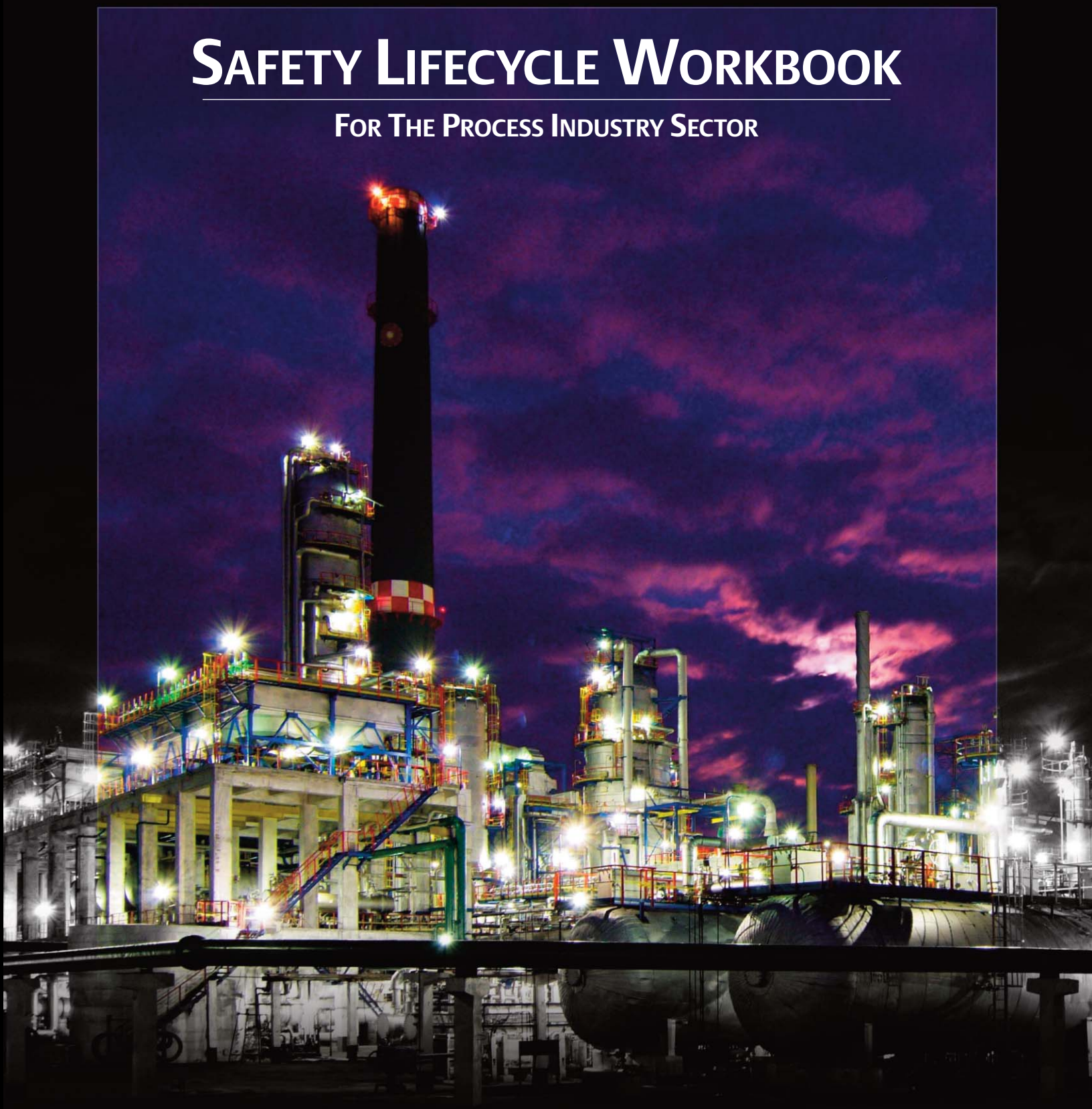
Safety Lifecycle Workbook

For The Process Industry Sector



EMERSON™
Process Management

SAFETY LIFECYCLE WORKBOOK

FOR THE PROCESS INDUSTRY SECTOR

The information and any recommendations that may be provided herein are not intended for any direct or specific application and are presented as being informative in nature. As such, Emerson Process Management assumes no responsibility and disclaims all liability of any kind, however arising, as a result of using the information contained herein. Any equipment and all equipment configurations that might be referenced or selected by the authors are provided as an example only. No representation, expressed or implied, is made with regard to the availability of any equipment, process, formula, or other procedures contained herein.

Notice

Form W-00002 / Printed in USA / 500 AQ / 5-10

We invite you to share your thoughts and practical knowledge about SIS for the benefit of others in the industry.
Join our DeltaV SIS Process Safety System LinkedIn group at:
http://www.linkedin.com/groups?home=&gid=2309437&trk=anet_ug_hm

If you would like to learn more about Emerson's process safety system, please visit our website at
www.DeltaVSIS.com.

EMERSON
Process Management

SAFETY LIFECYCLE WORKBOOK

FOR THE PROCESS INDUSTRY SECTOR

EMERSON
Process Management

This page intentionally left blank

TABLE OF CONTENTS

SAFETY LIFECYCLE WORKBOOK

FOR THE PROCESS INDUSTRY SECTOR

EMERSON
Process Management

Safety Lifecycle continued

Supplier Qualification

Glossary

SAFETY LIFECYCLE WORKBOOK

FOR THE PROCESS INDUSTRY SECTOR

This Safety Lifecycle Workbook was developed to help business leaders and managers in the process industries gain a general understanding of existing industry standards and best practices for Safety Instrumented Systems (SIS). It also provides a practical overview of the safety lifecycle, including checklists and key considerations for each phase.

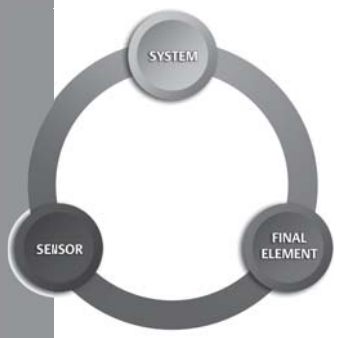
Safety is Mandatory

Of all of the issues facing today's process manufacturers, ensuring safe operations and guaranteeing shutdown when necessary are paramount. Companies that do not plan and manage process operational risks face fines, production outages, equipment damage and serious injury or loss of life.

Conversely, the unwanted consequences of any part of the safety system failing safely as designed, but resulting in nuisance trips, drive an equally important consideration in the application of industrial safety systems.

For that reason, process manufacturers must ensure that design of the SIS is at the heart of an effective safety lifecycle methodology that will enable proper process design and implementation to meet the requirements for both safety and process availability.

With today's technology and best practices, there is no reason not to put safety first. Process manufacturers should be familiar with key international safety standards and concepts to effectively implement safer operations. It is important that process manufacturers work with suppliers that have SIS sensors, logic solvers, and final control elements that meet IEC 61508 standards to enable compliance with IEC 61511 / ISA84 best practices.



To meet safety requirements, the safety loop must take into consideration the sensor, logic solver, and final control element.

EMERSON
Process Management

This page intentionally left blank.

Business Challenges

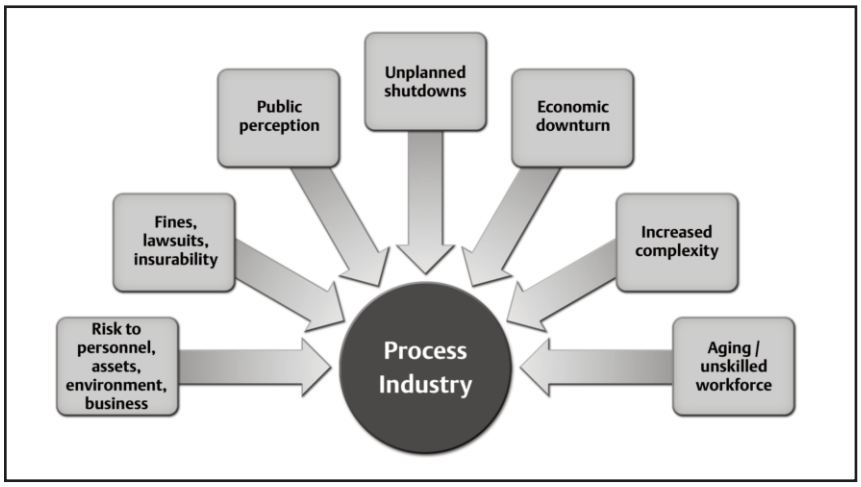


Figure 1: Process Industry Challenges

The business pressures facing process manufacturers today are challenging. The need to optimize plant performance increases as competition grows. These forces drive operational decisions and include:

- Managing risk
- Avoiding fines and lawsuits and maintaining insurability
- Managing public perception and be a community partner
- Avoiding unplanned shutdowns to increase throughput
- Managing costs to quickly response to a changing economy
- Managing the increased complexity of business and processes
- Managing an aging and unskilled workforce.

These business pressures require process manufacturers to improve plant performance.

At the end of the day, every company has a single goal—to increase return on investment. The process safety needs of manufacturers are to optimize process reliability, the flexibility to meet their project goals, increased visibility into their process so that they can better see the status of their equipment, reduced engineering and complexity to help drive costs down, and to simplify regulatory compliance.

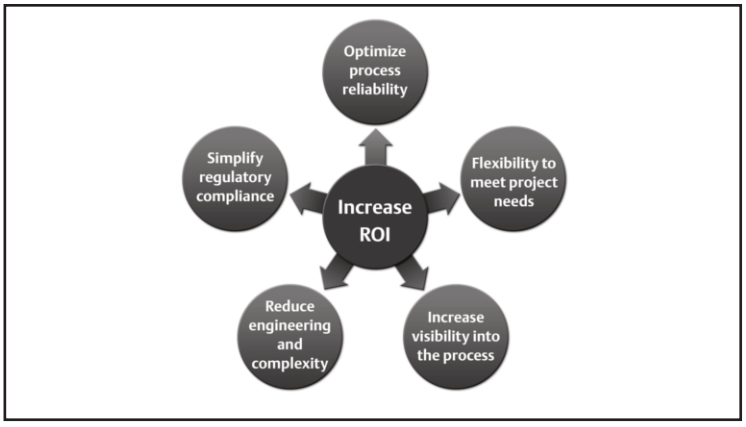


Figure 2: Factors that can increase ROI

EMERSON
Process Management

This page intentionally left blank.

Safety Basics

To understand the requirements for implementing an industrial process safety program, it is necessary to first understand the language of the widely-adopted safety standards. While the list of safety specific concepts is extensive, the most basic terms and frequently used acronyms are summarized below.

Additional acronyms, terms and definitions can be found in the IEC 61508, IEC 61511 and ANSI/ISA 84 standards.

International Safety Standards — IEC & ANSI/ISA

In review of current safety practices, three standards organizations are playing a key role in the development of practical processes that are being used throughout the process industries; International Electrotechnical Commission (IEC) and American National Standards Institute—International Society of Automation (ANSI/ISA). The two leading safety standards documents include:

- IEC 61508 addresses the requirements for manufacturers of safety components used on SIS applications
- IEC 61511 (ANSI/ISA 84) outlines the requirements for end-users and integrators.

IEC 61508 provides guidance to suppliers for the design, development and certification of electronic and programmable electronic devices certified for use in functional safety applications. This certification provides application developers the evidence needed to demonstrate that their application, including the device, is compliant with these requirements.

IEC 61511 (ANSI/ISA 84) provides an application specific adoption of IEC 61508 for the Process Industry Sector and is based on two fundamental concepts: the safety lifecycle and safety integrity levels. The safety life cycle is defined as an engineering process that includes all of the steps necessary to achieve required functional safety.

ANSI-ISA 84 standard fully adopted the process and philosophies detailed in the IEC 61511 document.

