SAFETY CONTROLS, ALARMS, AND INTERLOCKS (SCAI)

Table of Contents

Page

List of Figures

List of Tables

1.0 SCOPE

This data sheet contains loss prevention recommendations for operations and equipment where safety instrumentation and control systems are present or needed. The goal of this document is to provide risk-reduction solutions from a property protection and business continuity perspective.

For the purposes of this document, a safety instrumentation and control system is defined as a combination of hardware systems and software programs designed to prevent, control, or mitigate hazardous events and/or take a process to a safe state when predetermined conditions are breached.

This data sheet applies to safety controls that are integrated into the primary control system, as well as dedicated safety instrumented systems (SIS). This data sheet also applies to safety-critical alarms that require manual intervention.

This data sheet does **not** cover the following:

A. Detailed design of safety instrumentation and control systems.

B. ICS communication networks and cyber hazards (refer to Data sheet 7-110, *Industrial Control Systems*).

C. Information technology (IT) and data storage/retrieval systems used for general business (e.g., systems intended to send and receive email, systems with open access to the internet).

D. Basic criteria to be considered with respect to location, construction, and protection of control or equipment rooms. Guidance on this can be found in Data sheet 7-110, *Industrial Control Systems*.

E. Operational alarms that occur during the normal process of operations.

F. The design of systems and processes from a human factor perspective. This is performed by those specially trained for such functions, including system designers, human performance specialists, and psychologists.

This data sheet provides general guidance for safety instrumented control systems. If data sheets exist for specific equipment or processes, the recommendations in those documents supersede the guidance presented here.

1.1 Hazards

Safety controls, alarms, and interlocks (SCAI) are process safety safeguards implemented with instrumentation and controls whose function is to bring about or maintain a safe state of operation for a process or piece of equipment in response to a hazardous event.

There are various subcategories of SCAI, including safety-critical controls, safety alarms, safety interlocks, and safety instrumented systems (SIS), all possessing certain common elements.

These systems range in complexity and are required to operate with a high degree of reliability to provide the desired risk reduction. Often, human interaction may be part of a SCAI system. Such interaction in the system requires additional scrutiny to ensure the system can provide the level of risk reduction it was designed for.

Failure of these systems can often lead to fires, explosions, damage to people and equipment, and other impacts such as contamination of property and the environment. This is due to the fact that the layer of protection these systems were installed to provide is lost upon their failure, allowing the undesired event to occur.

1.2 Changes

July 2023. Interim revision. The following major change was made:

A. Relocated guidance for Safety Instrumented System (SIS) used in lieu of overpressure protection and High Integrity Pressure Protection Systems (HIPPS) to Data Sheet 7-49, *Emergency Venting of Vessels.*

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

Safety controls, alarms, and interlocks (SCAI) are process safety safeguards (typically automation) whose function is to achieve or maintain the safe state of a process or equipment in response to a hazardous event.

There are many terms used to further classify SCAI systems, with the four most common being safety controls, safety alarms, safety interlocks, and safety instrumented systems (SIS). Additional guidance on these can be found in Section 3.0.

The terminology used in this data sheet is consistent with IEC 61511:2016, *Functional Safety - Safety Instrumented Systems for the Process Industry Sector*, a common industry standard.

Use FM Approved equipment, materials, and services whenever they are applicable and available. For a list of products and services that are FM Approved, see the *Approval Guide*, an online resource of FM Approvals.

2.2 Equipment and Processes

2.2.1 Determination of Necessary Safety Functions

2.2.1.1 Adhere to the recommendations in FM Property Loss Prevention Data Sheets for specific processes, hazards, and/or equipment as applicable.

2.2.1.2 Develop critical safety functions and controls using one of the following options:

A. Use a recognized industry standard that considers the relevant hazards of the process or piece of equipment. This would include any nationally- or internationally-recognized organization that has published codes, standards, and recommended practices, such as NFPA, ANSI, API, ASME, ISA and IEC.

B. Conduct a detailed process hazard analysis (PHA) that identifies safety functions and associated devices in accordance with the guidance in Data Sheet 7-43, *Process Safety*.

2.2.1.3 Verify the necessary safety functions are provided, at a frequency commensurate with the hazard(s). This may include revalidation of a process hazard analysis (PHA) or a review of more recent versions of a code or standard. For high-hazard processes, refer to the guidance in Data Sheet 7-43, *Process Safety*.

2.2.2 Implementation and Design Considerations

2.2.2.1 Design the SCAI system to accomplish all of the safety functions identified in Section 2.2.1.

2.2.2.2 Design the SCAI system with a reliability commensurate with the hazards. If a specific system's reliability is needed, use a dedicated safety instrumented system (SIS) designed in accordance with ISA/IEC 61511.

A. Design, build, and certify SIS systems using qualified specialists. SIS systems are also referred to as safety integrity level (SIL) rated.

B. Provide individual SIS elements, including sensors, logic solvers, and final elements, with a reliability as defined by IEC 61508.

C. Anticipate environmental conditions that could affect sensitive electronic equipment, such as dirty air, temperature excursions, excessive vibrations, electromagnetic interference, fire, blast, and dropped objects when selecting SIS equipment. Take into account the required survival and operating modes of systems following a major incident. (For additional loss prevention features of the control or equipment room containing SIS hardware, see Data Sheet 5-32, *Electronic Data Processing Systems*.)

D. In establishing the requirements of any safety instrumented system, do not consider operator intervention as an independent protection layer (IPL) for the purposes of reducing the required safety integrity level (SIL) of the SIS.

2.2.2.3 Where possible, design components and systems to fail safe.

2.2.2.4 Provide a process to identify components of the SCAI with unique, permanent labels. This can be done via drawings and documentation such as P&IDs, electrical diagrams, and valve/instrument lists.

2.2.2.5 Ensure there is no single point of failure for critical links (e.g., from physical damage, fire, loss of utilities). Provide redundant links with diverse routing as required by the PHA. Where practical, avoid high risk or vulnerable areas for the installation of cables for “energize to execute” circuits (e.g., high EMI, high voltage). Additional guidance for the protection of cables and cable trays can be found in Data Sheet 7-14, *Fire Protection for Chemical Plants*, and Data Sheet 5-31, *Cables and Bus Bars*.

2.2.2.6 Do not use manual valves or bypasses that can prevent a safety function from operating on demand. For cases where their installation is necessary for maintenance or other operating function purposes, manual valves or bypasses are acceptable if both of the following conditions are met:

A. They conform to the guidance in Data Sheet 7-49, Emergency Venting of Vessels, regarding manual isolation valves.

B. Valve position monitoring is provided to meet the required SIL for the current function of the valve. If valve position switches are required, they should be tested to maintain the same integrity as the safety function.

2.2.2.7 Prior to startup, inspect all manual valves that can impact on the efficacy of the safety function, regardless of the existence of position switches.

2.2.2.8 Design utilities and support systems to ensure reliability at least equivalent to the underlying SCAI. This may require redundant systems such as backup generators, uninterruptible power supplies (UPS), etc.

2.2.2.9 Prior to the operation of a SCAI system, perform a commissioning test to verify it has achieved the requirements and recommendations determined to be necessary in the design phase. Include in the test all relevant process operating modes (normal and abnormal) and associated equipment in a step-by-step testing procedure to ensure their proper functionality and verify they perform their safety functions. Address and document any discrepancies before system operation.

2.2.3 SCAI Systems in Lieu of Other Safety Devices

2.2.3.1 SCAI systems may be used in lieu of other active or passive safety devices normally present on equipment or processes, provided **all** of the following conditions are met:

A. A detailed process hazard analysis (PHA) has been conducted to ensure all potential upset conditions that would have been addressed by the omitted safety device have been accounted for. See Data Sheet 7-43, *Process Safety*, for more information on PHA.

B. The installed SCAI system has an equal or greater reliability on demand than the safety device it is replacing. Such systems usually require a detailed reliability analysis and are rated at the appropriate SIL level for the risk.

C. The SCAI system design considers common failure modes that may simultaneously initiate an unsafe condition and compromise the reliability of the SCAI system to function as designed. Common cases include a failure of the primary control system and loss of power.

For guidance on safety instrumented systems (SIS) used in lieu of mechanical overpressure devices see Data Sheet 7-49, *Emergency Venting of Vessels*.

2.2.4 SCAI Systems Combined with Other Safety Devices

2.2.4.1 SCAI systems may be used in combination with other active or passive safety devices where the SCAI system protects from some upset conditions and other safety devices handle the remaining scenarios. Such systems are common when the traditional safety device is insufficient to handle every scenario, or a higher level of reliability is needed over the single safety device alone (multiple layers of protection). This approach is acceptable provided every scenario is accounted for and the conditions in Sections 2.2.3 and/or Data Sheet 7-49, *Emergency Venting of Vessels,* for safety instrumented systems (SIS) used in lieu of mechanical overpressure devices are met.

2.3 Human Factors

2.3.1 Management of Change

2.3.1.1 To ensure SCAI performance is maintained, review and evaluate any changes in accordance with Data Sheet 7-43, *Process Safety*. Changes to safety systems are critical and should be addressed as such under MOC procedures.

2.3.1.2 If the system has a certified safety integrity level (SIL), perform all tests and update documentation required to maintain certification. This can include, but is not limited to, the following:

- System failures
- System modifications (software and hardware) and the impact analysis of those modifications
- System demands and outcomes
- System integrity assessments
- Changes to the scope or frequency of testing

2.3.1.3 Establish an administrative control procedure for SCAI systems or components that are temporarily disabled or taken out of service. Include a hazard review that includes management approval. Maintain a safety bypass log of all bypassed safety devices, including the duration of each bypass, in a visible and prominent location that is accessible to the appropriate authorized personnel. Review the safety bypass log at the beginning of each shift. For additional guidance on management of change, see Data Sheet, 7-43 *Process Safety*, and Data Sheet 10-8, *Operators*.

