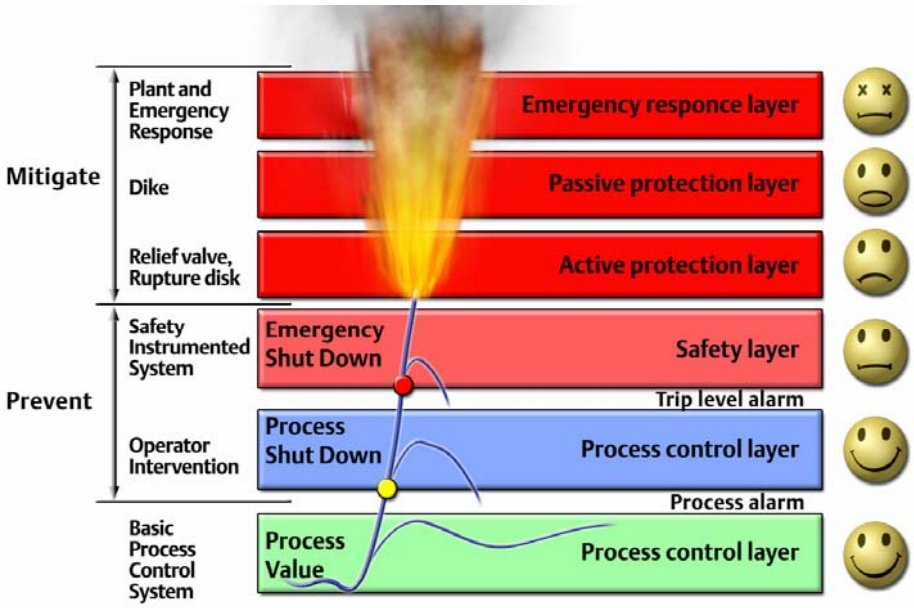
ARC WHITE PAPER

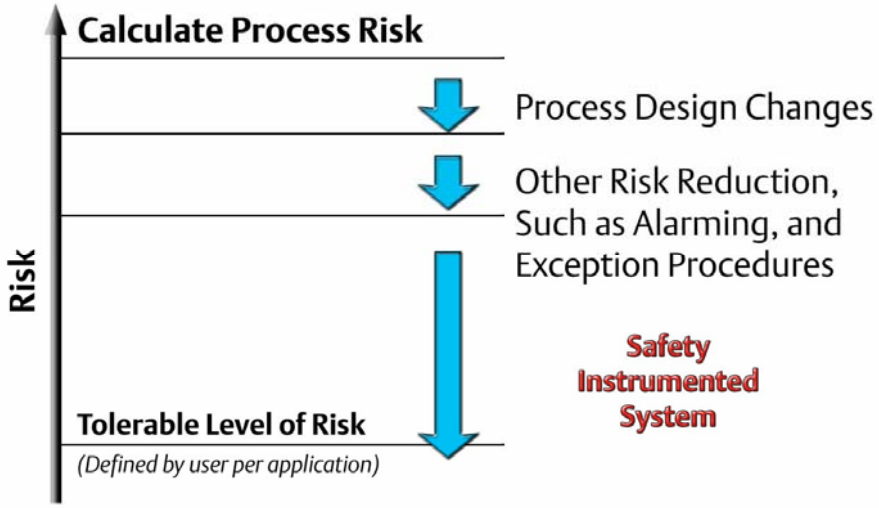
By ARC Advisory Group

SEPTEMBER 2004

Reduce Risk with a State-of-the-Art Safety Instrumented System



Safety Through Layers of Protection



Risk Reduction is the Highest Priority

Executive Overview

Since the publication of the IEC 61508 safety standard and, more recently, the IEC 61511 standard for process safety, the interest in performing rigorous hazard and risk analysis and applying certified Safety Instrumented Systems (SIS) has increased considerably within the user community. As users become more knowledgeable about safety issues, they are sharpening their focus on overall safety with automated monitoring and testing of field devices. Users want their safety-instrumented systems (SISs) to satisfy their needs in a more cost-effective way through integration with control systems, less frequent proof testing, and scalable architectures. They are also looking for increased capability to modify alarm limits based on process conditions and orderly shutdown procedures in case of an emergency. With the release of the IEC 61511 safety standard for process industries there is now no excuse for users not to cost-effectively put safety as the first priority.