Process Hazard Analysis (PHA)

A PHA is the first step in an organized and systematic effort to identify and analyze the significance of potential hazards associated with the processing or handling of highly hazardous chemicals. It provides information which will assist employers and employees in making decisions to improve safety and reduce the consequences of unwanted or unplanned releases of hazardous chemicals. A PHA is directed toward analyzing potential causes and consequences of fires, explosions, releases of toxic or flammable chemicals and major spills of hazardous chemicals. It focuses on equipment, instrumentation, utilities, human actions (routine and non-routine), and external factors that might impact the process. These considerations assist in determining the hazards and potential failure points or failure modes in a process.

Several methods of analysis can be used, including:

- Hazard Operability (HAZOP) Study
- What If? / Checklist
- Failure Mode Effect Analysis (FMEA)
- Fault Tree Analysis
- Event Tree Analysis
- Layers of Protection Analysis

Layers of Protection

One of the goals of the PHA is to validate that the plant design is inherently safe. The design of the process can eliminate many hazards. The remaining hazards need to be identified and accessed in terms of risk. The corresponding safety function used to prevent, control or mitigate each hazard must be assigned to a layer of protection. A typical, risk reduction methods using layers of protection in process plants is shown in Figure 3.

One of the goals of the PHA is to validate that the plant design incorporates the necessary Layers of Protection to make the plant inherently safe. Layer of Protection Analysis (LOPA) is a PHA tool that starts with data developed in the Hazard and Operability analysis (HAZOP study) and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the hazard.

The total amount of risk reduction provided by the layers can then be determined and the need for more risk reduction analyzed. If additional risk reduction is required and if it is to be provided in the form of a Safety Instrumented Function (SIF), the LOPA methodology allows the determination of the appropriate Safety Integrity Level (SIL) for the SIF.

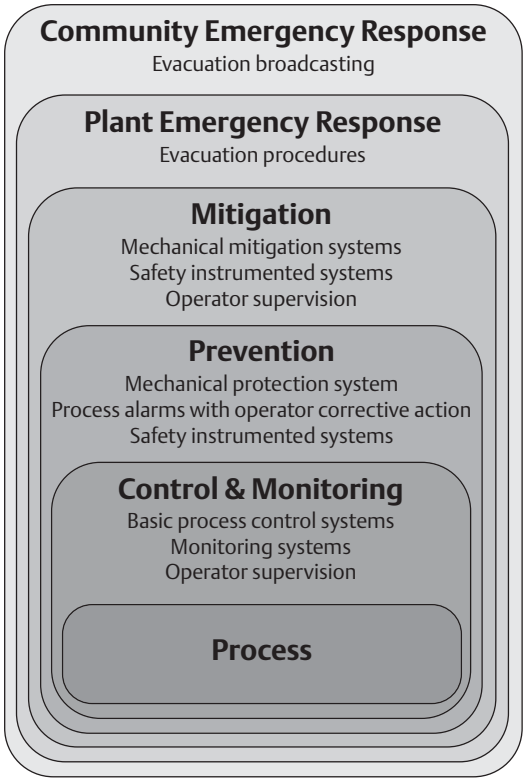


Figure 3: Risk reduction methods used in process plants[1]

Safety Integrity Level (SIL)

The output of the Process Hazards Analysis effort is the operational definition and the assignment of a SIL rating to each safety loop. SIL is defined as a discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest level of risk mitigation. SIL 3 is highest rating used in the process industries.

EMERSON
Process Management

[1]IEC 61511-1 ed. 1.0 Copyright © 2003 Geneva, Switzerland. www.iec.ch

	Probability of failure of SIF	
SIL	Demand mode (probability of a dangerous failure demand)	Continuous mode (probability of failure in an hour)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Table 1: SIL ratings definition[2]

To better understand the impact on safety based on SIL, a more qualitative view of SILs has developed in terms of consequence of the SIS failure. The table below defines the consequence in terms of facility damage, personnel injury, and the public or community exposure.

SIL	Generalized View
4	Catastrophic Community Impact
3	Employee and Community Impact
2	Major Property and Production Protection. Possible Injury to Employee
1	Minor Property and Production Protection

Table 2: SIS Failure consequence based on SIL rating[3]

The international standards IEC 61508 and IEC 61511 define SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL.

The SIL requirements for hardware safety integrity are based on probabilistic analysis of the device. To achieve a given SIL, the device must have less than the specified Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{avg}). These failure probabilities are calculated by performing a Failure Modes, Effects, and Diagnostic Analysis (FMEDA). The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used.

[2]IEC 61511-1 ed. 1.0 Copyright © 2003 Geneva, Switzerland. www.iec.ch
[3]Summers, Angela E., Ph.D. "Techniques for Assigning a Target Safety Integrity Level." ISA Transactions 37 (1998) 95-104. Geneva, Switzerland.

The SIL requirements for systematic safety integrity define a set of techniques and measures required to prevent systematic failures (bugs) from being designed into the device or system. These requirements are met by establishing a rigorous development process as summarized in IEC 61508 Section 7.

Alternatively, the end user can self-certify the device by establishing that the device has sufficient operating history to certify that the device has been "proven in use".

Safety Instrumented System (SIS)

IEC 61511 defines a safety instrumented system (SIS) as an "instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s)."

Safety Instrumented Function (SIF)

A SIF is designed to respond to the conditions within a plant that may be hazardous in themselves, or if no action is taken, could result in a hazardous event. Each SIF is assigned a specified SIL necessary to achieve functional safety. A SIF can be addressed through either a safety instrumented protection function or a safety instrumented control function (SIS). A SIF is designed to respond to the conditions within a plant that may be hazardous in themselves, or if no action is taken, could result in a hazardous event. The challenge in SIF design is to select the equipment that mitigates the risk defined in the PHA, meets lifecycle cost goals and meets safety integrity goals.

How do SIFs and SILs relate to each other?

Based on the specific process application, a risk reduction factor (SIL rating) must be defined for each safety loop (SIF). The required SIL level of a specific SIF is determined by taking into account the required risk reduction factor (defined in the PHA process) that is to be provided by that function. SIL ratings vary for SIFs that operate in continuous mode verses demand mode.

INDUSTRY STANDARDS

As a benchmark for the reduction of risk associated with personnel, environmental and property protection systems, international standards are now being used as guidelines to demonstrate that "best engineering practice" has been applied in the development of safety instrumented systems.

Complimenting a breadth of prescriptive standards traditionally used by the process industry, it has become important to ensure that the safety system has been designed to fully comply with the performance-based requirements of IEC 61508, ANSI/ISA 84, and/or IEC 61511.

While these standards and guidelines do not have the force of law in most countries, increasing dependence on SIS systems compels process manufacturers to ensure that a methodical approach is used to verify that the tolerable risk target has been achieved. In addition, the organization must ensure and document individual and organizational competency in the design and functional safety management processes.

> "All persons involved in any overall, E/E/PES or software safety lifecycle activity, including management activities, should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform. The training, experience and qualifications of all persons... should be assessed in relation to the particular application."[4]

To meet industry's demand for competency, process manufacturers and safety suppliers are increasingly required to have formalized certification programs that ensure their employees are trained and the safety applications are implemented in accordance with a process compliant to ANSI/ISA 84, IEC61508 and IEC61511. To provide assurance of adherence to these standards, TÜV, Exida and other third-party certification organizations can audit these programs to ensure that the certified quality processes are being strictly followed.

This section briefly reviews the performance-based standards (IEC 61508, IEC 61511, and ANSI/ISA 84) to provide a context for their use and implementation.

IEC 61508 –SIS Hardware / Software Design Guidance

The IEC 61508 Functional Safety Standard published by the International Electrotechnical Commission (IEC) is applicable to a wide range of industries and applications and is written as primary guidance for the supplier community in relation to the development of systems used for the reduction of risk. Targeted at suppliers of safety-related equipment, IEC 61508 defines a set of standards for functional safety of electrical/ electronic/programmable electronic (E/E/PE) safety related systems.

Functional safety is defined as the overall program to ensure that the safety-related E/E/PE system brings about a safe state when called upon to do so.

EMERSON
Process Management

[4]IEC 61508-1 ed. 1.0 Copyright © 1998 IEC Geneva, Switzerland. www.iec.ch

The IEC 61508 standard is composed of seven parts, including general safety requirements, specific system and software requirements, and guidelines to applications. The standard is generic and can be used directly by industry as a standalone standard. International standards organizations can use this standard as a basis for the development of industry-specific standards, such as the machinery industry sector, the process industry sector, or for the nuclear industry sector. It is suggested that when evaluating a safety system, or related services, the user/owner should consider selecting a company that is certified to IEC 61508 by an independent third-party, such as TÜV or Exida.

The IEC 61508 standard requires the product developer to validate the safety integrity of a system considering all causes of failure, both random hardware failures and systematic failures, including hardware failures, software induced failures, failures due to electrical interference and other environmental stresses.

IEC 61508 –SIS Hardware Design Validation

Some of these types of failures, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand.

A Failure Modes, Effects, and Diagnostic Analysis (FMEDA) should be performed on the safety component as part of a full assessment according to the functional safety standard IEC 61508. This full assessment includes an assessment of all fault avoidance and fault control measures during hardware and software development and demonstrates full compliance with IEC 61508 to the end-user.

The FMEDA document describes the results of the hardware assessment to determine the fault behavior and failure rates from which the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{avg}) are determined. It provides the safety instrumentation engineer with the required failure data as per IEC.

IEC 61508 –SIS Software Design Validation

IEC 61508 Part 3 covers the software requirements within this standard. It applies to any software used in a safety-related system or software used to develop a safety-related system. This software is specifically referred to as safety-related software. This part of the standard provides details of the software safety life cycle, a process to be used when developing software.

To insure integrity in the software used in safety systems, the IEC 61508 standard requires that the SIS vendor have a rigorous Software Quality Plan as outlined in Part 3; Clause 7, including the following software safety lifecycle requirements:

7.1 General Requirements
7.2 Software safety requirements specification
7.3 Software safety validation planning
7.4 Software design and development
7.5 Programmable electronics integration (hardware and software)
7.6 Software operation and modification procedures
7.7 Software safety validation
7.8 Software modification
7.9 Software verification

In the standard IEC 61508-3 Annex A provides a listing of "techniques and measures" used for software development where different development techniques are chosen depending on the SIL level of the software.

Annex B has nine detailed tables of design and coding standards as well as analysis and testing techniques that are to be used in the safety-related software development, depending on SIL level of the software and in some cases the choice of the development team.

IEC 61511 – SIS Design Guidance for the Process Industry Sector

Since the publication of the IEC 61508 safety standard and, more recently, the IEC61511 standard for the process industry sector (including ANSI/ISA 84.00.01-2004), interest in performing rigorous hazard and risk analysis and applying certified safety instrumented systems has increased considerably within the user community.

These standards provide guidance on best practice and offer recommendations, but do not absolve their users of responsibility for safety. The standards deal not only with technical issues but also include the planning, documentation and assessment of all activities required to manage safety throughout the entire life of a system.

The standard is based on two fundamental concepts: the safety life cycle and safety integrity levels. The safety life cycle is defined as an engineering process that includes all of the steps necessary to achieve required functional safety. The standard includes extensive documentation requirements and utilizes statistical techniques for the prediction of hardware failures. The standard focuses attention on risk-based safety-related system design and requires significant attention to detail that is vital to safety system design.

The basic philosophy behind the safety life cycle is to develop and document a safety plan, execute that plan, document its execution (to show that the plan has been met) and continue to follow that safety plan through decommissioning – with further appropriate documentation being generated throughout the life of the system.

Changes along the way must similarly follow the pattern of planning, execution, validation, and documentation. The IEC61511 standard is comprised of three parts which mirror the structure of ANSI/ISA-84.00.01-2004 for consistency:

IEC 61511-1: Framework, definitions, system, hardware and software requirements (Serves as the basis for this workbook).
IEC 61511-2: Guidelines on the application of IEC 61511-1
IEC 61511-3: Guidance for the determination of the required safety integrity levels

ANSI/ISA-84.00.01-2004 SIS for the Process Industry Sector

This international standard addresses the application of safety instrumented systems based on the use of electrical/electronic/programmable electronic technology. This standard has fully adopted the processes and philosophies detailed in the IEC 61511 document with the exception of a "grandfather" clause which provides a provision to allow safety systems built prior to the issuance of the 1996 standard to remain in operation by stating:

> "For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner."[5]

The concept of the "grandfather clause" originated with OSHA 1910.119. The grandfather clause's intent is to recognize prior good engineering practices and to allow their continued use with regard to existing SIS systems. This alignment is intended to lead to a high level of consistency of underlying principles, terminology, and information within the process industries worldwide.