2.4 Operation and Maintenance

2.4.1 Operation

2.4.1.1 Develop management systems and procedures with the appropriate responsible person(s) to ensure all activities associated with the SCAI are properly managed. This includes planning, execution, documentation, maintenance, and training to ensure the required performance.

2.4.1.2 Create and maintain documentation that is available and accessible to all relevant personnel. Include documentation on the following:

- Design basis and capabilities
- Safe operating limits (SOL) and integrity operating windows (IOW) for operating parameters
- Consequences of deviation
- Engineering drawings and calculations
- Process flow diagrams, piping and instrumentation diagrams (P&ID) relevant to the SCAI
- Specifications for instruments, controls, and final elements
- Critical utilities and support systems
- Associated non-instrumented systems such as relief valves

2.4.1.2.1 Ensure documentation is clear, precise, certifiable, maintainable, and feasible. If documents are in an electronic format, provide additional protection against unauthorized access. Refer to Data Sheet 7-110, *Industrial Control Systems*, for additional guidance.

2.4.1.3 Have administrative procedures and physical controls in place to ensure only appropriate authorized personnel have access to change control data or programs.

2.4.1.3.1 Consider the potential for cyber attacks, including cyber vulnerability to the control system. Refer to Data Sheet 7-110, *Industrial Control Systems*, for detailed loss prevention recommendations.

2.4.1.3.2 Use a password control management program to manage critical passwords for SCAI systems. For safety systems, use unique passwords that are different from those used for primary industrial control systems (ICS). Limit access to designated personnel only (usually not including operators). Do not use default factory passwords.

2.4.1.4 In the event of an SCAI system activation or failure, determine the cause prior to restoring the process/equipment to service. Conduct a near-miss incident investigation after any actuation or failure of an SCAI system.

2.4.2 Operator Interface

2.4.2.1 To the extent possible, design SCAI systems to be automated and perform without operator interaction.

2.4.2.1.1 Avoid the use of bypass and abort devices (e.g., switches that prevent activation of a safety system).

2.4.2.1.2 Fully automatic safety functions are the preferred option for SCAI. However, manual intervention can be considered acceptable if **all of** the following conditions are met:

A. The deviation condition of the process or equipment has been previously determined by a process hazard analysis to be a situation in which a manual response is an acceptable layer of protection.

B. Unsafe conditions are alarmed to a constantly attended location.

C. Safety alarms are prominently displayed in a way that requires action.

D. Initial and refresher training is provided on required actions, including required response time(s).

E. The action required can be performed under the adverse conditions of the upset situation.

F. There is enough time for the operators to react to abnormal conditions and take corrective actions to bring the equipment or process to a safe condition. See Section 3.4.2 for additional guidance.

2.4.2.2 Ensure safety alarms have the appropriate visibility. Arrange alarms so they do not overload the operator (cause “alarm showers”) during an upset condition. If necessary, reevaluate and redesign the alarm system to ensure the operator can successfully address upset conditions. Set a critical alarm when electronic devices with a run/program mode are in program mode during normal operation. For detailed recommendations on alarm management, refer to Data Sheet 10-8, *Operators.*

2.4.2.3 Authorize operators to shut down the process in the event of an unsafe condition. For additional guidance, refer to Data Sheet 10-8, Operators.

2.4.3 Inspection, Testing, and Maintenance (ITM)

The purpose of inspection, testing, and maintenance is to ensure the performance standards and reliability set in the initial design are maintained throughout the lifecycle of the SCAI.

2.4.3.1 Maintain all components and the overall system in accordance with the original equipment manufacturer’s guidance. Include the following activities:

- Preventive maintenance
- Calibration
- Functional testing
- Loop testing
- Mechanical exercising
- Environmental condition monitoring
- Periodic visual inspection

2.4.3.2 Keep adequate spare parts available to reduce facility outages and bypass durations. For detailed recommendations refer to Data Sheet 9-0, *Asset Integrity*.

2.4.3.3 Apply the management of change (MOC) procedure for any replacements to the SCAI that are not in kind.

2.4.3.4 Maintain a history of the reliability of the system and the components. Assess the implications of any failures and, where required, carry out modifications to equipment, components, or procedures to minimize the likelihood of repeat occurrences. Take into consideration manufacturers’ bulletins or statistical failure information.

2.4.3.5 Provide the capability to complete online testing of all system components, including power supplies and field equipment, unless adequate safety integrity can be achieved by testing during planned shutdowns (e.g., when a SIS is restored after a maintenance shutdown). Commissioning tests are covered in Section 2.2.2.9 of this data sheet.

2.4.3.6 Perform inspection and maintenance activities for utilities and support systems used by SCAI (e.g., batteries, uninterruptible power supplies, generators) in accordance with the guidance in Data Sheet 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.4.3.7 Establish written authorization procedures to communicate to all parties involved the scope of any maintenance activity prior to the start of the work.

2.5 Training

2.5.1 Train operators on the functions and required actions associated with the SCAI system. Conduct refresher training as needed. At a minimum, include the following in the training:

- Hazard(s) the SCAI system is protecting against
- Information displayed on the interface (process sequence, SCAI actions, bypassed functions, failed component or subsystem, status of field devices, etc.)
- Actions to take or not take in the event of system actuation
- Post-event recovery actions
- Bypassing procedures and the associated consequences, including when bypassing is permitted or prohibited
- Testing and diagnostic procedures
- Shutdown and startup activities

For additional guidance refer to Data Sheet 10-8, *Operators*.

2.5.2 Train and certify maintenance personnel on procedures and activities required to sustain the reliability of the SCAI system.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Safety Functions

3.1.1 Risk and Layers of Protection

Risk can be calculated as the product of the consequence of an accident times the likelihood (probability) of that accident occurring. Manufacturing and industrial processing has inherent risks that should be evaluated and reduced to an acceptable and tolerable level. The evaluation process for risk reduction is to first identify and quantify the potential risks, then establish mitigating strategies. Allocation of safety functions and/or the use of protection layers can be used to reduce the risk to acceptable levels.

IEC 61511-1:2016 defines a protection layer as any independent mechanism used to prevent undesired events from happening, or to mitigate the consequences once the event has occurred. Figure 3.1.1 shows a typical protection layer representation that can be applied to any industry or process.

The starting point involves the process design, in which steps can be taken to minimize the exposure to an incident. The ideal is an inherently safer system. An inherently safer design avoids hazards by removing or reducing the amount of hazardous material involved or the number of hazardous operations.

The second layer includes the basic process control system (BPCS). This layer is predominantly a quality assurance measure (e.g., smooth-running operations result in higher quality and quantity of product). The operator monitors and adjusts process variables, such as temperature, pressure, and flow rate, to meet process needs. The control system is expected to maintain the process at the set points established by the operator and within safe limits of operation.

The third layer involves critical alarms and operator intervention. This could be an extension of the control system and, at this level, manual intervention of the operator could contain the excursion.

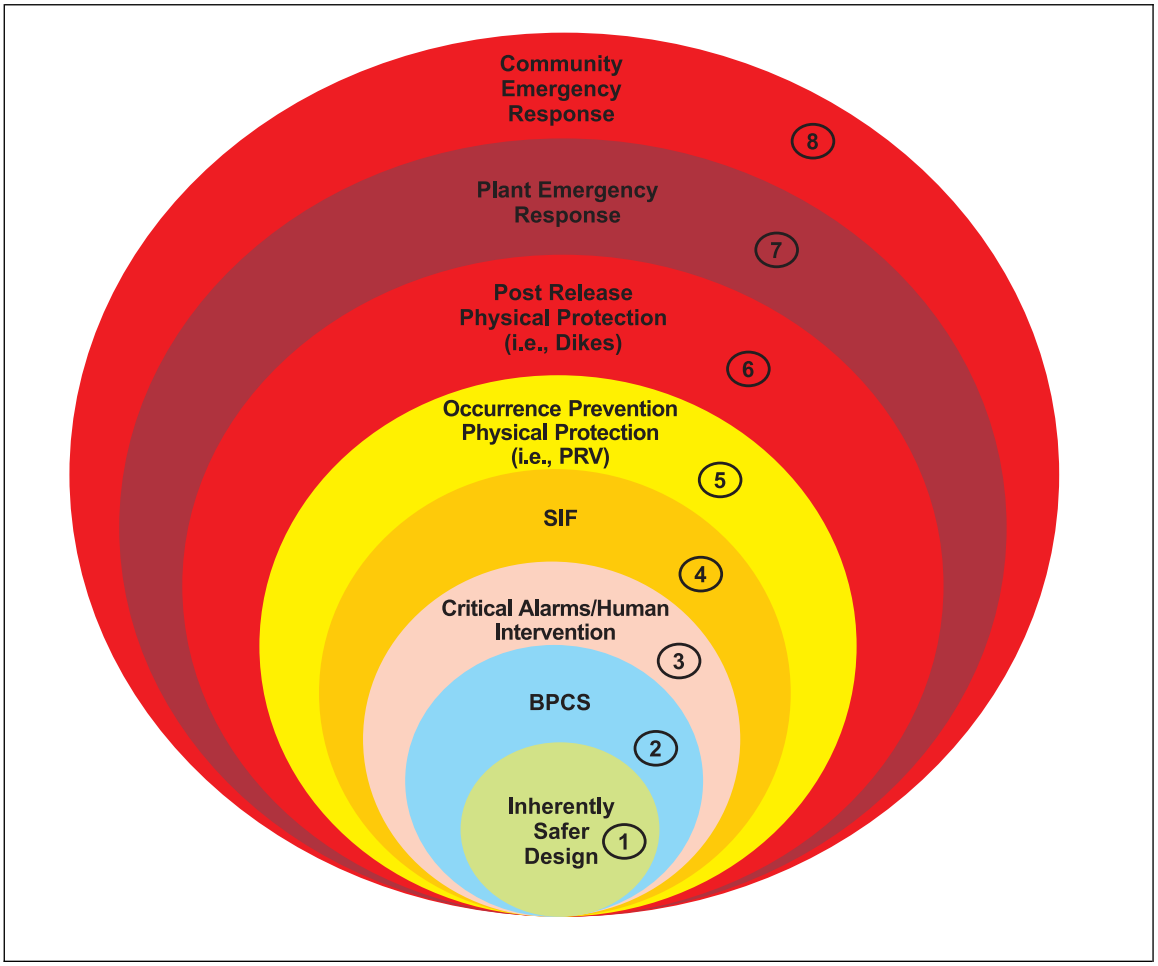

Fig. 3.1.1. Layers of protection

The fourth layer involves safety systems in which safety instrumented functions (SIF) are included to automatically respond if and when the previous layer fails. This layer may include SCAI, SIS, or an emergency shutdown system (ESD).