Major Trends in Process Safety

Today, the main cause of SIS failure is not the failure of logic solvers, but the failure of field devices. A protective system needs to address overall health of safety loops by incorporating the checking of field devices in its overall design. Consequently, the ability to provide an integrated safety solution from sensor to actuator should be an important criterion when selecting an SIS.

Control valves are available now that have very low probability of stem seizure and packing failure. TÜV-certified valve controllers and actuators are also available in the marketplace. The SIS design should include limited valve movement testing as an integral design feature.

Suppliers are now offering similar systems for control and SIS where similar configuration procedures, programming languages, and maintenance procedures are used. The two systems communicate with each other but with adequate protection from corruption of one by the other. Choose a system that provides flexibility in the configuration of logic solvers along with rich function block capabilities.

It is important to choose a system that integrates information about the health of the field devices into the logic. Users should choose a system that offers a transparently integrated configuration, operations and maintenance environment with the required separation between safety and control. Users should make sure to select a system that makes compliance with International Safety Standards as painless as possible.

Risk Reduction Is the Highest Priority

Risk is usually defined as the combination of probability and the severity of an unplanned event. That is, how often can it happen and how bad is it when it does. Examples of events and their associated risks in manufacturing operations include loss of life or limb, environmental impact, loss of capital equipment, and loss of production. For many manufacturers, loss of company image can also be a significant risk factor. Add to these issues the realities of increased environmental awareness, regulatory concerns, and threat of litigation and it is easy to see why risk reduction is becoming increasingly important to most manufacturers.

Factors that Increase Risk
Operating plant & machinery close to their limits
Transient operation states (startup, shutdown, shift change, work force transitions)
Use of hazardous raw materials
Manufacture of hazardous intermediates
Presence of untrained personnel
Absence of safety culture

The best way to reduce risk in a manufacturing plant is to design inherently safe processes. However, inherent safety is rarely achievable in today's manufacturing environments. Risks prevail wherever there are hazardous or toxic materials stored, processed, or handled.

Forces Driving Lower Risk
Higher environmental awareness
Increased regulatory considerations
Emergence of safety standards
Maintaining company image

Since it is impossible to eliminate all risks, a manufacturer must agree on a level of risk that is considered tolerable. After identifying the hazards, a hazard and risk study should be performed to evaluate each risk situation by considering likelihood and severity. Site-specific conditions, such as population density, in-plant traffic patterns, and meteorological conditions should also be taken into consideration during risk evaluation.

Once the hazard and risk study has ascertained the risks, it can be determined whether they are below acceptable levels. Basic process control systems, along with process alarms and facilities for manual intervention, provide the first level of protection and reduce the risk in a manufacturing facility. Additional protection measures are needed when a basic control system does not reduce the risk to a tolerable level. They include safety-instrumented systems along with hardware interlocks, relief valves, and containment dikes. To be effective, each protection subsystem must act independently of all others.

Safety Standards Guide Best Practices

Since the publication of the IEC 61508 safety standard and, more recently, the IEC 61511 standard for process safety, interest in performing rigorous hazard and risk analysis and applying certified safety instrumented systems has increased considerably within the user community. These standards give 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.

IEC 61508

The IEC 61508 Safety standard published by the International Electrotechnical Commission (IEC) is applicable to a wide range of industries and applications and is written primarily for the supplier community. The IEC 61508 standard is composed of seven parts, starting with general safety requirements to specific system and software requirements and guidelines to applications. The standard is generic and can be used directly by industry as a 'standalone' standard and by international standards organizations as a basis for the development of industry specific standards, such as for the machinery sector, the process sector, or for the nuclear sector. It is suggested that in evaluating a safety system a user should select one that is certified by an independent third party, such as TÜV or FM.

