SIF brings the process to a safe state either automatically or by trained operator response to an alarm.

Safety Instrumented System (SIS) – An instrumented system composed of any combination of sensors, logic solvers, and final elements. A safety instrumented system may implement multiple safety instrumented functions.

Safety Integrity Level (SIL) – Discrete level (one out of a possible four SIL categories) used to specify the probability that a SIF will perform its required function under all operational states within a specified time period.