The fifth layer represents physical protection to prevent the occurrence of an undesired event. It is designed to minimize the extent of damage during a major upset. This layer represents the final protection prior to an out-of-control situation.

Once the undesired event has occurred, post-release physical protection (containment dikes, fire walls, emergency drainage, etc.) and layers seven and eight, such as an onsite fire brigade or the public fire service and emergency response, minimize the impact on the business and community.

3.1.2 Industry Codes, Standards, and Recommended Practices

Recognized industry codes, standards, and recommended practices can be used to determine safety functions for specific equipment and/or processes. These documents are developed and published by locally, nationally, and/or internationally recognized organizations such as NFPA, ANSI, API, ASME, ISA, and IEC. These organizations have different review cycles for their codes and standards, with updates incorporating safety enhancements, new products, and technologies.

The following are some of the recognized standards in which SCAI are addressed:

- ISA TR 84.00.05, *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)*

- ISA TR84.00.02-Part 1, *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques, Part 1*
- IEC 61511, *Safety Instrumented Systems for the Process Industry*
- IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*
- ANSI/ISA-84.00.01, mditSafety Instrumented Systems for the Process Industry Sector
- API 556, *Instrumentation, Control, and Protective Systems for Gas-Fired Heaters*
- API 521, *Pressure-Relieving and Depressuring Systems*
- NFPA 85, *Boiler and Combustion Systems Hazard Code*
- NFPA 86, *Standard for Ovens and Furnaces*
- NFPA 87, *Standard for Fluid Heaters*
- ASME Section VIII, *Boiler and Pressure Vessel Code*

3.1.3 Process Hazard Analysis (PHA)

A process hazard analysis (PHA) is a systematic approach for the identification, evaluation, and control of hazards associated with a process. PHA represents the first step in the design process of a safety system. The objectives of a PHA are to determine the following:

- The hazardous events of the process and associated equipment
- The sequence of events leading to the hazardous events
- The process risk associated with the hazardous events
- The requirement for risk reduction
- The safety functions required to achieve the necessary risk reduction

Third-party consultants hired to assist in a PHA should be subject matter experts (either licensed or otherwise qualified). Qualified facility personnel often participate in the PHA process as well.

The intent of a PHA is to determine the potential causes and consequences of events and evaluate factors that may affect the process. If multiple operations or processes exist, an analysis is required for each process and safety system combination to determine the effect on the required SIL. Further guidance on PHAs, including methodologies, can be found in Data Sheet 7-43, *Process Safety*.

3.2 Implementation and Design

3.2.1 BPCS, SIS, and SCAI

Basic process control systems (BPCS) and safety instrumented systems (SIS) play a significant role in the management of hazards in the process industry. SIS are recognized for reducing the likelihood and consequences of events involving potential damage of assets and production interruption. The roles of these systems could include prevention of overpressure or over-speeding, limiting high and low levels, detecting fire and flammable or toxic gas release, shutdown and isolation of plant and inventories, initiation of firefighting systems, etc.

SIS perform differently than BPCS. They are dormant, and are activated only when the parameters established in the safety functions exceed the safety limits. SIS need to be tested and maintained regularly to ensure the proper operation of the system when needed.

BPCS elements actively provide input/output, perform calculations, and have feedback loops. These systems must be flexible enough to allow frequent process changes.

Independence and physical separation can be done for BPCS and SIS to prevent common cause failures, as shown in Figure 3.2.1-1, where the final element could be an on/off valve that is normally open to allow the flow control valve to regulate the process feed under normal operating conditions. In the event of an upset condition, the safety valve is commanded shut by the safety system, independent of what the control system is signaling to the flow control valve.

Final elements are parts of the BPCS or SIS that implement the physical action necessary to achieve or maintain a safe state. Some examples include valves, switch gear, motor controllers, and alarms (visual and

audible). However, there are cases in which the SIS is connected to the BPCS as shown in Figure 3.2.1.-2 (a modern electronic overspeed system integrated into the overall control system of a turbine).

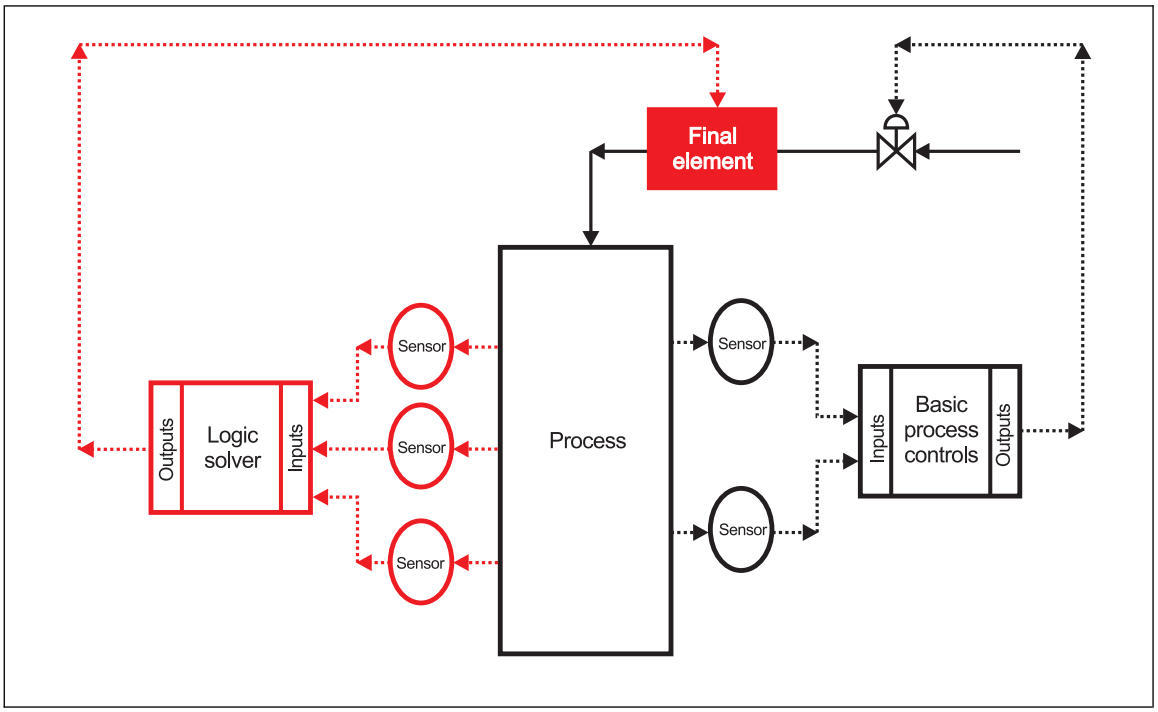

Fig. 3.2.1-1. Separated BPCS and SIS

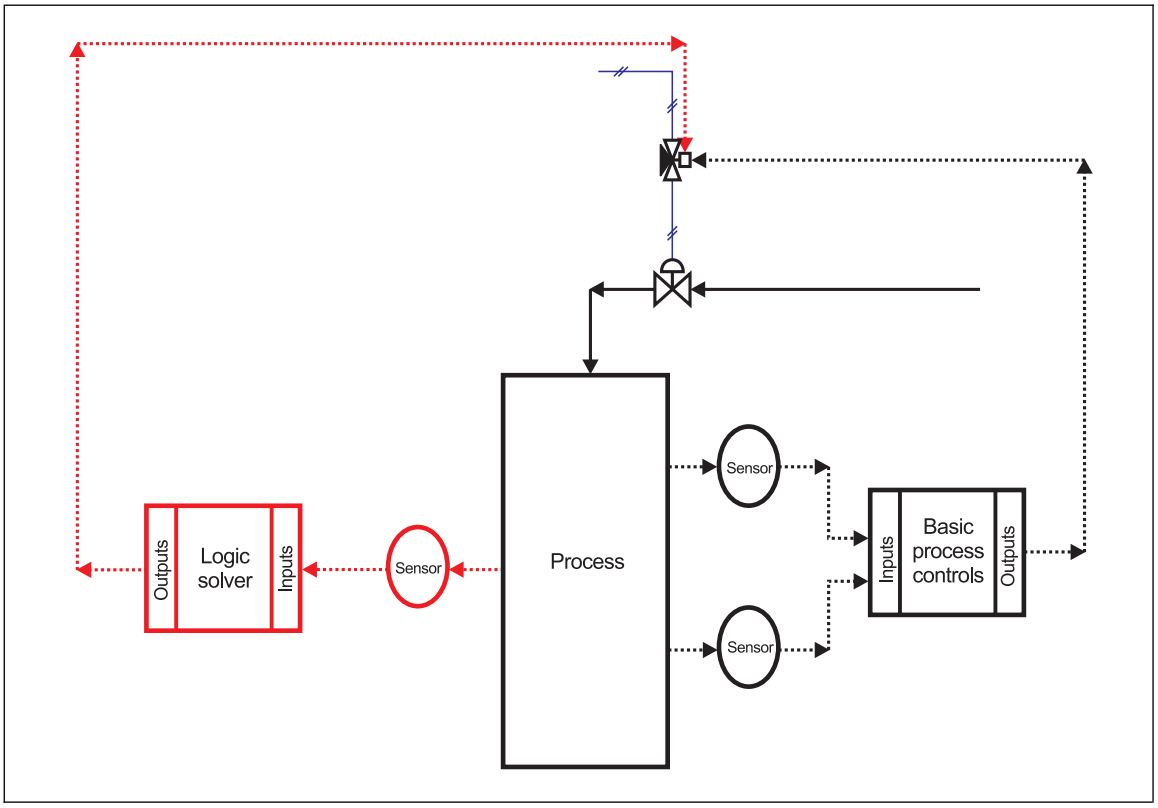

Fig. 3.2.1-2. Interconnected BPCS and SIS

It is important to note there are two independent functions: the control of the process (BPCS), and its safety. Process control systems ensure the quality and quantity of the product and frequently reduce the need/reliance on an operator to produce the product. The SIS activates when the BPCS fails to perform. A well-designed BPCS can significantly reduce the demands on the SIS and reduce the overall risk presented by the process.