Note that the certificate from the independent body should be reviewed in parallel with the User Safety Manual. This is a document that defines the

restrictions on use of an SIS component. The manual for a good safety system is very thin, with a minimal number of restrictions. Beware of a thick safety manual; it indicates that there are many complexities and limitations associated with the use of the SIS.

Safety Integrity Levels

Safety integrity is defined as the likelihood of a safety instrumented system satisfactorily performing the required safety functions under all stated conditions within a given period. A safety integrity level (SIL) is defined as a discrete level for specifying the safety integrity requirements of safety functions. A safety integrity level is derived from an assessment of risk; it is not a measure of risk. It is a measure of the intended reliability of a system or function.

Safety Integrity Level (SIL)	Probability of Failure on Demand Mode	Probability of Failure on Continuous Mode
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

Safety Integrity Levels

Notes:

Demand Mode: Where actions are taken in response to process or other conditions (no more than once per year)

Continuous Mode: Functions that implement continuous control to maintain functional safety

IEC 61511: The Safety Standard for Process Industries

The IEC 61511 standard is targeted specifically at end users in the process industry. This standard provides best safety practices for all users to follow in the implementation of a modern SIS. While IEC 61508 is composed of seven parts, IEC 61511 has only three:

- Part 1: Framework, definitions, system, hardware, and software requirements
- Part 2: Guidelines on the application
- Part 3: Guidance for the determination of the required safety integrity levels

IEC 61511 Part 1 is primarily normative while Parts 2 and 3 are informative. Part 1 of the IEC 61511 standard is structured to adhere to a safety lifecycle model. The hazard and risk analysis utilizes the concept of protection layers and specifies the safety integrity level concept developed by the IEC 61508 standard. It also lists key issues that need to be addressed when developing a safety requirement specification. Issues like separation, common cause, response to fault detection, hardware reliability, and proven-in-use are also addressed in this part.

IEC 61508	IEC 61511
Generic safety standard for broad range of applications	Sector-specific safety standard for the process industries
Applies to all safety-related systems and external risk reduction facilities	Applies only to safety-instrumented systems
Primarily for manufacturers and suppliers of safety systems and devices	Primarily for system designers, integrators, and users of safety systems and devices

Main Differences Between IEC 61508 & IEC 61511 Standards

Software safety requirement specifications are included, addressing such items as architecture, relationship to hardware, safety instrumented functions, safety integrity levels, software validation planning, support tools, testing, integration, and modification. In addition, a section is dedicated to Factory Acceptance Testing requirements, and another section lists the installation and commissioning requirements.

Part 2 of the standard provides "how to" guidance on the specification, design, installation, operation, and maintenance of safety instrumented functions and related safety instrumented system as defined in Part 1 of the standard. It has borrowed heavily from the ISA technical report dTR84.0.02, which provides guidance on methods to calculate the performance of safety instrumented systems.

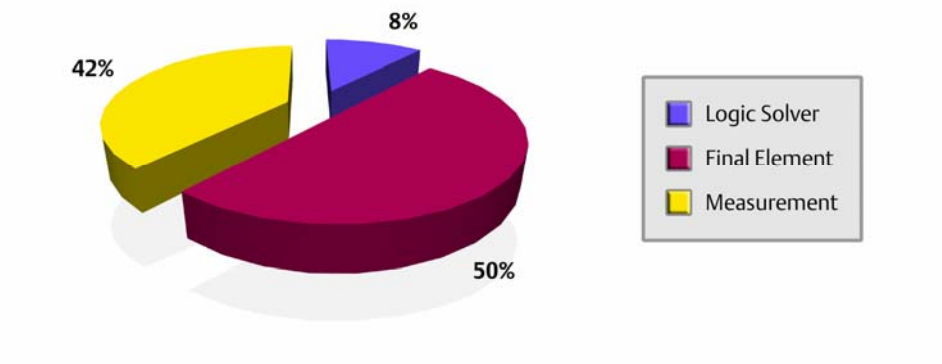
Part 3 of the standard provides guidance for development of process hazard and risk analysis. It provides information on the underlying concepts of risk and the relationship of risk to safety integrity and the determination of tolerable risks. The ANSI/ISA-84 safety standard, which predates the international safety standards, will soon be updated to closely follow the IEC 61511 standard.