In accordance with IEC 61511, the ANSI/ISA-84 addresses all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning. It requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems and sets out an approach for all safety life-cycle activities to maintain these defined requirements.

[5] Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA 84.01-2004, "Application of Safety Instrumented Systems (SIS) for the Process Industry," Research Triangle Park, NC (2004).

The ANSI/ISA-84 standard is comprised of three main documents (mirroring IEC 61511), plus a series of Technical Reports (TR) which include:

- ANSI/ISA-84.00.01-2004 Part 1 - Framework, Definitions, System, Hardware and Software Requirements
- ANSI/ISA-84.00.01-2004 Part 2 - Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1
- ANSI/ISA-84.00.01-2004 Part 3 - Guidance for the Determination of the Required Safety Integrity Levels
- ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 1: Introduction
- ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 2: Determining the SIL of a SIF via Simplified Equations
- ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL); Evaluation Techniques, Part 3: Determining the SIL of a SIF via Fault Tree Analysis
- ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 4: Determining the SIL of a SIF via Markov Analysis
- ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 5: Determining the PFD of Logic Solvers via Markov Analysis
- ISA-TR84.00.03-2002, Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS)
- ISA-TR84.00.04-2005, Part 1: Guideline on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)
- ISA-TR84.00.04-2005, Part 2: Example Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)
- ANSI/ISA-91.00.01-2001, Identification of Emergency Shutdown Systems and Controls that are Critical to Maintaining Safety in Process Industries
- ISA-TR91.00.02-2003, Criticality Classification Guideline for Instrumentation.

Additional Industry Standards

The table below lists some additional standards that may relate to functional safety in the process industry.

American Petroleum Institute (API)	
API RP 500A (1997)	Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities Classified as Class 1, Division 1 and Division 2
API RP 551 (1993)	Process Measurement Instrumentation
Council of the European Union	
Seveso Directive 96/82/EC	Control of Major-Accident Hazards Involving Dangerous Substances
Factory Mutual (FM)	
FM 3611 (10/99)	Non-incendive Electrical Equipment for Use In Class I and II, Div. 2 & Class III, Divisions 1 & 2 Hazardous (Classified) Locations
Fieldbus Foundation	
FF-816	Fieldbus Specification 31.25 K Baud Physical Layer Profile
AG-181	Foundation Fieldbus System Engineering Guidelines
International Electrotechnical Commission (IEC)	
IEC 61511-1, 2, & 3 -2003	Functional safety – Safety instrumented systems for the process industry sector, Parts 1, 2, and 3
IEC 61508-2 - 2000	Functional safety of electrical/electronic/programmable electronic safety-related system – Part 2
IEC61000-4-3	Radio Frequency Interference and Immunity Standard
Institute of Electrical and Electronic Engineers (IEEE)	
IEEE 518-1982	Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources.
Instrumentation, Systems and Automation Society (ISA)	
ANSI/ISA-84.00.01-2004 (IEC 61511 modified) Part 1, 2, & 3	Functional safety – Safety instrumented systems for the process industry sector – Parts 1, 2, and 3
ISA-12.2	Non-incendive Design and Wiring Practices
ISA-5.1-1984 (R1992)	Instrumentation Symbols and Identification.
ISA-5.2-1976 (R1992)	Binary Logic Diagrams for Process Operations.
ISA-5.3-1983	Graphic Symbols for Distributed Control/Shared Display Instrumentation, Logic and Computer Systems.
ISA-5.4-1991	Instrument Loop Diagrams.
ANSI/ISA-12.12.01-2002	Non-incendive Electrical Equipment for Use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations
ISA-18.1-1979 (R1992)	Annunciator Sequences and Specifications.
ISA 71.01	Environmental Conditions for Process Measurement and Control Systems: Temperature and Humidity
ISA-71.04	Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants
National Electrical Manufacturers Association (NEMA)	
NEMA ICS 6-1993 (R2001)	Industrial Control and Systems: Enclosures
National Fire Protection Association (NFPA)	
NFPA 70 (2002)	National Electrical Code
Occupational, Safety and Health Administration (OSHA)	
29 CFR 1910.119	Process Safety Management Regulation
Environmental Protection Agency (EPA)	
40 CFR 68	Risk Management Plan Regulation

Safety Instrumented Systems Architecture

A Safety Instrumented System (SIS) is defined as an instrumented system used to implement one or more safety instrumented functions (SIF) composed of any combination of sensor(s), logic solver(s), and final elements(s). These systems are designed to take action to bring the equipment under control to a safe state when a process is beyond the range of normal operating limits and other layers of control, including operators and the basic process control system (BPCS), are unable keep the process within safe operating limits.

There are two basic architectures for SIS systems:

1. **Standalone SIS systems** are isolated systems; or they can be integrated into the control system by mapping the necessary data across a physical communications layer to provide integrated control and operator access to safety information.

2. **Integrated Control and Safety Systems** (ICSS) are based upon a native communications structure between the BPCS and SIS systems—sharing engineering, operations, and maintenance environments, with physically separate and independent power supplies, communication channels, and control hardware/software functions.

Separation and Diversity

With either architecture, experienced industry professionals support a rigorous philosophy of separation and diversification for the BPCS and SIS.

IEC61511 defines this separation in the following clauses:

9.5.2 Assessment shall consider SIF independency, diversity and physical separation.

10.3.1 "Note: Non-safety instrumented functions may be carried out by the SIS to ensure orderly shutdown or faster startup. These should be separated from the safety instrumented functions."[5]

11.2.4: "If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised."[6]

The design requirements detailed in IEC61508 focus on the separation of safety and BPCS control functions in different controllers for the following reasons:

- **Independent failures**—Minimize the risk of simultaneous failure of a control system along with the SIS.
- **Security**—Prevent changes in a control system from causing any change or corruption in the associated SIS.

EMERSON
Process Management

[6]IEC 61511-1 ed. 1.0 Copyright © 2003 Geneva, Switzerland. www.iec.ch

- **Different requirements for safety controllers**—A safety system is normally designed to fail in a safe way; whereas, a BPCS is usually designed to maximize process availability.
- **Safety functionality**—An SIS is based upon the functionality of extended diagnostics, special software error checking, protected data storage and fault tolerance. The design of the BPCS should include not causing any change or corruption in the associated SIS.

Stand Alone Safety Instrumented Systems

Traditionally, stand-alone safety systems have been used to maintain the separation between the control and safety functions. This means that data exchange between the divergent operator interfaces, engineering workstations, configuration tools, data and event historians, and asset management systems had to be engineered using a ModBus, OPC or IP gateway. The gateway would pass select information from the safety system to the control system by mapping specific data points for use by the operator interface.

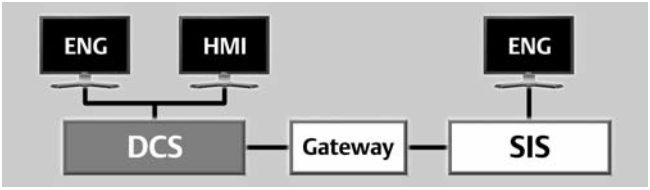


Figure 4: Disparate BPCS and SIS Architecture

More recently this approach is being used when the safety system must be upgraded but the legacy control system is still in its active lifecycle with continued investment and support by the equipment manufacturer.

Justification for the standalone approach must account for the added cost of engineering the communication subsystem so that data from the SIS can reliably be displayed on the control system operator interface. In addition, much of the useful diagnostic data provided by smart instruments is stranded at the device because data mapping of all information through the gateway becomes cost prohibitive.

Considerations also exist for the long term operational expense of the divergent BPSC and SIS systems, including personnel training, maintenance, spare parts, and the respective support contracts that must be maintained.

Integrated Control and Safety Instrumented (ICSS)

Today, integrating physically separate and functionally independent control and safety systems into a common communication framework is a cost effective solution for many manufacturers. This common framework has become a reality because the safety standards for process industry applications support an integrated approach to the common functions of the two systems.

Figure 5: Integrated yet Separate BPCS and SIS Architecture

With this integrated approach, common communication systems allow free information exchange between the BPCS, SIS and ancillary systems—while providing safeguards to prevent corruption of the systems by the exchanged data. In addition, overhead functions can be shared between the BPCS and SIS systems because they are considered outside of the safety function. These functions include configuration, operations, maintenance, asset management, training, time synchronization, alarm handling, audit trail, version control, event recording, user security, and historical archiving.

In keeping with the philosophy of architectural independence, ICSS system isolation should include physical separation and both hardware and software diversification between the integrated BPCS and SIS system platforms. In the SIS system, the power supplies, communication channels, hardware, and real-time operating systems must be ***completely independent*** of the BPCS—maintaining the separation promoted by mainstream safety philosophies.

The integrated configuration environment simplifies and streamlines the engineering effort. This approach eliminates the need for expensive data mapping, and handshaking logic that is common in disparate solutions. The result of the ICSS integrated but separate architecture allows operators to more effectively manage the process from a single operating environment.

Keep in mind that ICSS solutions are not simply a product or a specific control and safety system brand name. ICSS has become a proven strategy for building an all digital architecture, a blueprint for building solutions that optimize plant performance by:

- **Leveraging digital intelligence** —The intelligence (smarts) available in today's field devices represents a new source of previously unavailable information, including diagnostics that enable predicting and preventing problems before they impact process availability.

- **Connecting the plant** — Open communication standards link devices, systems, and applications in a secure, robust plant-wide network designed to ensure that process and equipment information is available wherever it's needed.

- **Controlling your process** — The more you know about your process and its operating equipment, the easier it is to improve production and achieve high-integrity process availability.

- **Optimizing your assets**—Digital technologies permit tapping into the architecture's information flow in order to increase uptime, optimize performance, and reduce maintenance costs.

The resulting cost benefit of an ICSS effects all phases of the system lifecycle, including reduced hardware, configuration, training, maintenance, spare parts inventory and common support contracts.

This page intentionally left blank.

SAFETY LIFECYCLE

The safety lifecycle is defined as an engineering process that includes all of the steps necessary to achieve required functional safety. The lifecycle addresses all necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.