SCAI are process safety safeguards, implemented with instrumentation and controls that are used to achieve or maintain a safe state for a process and that are required to reduce the risk(s) associated with a specific hazardous event.

SCAI are the most common safeguards used to prevent abnormal operations from becoming a loss event. There are four basic types of SCAI: safety controls, safety alarms, safety interlocks, and safety instrumented systems (SIS).

SCAI can be implemented using BPCS or SIS equipment. IEC 61511 specifies that unless the BPCS equipment is designed and managed per IEC 61511, the SIS equipment must be independent and separate from the BPCS equipment to the extent that the safety integrity of the SIS is not compromised. Operating information can be exchanged but should not compromise the functional safety of the SIS. Devices of the SIS can also be used for functions of the BPCS if it can be demonstrated that a failure of the BPCS does not compromise the SIF or the SIS.

3.2.2 Design Considerations

Safety instrumented systems (SIS) are a subset of SCAI. Like SCAI, SIS systems are made up of instrumentation and controls, usually a combination of logic solver(s), sensor(s), and final element(s), designed to carry out a safety function. These systems prevent or mitigate hazardous events by taking the process to a safe state when predetermined conditions are met.

The overall conceptual approach of IEC 61511 for a SIS safety life-cycle consists of three main stages: analysis, implementation, and operation. Figure 3.2.2 illustrates the typical activities from initial conception through decommissioning that correspond to each one of the stages.

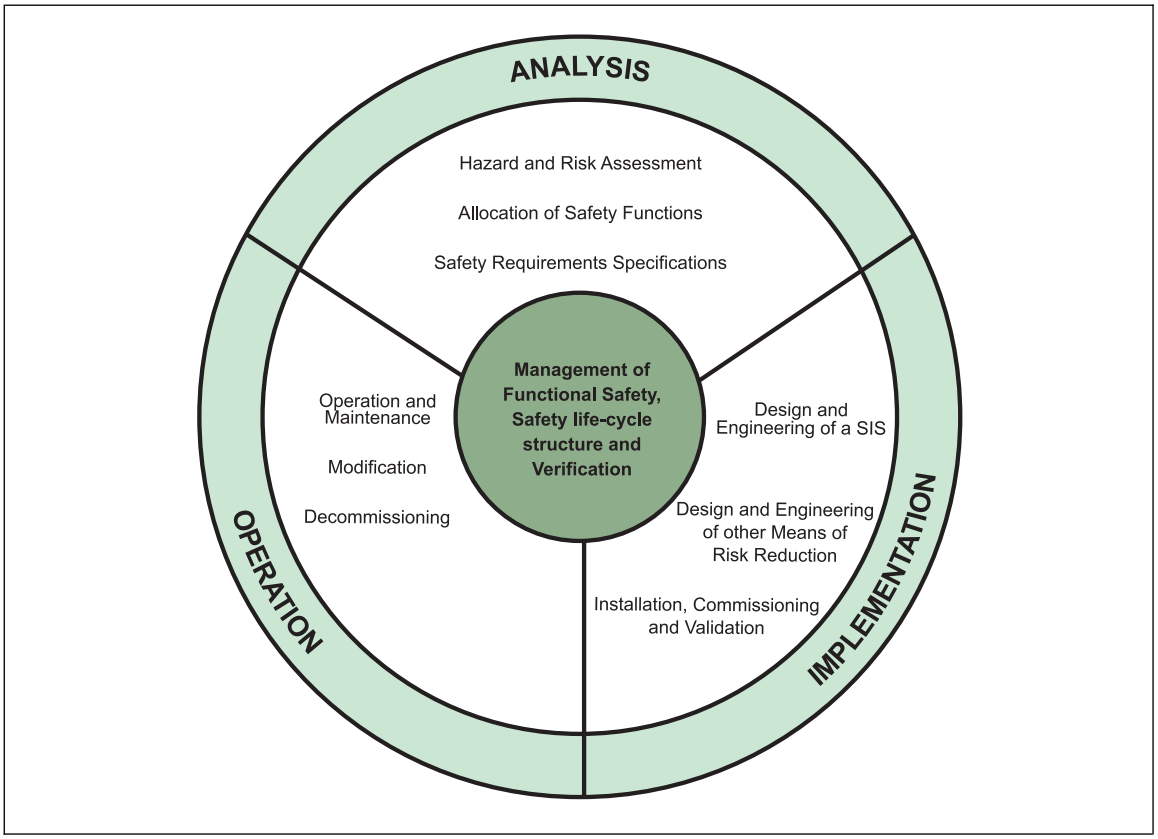

Fig. 3.2.2. Safety life-cycle of a SIS

3.2.3 Safety Integrity Level (SIL)

Safety integrity levels (SIL) are defined by discrete levels (1 to 4) allocated to safety functions. Each safety function is assigned its own SIL required to prevent or mitigate the specific hazard associated with the function. SIL gives a measure of safety or risk reduction to a tolerable limit for a given process.

3.2.3.1 SIL Determination

The SIL assessment can be done using one or more methods such as safety matrix, risk graph, layers of protection analysis (LOPA), fault tree analysis (FTA), as low as reasonably practicable (ALARP), and direct calculation.

The method is commonly selected based on the following:

- The complexity of the process or equipment
- The nature of the risk and the required risk reduction
- The knowledge and experience of the people assigned
- The information related to the risk available

For detailed information about these or other methods, referred to Data Sheet 7-43, *Process Safety*.

3.2.3.2 SIL Structure

Safety systems are quantitatively evaluated through SIL values. If a SIL value is not available, the generalizations shown in Table 3.2.3.2 can be used for preliminary screening purposes. Some factors that affect the reliability (SIL) of a particular system include redundancy, diversity, voting, diagnostics, and maintenance and testing frequency; any “adequacy for service” decisions should be based on a detailed evaluation of an existing or proposed system.

Table 3.2.3.2. SIS Interlock Design Structure for Each Integrity Level

Integrity Level	*Minimum Design Structure*
1	Non-redundant. Best single path designs (see Figure 3.2.3.2-1).
2	Partially redundant. Redundant independent paths for elements of lower availability. There may be some diagnostic capabilities (see Figure 3.2.3.2-2).
3	Totally redundant. Redundant independent paths for the total interlock system. Diversity, separation, redundancy, and exhaustive diagnostic capabilities are key aspects of this level. A single fault in a SIS component is unlikely to result in loss of process protection (see Figure 3.2.3.2-3).

Note: A nonprogrammable, relay-based safety system, common in smaller boilers for combustion safety, could be considered equivalent to a SIL 1 programmable system.

Redundancy is an important factor in achieving the minimum hardware fault tolerance, supporting the desired proof of test interval, or achieving the target risk reduction and spurious trip rate. The redundancy scheme can be defined as the total number of devices (N) available to operate and the minimum number of devices (M) required to successfully trip the safety function (MooN). For instance, a 2oo3 redundancy scheme indicates that 2 out of 3 devices must operate successfully to trip the safety function. Redundancy schemes can be applied to any subsystem, including field devices, I/O cards, processors, and communications.

