

What Every Manager Should Know About The New SIS Standards

Angela E. Summers, Ph.D., P.E,
President, SIS-TECH Solutions, LLC
PMB-295, 2323 Clear Lake City Blvd, Houston, TX 77062

KEYWORDS

ANSI/ISA 84.01-1996, IEC 61511, Safety Instrumented Systems (SIS), Redundancy, Functional Testing, Layer of Protection Analysis (LOPA), Safety Instrumented Systems (SIS), Safety Integrity Levels (SIL)

ABSTRACT

The impact of ANSI/ISA 84.01-1996 and IEC 61511 on the design and implementation of safety instrumented systems (SIS) has proven to be greater than many people expected. This was surprising to many users, since these standards are performance-based rather than prescriptive. However, the SIS performance is often the predominant reason for the installation of redundant equipment and the requirement for more frequent functional testing. The impact snowballs when the design criteria and testing requirements are established late in detailed design. This paper will present what every manager should know to prevent ANSI/ISA 84.01-1996 and IEC 61511 from turning into an avalanche of project problems.

INTRODUCTION TO THE SIS STANDARDS

THE US STANDARD, ANSI/ISA 84.01-1996.

On March 23, 2000, ISA, the instrumentation, systems and automation society, received a letter from the United States Occupational Safety and Health Administration (OSHA). This letter was written in response to ISA's inquiry regarding the relationship between ANSI/ISA 84.01-1996 (1) and OSHA's Process Safety Management (PSM) (2). In the letter, OSHA states that the Agency considers ANSI/ISA 84.01-1996 (ISA 84) to offer generally accepted, good engineering practice for establishing

SIS under PSM. OSHA's letter also states that, when implementing SISs in processes that are not covered by PSM, operators could be found in violation of the General Duty Clause of the OSH Act, if an incident occurs and the SIS in place at the facility are determined to not conform to the specific requirements of ISA 84.

ISA 84's objective is to define the requirements for instrumented systems that are designed to prevent or mitigate potentially unsafe conditions. In the past, these systems were typically called interlocks, emergency shutdown systems, or safety critical systems. ISA 84 refers to these instrumented systems as safety instrumented systems (SIS).

ISA 84 includes a "grandfather clause" (3) for addressing existing SIS that states that the owner/operator of a SIS designed and constructed prior to the issuance of the standard must demonstrate that the process is "designed, maintained, inspected, tested and operating in a safe manner." This "grandfather clause" releases the owner/operator from ISA 84 requirements, if the criteria of the clause are met. Engineers involved in the modification of existing process units, or design of new grass-roots facilities must implement ISA 84.

THE INTERNATIONAL STANDARD, IEC 61511.

Under the direction of the International Electrotechnical Commission (IEC), an international committee is working to finalize a SIS standard for the chemical process industries. When accepted by the member countries, this standard, IEC 61511 (4), will take the lifecycle concept of ISA 84 worldwide. In the future, SIS design criteria will not be affected by the location of the installation. Rather, all SISs will be specified, designed, operated, and maintained according to the same global standard. This standard is scheduled for release as a final draft international standard in 2002, which will result in many countries requiring compliance to IEC 61511 as early as the fall of 2002.

Although the IEC 61511 uses a lifecycle concept, it is no mirror image of ISA 84. An international standard must harmonize the standards of many countries. Consequently, the standard will add new requirements for component selection, design architecture, software development, pre-startup safety reviews, operation and maintenance procedures, and management of change. The most important similarity is the assignment of safety integrity level, which is a significant checkpoint for achieving ISA 84 compliance. IEC 61511 will strengthen the importance of the SIL by requiring a quantitative assessment of the SIS design to ensure that it meets the SIL.

Finally, IEC 61511 does not contain a specific grandfather clause for existing installations. The standard states the User should evaluate the safety of the process and determine whether the requirements of the standard should be implemented. Consequently, implementation on existing installations is considered a User choice. However, regulators, insurers, and legal departments may have their own opinions concerning when to implement this standard on existing installations, so it is

important to check whether compliance is required. New installations or major retrofits must incorporate the concepts of IEC 61511.

EIGHT QUESTIONS AND ANSWERS

WHAT IS THE SIS?

ISA 84 uses the term “safety instrumented system” to refer to both an instrumented loop used to mitigate process risk related to catastrophic incidents and a collection of instrumented loops in a PLC. This has led many people to believe that the PLC constitutes the safety instrumented system. IEC 61511 clarifies this situation by using the term “safety instrumented function” (SIF) to refer to an instrumented system designed to mitigate a specific process risk and the term “safety instrumented system” to refer to a collection of SIFs.

WHAT ARE INDEPENDENT PROTECTION LAYERS?