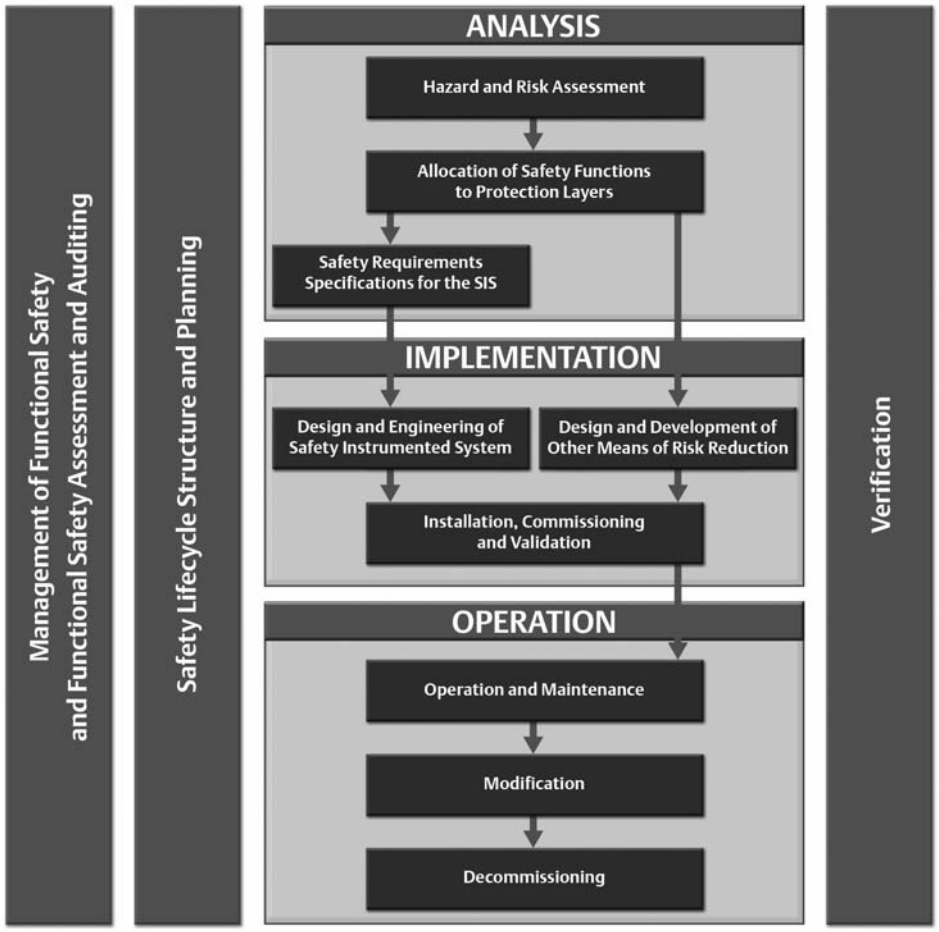


Figure 6: IEC 61511 / ISA84 Safety Lifecycle[7]

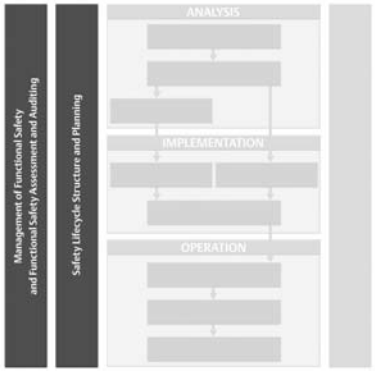
This workbook overviews each phase of the IEC 61511 / ISA 84 safety lifecycle as well as provides checklists and key considerations based on practical experience. ***The activities represented by the tall vertical boxes are in place throughout the entire lifecycle.***

EMERSON
Process Management

[7]IEC 61511-1 ed. 1.0 Copyright © 2003 Geneva, Switzerland. www.iec.ch

Safety Lifecycle Overview

Throughout the Lifecycle



Management of Functional Safety and Functional Safety Assessment and Auditing

This phase identifies the management activities that are necessary to ensure functional safety objectives are met. A Safety Management System (SMS) must be in place to ensure that functional safety objectives are met and appropriate auditing processes are defined.

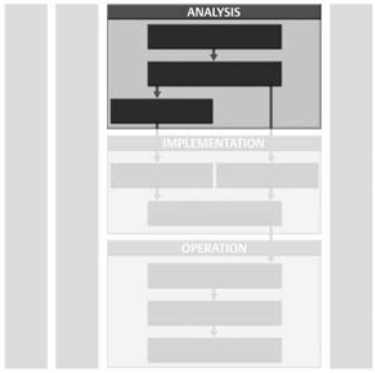
Safety Lifecycle Structure and Planning

The SMS should establish the safety lifecycle phases and requirements to ensure that the SIS meets safety requirements. The Management of Functional Safety & Functional Safety Assessment and Auditing phase and the Safety Lifecycle Structure and Planning phase are both addressed on the pages titled, Safety Management System.

Verification

Verification demonstrates by review, analysis, and/or testing that the outputs satisfy the requirements. Each phase of the safety lifecycle must include verification activities.

Analysis Phase



Hazard and Risk Assessment

This assessment is conducted to fully understand the hazards that the system will be designed to mitigate and to identify the architecture and related SIS system design requirements.

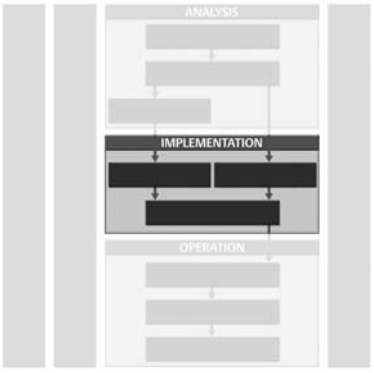
Allocation of Safety Functions to protection Layers

Allocation of safety functions involves assigning integrity levels to each of the safeguards that are used in the process to achieve the required level of safety in the process.

Safety Requirements Specifications for the SIS

Safety Requirement Specification (SRS) is the document that ensures the safety requirements are adequately specified prior to proceeding to detailed design.

Implementation Phase



Design and Engineering of SIS

The objective of this phase is to design the SIS to provide the necessary safety instrumented functions with the specified safety integrity levels.

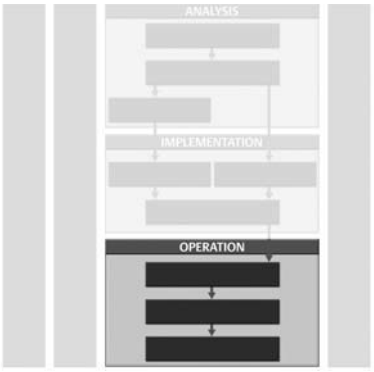
Design and Development of Other Means of Risk

The objective of this phase is to design and engineer the other layers of protection to meet safety requirements.

Installation, Commissioning, and Validation

Following physical installation and loop testing of the safety related equipment, validation involves the pre-startup verification of the integrated system against the requirements stated in the Safety Requirements Specification.

Operation Phase



Operation and Maintenance

Operation and Maintenance involves procedure-based response to system alarms and the performance of periodic functional testing of each SIF component to ensure as-designed system operation.

Modification

Modifications to the SIS must be properly planned, reviewed, and approved prior to making the change. The required safety integrity level for each SIF must be maintained despite any changes to the SIS.

Decommissioning

Proper review and approval must be conducted prior to the decommissioning of any SIS from active service.

Safety Management System

Objective

The manufacturer should have a written program to define the overall strategy with respect to Safety Instrumented Systems (SIS). This policy declares the use of a safety life cycle approach that meets the requirements of the IEC 61511 standard, from hazardous analysis to specification to system validation and eventual decommissioning. The scope of the Safety Management System (SMS) is separate and distinct from all other general health and safety measures that are necessary for the achievement of safety in the workplace.

The SMS addresses the ongoing Management of Functional Safety and Functional Safety Assessment and Auditing, as well as the Safety Lifecycle Structure and Planning phases of the lifecycle and the corresponding activities.

Description

The SMS should address the following:

- Functional safety management
  - ❑ Safety organization
  - ❑ Safety leadership team
  - ❑ SIS management team
  - ❑ Project leadership
  - ❑ Safety audit and revision
  - ❑ Competency policy
- Safety lifecycle
- Supporting processes
  - ❑ Selection and approval of contractors
  - ❑ Selection and approval of supplier equipment
  - ❑ Selection and approval of safety tools
  - ❑ Safety modification process.

Outputs

Documented Safety Management System

Verification Activity

Review and approval of SMS and associated auditing processes before the project begins

Responsibility

Process manufacturer

SMS Considerations

Safety Organization	A distinct organization should be defined to handle all matters related to functional safety. Only those resources identified and certified as being part of that organization will work on the SIS content of the project. The requirements for functional safety will apply equally to external resources.
Safety Leadership Team	A SIS leadership team shall be responsible for the operation of functional safety and the content of the procedures. This team will perform the following safety-related tasks: · Propose SIS company policies for adoption · Advise personnel of corporate policies and ensure polices are adhered to with regard to the sale, engineering, supply, and support of SIS products and services · Advise personnel of corporate training and certification standards · Ensure that corporate training and certification standards for SIS personnel are met and maintained · Support quality and SIS evaluations of potential sub-vendors, in accordance with company procedures · Perform periodic reviews of SIS procedures · Support periodic quality audits of operational centers to ensure compliance with company SIS procedures.
SIS Management Team	The SIS management team will meet annually to address any outstanding issues and constantly work towards company-wide standardization of SIS processes, but may convene at anytime to respond to specific circumstance.
Project Leadership	Each project will have a designated SIS leader, who will be responsible for the SIS content of that project.
Safety Audit and Revision	Audits and inspections may be performed by project personnel or by independent persons (e.g., operations group, QA department, regulators, customers, or third parties). Audits will include any aspects of SIS activities in compliance with Quality Management Standards (QMS).
Competency Policy	All resources used in roles which effect Functional Safety will be described in a separate document and certified as competent to perform that role. The competencies required for each role, as well as the certification procedure, will also be described. Prior to using a particular resource in a role, it will be the responsibility of the resource's supervisor within the safety organization to ensure that the resource is competent to perform the role.

Verification

Objective

A Safety Verification Plan manages changes and demonstrates by review, analysis and/or testing that the system satisfies the requirements defined in the Safety Requirements Specifications.

Description

The Safety Verification Plan (SVP) should address:

- Technical basis for the change
- Impact of the change on safety and health
- Procedures to be used for non-conformances
- Activities to take place and items to be verified
- Any modification to operating procedures
- Time period for the change
- Authorization requirements.

Employers should notify and train affected employees and update process safety information and operating procedures as necessary.

Outputs

- Project-specific Safety Verification Plan
- Operational Safety Verification Plan
- Results of verification efforts with appropriate authorization

Verification Activity

During project implementation, a project-specific SVP provides a systematic and structured list of all activities for each stage of the safety lifecycle, as well as verification of these completed activities.

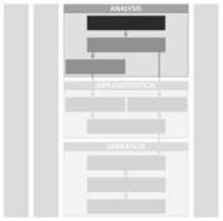
During operation, a separate SVP defines the ongoing process to manage and verify changes.

Responsibility

Project-specific Safety Verification Plan:
Process manufacturer and service provider
Operational Safety Verification Plan:
Process manufacturer
Results of verification efforts:
Party making the changes

Example Verification Checklist

Activity	Documentation	Responsibilities		Verification of Completed Activity	
		Service Provider	End User	Signature	Date
Hazard & Risk Assessment					
Documentation Validation	Process Flow Diagrams (PFDs) P&IDs Operating Information		Produce and Approve		
Process Hazard Analysis (PHA)	PHA method and resulting analysis		Produce and Approve		
Risk Assessment	Existing risk matrices and risk standards PHA SIL assignment method		Produce and Approve		
Allocation of Safety Functions to Protection Layers					
Allocate non-instrumented protection layers and SIS layers	Description of hazards, existing safeguards and required risk reduction		Produce and Approve		
Allocate safety instrumented protection layers	Description of hazards, risk assessment and residual risk reduction required after other layers of protection have been applied		Produce and Approve		
Safety Requirements Specification for SIS					
SRS	General requirements System requirements SIF requirements		Produce and Approve		
Design and Engineering of SIS					
Logic Design (conceptual and detailed)	I/O details Field wiring details Panel layout and power requirements	Produce	Approve		
SIL Test Procedures	SRS P&IDs SIF list Equipment list	Produce	Approve		
Factory Acceptance Test (FAT)	Test specifications Detailed design	Produce	Approve		
Installation, Commissioning and Validation					
Site Acceptance Test (SAT)	Test specifications Installation manuals	Produce	Approve		
Commission field equipment	Approved calibration methods Instrument specifications Calibration certificates	Produce	Approve		
SIS validation	Approved written test procedures SRS SIF list		Produce and Approve		



Hazard and Risk Assessment

Objective

This assessment is conducted to identify hazards and hazardous events of the process and associated equipment, process risks, requirements for risk reduction, and safety functions necessary to achieve an acceptable level of risk.

Description

A hazard and risk assessment is carried out on the process and associated equipment.

Outputs

A description of the hazards, of the required safety function(s), and of the associated risks, including:

- Identified hazardous events and contributing factors
- Consequences and likelihood of the event
- Consideration of operational conditions (startup, normal, shutdown)
- Required risk reduction to achieve required safety
- References and assumptions
- Allocation of safety functions to layers of protection
- Identified safety functions as SIFs.