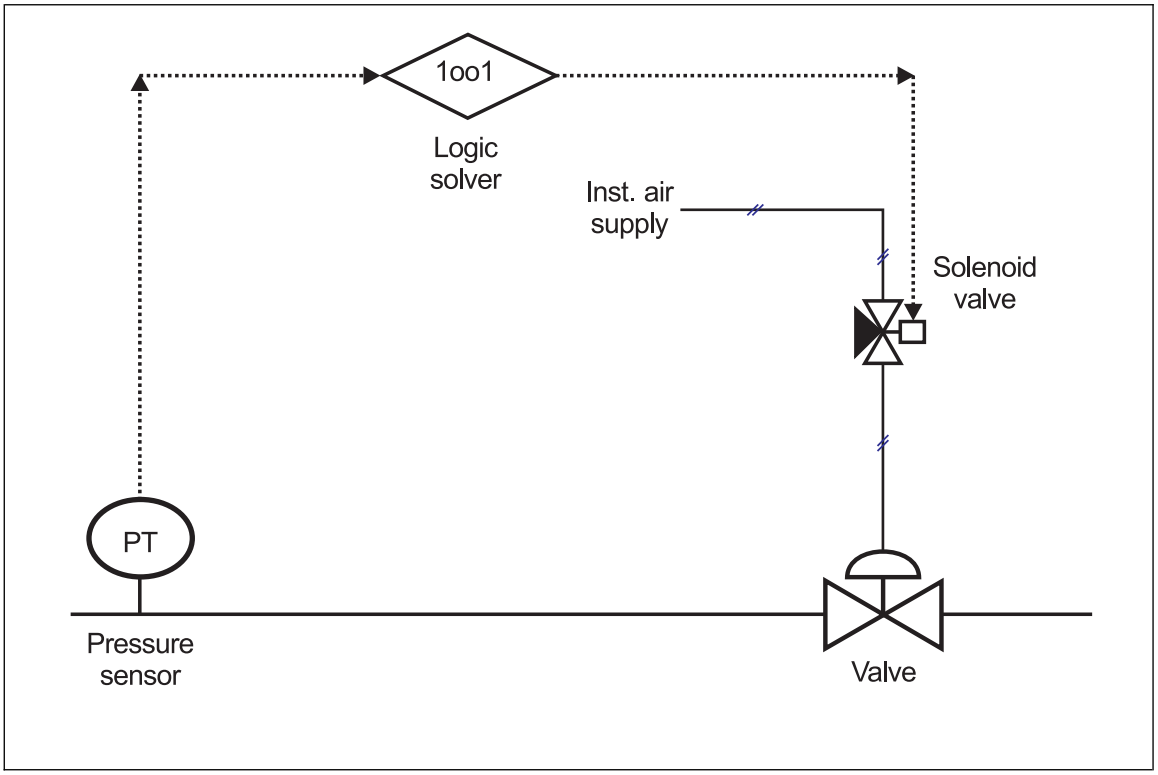

Fig. 3.2.3.2-1. Typical SIL 1 structure

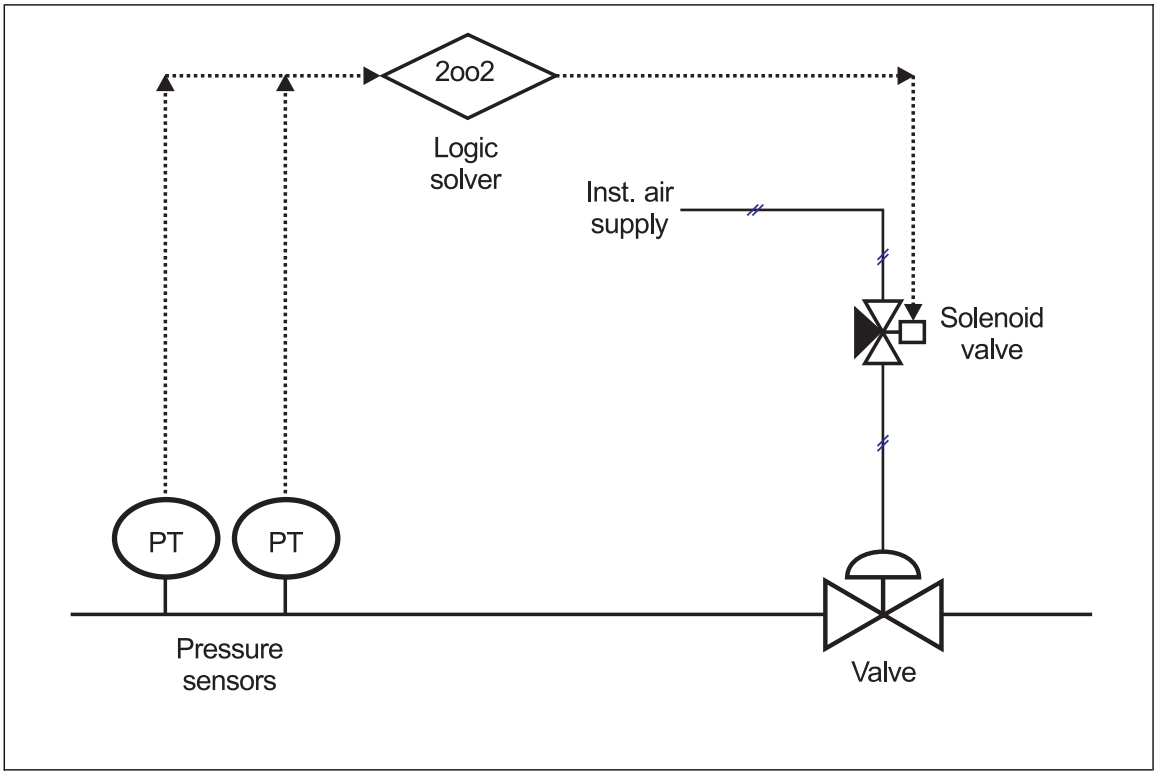

Fig. 3.2.3.2-2. Typical SIL 2 structure

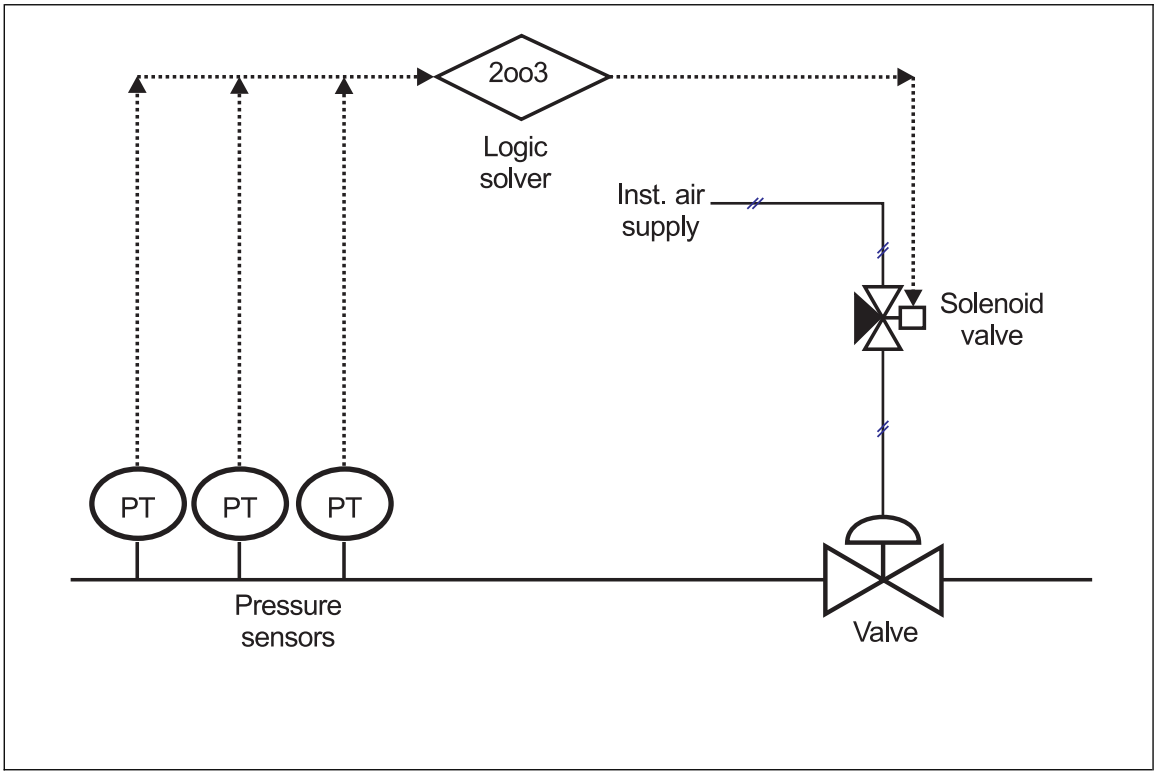

Fig. 3.2.3.2-3. Typical SIL 3 structure

3.2.3.3 SIL for Safety Instrumented Loops

Safety functions are executed in a SIS through safety instrumented loops. Typical safety loops consist of a sensor, input signal processing section of the programmable logic controller (PLC), logic solver, output signal processing section of the PLC, and final element.

Safety function applications will operate in low-demand mode or high-demand/continuous mode. Low-demand mode is where demands to the system are normally infrequent. To calculate the SIL of the loop in low-demand mode, all the elements should be considered. The probability of failure on demand (PFDavg) of the loop is equal to the sum of all the PFD of the elements involved.

High-demand mode applications could be considered as continuous mode if the hazardous event typically occurs as soon as the SIS fails to function (e.g., burner or turbine speed control functions).

Table 3.2.3.3-1 shows the safety integrity level requirements for low-demand and high-demand/continuous operation mode.

Table 3.2.3.3-1. Safety Integrity Level (SIL) Requirements

Safety Integrity Level (SIL)	*Probability of Failure on Low Demand Mode (PFD_{avg})*	*Average Frequency of Dangerous Failures on High Demand/Continuous Mode (failures per hour)*
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

The SIL of an element can be affected by parameters such as the following:

- Architectural constrains (AC)
- Hardware fault tolerance (HFT)

- Safe failure fraction (SFF)
- Probability of failure on demand (PFD_{avg})
- Probability of failures per hour (PFH)
- Testing interval (refer to Section 3.5.1)

Architectural constraints divide the instruments in two types, A and B:

Type A: The failure modes of all constituent components are well defined and the behavior of the element under fault conditions can be completely determined. There is also sufficient dependable failure data to show the claimed rates of failure for detected and undetected dangerous failures are met.

Type B: The failure mode of at least one constituent component is not well defined, or the behavior of the element under fault conditions cannot be completely determined. There is also insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.

Failure modes are different types of failures, safe or dangerous, that may occur to devices in a SIS. These can be classified as detected or undetected. Some failure modes include fail-safe state, fail safe, fail dangerous, fail high, and fail low. Failure rates can be evaluated based on a failure modes and effects analysis (FMEA), which is a systematic approach used to evaluate different component failure modes to determine what could eliminate or reduce the failure probabilities.

Hardware fault tolerance (HFT) is the ability of the hardware (including hardware and software of the transmitter) to continue to perform a specific safety function in the presence of faults or errors. An HFT of 0 means if there is one fault, the transmitter will not be able to perform its function. HFT of N means that N+1 faults will cause loss of safety functions for the unit.

The safe failure fraction (SFF) ratio is the ratio at which a device experiences safe or detected failure.

The SIL of a safety function can be affected by the HFT and SFF for devices type A (Table 4) and B as shown in Table 3.2.3.3-2.