Major Trends in Safety Instrumented Systems

As manufacturers become more knowledgeable about safety issues, they are performing more thorough hazard and risk analysis to determine their needs more accurately. They are looking for reduction of risk by increasing their focus on overall safety. They would like their SIS to satisfy their needs in a more cost effective way by closer integration of safety with control systems. They are also looking for a flexible architecture along with more scalability; increased functionality for modifying alarm limits based on process conditions; and orderly shutdown procedures in case of emergency.

Increased Focus on Overall Safety

The main cause of an SIS failure is not the failure of logic solvers, but the failure of field devices. There has been a significant advance in the development of the architecture of logic solvers with voting circuits and advanced diagnostics. However, they do not address over 90 percent of the causes for failure, which are due to the failure of sensors and actuators.



Main Causes of SIS Failures

Today a protective system should address the need for checking the health of the I/O and field devices. In fact, it needs to incorporate monitoring of I/O components in its overall design. Examples include:

- Sensor validation
- Environment condition monitoring, such as temperature and humidity that can cause sensor degradation
- Transmitter drift

Common failures of electronic components are frequently due to environmental conditions. Many electronic devices fail when exposed to elevated humidity and temperature conditions, which need to be monitored closely. Sensor calibration is also becoming an integral part of an SIS. Use of open protocols, such as HART and, in principle, FOUNDATION Fieldbus, allows for remote monitoring, diagnostics, and validation.

1.	Integrate health data from field devices into logic solvers
2.	Degrade the quality of the signal from a field input/device when the input is dubious
3.	Compare digital and analog values to check the validity of an input

An Integrated Approach to Process Safety

High performance valve technologies are now being used. Use of valve controllers that do not automatically diagnose the health of the valve assembly in safety applications gives rise to continual concern about the ability to trip on demand. Control valves are designed to have very low probability of stem seizure and packing failure and TÜV-certified actuators and controllers are now commercially available to test and diagnose their health. The SIS design should include limited valve movement testing as an integral design feature.

Automated Monitoring and Testing of Field Devices

Certified smart sensors and final control elements that can report their health to the logic solver are now available. This increases availability as an unhealthy sensor can be replaced promptly or its input ignored for a voting strategy. Also, problems with final control elements can be diagnosed more rapidly thus averting dangerous situations.

Partial stroke testing is also possible with a smart valve controller. This gives a much richer diagnostic than is possible with manual testing, and also stops exposing personnel to risk while they manually test in the field. Additionally, a valve need not be removed from the safety scheme while the test is carried out.

It is a requirement of the IEC 61511 standard that all components of an SIS are taken off-line and fully tested – the interval between tests depends on the components in question and the required SIL. Use of these automated testing techniques, combined with certified devices that have independently verified reliability figures, allows the proof test interval to be greatly extended, thereby increasing the length of a plant's runtimes.

Integration with, but Separation from, the Control System

Many manufacturing companies have kept controllers used for safety completely independent of those used for control and optimization. Controllers used for SIS come from specialized manufacturers who add extensive diagnostics and receive TÜV safety certification. In the past there was little choice other than using completely different systems for control and safety. Some users even mandated control systems and SIS from different manufacturers.