Independent Protection Layers (IPLs) are the safeguards used to mitigate the process risk. IPLs differ from the traditional view of a safeguard in that the IPL is generally required to meet certain criteria as outlined by CCPS (4, 5):

- ✓ Specific: The IPL is capable of detecting and preventing or mitigating the consequences of potentially hazardous event(s), such as runaway reaction, loss of containment, or explosion.
- ✓ Independent: The IPL is independent of all the other protection layers associated with the identified hazardous event. Independence requires that the performance is unaffected by the failure of another protection layer or by the conditions that caused another protection layer to fail. The protection layer must also be independent of the initiating cause.
- ✓ Dependable: The protection provided by the IPL reduces the identified risk by a known and specified amount.
- ✓ Auditable: The IPL is designed to allow periodic validation of the protective function.

The purpose of these criteria is to ensure that each IPL can achieve a measurable and predictable risk reduction. In many company standards, the risk reduction must be at least one order of magnitude to achieve IPL status.

WHAT IS IPL ANALYSIS?

IPL Analysis is the process used to define the IPLs and to establish the risk reduction that is required from each IPL. The most popular method for performing IPL Analysis is layer of protection analysis (LOPA), supported by either qualitative targets (risk matrix) or quantitative targets (defined tolerable risk). A team identifies and discusses potentially hazardous events and evaluates the consequences of these events in terms of safety, environmental, and economic losses. Then, the team determines what can initiate these hazardous events. The frequency of each initiating causes is assessed, based on either qualitative or quantitative estimation. Risk is measured in terms of frequency and consequence, so the risk of each hazardous event is now known. This risk can be compared to the tolerable risk criteria.

If the risk is higher than the tolerable risk, the team proceeds by examining each initiating cause to determine what IPLs are installed that can stop the propagation of the initiating cause to the final undesired consequence. Typical IPLs are critical control loops, alarms with operator response, SIF, pressure relief valves, rupture disks, etc. Each IPL is then allocated an amount of risk reduction based on the specific IPL design. If there is insufficient risk reduction, the team must determine what additional IPLs can be added to the design.

WHEN DO YOU DO IPL ANALYSIS?

IPL Analysis can be used at any point in a project lifecycle, but it is most cost effective when implemented at the earliest stages of detailed design when the first round of P&IDs are complete. IPL Analysis is typically applied after a preliminary process hazards analysis has identified hazardous events, which result in significant impact to human life, the environment, or equipment. For existing processes, it can be used at any time. The most important thing is to start as soon as possible in the project. The later the analysis is started, the more detailed design changes can be induced by the modification. In early design, these changes are minor documentation changes. In late detailed design, these changes can result in rush orders for instrumentation and PLC hardware, extensive programming modifications, and massive documentation updates.

WHAT IS SAFETY INTEGRITY LEVEL?

During the IPL Analysis, SIF are identified and each is allocated an amount of risk reduction. In ISA 84, there are three SIL classes, while in IEC 61511 there are four SIL classes. Each class provides an additional order of magnitude risk reduction as shown below. Consequently, once the required risk reduction for the SIF is known, the SIL is also known.

SIL	PFD	Risk Reduction (1/PFD)
4	0.0001 to 0.00001	10,000 to 100,000
3	0.001 to 0.0001	1,000 to 10,000
2	0.01 to 0.001	100 to 1,000
1	0.1 to 0.01	10 to 100

WHAT AFFECTS THE SIL OF A SIF?

The safety integrity level is affected by the following parameters:

1. Device integrity (i.e. failure rate and failure mode)
2. Redundancy and voting (i.e. the use of two sensors, where a trip signal from either sensor can result in the failsafe action)
3. Functional testing interval (i.e. at a specific time interval, testing is performed to determine that the device can achieve the failsafe condition)
4. Diagnostic coverage (i.e. automatic, on-line testing of various failure modes of a device)
5. Other common causes (including those related to the device, design, systematic factors, and human error)

The parameters, device integrity, diagnostic coverage and common cause, are typically limited by the SIF device and installation practices. The redundancy requirements and functional test interval have the greatest impact on current design and operation/maintenance practices in existing process units.

The device integrity is often established through use of the device in control applications prior to being specified for a SIF application. An understanding of the failure rate and failure modes in the intended operating environment is important for successful implementation of any instrumentation. In fact, one technique for selecting devices according to IEC 61511 (4) is based on historical use of the device. This concept is known as “proven-in-use.”

Failure rates and failure modes can also be obtained from the device vendor. Unfortunately, vendor data is often based on bench or laboratory testing or on predictive failure models. This data provides the user with an understanding of how the device behaves in the manufactured state. This “shelf-state” information can be used as a screening tool, but this data should not be used for the SIL calculation. The shelf-state data does not include the impact of the process environment, because this is too application dependent for any vendor to predict. In addition, installation, operation and maintenance practices, such as closed coupling versus instrument taps can affect the device performance. When the

SIL for the SIF is calculated, the failure rates and failure modes in the intended operating environment (application state) must be used, because this represents the true performance of the device.

The diagnostic capability is limited by the selected device and the external diagnostics that can be used with the device. For example, if discrete inputs, such as switches, are used, very little diagnostic coverage will be available, even when redundancy is provided. When analog devices are used, the signals from redundant devices can be compared. When the signals deviate unacceptably, an alarm can be generated, notifying the operator that repair should be initiated. This provides diagnostic coverage.