Table 3.2.3.3-2. Maximum SIL for a Safety Function of Devices Type A and B

	HFT Type A			*HFT Type B*		
SFF	0	1	2	0	1	2
60%	SIL1	SIL2	SIL3	Not allowed	SIL1	SIL2
60% to <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% to <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

3.3 Management of Change

Management of change (MOC) means evaluating all changes except replacement-in-kind (RIK). In the case of safety controls, alarms, and interlocks (SCAI), this includes changes to technology, instrumentation, equipment, and personnel. Evaluation at the earliest possible stage is necessary to determine any potential impact on property loss prevention. Management of change includes a review and authorization process for evaluating proposed adjustments to design, operations, organization, or activities prior to implementation to make certain that no unforeseen new hazards are introduced and that the risk of existing hazards has not unknowingly increased.

Replacement-in-kind is the exchange or replacement of one piece of equipment or component that meets all the original design specifications with no deviations (size, pressure rating, temperature rating, flow rating, metallurgy, etc.). These would not be considered a change and would therefore not require completion of the MOC process.

MOC also includes steps to help ensure potentially affected personnel are notified of the change, and that pertinent documents, such as procedures, process safety knowledge, and other key information, are kept up to date.

A written procedure is needed to define what a change is and how it will be requested, reviewed, approved, and implemented. For additional guidance, refer to Data Sheet 7-43, *Process Safety*.

3.3.1 Changes can be divided into two main categories: technology/process and personnel/organization.

A. Changes in technology/process arise whenever the process or mechanical design is altered. Typical instances in which these changes may impact SCAI include the following:

1. Changes to process equipment, design parameters, materials of construction and equipment configuration
2. Changes to support systems and utilities (power, steam, air, etc.)
3. Bypasses or connections that are temporary in nature, such as the following:
    a. Piping, connections, hoses, or wiring
    b. Utility connections (steam, power, water, etc.)
    c. Software configurations, jumpers, shortened algorithms, bypassed controls
    d. Bypass connections around safety equipment that is normally in service (forces and jumpers)
4. Changes in operating procedures, including startup, normal shutdown, and emergency shutdown
5. Changes to safety system software and hardware
6. Significant changes to operating conditions, including increasing throughput or introducing new materials
7. Changes to the overall site infrastructure that may impact the safety systems

Both forces and jumpers are changes and should be covered under an MOC program. In practice, however, these are typically managed using a separate system. Important aspects of this program are hazard evaluation, notification of all affected operators, contingency plans to reduce the risk, and formalized plans to complete repairs.

For software and hardware, before a change goes live, a period of testing is typically conducted. This can be done online or via an offline simulation program. The tests conducted validate all the operating scenarios for the proposed change. The results of this testing are then used in the training of the operators.

B. Change in Personnel or Organization are those in which key responsibilities are affected. These changes might cause a lapse in continuity of responsibility.

Personnel changes that could impact SCAI systems or procedures may include:

- Retirement
- Promotions
- Sickness
- Death
- Leave-of-absence
- Changes in staff experience
- Use of outside contractors
- Staff movement between departments
- New personnel being assigned to a position for the first time

Organizational changes may include:

- Changes in staffing levels (downsizing or increasing staffing levels)
- Change in the duration of the shift schedules. This can impact the human factor element of process safety.
- Policy changes such as a significant cut in a maintenance department’s budget could require an employer to alter its mechanical integrity procedures concerning the timeliness or frequency of tests, inspections, repairs, or replacements.

3.3.2 The duration of a change could also impact SCAI. Change durations are usually defined as permanent, temporary or emergency.

A. Permanent changes are where a permanent modification to the facility, technology or personnel is made. An advance review of the proposed change is needed following the normal management of change (MOC) process.

B. Temporary changes are changes not intended to be permanent, instead having a predetermined termination date and time.

C. Emergency changes are those made to maintain or resume safe operations (e.g., a plant breakdown or shutdown). Additional safeguards might be implemented for the duration of the change (e.g., frequent monitoring, rounds).

The MOC process account for the allowed duration of the change based on conditions and other factors such as the level of risk. Action items are occasionally deferred based on the lower risk they pose.

3.4 Operations and Training

3.4.1 Operations

The subject of SCAI and safety instrumentation is not solely a topic related to instrumentation and control systems (both software and hardware). For a safety system to be effective it requires knowledge, experience, and support from a variety of other disciplines. Along with this a commitment from all levels of management within an organization is critical. Without such support and commitment, it is unlikely that a safety program will function as designed, thereby impacting the level of safety it provides.

3.4.1.1 Integrity Operating Windows (IOW) and Safe Operating Limits (SOL)

The integrity operating window (IOW) is the allowable range of the operating parameters for a piece of equipment and are determined by the PHA. The upper and lower limits that define the IOW boundaries are called the safe operating limits (SOLs). When operated within these limits, the equipment can meet process and design parameters with a lower likelihood of breakdown. This relationship can be seen in Figure 3.4.1.1. Operating outside of the SOLs will result in accelerated deterioration and increased likelihood of failure. The IOWs and SOLs are dependent on the condition of the equipment and are subject to change over time. Operators need to fully understand the equipment IOWs and SOLs as detailed in the operating procedures and training.

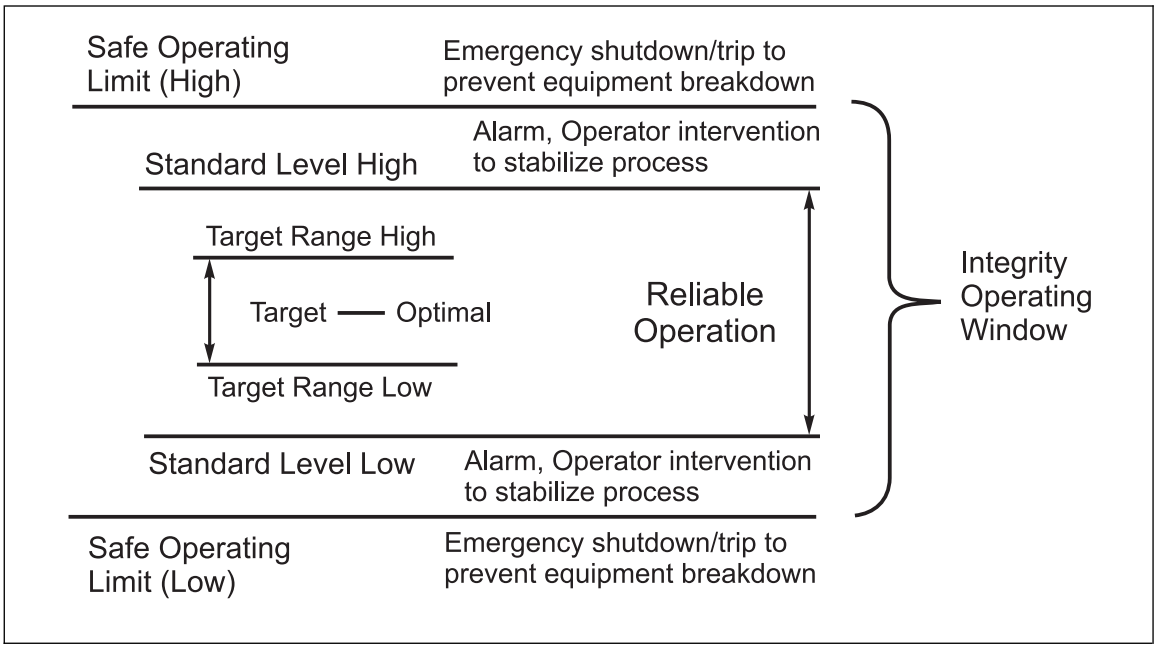

Fig. 3.4.1.1. IOW and SOL

3.4.1.2 Operating Conditions

Changes in process operations can introduce the potential for increased risk. Often these changes are transitional in nature; for example, a process upset. Operators need to understand the upset condition, formulate an action plan and take proactive measures before the safe operating limits are reached.In transitional situations like start-up and shut down potential risks may be increased when compared to normal operations. Additional knowledge and training may be needed to potentially reduce the possible risks created during operations like these.

3.4.1.2.1 Normal Operations

These are the routine operations (within the reliable operations window as shown in Figure 8) an operator may be required to perform to maintain control over the plant, process or equipment. It is important that operators are familiar with normal operating parameters and their associated limits, as well as how to recognize when operating conditions change due to process upsets, and respond to maintain them within operational limits. Items to consider include the following:

- Monitoring of control loops - both automatic and manual
- Monitoring of set-points
- Monitoring the status of any safety systems related to the process or equipment
- Routine alarms and the necessary response required
- Identification of process variables (temperature, flow rate, pressure etc.) that are outside the normal profiles for the operation
- Rationalizing observed flows compared to indicated valve positions

3.4.1.2.2 Startup

Additional knowledge and training may be needed to cover the increased risks associated with the transitional nature of startup operations. This may include, but not be limited to the following:

- System design and operation
- Line-up of equipment and systems for safe startup
- Proper startup sequencing and startup operating procedures
- Knowledge of permissive and interlocks associated with proper startup sequencing
- Alarms and their meaning
- The proper use of jumpers and bypasses if required for safe start-up

3.4.1.2.3 Shutdown

Shutdowns can occur as a result of abnormal conditions or following normal operation. Operators should be familiar with the following:

- Shutdown sequencing for normal system operation
- Emergency shutdown procedures when system upsets cannot be controlled within safe limits
- How to maintain the system in a safe state after shutdown has occurred
- Ensuring system parameters are returned to normal state prior to subsequent startup
- Emergency response procedures should a safe shutdown not be successful

Shutdowns are typically an opportunity to make changes to a process. This can include updating software, conducting functional testing of SIS systems, and inspecting and testing system components.

Using a management of change procedure is critical when making these changes to prevent problems that may occur when the process is eventually restarted.