Responsibility

Process manufacturer

This assessment is conducted to fully understand the hazards that the system will be designed to mitigate and to identify the architecture and related SIS system design requirements.

Each phase of the lifecycle must include Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

Hazard and Risk Assessment Methods

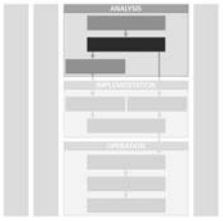
In a process plant, the manufacturer converts raw materials into valuable products. This conversion requires processes that can create hazardous conditions with significant consequences if not properly controlled. These hazardous conditions can be caused by a variety of factors, including toxic materials, flammable materials, and dangerous process conditions (i.e. high pressure or temperature). A Process Hazard Analysis (PHA) is performed to identify potential hazards in the operation of a process manufacturing plant.

When conducting a PHA, the following requirements need to be considered:

- Hazards of the process
- Previous incidents with catastrophic potential
- Engineering and administrative controls and consequences of failures
- Facility setting
- Human factor
- Qualitative evaluation of effects of failure
- Personnel qualifications
- Ongoing follow up.

Methods used for PHA can vary from simple checklists to complex Hazard and Operability Studies (HAZOP). The list below includes common techniques used for PHA :

1. Checklist:	This technique is typically used with mature processes and equipment where the process is stable and no changes are made. It involves making a list of issues to address based on the process and equipment used.
2. What If?	This technique is conducted with a multi-disciplinary team and uses brainstorming to ask questions. It can focus directly on a problem area and relies heavily on the facilitator and experience of the team members.
3. What If/ / Checklist:	This technique combines both of the above approaches.
4. HAZOP:	This technique provides a prioritized basis for the implementation of risk mitigation strategies. It provides a formal structure and includes: review of P&ID drawings, examination of deviations from design conditions, identification of all failure causes, and identification of existing safeguards and protection.
5. FMEA:	The Failure Mode Effect Analysis technique is a systemic method of analysis and is typically used for mechanical failures. It examines the effect of multiple failure combinations.
6. Fault Tree Analysis:	This technique provides an efficient means of evaluating the likelihood of an unwanted event taking place. The Fault Tree does not identify the "top event" or hazard. It relies on another PHA to identify this hazard.
7. Event Tree Analysis:	This approach consists of one initiating event branching through several intermediate events to one of all possible outcomes.
8. Layers of Protection Analysis:	This technique provides alternative safe paths when a deviation is moving towards hazardous consequences.



Allocation of Safety Functions to the Protection Layers

Objective

This phase allocates safety functions to protection layers and for each safety instrumented function (SIF), the associated safety integrity level (SIL).

Description

This allocation activity includes the analysis of the protection needed for specific safety functions for the purpose of prevention, control or mitigation of hazards from the process and its associated equipment.

Outputs

A description of allocation of safety requirements, including:

- Determine the allocation of safety functions to protection layers
- Define SIFs
- Determine SIL for each SIF.

Responsibility

Process manufacturer

Allocation of Safety Functions involves assigning integrity levels to each of the safeguards that are used in the process to achieve the required level of safety the that process.

Each phase of the lifecycle must include Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

SIL Assignment

Once the hazard and risk assessment has is completed, the risk associated with the process in terms of event severity and likelihood should be understood. There are no regulations that assign a SIL to particular processes or hazards. The assignment of SIL is a company decision based on risk management and risk tolerance philosophy.

> "ANSI/ISA S84.01-1996 does mandate that companies should design their safety instrumented systems (SIS) to be consistent with similar operating process units within their own companies and at other companies. Likewise, in the US, OSHA PSM and EPA RMP require that industry standards and good engineering practice be used in the design and operation of process facilities. This means that the assignment of safety integrity levels must be carefully performed and thoroughly documented."[8]

Various methods, both qualitative and quantitative, are used to convert PHA data into SIL levels. The most common methods are listed below:

- **Modified HAZOP:** This approach is an extension of the HAZOP process and relies on the subjective assignment of SIL based on the team's expertise. Since this method is subjective, team member consistency from project to project needs to be addressed.

- **Consequence only:** This method uses an estimation of the potential consequence of the incident and does not take into effect the frequency. Therefore, all incidents involving a fatality would have the same SIL regardless of likelihood. This approach is the simplest to use, but also the most conservative.

SIL	Generalized View
4	Potential for fatalities in the community
3	Potential for multiple fatalities
2	Potential for major serious injuries or one fatality
1	Potential for minor injuries

- **Risk matrix:** This technique provides a correlation of risk severity and risk likelihood to the SIL. This approach is commonly used.

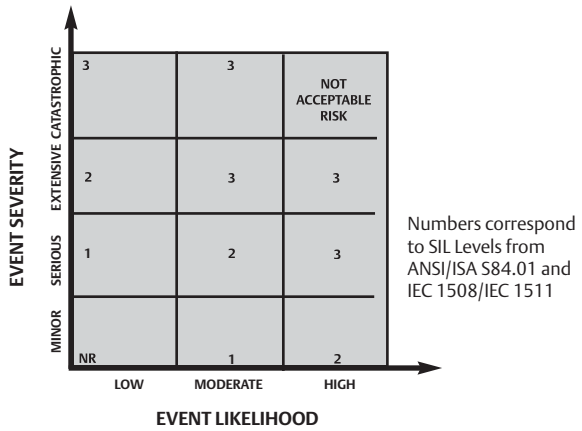
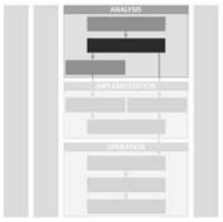


Figure 7: Risk Matrix[7]

[8]Summers, Angela E., Ph.D. "Techniques for Assigning a Target Safety Integrity Level." ISA Transactions 37 (1998) 95-104. Geneva, Switzerland.



SIL Assignment

- **Risk graph:** This approach provides a correlation based on four factors:
  - ❑ Consequence (C)
  - ❑ Frequency and exposure time (F)
  - ❑ Possibility of avoiding the hazardous event (P)
  - ❑ Probability of the unwanted occurrence (W)

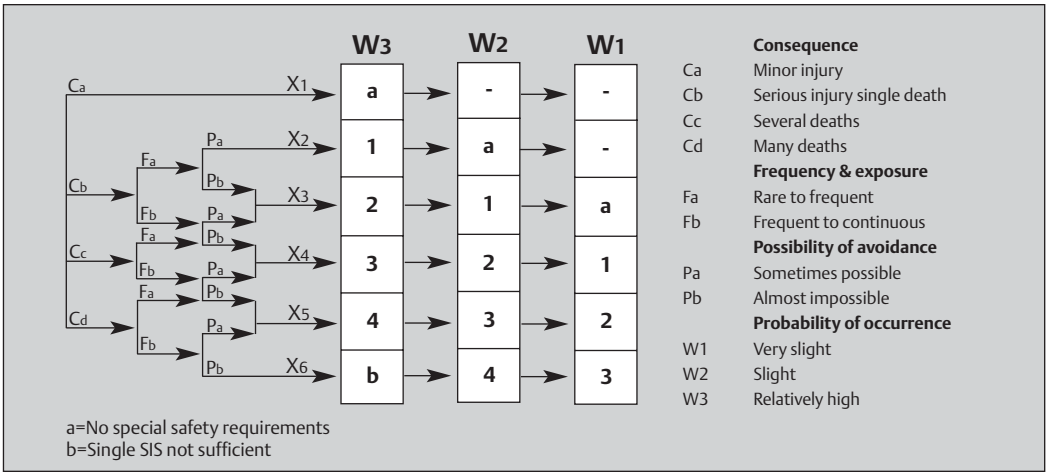


Figure 8: Risk Graph[9]

- **Quantitative assessment (i.e. fault tree or process demand):** This technique assigns SIL by determining the process demand or incident likelihood and requires an extensive understanding of potential causes and probability of failure. This quantitative approach is the most rigorous technique.

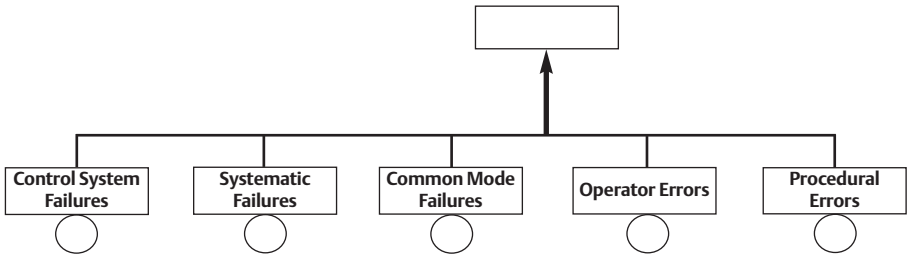


Figure 9: Risk Graph[10]

[9] Gruhn, Paul and Henry L Cheddie, "Safety Instrumented Systems: Design Analysis and Justification". 2nd edition (2006) 94 Research Triangle Park, NC.
[10] Summers, Angela E., Ph.D. "Techniques for Assigning a Target Safety Integrity Level." ISA Transactions 37 (1998) 95-104. Geneva, Switzerland.

- **Company mandated SIL:** This approach assumes that the greatest cost increase occurs when a SIL is greater than 1; therefore, the company takes the approach that all SIFs shall be SIL3. This assignment technique is the least time consuming, reduces documentation of SIL selection and ensures consistency.

Assigning SIL levels requires the examination of safety, community, environmental, and economic risks. Documented procedures must be developed to ensure that SIL assignment is consistent within the company.

Safety Requirements Specification for the SIS

Objective

The SRS specifies the requirements for the SIS in terms of the required safety instrumented functions in order to achieve the required functional safety.

Description

This phase of the lifecycle is critical to the success of the SIS. 44% of SIS failures are due to incorrect specifications—not the design and implementation of these requirements.

Outputs

The Safety Requirements Specifications (SRS) should include the following information:

- Identified all SIFs necessary for required functional safety
- Identified common cause failures
- Defined safe state for each SIF
- Demand rate for SIFs
- Proof test intervals
- Response time required
- SIL for each SIF
- SIS process measurements and trip points
- SIS process outputs for successful operation
- Relationship of inputs, outputs and logic required
- Manual shutdown, overrides, inhibits, and bypass requirements
- Starting up and resetting of SIS
- Allowable spurious trip rate
- SIF requirements for each operational mode
- Meantime to repair for SIS
- Identified dangerous combination of SIS output states
- Identified extreme environmental conditions
- Identified normal and abnormal modes and requirements for SIS to survive major event.

Responsibility

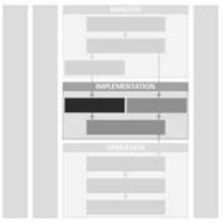
Process manufacturer with support from the engineering contractor and/or SIS supplier

Safety Requirement Specification is the document that ensures the safety requirements are adequately specified prior to proceeding to detailed design, construction, installation, and commissioning.

Each phase of the lifecycle must include Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

Example Safety Requirements Specifications Checklist

General Requirements	Completed
List the regulations, codes, and standards with which the SRS will comply.	
Define the extremes of environmental conditions that are likely to be encountered by the SIS.	
Describe modes of operation for the plant, including normal and abnormal.	
System Requirements	**Completed**
Identify dangerous combinations of outputs that need to be avoided.	
Define interfaces between SIS and other systems.	
Define feasible mean time to repair for SIS.	
Define failure modes and desired response from SIS.	
Define SIS response time to bring process to safe state.	
Identify sources for common cause failures.	
Define manual shutdown requirements.	
Define actions required to achieve a safe state if SIS detects a fault.	
Define maximum allowable spurious trip rate.	
Provide engineering units for each process variable.	
SIF Requirements	**Completed**
Describe all SIFs necessary to achieve required functional safety.	
Provide operational description of each SIF.	
Provide unique name for each SIF.	
Define SIL rating for each SIF.	
Define demand mode and demand rate for each SIF.	
Define the safe state of the process for each SIF.	
Define proof test interval for each SIF.	
Define process safety response time for each SIF.	
Define trip and alarm information for each SIF.	
Define reset requirements for each SIF.	
Define the operation and clearing of an override/inhibit/bypass for each SIF.	
Define failsafe or fault tolerance for each SIF.	