There are many other good reasons to put safety and control functions in different controllers. They include:

- Independent failures – minimizing the risk of simultaneous failure of a control system along with the SIS
- Security – preventing changes in a control system from causing any change or corruption in the associated SIS
- Different requirements for safety controllers – a safety system is normally designed to fail in a safe way, whereas a BPCS will usually maximize availability. An SIS also has special features like extended diagnostics, special software error checking, protected data storage and fault tolerance

Common data mapping
Increased security
Similar engineering tools
Visual differentiation between control and safety environments at workstation level
Proper access protection
Significant reduction in integration efforts

Benefits of Improved Integration of Safety Systems with Control Systems

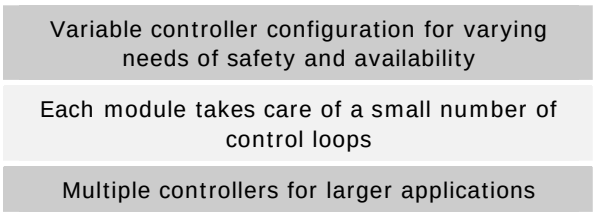
The IEC 61508 safety standard is somewhat ambiguous on this issue; it strongly recommends separation but does not mandate it. Today, a large number of users are finding logical reasons for using similar systems for control and safety functions, as this will reduce the problems associated with different programming procedures, languages, installation requirements, and maintenance. There is always the risk associated with these different procedures contributing to human error and possible safety problems.

The financial benefits of using similar systems are also clear; reduced hardware, configuration, training, and inventory costs result from the reduced range and quantity of equipment that is required. In addition the burden of different service and support help associated with disparate systems is removed.

Some control and SIS suppliers now offer similar systems for either function, which incorporate similar HMI, configuration procedures, programming languages, and maintenance procedures. The key is to ensure that the even though the two systems are separate, with different hardware and software, they have a common configuration, operations and maintenance interface. This allows the users to achieve the operational benefits of integration while meeting the safety requirement for separation. The control and safety systems communicate transparently with each other, but have adequate protection from corruption of one by the other.

Increased Flexibility & Scalability

The installed base of SISs for critical control or safety shutdown is largely TMR (2oo3) and Duplex (1oo2D) systems. However, SIS suppliers are increasingly offering other architectures. They include Quad (2oo4D), Pair and Spare, and Clustering configurations. Increasingly, suppliers are offering configuration flexibility, where the user has the choice of putting together two or more safety PLCs to reduce failure rate and increase availability.



Elements of Process Safety System Flexibility and Scalability

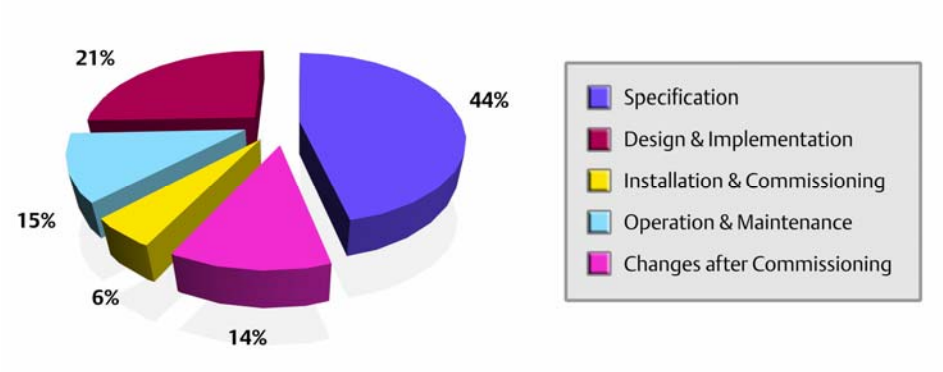
Safety controllers are becoming more scaleable. They are getting smaller, where one controller handles a limited number of I/O, but a number them working together can handle a much larger application. This is a boon to users, as they no longer have to invest in large and expensive systems that are not needed for many of their applications.