3.4.1.2.4 Abnormal/Upset Conditions

Abnormal or upset conditions during operation can result in the need for quick and decisive corrective action to prevent safe operating limits being exceeded. Process control systems can limit the potential for upsets; however, operators also need to be able to assess and take appropriate actions to avert emergencies. Operators should be familiar with and have training in the following:

- Common process upset scenarios and how to control them

- Emergency operating procedures and how to apply them
- Prioritization of emergency actions in times of crisis
- Joint emergency drills with operations and maintenance personnel

3.4.1.3 Personnel

For an effective safety management system, competent personnel must be involved at all stages in the systems lifecycle. The requirements for competent personnel involved in SIS safety life-cycle activities include the following:

A. Engineering knowledge training and experience appropriate to the process application, technology, sensors and final elements

B. Safety engineering knowledge

C. Knowledge and understanding of legal and regulatory requirements that may apply

D. Understanding of the potential hazards and failures of the equipment or process for which they are responsible - including safety devices - and the consequences that potentially can result

3.4.1.4 Documentation

Good practice is to have all administrative controls (procedures, documentation, drawings, etc.) available to the relevant personnel when needed. These can be in hard-copy format or electronic. Examples of documents to keep available include the following:

- Operation instructions
- Inspection records
- Training records
- Testing records
- Maintenance repairs
- System failures
- System modifications (software and hardware) and the impact analysis of those modifications
- System demands and outcomes
- System integrity assessments
- Subsequent changes to the scope or frequency of testing

3.4.2 Manual Response Time (MRC)

Automatic safety systems operation mode is preferred over manual operation. However, when automatic mode is not possible or available, manual response can be considered if operators are provided with adequate time to respond in an emergency.

Figure 3.4.2 shows the elements that need to be considered when determining the manual response time (MRT). As shown, the MRT is made up of the operator response time plus the process response time.

The operator response time is made up of the sum of the time needed to detect (and acknowledge) the alarm, plus the time the operator needs to diagnose and determine the necessary corrective actions, plus the time taken to respond and complete those actions.

The process response time is the time taken for the process to then respond after the operator has completed their actions. An example is the time taken for a manually activated valve to close or the amount of time for a process to cool or spin-down so that lubrication or cooling media can be turned off.

If the MRT is greater than the time to unsafe condition (TUC), which is the amount of time from the original upset condition or alarm to the unsafe condition, then the probability of the hazardous event occurring is greatly increased.

Typically, the MRT and TUC are evaluated during the design phase of the safety system and are revalidated at regular intervals or whenever a change is made.

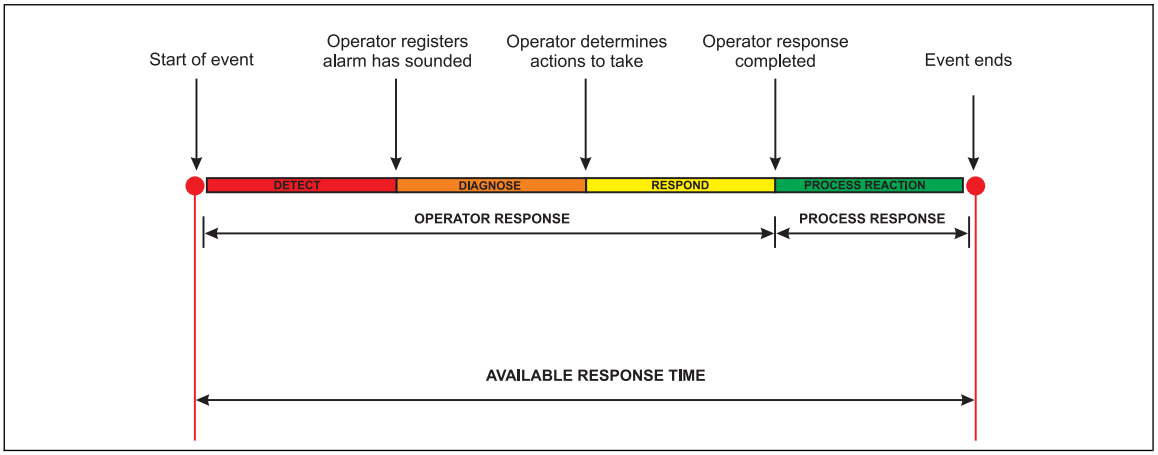

Fig. 3.4.2. Elements involved in determining manual response time (MRT)

3.5 Inspection, Testing, and Maintenance (ITM)

3.5.1 Functional Testing

The main objective of SCAI functional testing is to validate the reliability of all the elements in the system. Logic solvers, measurements and final control elements, are validated through a variable process manipulation in a simulating mode under various operating conditions, reflecting real operating conditions as accurately as possible, without actually driving the system to the demand conditions. The tests reveal undetected failure modes that would prevent any SCAI from proper functioning and generate proof that the system will operate accordingly to design specifications. There are two primary types of testing:

A. Offline testing. The test is performed when the process is not operational. It covers a more comprehensive evaluation for newly installed equipment or after changes or modifications to the system has been made.

B. Online testing. The test is performed while the process is operational. It requires special safety considerations to prevent abnormal operational conditions during the testing process. In some cases, additional sensors, test taps, bypass or isolation valves may be required.

Testing intervals are determined based on the SIL requirements, mode of operation (low or high demand), dangerous failure rates (detected and undetected), common cause failures (β-factors) and architecture type (redundancy). The equations from IEC 61508-6:2010 Annex B, can be used to calculate the testing intervals of a SIS.

Procedures need to be followed to ensure the quality and consistency of proof testing, and to ensure adequate validation is performed after replacement of any device.

If end-to-end testing is not possible, testing of each individual component can be made at different times. Items such as bypasses or overrides need to be handled under strict controls to ensure subsequent removal.

Batteries, uninterruptible power supplies (UPS), generators, compressed-air tanks, and other emergency power supply to a SIS should be subject to routine ITM in order to ensure that the reliability of the SIF is maintained, as defined by a recognized standard or defined by the PHA and SIL analyses.

3.5.2 Periodic Visual Inspection

SCAI should be visually inspected periodically to verify that no unauthorized modifications have been made and no observable deterioration exists. The following are some things that are commonly observed during visual inspections:

- Missing bolts
- Missing instrument covers
- Rusted brackets
- Open wires

- Broken conduits
- Broken heat tracing
- Missing insulation

It is important to document the results of the proof testing and visual inspection and retain the records to allow for reexamination of previous results to see if there is a history of device failure.

Deficiencies found during the proof testing and visual inspection need to be recorded and repaired in a safe and timely manner. A proof test should be repeated after the repair is completed.

3.5.3 Preventive Maintenance

Preventive maintenance activities are directly associated with the level of risk reduction required, which means that the higher the risk reduction, the greater attention is needed to ensure continued safe operation. When these programs are performed timely and according to specifications, a reduction of faults can be achieved as well as early detection of degradation signs. Preventive maintenance procedures should be followed for all the activities performed to maintain the design reliability of the SCAI and be developed according to manufacturer's recommendations. Examples include the following:

A. Running offline diagnostics to check hardware and software functionality.

B. Replacing parts or equipment that has completed its useful life.

C. Cleaning equipment to remove dust or other foreign materials.

3.5.4 Maintenance

Maintenance procedures and activities for SCAI are intended to ensure the equipment is operating in "as good as new" condition. For this condition to occur, procedures should include the following:

- Fault diagnostic and repair
- Revalidation and testing after replacement of any device
- Equipment calibration
- Specific maintenance activities and frequencies per element or device
- Activities to prevent unsafe conditions during maintenance operations
- Identification of personnel roles and responsibilities
- Maintenance bypasses

3.7 Loss History

An analysis was made of FM client losses in high-hazard occupancies (where SCAI are more commonly used for protection of processes and equipment) for the period 2007-2016. The SCAI loss percentages by occupancy (Figure 3.7) show that power generation is the industry with the most losses (39%), followed by nonhazardous chemical (23%), and pulp and paper (20%).

Table 3.7 presents a summary of these losses by peril. As shown in the table, a large percentage, relative to both the frequency and cost of the events, were attributed to electrical/mechanical breakdown. Explosions resulted in 20% of the losses by number and nearly one-third by loss cost. Fire events resulted in 16% of the losses by number, which corresponded to 14% of the loss cost.

Table 3.7. Losses by Peril, 2007-2016

Peril	*Percentage by Number of Losses*	*Percentage by Loss Cost*
Electrical, mechanical breakdown	53%	51%
Explosion	20%	30%
Fire	16%	14%
Implosion	2%	1%
Contamination	2%	1%
Molten material	4%	2%
Escaped Liquid	2%	1%
Total	100%	100%