Design and Engineering of SIS

Objective

This phase includes the design of the SIS to meet the requirements for safety instrumented functions and safety integrity.

Description

In this phase, one or multiple SIS systems are designed and developed to provide the SIFs and meet the SILs detailed in the Safety Requirements Specifications. This design activity needs to take into account:

- Requirements for operability, maintainability, and testability to facilitate human factor requirements
- Human capabilities and limitations suitable for the task
- Placing the process in a safe state until the SIS is reset
- Manual means for shutdown independent of the logic solver
- Independence between the SIS and BPCS and the SIS and other protection layers
- Dedicated SIF devices
- Loss of power

During this phase, a documented application software life cycle should be used that includes:

- Requirements
- Architecture design
- Software development
- Module development
- Code development and testing
- Module testing
- Software testing
- Integration testing

Outputs

The design documents generated in this phase include:

- Conceptual Design Guidelines
- Software conceptual design
- Hardware conceptual design
- Software test plans
- Hardware test plans
- Integration Test plans
- FAT planning and test plans

Responsibility

Process manufacturer, engineering contractor, or SIS supplier

Design and engineer the SIS to provide the SIFs and meet the specified SILs.

Each phase of the lifecycle must include Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

SIS Design and Engineering

The design and engineering for the SIS includes all SIF components—sensor(s), logic solver, and final control element(s).

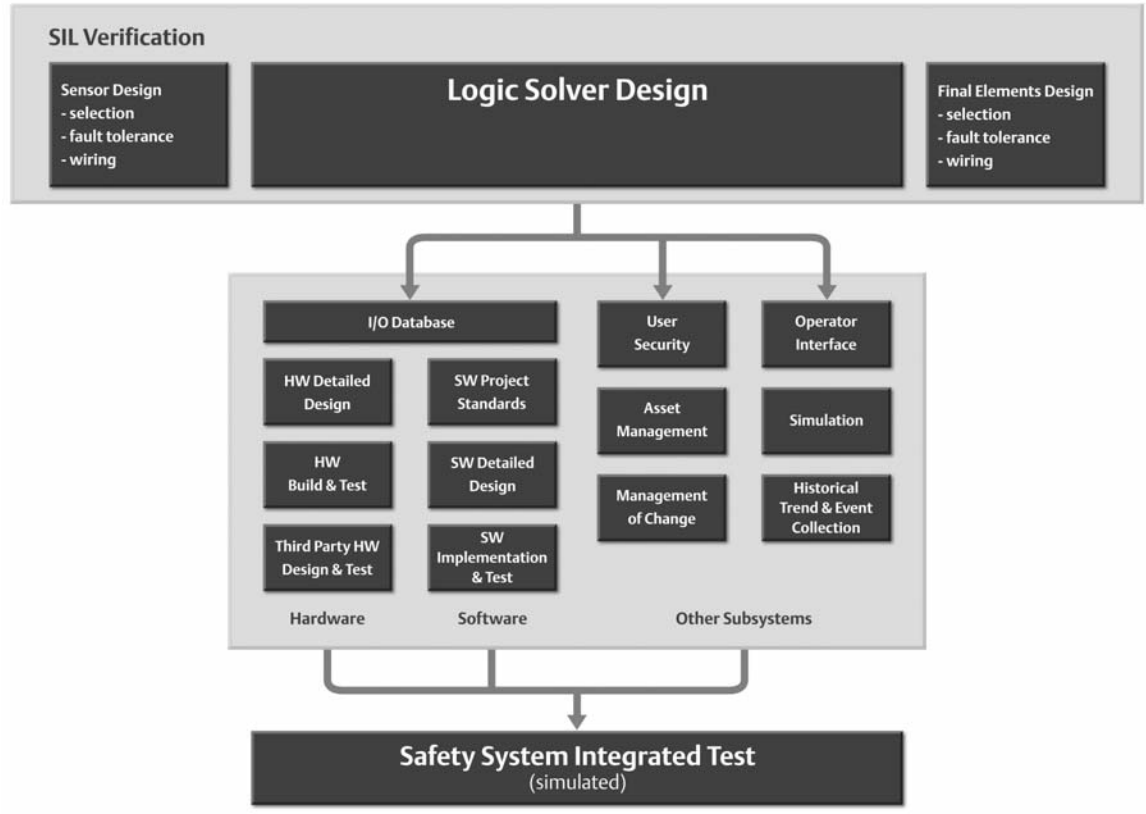
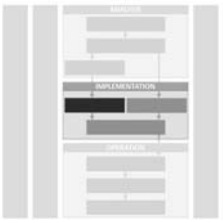


Figure 10: SIS Design includes all SIF components.



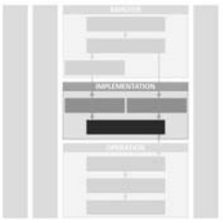
Example Design Checklist

General Design Requirements	Completed
Design of SIS is in accordance with SRS.	
Non-safety functions in the SIS that can negatively affect any SIF shall comply with highest SIL level.	
If BPCS is not qualified, BPCS must be separate and independent from SIS.	
Operability, maintainability, and testability shall facilitate human factor requirements in the SIS design. HMI shall take into account human capabilities and limitations.	
Manual means (independent of logic solver) shall be provided to actuate the SIS final control elements unless otherwise stated in the SRS.	
A device used as part of a SIF shall not be used for basic process control if that device failure causes loss of process control and subsequent demand on the SIF – unless risk is acceptable.	
Components and Subsystems Design	**Completed**
Selected components and subsystems shall comply with IEC 61508-2 and IEC 61508-3 standards as appropriate.	
For each SIF, the sensor(s), logic solvers, and final elements(s) shall have a minimum fault tolerance.	
Suitability of selected components and subsystems shall be demonstrated.	
Components and subsystems shall be consistent with SRS.	
Software Design	**Completed**
Define system interfaces and required communications.	
Verify that each I/O point type and service description complies with the SRS.	
Verify that the installed spare capacity meets SRS.	
Verify that each SIF name, description, SIL level, Risk Reduction Factor, and references comply with SRS.	
Verify that all SIFs listed in the SRS are accounted for in the software design.	
Verify that the plant area allocation is consistent with BPCS design philosophy.	
Ensure that the plant alarm priority philosophy has been considered. Ensure SIS alarm priorities are consistent with BPCS design.	
Ensure that the primary display for each SIF has been considered.	
Ensure that the alarms generated provide enough detail to enable correct operator response.	
Verify that any HOLDs have been considered.	
Ensure operator interface design considerations been considered.	

Example FAT Planning and Checklist

FAT Planning (Items to be specified)	Remarks
Type of tests to be performed	
Test cases, test description and test data	
Dependence on other systems/interfaces	
Test environment and tools	
Logic solver configuration	
Test criteria	
Procedures for corrective action	

FAT Checklist	Remarks
System Set-up and basic tests have been completed as per the requirements.	
Carryout HW FAT	**Remarks**
All HW documents required for FAT are available.	
All wiring is correctly terminated and labelled	
All panel and hardware labels are clear and present.	
Power supply voltages and fusing are correct.	
Redundancy checks have been completed.	
HW diagnostics are as expected	
Carryout the required percentage of HW I/O checks	
Ensure all witnessed tests are signed off by the responsible FAT team member including the end user.	
Record HW FAT results.	
Carryout SW FAT	**Remarks**
All SW documents required for FAT are available.	
Correct versions of SW and Firmware including patches and hot-fixes are installed.	
By using the agreed FAT methods demonstrate to the end user against his supplied documentation: · I/O Database · Diagnostics · Logic · Operator Interface · Historical Trend & Event Collection	
Ensure all witnessed tests are signed off by the responsible FAT team member including the end user.	
Record SW FAT results.	



Installation, Commissioning and Validation

Objective

This activity ensures that the SIS is installed according to specifications, commissioned to prepare for final system validation, and is validated through inspection and testing that the SIS achieves the requirements stated in the SRS.

Description

The installation and commissioning activity should address:

- Procedures, measures and techniques to be used
- Schedule of activities to take place
- Persons and organization responsible for the activities.

The validation activity should include:

- Validation of SIS with SRS
- Validation of relevant operational modes
- Procedures, measures, and techniques to be used
- Schedule of activities to take place
- Persons and organization responsible for the activities
- Reference information against which validation will be carried out.

Outputs

Appropriate records that the SIS has been installed properly according to design and installation plans.

Appropriate records that the SIS has been commissioned properly.

Appropriate records that the SIS has been validated, including:

- SIS validation plan version
- SIF function number test with reference to SRS
- Tools and equipment used, along with calibration data
- Results of each test
- Test specification version
- Acceptance criteria for integration tests
- SIS hardware and software versions tested
- Discrepancy between expected and actual results
- Analysis and decisions made based on discrepancy.

Responsibility

Process manufacturer with support from engineering contractor and/or SIS supplier.

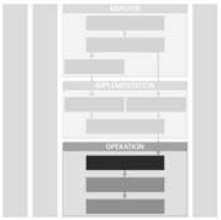
Following physical installation and loop testing of the safety related equipment, validation involves the pre-startup verification of the integrated system against the requirements stated in the Safety Requirements Specification.

Each phase of the lifecycle includes Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

Example Checklists

Installation and Commissioning Checklist	Test Results		
	P	F	N/A
Is the grounding properly connected?			
Is power properly connected and operational?			
Has the packing materials and transportation stops been removed?			
Is any physical damage evident?			
Have all instruments been properly calibrated?			
Are all field devices, I/O, and logic solvers operational?			
Are SIS interfaces to other systems operational?			

Validation Checklist	Test Results		
	P	F	N/A
Verify that SIS performs under normal and abnormal operating modes as identified in SRS.			
Confirm that adverse interaction between BPCS and other connected systems do not affect the SIS.			
Verify that the communication between BPCS and other connected systems works properly.			
Confirm that the sensors, logic solvers, and final elements perform as defined in SRS.			
Verify that the SIS documentation consistent with installed system.			
Confirm that SIFs perform as specified on invalid process variable values.			
Verify that proper shutdown sequence is activated.			
Confirm that the SIS provides proper annunciation and proper operation display.			
Verify that computations included in the SIS are correct.			
Confirm that bypass functions operate correctly.			
Confirm that start-up overrides operate correctly.			
Confirm that manual shutdown systems operate correctly.			
Verify that proof test intervals are documented in maintenance procedures.			
Verify that diagnostic alarm functions perform as required.			
Verify that the SIS performs as required on loss of utilities.			
When utilities are restored, confirm that the SIS returns to the desired state.			
Confirm that the EMC immunity, as defined by the SRS, has been achieved.			



Operation and Maintenance

Objective

The operation and maintenance phase ensures that the required SIL of each SIF is maintained and the functional safety of the SIS is maintained.

Description

During this phase, the SIS operation and maintenance activities should address:

- Routine and abnormal operation
- Proof testing, preventive and breakdown maintenance
- Procedures, measures and techniques to be used
- Verification of adherence to procedures
- Schedule of operation and maintenance activities
- Persons and organization responsible.

Outputs

Appropriate records of operation and maintenance activities need to be kept, including:

- Routine actions to maintain functional safety
- Actions and constraints to prevent an unsafe state or reduce the consequence of a hazardous event
- System failure and demand rates
- SIS audit and test results
- Maintenance procedures when failures occur
- Proper calibration of test equipment.

Responsibility

Process manufacturer with support from SIS supplier.

Operation and Maintenance involves procedure based response to system alarms and the performance of periodic functional testing of each SIF component to ensure as-designed system operation.

Each phase of the lifecycle includes Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

Online Testing

Testing of SIS devices is required to maintain SIL level ratings. The frequency of this testing is defined by the SIL analysis. Each component of the SIF, sensor(s), logic solver(s), final control element(s), must be tested.