Taking Care of Varying States of a Process

A state of the art SIS provides facilities for simple sequencing (usually without looping) to allow orderly shutdown of a process on detection of a dangerous condition. While a basic process control system may shutdown a unit in case of an extreme alarm condition, incorporating the plant shutdown function into an SIS leads to a significant reduction of risk. Rich function blocks in an SIS can also handle the implementation of process dependent trip-levels that are typical in a batch control system.

The IEC 61511 standard requires that all current bypasses and over-rides are displayed in the alarm/event log and that they are rigorously managed.

A state-of-the-art SIS can help with this, by providing this functionality as standard. That will ensure that the required authority levels are automatically configured in accordance with the SIL requirements of the loop in question and that no additional configuration is required to display the active bypasses and over-rides.



The Majority of SIS Failures are Engineering Related

There is another good reason for seeking an SIS with rich, certified functionality built-in. A study by the UK HSE (Health Safety & Environmental Agency) found that 85 percent of all SIS failures are engineering-related, with about 60 percent built-into the SIS before installation. Therefore it is clear that the SIS should be provided with functionality to make it as easy as possible to follow safety best practices, as laid out in IEC 61511, and configure the system accordingly. It is easier to meet both of these goals with certified rich function blocks.

Increased Use of Industry Standard OPSYS

It is critical to the performance of an SIS logic solver that it uses a highly reliable operating system (OPSYS); in fact an SIS's operating system must be certified to a level of criticality at least as high as that of the SIL rating of the loops that the SIS is protecting. At the same time, the need to reduce maintenance costs combined with the availability of modern processor technology has created a demand for commercial off-the-shelf operating systems for logic solvers in safety-instrumented systems. A commercial off-the-shelf OPSYS that has been certified by a third party therefore offers significant advantages to SIS suppliers and users.

Proven in use
Thoroughly tested
Accurate field failure notification and correction system

Benefits of Employing an Industry Standard Operating System in an SIS

Recommendations to End Users

- Adopt IEC 61511 as your safety implementation standard.
- Perform rigorous standards-based hazard and risk analysis to decide on the right level of protection for your manufacturing plants.
- Based on the hazard and risk analysis, select a certified safety instrumented system that meets all of your risk management needs.
- Choose a safety instrumented system that is tightly integrated into your basic process control system while still providing the required degree of separation.
- Choose a system that provides an integrated safety solution from sensor to actuator.
- Continuously monitor the health of the field devices and automatically test them where appropriate.
- Choose a system with flexible configuration that will allow flexible geographical deployment and scalability.
- Choose a system with certified rich function blocks that take the health of field devices into account when executing their logic and facilitate the ease of design and configuration.
- Give due importance to systems with off-the-shelf operating systems certified for safety applications.
- Choose a system that maximizes safety while simultaneously maximizing availability by using automated proof testing and improved diagnostics that cover the whole loop.
- Beware of thick safety manuals. Choose a system with few restrictions.

Analyst: Asish Ghosh
Editor: Chantal Polsonetti

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/Community/terms/terms.htm

ANSI	American National Standards Institute
BPCS	Basic Process Control System
DCS	Distributed Control System
ESD	Emergency Shutdown (system)
FM	Factory Mutual
HART	Highway Addressable Remote Transducer
HAZOP	Hazard & Operability
HMI	Human Machine Interface
HSE	Health, Safety and Environmental Agency
IEC	International Electrotechnical Commission
OPSYS	Operating System
OSHA	Occupational Safety & Health Administration
PLC	Programmable Logic Controller
PSM	Process Safety Management
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TMR	Triple Modular Redundancy
TÜV	Technischer Uberwachungs Verein (Technical Inspection Association)

3 ALLIED DRIVE DEDHAM MA 02026 USA

BOSTON, MA | PITTSBURGH, PA | PHOENIX, AZ | SAN FRANCISCO, CA