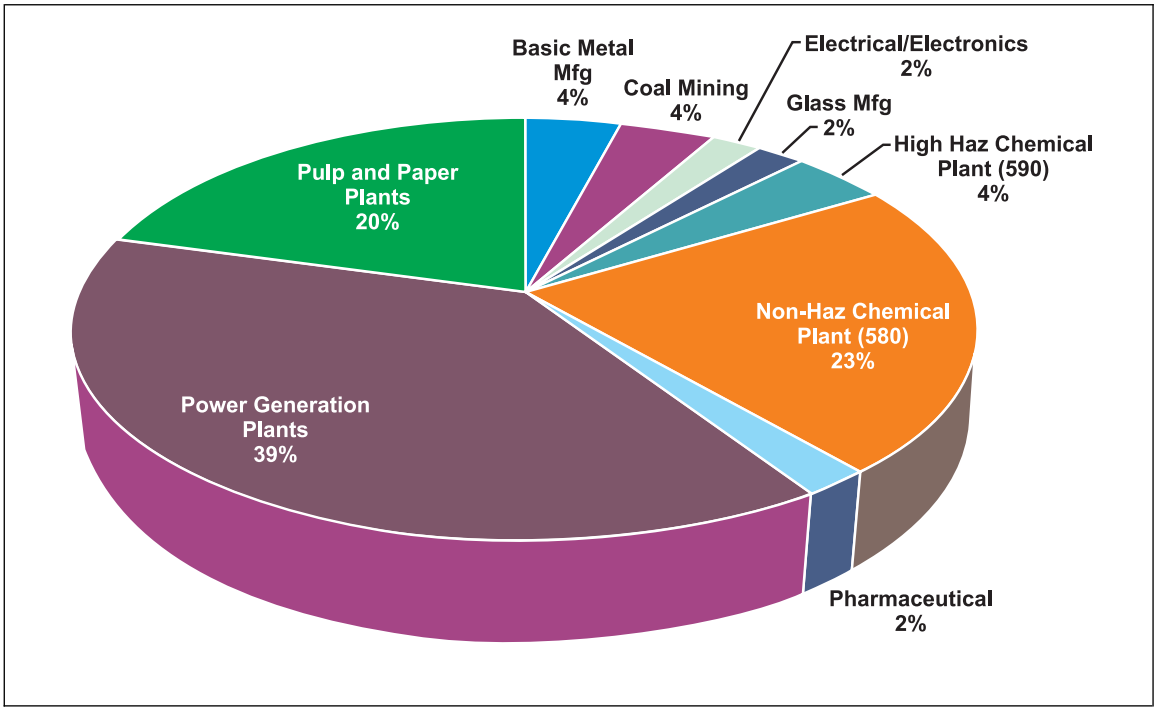

Fig. 3.7. SCAI losses, percentage by occupancy (2007-2016)

4.0 REFERENCES

4.1 FM

Data Sheet 5-23, *Design and Protection for Emergency and Standby Power Systems*
Data Sheet 5-31, *Cables and Bus Bars*
Data Sheet 5-32, *Design and Protection for Emergency and Standby Power Systems*
Data Sheet 7-14, *Fire Protection for Chemical Plants*
Data Sheet 7-43, *Process Safety*
Data Sheet 7-49, *Emergency Venting of Vessels*
Data Sheet 7-110, *Industrial Control System*
Data Sheet 9-0, *Asset Integrity*
Data Sheet 10-8, *Operators*

4.2 Others

American Petroleum Institute (API). API 556, *Instrumentation, Control, and Protective Systems for Gas-Fired Heaters*.

American Petroleum Institute (API). API 521, *Pressure-Relieving and Depressuring Systems*.

ASME International (ASME). ASME Section VIII, *Boiler and Pressure Vessel Code*.

International Electrotechnical Commission (IEC). IEC 61508, *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems*.

International Electrotechnical Commission (IEC). IEC 61511, *Safety Instrumented Systems for the Process Industry*.

International Society of Automation (ISA). ISA TR 84.00.05, *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)*.

International Society of Automation (ISA). ISA TR84.00.02-Part 1, *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques, Part 1*.

International Society of Automation (ISA). ISA-84.00.01, *Safety Instrumented Systems for the Process Industry Sector*.

National Fire Prevention Association (NFPA). NFPA 85, *Boiler and Combustion Systems Hazard Code*

National Fire Prevention Association (NFPA). NFPA 86, *Standard for Ovens and Furnaces*

National Fire Prevention Association (NFPA). NFPA 87, *Standard for Fluid Heaters*

APPENDIX A GLOSSARY OF TERMS

Basic process control system (BPCS): A system that responds to input signals from the equipment under control (EUC) and/or from an operator and generates output signals, causing the EUC to operate in the desired manner. Examples include control of an exothermic reaction, anti-surge control of a compressor and fuel/air controls in fired heaters. Also, referred to as Process Control System.

Bypass: Action or facility to prevent all or specific parts of a safety system from being executed. Bypass can also be known as override, defeat, disable, force, inhibit or muting. An example would be when the output signal from the trip logic to a final element is held in the normal state, preventing final element operation.

Consequence: A consequence is an undesirable result of an incident, usually measured in health and safety effects, environmental impacts, loss of property and business interruption

Demand rate: The frequency with which a protective system is called upon to perform its protective function. It can be calculated considering the number of demands divided by the total elapse operating time during which the demands occurred.

Process operating mode: Any planned state of process operation, including modes such as Start-up (normal and after emergency shutdown), temporary operations, emergency shutdown and shutdown.

Proof test: Periodic test performed to detect dangerous hidden faults.

Emergency stop: The ability to shut down a process independently of safety and process control systems.

Fail dangerous: Failure that deviates the output by more than 2% of span, leaving the output within active scale.

Fail high: Failure that causes the output signal to go to the maximum output current (>20.9 mA, output saturate high) or high alarm (>21 mA).

Fail low: Failure that causes the output signal to go to the minimum output current (<3.7 mA, output saturate low) or low alarm (3.5, 3.75 mA).

Fail-safe: Capability to go to a predetermined safe state in the event of a specific malfunction. These are divided in safe detected (SD) and safe undetected (SU). This failure can cause the instrument to go to the fail-safe state without demand from the process.

Fail-safe state: The output going to fail low or fail high and state where the process reaches a safe situation.

Field devices: Equipment connected to the field side of the SIS I/O terminals. Such equipment includes field wiring, sensors, final control elements and operator interface devices hard-wired to SIS I/O terminals.

Final control element: a device that manipulates a process variable to achieve control.

Hardware fault tolerance (HFT): is the ability of the device to continue to perform a specific safety function in the presence of faults or errors. HFT of N means, that N+1 faults will cause loss of safety functions for the unit.

Hardwired systems: systems are not programmable and require physical changes to wiring or links to change their function. Examples include relay logic and non-programmed electronic logic as well as fiber optic communications links.

Hazardous event: It is defined as an event that can cause harm, which may include danger to people, environment or property

Independent protection layer (IPL): a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event. The effectiveness and independence of an IPL must be auditable.

Input/output (I/O): This all-encompassing term describes input and output modules and devices, or a particular mode of input or output.

Logic solver: The E/E/PES components or subsystems that execute the application logic. The logic solver excludes trip amplifiers, input cards and output cards. Examples are electromechanical relays, solid-state/ magnetic-core logic and the Central Processing Unit (CPU) section of programmable electronic systems.

Output device: an external device that takes a signal created as a result of a PES decision and performs an action.

Output module: a device that either converts digital output from the PES to analog output, or changes the digital output voltage to a level sufficient to operate the output device.

Process control system: See BPCS.

Programmable electronic system (PES): A system based on one or more central processing units connected to sensors and/or actuators in a plant for the purpose of control, monitoring or protection.

Programmable logic controller (PLC): A component of a PES. A digitally operating electronic apparatus using programmable memory. Memory stores instructions and implements specific functions such as logic, sequencing, timing, counting, and arithmetic to control various types of machines or processes via digital and analog input/output devices.

Redundancy: use of multiple elements or systems to perform the same function. Redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

Reliability: probability that a system can perform a defined function under stated conditions for a given period of time.

Risk: the product of the consequence of an accident times the likelihood (probability) of that accident occurring.

Safety controls, alarms, and interlocks (SCAI): Process safety safeguards implemented with instrumentation and controls, used to achieve or maintain a safe state for a process, and required to provide risk reduction with respect to a specific scenario (ANSI/ISA 84.91.01, 2012c).

Safe failure fraction (SFF) ratio: The ratio at which a device experiences safe or detected failure.

Safety function (SF): Function stablished to maintain a safe state of a process from a specific hazardous event.

Safety instrumented function (SIF): See safety function.

Safety integrity level (SIL): One of four possible discrete levels for specifying the safety integrity (reliability) requirements of the safety functions in safety-related systems. SIL 4 has the highest level of safety integrity and SIL 1 the lowest.

Safety instrumented system (SIS): An instrumented system used to implement one or more SIF. SIS are composed of sensors, logic solvers, and final control elements designed to take the process to a safe state when predetermined conditions are violated. Other commonly used terms include emergency shutdown system (ESD, ESS), safety shutdown system (SSD), safety system, and safety interlock system.

Safety system: See safety instrumented system.

Sensor: See input device.

Voting system: Redundant system that requires at least m of the n (MooN) channels to be in agreement before the SIS can take an action.

APPENDIX B DOCUMENT REVISION HISTORY

The purpose of this appendix is to capture the changes that were made to this document each time it was published. Please note that section numbers refer specifically to those in the version published on the date shown (i.e., the section numbers are not always the same from version to version).

July 2023. Interim revision. The following major change was made:

A. Relocated guidance for Safety Instrumented System (SIS) used in lieu of overpressure protection and High Integrity Pressure Protection Systems (HIPPS) to Data Sheet 7-49, *Emergency Venting of Vessels.*

January 2021. Interim revision. The following changes were made:

A. Clarified 2.2.4 to state that safety instrumented systems should be used in lieu of mechanical overpressure devices.

B. Replaced information on the different process hazard analysis (PHA) methodologies in 3.2.3.1 with a reference to Data Sheet 7-43, *Process Safety*.

October 2019. This document has been completely revised. The following major changes were made:

A. Changed the title to *Safety Controls, Alarms, and Interlocks (SCAI)* (from *Instrumentation and Control in Safety Applications*).

B. Reorganized sections and information to align with current industry practices.

C. Redefined the scope of the data sheet to include safety controls and equipment that are in industries other than chemical.

D. Moved the protection guidance for control and equipment rooms to Data Sheet 7-110, *Industrial Control Systems*.

E. Added recommendations for SCAI systems in lieu of other active or passive safety devices.

F. Updated the terminology to bring the data sheet in line with current industry usage.

G. Added guidance on the analysis of process hazards to align with Data Sheet 7-43, *Process Safety*.

H. Added guidance for operators and training to align with Data Sheet 10-8, *Operators*.

September 2000. This revision of the document has been reorganized to provide a consistent format.

October 1998. Major update with emphasis shifted to safety systems rather than process control.

July 1974. Initial document with emphasis on process control and measurement devices.