Automatic online testing can conducted on sensors and logic solvers if configured properly. These elements have the capability to perform self diagnostic testing and do not require offline testing except during scheduled plant shutdowns. The frequency of the SIF component testing will help extend the proof test interval.

Partial stroke testing (PST) can be used to reveal a majority of failures in the final control elements—which are the most likely to fail of the SIS devices. Automatic partial stroke testing has several advantages over manual partial stroke testing, including:

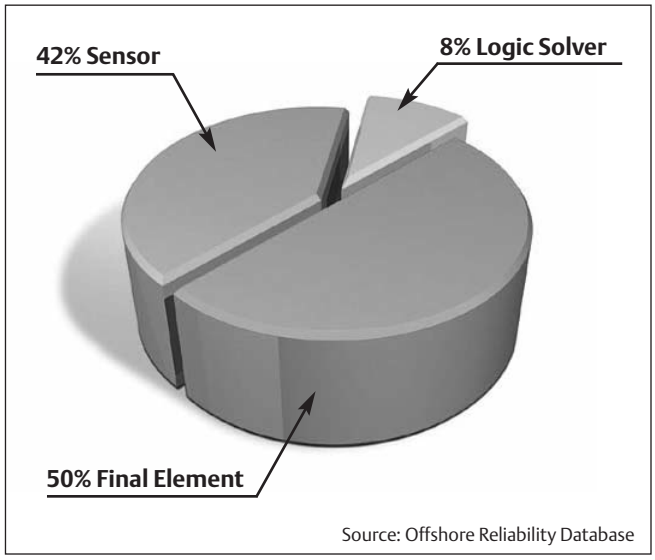
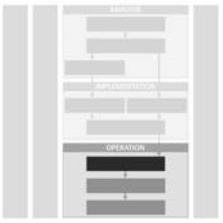


Figure 11: Failure rates of SIS components

- Provides a real time view into the overall health of the device
- Avoids significant recurring labor costs
- Initiates on specified test intervals to reduce the possibility of non-operability
- Removes blocking requirements of conventional safety valve testing methods
- Provides automated documentation for easy compliance
- Improves reliability of testing
- Does not reduce SIS availability
- Provides confirmation that the valve is back in the proper mode and position
- Eliminates need for training to PST procedure.



Proof Testing

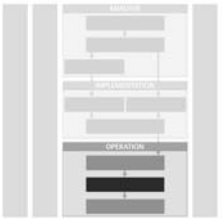
Proof testing is conducted offline at intervals defined in the SIL analysis. A schedule must be setup and executed at the specified frequencies in order to maintain the SIL rating.

SIF Proof Tests	Test Procedure	Frequency (months)
Sensors		
Logic Solver		
Final Element		
Partial Stroke		

Documentation

To maintain compliance with standards, the documentation for both online and proof testing must be maintained throughout the safety lifecycle. This documentation can be collected manually or electronically and should include the following information:

Test Documentation	Remarks
Test /Inspection Performed	
Test/Inspection Date	
Name of Person Conducting Test	
Serial Number or Unique Identifier of System Tested	
Results of the Test/Inspection	



Modification

Objective

This phase ensures that modifications to the SIS are properly planned, reviewed and approved prior to making the change. Additionally, the required safety integrity level for each SIF must be maintained despite any changes made to the SIS.

Description

During this phase, it is important that procedures and a documented process for authoring and controlling changes is in place prior to making changes to the SIS.

Outputs

Appropriate record of modifications should be kept, including:

- Description of the change
- Reason for the change
- Identified hazards
- Analysis of the impact
- All required approvals
- Tests used to verify that the change was properly implemented and the SIS performs as required
- Configuration history/audit trail
- Tested used to verify that the change has not adversely impacted parts of the SIS that were not changed.

Responsibility

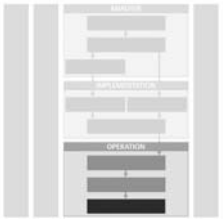
Process manufacturer

Modifications to the SIS must be properly planned, reviewed, and approved prior to making the change. The required safety integrity level for each SIF must be maintained despite any changes to the SIS.

Each phase of the lifecycle includes Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

Modification Procedures

Scope	Defines the method to be used to manage changes to an SIS.
Purpose	Provides a consistent approved process for the capture and control of modifications to an SIS, so that the modified system remains in compliance with IEC 61511.
Change Request Record	The change request record will include: · Reason for the change · Technical basis for the change · Safety and health considerations
Change Request Evaluation	Prior to any modification, a broad assessment of safety and environmental implications will be performed to identify the impact: · On all stages of the safety lifecycle · To other SIFs in the SIS · To other layers of protection outside of the SIS · To the operating plant and other site activities Where the impact of the change is minor and well understood, a checklist will be reviewed by an authorized person, who will communicate the changes to others, who will be effected. For a more complex or significant design change, a hazard evaluation procedure with approvals by operations, maintenance, and safety departments, will be appropriate. All review conclusions, in terms of each safety life-cycle stage that will be affected and the extent of revalidation that will be required, will be recorded.
Change Request Approval and Authorization	Prior to implementing an SIS modification, the appropriate approval and authorization of the requested change is required.
Change Request Implementation	All SIS modifications will only be performed in accordance with the marked-up or reissued design documentation, after the completion of all previous verification steps and approvals. Modification must address, in addition to the technical change: · training and communications for those involved in the operation and maintenance of the process prior to start-up of the process · pre-start-up inspection · documentation citing that equipment and procedures be returned to their original or designed conditions at the end of the temporary change Each SIF associated with a modified logic solver will require revalidation, and all other logic solvers will require verification to ensure that their configuration has been unaffected by the modification.
Documentation	Modification documents include the change control request, supporting documents, as-built records, and test results.



Decommissioning

Objective

Prior to decommissioning any SIS from active service, a proper review should be conducted with required approvals. During decommissioning activities, required SIFs must remain operational.

Description

During this phase, procedures for authorizing and controlling changes should remain in place during decommissioning activities.

Outputs

Appropriate record of modifications should be kept, including:

- Procedures identifying and requesting work to be done
- Identifying hazards that may be affected
- Analysis of the impact on functional safety as a result of the proposed decommissioning activity
- Results of the impact analysis
- Proper authorization before decommissioning.

Responsibility

Process manufacturer

Proper review and approval must be conducted prior to the decommissioning of any SIS from active service.

Each phase of the lifecycle includes Verification activities. Verification demonstrates by review, analysis and/or testing that the outputs satisfy the requirements.

Management of Change

Throughout the safety lifecycle, it is important to keep records of actions taken to ensure that the SIS performs correctly. The standards require that every change made to the system be documented. Various types and sources of information will need to be recorded and organized.

With the use of technology, this once overwhelming task can be addressed with minimal effort.

For engineering modifications, embedded system functionality such as version control and audit trail enables you to keep a complete history of logic changes, including:

- Change rational
- Impact of the change
- Testing required
- Date
- Author
- Approver.

In addition, instrument/device configuration and calibration information need to be recorded.

For online changes, role-based user access can provide flexibility to define the security structure to match your operating philosophy. User groups and assigned privileges help ensure that only appropriate personnel are authorized to make changes. Electronic signatures can require confirmation in which the user's name and password is needed to execute, as well as additional user name and password if required.

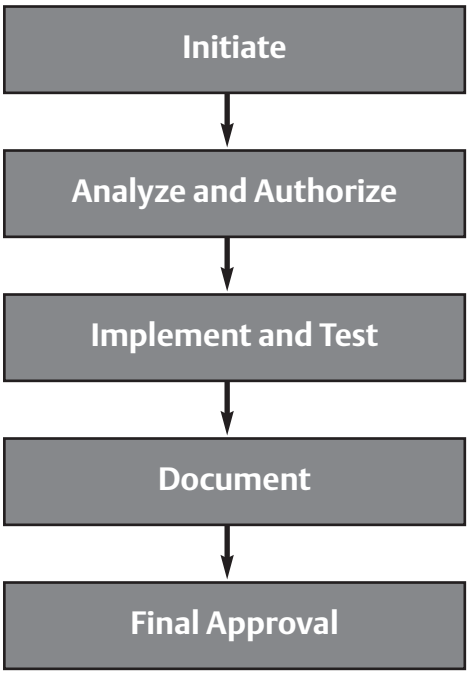
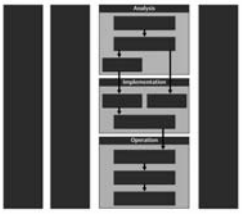


Figure 12: MOC Process

To support compliance requirements during operation, a comprehensive history of process events, alarms, and operator actions needs to be automatically recorded.



Security

To safeguard your assets and ensure proper access, system security is important and should be defined in the SRS—both physical and cyber access to the system. Security is about ensuring business continuity and it is best achieved by designing a unified defense-in-depth strategy and architecture that can defend against a myriad of possible business interruptions.

> "The underlying premise of a unified depth-in-defense strategy is simple—no single mechanism offers adequate protection against the variety of attackers and their evolving weapons. Therefore, it is best to create a series of protection layers designed to impede attackers in the hopes that they can be detected and repelled or simply give up and go elsewhere to seek less fortified installations."[11]

A sounds security strategy must include extensive policies, practices and enforcement.

System access using passwords can offer further benefits of ensuring personnel qualification and training through the use of role-based passwords access.

Physical security can also be supported with secure switches, firewalls, and intrusion protection. Security is critical to prevent unauthorized changes to your safety system.

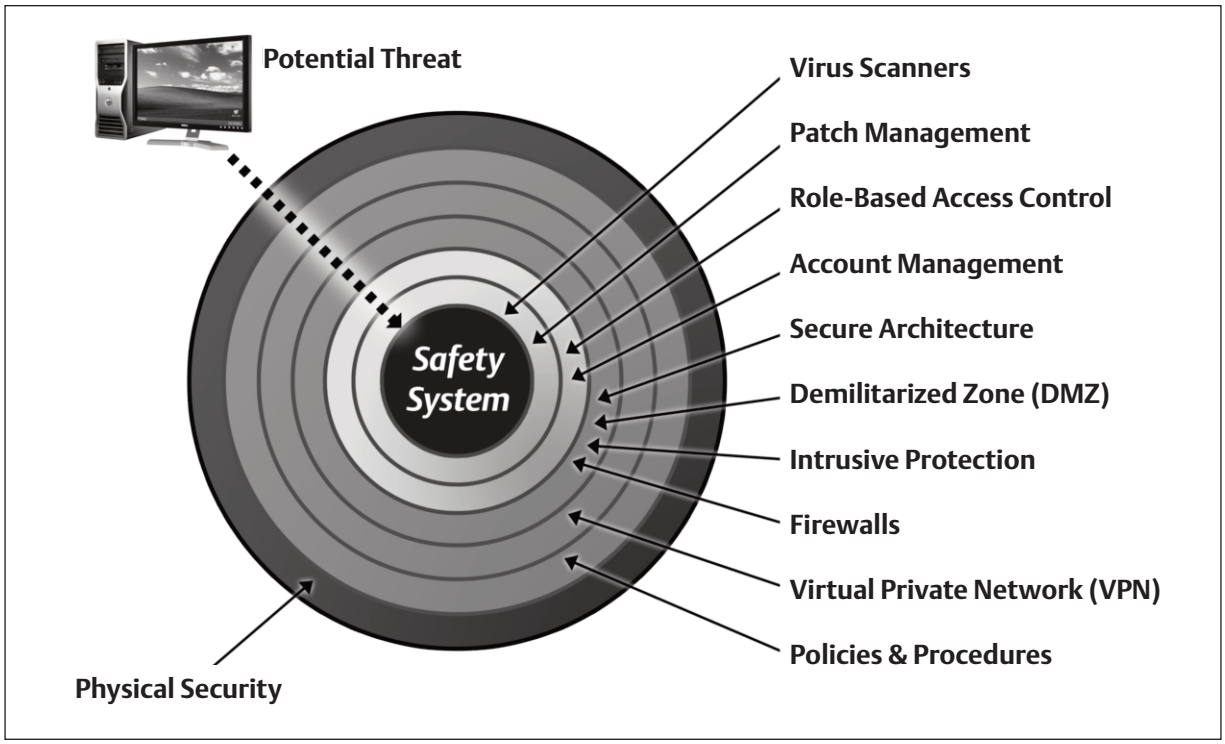


Figure 13: SIS Cyber Security

[11] *Bob Huba and Chuck Miller, "Addressing SIS Cyber Security: First or Last?", Control Engineering, May 2009.*

SUPPLIER QUALIFICATION

Quality cannot be tested into software or products. It must be built in. A process manufacturer should have evidence that a supplier's products and/or services are high quality. This assurance can be from:

- Certification of IEC 61508 compliance by a third-party for a safety-related product
- Prior-use data that supports the conclusion that the product is safe to use in that application
- Certification of IEC 61511 compliance by a third-party of a service provider.

To gather further evidence of a vendor's quality product and/or service, a process manufacturer can evaluate and qualify a supplier's business and quality practices.

Expectations

- **Financial stability**—helps ensure that supplier will be in existence to provide future support
- **Proven experience in the safety industry**—provides evidence that the supplier understands your needs
- **Previous business experience**—your company's past project experience with this supplier. Did the supplier perform to expectations (quality, cost, schedule)?
- **Active quality programs and standards certification**—helps ensure that consistency and quality are part of the supplier's processes and culture
- **Formal documented product development methodology based on IEC 61508 standards**—helps ensure that product development is not dependent on an individual's creativity, but is a result of a planned process
- **Formal documented application software product development methodology based on IEC 61511 standards**—helps ensure that application software is not dependent on an individual's creativity, but is a result of a planned process for generating modular, consistent, documented quality application software
- **Established change control procedures** as part of the product development—helps ensure that each version of product software functions as expected, with proper levels of testing and documentation
- **Defined personnel qualifications**—ensures that properly trained and certified individuals develop both product software and application software
- **Factory training and support**—supports your compliance efforts during the operation and maintenance phases of the lifecycle.

Product and Service Certification

Suppliers that provide safety products and/or services to the process industries should be certified by a third-party or provide prior-use data to verify compliance with IEC standards.

PRODUCTS:

- IEC 61508 certification by third-party
- Prior-use data

SERVICES:

- IEC 61511 certification by third-party
- Safety certified personnel.

EMERSON
Process Management

Supplier Evaluation Checklist

Company	
Location	

FOCUS AREA	Rating		Remarks
	Pass	Fail	
Financial stability			
Industry Expertise			
Previous Business Experience			
Quality processes/certification			
Product development per IEC 61508 and other industry best practices			
Application software development and hardware design per IEC 61511 and other industry best practices			
Change control/software release procedures			
Personnel qualifications for product development			
Application qualifications for application development			
Factory training			
Ongoing support, including on-site services, technical support, and product upgrades			

GLOSSARY[12]

architecture	arrangement of hardware and/or software elements in a system
asset protection	function allocated to system design for the purpose of preventing loss to assets
basic process control system (BPCS)	system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL 1
common cause failure	failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure
common mode failure	failure of two or more channels in the same way, causing the same erroneous result
component	one of the parts of a system, subsystem, or device performing a specific function
configuration management	discipline of identifying the components of an evolving (hardware and software) system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life cycle
dangerous failure	failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state
device	functional unit of hardware or software, or both, capable of accomplishing a specified purpose (for example, field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes field wiring, sensors, final elements, logic solvers, and those operator interface devices hard-wired to SIS I/O terminals)
electrical/electronic/ programmable (E/E/PE)	based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology
external risk reduction facilities	measures to reduce or mitigate the risks, which are separate and distinct from the SIS
failure	termination of the ability of a functional unit to perform a required function
final element	part of a safety instrumented system which implements the physical action necessary to achieve a safe state
functional safety	part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers
functional safety assessment	investigation, based on evidence, to judge the functional safety achieved by one or more protection layers

EMERSON
Process Management

[12]IEC 61511-1 ed. 1.0 Copyright © 2003 Geneva, Switzerland. www.iec.ch

functional safety audit	systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives
hardware safety integrity	failures in a dangerous mode of failure
hazard	potential source of harm
impact analysis	activity of determining the effect that a change to a function or component will have to other functions or components in that system as well as to other systems
input function	function which monitors the process and its associated equipment in order to provide input information for the logic solver
instrument	apparatus used in performing an action (typically found in instrumented systems)
logic function	function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions); logic functions provide the transformation from one or more input functions to one or more output functions
logic solver	that portion of either a BPCS or SIS that performs one or more logic function(s)
mitigation	action that reduces the consequence(s) of a hazardous event
mode of operation	way in which a safety instrumented function operates
demand mode safety instrumented function	where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS
continuous mode safety instrumented function	where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it
MooN	safety instrumented system, or part thereof, made up of “N” independent channels, which are so connected, that “M” channels are sufficient to perform the safety instrumented function
necessary risk reduction	risk reduction required to ensure that the risk is reduced to a tolerable level
operator interface	means by which information is communicated between a human operator(s) and the SIS (for example, CRTs, indicating lights, push-buttons, horns, alarms); the operator interface is sometimes referred to as the human-machine interface (HMI)
output function	function which controls the process and its associated equipment according to final actuator information from the logic function

phase	period within the safety life cycle where activities described in this standard take place
prevention	action that reduces the frequency of occurrence of a hazardous event
process risk	risk arising from the process conditions caused by abnormal events (including BPCS malfunction)
programmable electronics (PE)	electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units
programmable electronic system (PES)	devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices
proof test	test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality
protection layer	any independent mechanism that reduces risk by control, prevention or mitigation
proven-in-use	when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system
quality	totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs
random hardware failure	failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware
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)
risk	combination of the frequency of occurrence of harm and the severity of that harm
safe failure	failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state
safe state	state of the process when safety is achieved
safety	freedom from unacceptable risk
safety function	function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event
safety instrumented function (SIF)	safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function
safety instrumented system (SIS)	instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s)

safety integrity	average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a stated period of time
safety integrity level (SIL)	discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest
safety lifecycle	necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use
safety requirements specification	specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems
sensor	device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches)
application software	software specific to the user application. In general, it contains logic sequences, permissives, limits and expressions that control the appropriate input, output, calculations, decisions necessary to meet the safety instrumented functional requirements. See fixed and limited variability language
software life cycle	activities occurring during a period of time that starts when software is conceived and ends when the software is permanently disused
system	set of elements, which interact according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction
systematic failure	failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors
tolerable risk	risk which is accepted in a given context based on the current values of society
validation	activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification
verification	activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase

ACKNOWLEDGEMENTS

About the Authors

Chuck Miller is the Business Development Manager for Safety Instrumented Systems at Emerson Process Management in Austin Texas. He is responsible for strategic planning, channel support and organizational development for the DeltaV SIS safety system platform in the Americas. His career in the safety system industry spans two decades including product management, applications engineering, consulting, and business development roles with industry leading service providers including Industrial Control Services, Elsag Bailey and GE Industrial Services. Specializing in Process Automation and Industrial Safety, Mr. Miller has over 30 years experience in international sales, product management and marketing to the refining, petrochemical, exploration and production markets. Mr. Miller holds a degree in Electronics Design from UEI and is a Certified Functional Safety Professional (CFSP). He has authored numerous technical papers on issues relating to the application of safety systems, development of cyber security strategies and safety lifecycle competency development. He continues to develop and teach courses to increase safety system competency on both a domestic and international basis.

Joanne M Salazar is the DeltaV SIS Marketing Programs Manager at Emerson Process Management in Austin, TX. She is responsible for the global, strategic marketing plan for the DeltaV SIS process safety system, as well as the corresponding marketing collateral and promotional deliverables. During her career, Ms. Salazar has held various positions at Emerson including Pharmaceutical Industry Manager and FDA Validation Consultant. She has authored numerous technical articles, as well as developed and taught ISPE's validation course in the 1990's. She has been an active member of various industry committees; include the PDA and ISPE Computer System Validation Committees. Additionally, Ms. Salazar authored the Systems Validation Workbook which was widely used in the life science industry to provide practical application of the computer validation lifecycle. More recently, she has worked to launch Syncade Smart Operations Management Suite, Emerson's MES offering. Ms. Salazar has a Chemical Engineering degree from Purdue University and worked at Eastman Kodak Company in Rochester, N.Y. before joining Emerson.

The authors would like to express their gratitude to Brenda Forsythe and James Samson for their graphics expertise.

References

1. Gruhn, Paul and Henry L Cheddie, "Safety Instrumented Systems: Design Analysis and Justification". 2nd edition (2006) 94 Research Triangle Park, NC.

2. Huba, Bob and Chuck Miller, "Addressing SIS Cyber Security: First or Last?", Control Engineering, May 2009.

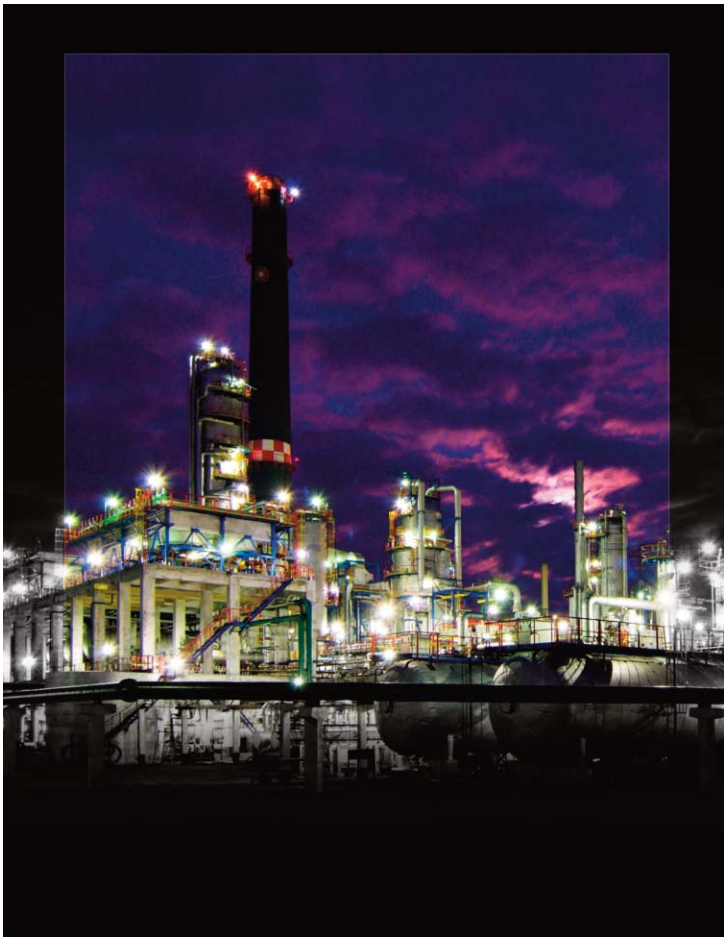
3. Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA 84.01-2004, "Application of Safety Instru mented Systems (SIS) for the Process Industry," Research Triangle Park, NC (2004).

4. International Electrotechnical Commission (IEC), "IEC 61508: Functional Safety of Electrical/Electronic/Program mable Electronic Safety Related Systems," (1998) Geneva, Switzerland

5. International Electrotechnical Commission, "IEC 61511-1: Functional Safety- Safety Instrumented Systems for the Process Industry" (2003): 42. Geneva, Switzerland

6. Summers, Angela E., Ph.D. "Techniques for Assigning a Target Safety Integrity Level." ISA Transactions 37 (1998) 95-104. Geneva, Switzerland.

EMERSON
Process Management



Safety Lifecycle Workbook

For The Process Industry Sector

This Safety Lifecycle Workbook was developed to help business leaders and managers in the process industries gain a general understanding of existing industry standards and best practices for Safety Instrumented Systems (SIS). It also provides a practical overview of the safety lifecycle, including checklists and key considerations for each phase.

EMERSON
Process Management

Form W-0002 / Printed in USA / 2K AQ / 7-10