And as far as common cause impact, there is only so much that can be done to minimize it. The plant can use good design, procedural, and installation practices. Beyond this, the potential for common cause exists. It may be small in some applications. It may be large in others. The best option is to design it out of the SIF as much as possible.

Most plant managers are completely unprepared for the device redundancy and functional test requirements. For example, in SIL 2 and SIL 3 applications, dual/triple inputs and dual outputs are often required to meet the PFD_{avg} and fault tolerance requirements. The concept of purchasing two or three devices to do the exact same job that one can do is sometimes a bitter pill to swallow. Of course, it is possible to design a fully simplex SIF that meets high SIL, but the required testing interval is typically intolerable to the maintenance staff. For SIL 2 and 3, low redundancy generally yields the requirement for on-line testing, while higher redundancy may extend the testing interval to turnaround.

Finally, the voting architecture can impact the spurious trip rate for the SIF. Simplex devices may meet the SIL at lowest capital and installed cost. This SIF may also have a high spurious trip rate, which often causes substantial production losses. Alternative designs may use redundancy to provide the fault tolerance. This may increase the installed cost, but will substantially decrease the spurious trip rate.

DO THE SIS STANDARDS AFFECT THE DCS?

The SIS standards require the separation of SIS and DCS functions, which complicates the control system installation. When the systems are combined, start-up, normal operation, and shutdown conditions exist within the same PLC space. The determination of the current operational state is as simple as looking at a register or flag. When these systems are separated, communications between the SIS and DCS become extremely important. Communication speed and reliability is essential for smooth process operation. It also can have a significant impact on the cost of the SIS project, due to the large number of points that may require communication. Successful handshakes between the DCS and SIS do not happen without planning. Unfortunately, communication implementation is often relegated to the late stages of a project, because it is considered a control system's issue that only

requires some “set-up” time. This is far from the truth. Poor inter-system communications has delayed many plant start-ups.

HOW DO THE SIS STANDARDS AFFECT OPERATIONS?

SIF cannot be viewed as the instrumentation that keeps the plant from running. SIF must be viewed as the instrumentation that keeps the plant safe. To drive this concept home, operating procedures must be viewed as more than a way to get a quality product or high production rate. The SIS standards require that operating procedures inform the operator of the specific process risks and the potential consequences if the process deviations are not brought under control. The procedures must provide the operator the following information related to the SIF:

- ✓ How installed SIF devices protect the process in the event of process deviation
- ✓ What to do if the SIF fails to shutdown the process during an upset event.
- ✓ What to do in response to detected instrumentation faults
- ✓ When and for how long bypasses can be initiated
- ✓ When to manually execute a safe shutdown.

The biggest impact to operation personnel lies in the latter two bullets. Many facilities do not specifically restrict the use of SIF bypasses, leaving their use to operator discretion. This has allowed many operators to play the odds during upset conditions by placing the SIF in bypass and attempting to ride out the trip condition. Further, no operator wants to be the one to manually initiate a safe shutdown unless there is ample evidence that it is absolutely necessary. This is because the operator knows that someone will always say that they could have saved the process and prevented the unnecessary shutdown. This tug-of-war within the operator’s head can only be managed by providing never exceed, never deviate instructions. If the process reaches a specific process condition (never exceed), the operator is to execute the safe shutdown (never deviate).

HOW DO THE SIS STANDARDS AFFECT MAINTENANCE?

The importance of functional testing is well documented in the SIS standards. In many cases, users will find that to achieve SIL 2 and SIL 3 SIF annual testing is required. In the past, device testing was largely performed during turnaround, when contract personnel are on-site and available to conduct testing. When annual testing must be conducted, maintenance resources, including manpower, scheduling, and test equipment, are overwhelmed. Maintenance tools must be improved for cost effective implementation of the SIS standards. These tools include better software for maintenance scheduling, tracking, and procedures.

To provide consistency in test performance, maintenance procedures should provide detailed instructions. The procedures should be written from the technician perspective with sufficient detail to ensure that all SIS devices are completely tested and returned to service. Poor maintenance is a major causal factor in many incidents. Good procedures reduce the potential for these incidents.1

SUMMARY

A proactive approach is necessary for cost effective implementation of ANSI/ISA 84.01-1996 and IEC 61511. The IPL Analysis should be conducted as soon as the first round of P&IDs have been completed. This analysis should identify the IPLs and assign each a required risk reduction. For the safety instrumented functions, the risk reduction is equivalent to the safety integrity level. The SIL often results in redundancy and functional testing requirements that are beyond current plant practice. Successful implementation also involves well-planned and reliable communication with the process control system.

An important mission of any SIS standard compliant program is to increase the knowledge and motivation of the operators and maintenance personnel. Operation procedures should include the correct response to process upsets, process alarms, and SIS diagnostic faults. Maintenance procedures should be sufficiently detailed to ensure that devices are properly tested and returned to service, guaranteeing SIS device performance.

REFERENCES

1. "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA-ISA 84.01-1996, ISA, Research Triangle Park, NC (1996).
2. "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," 29 CFR Part 1910, OSHA, Washington (1992).
3. "Is Your SIS 'Grandfathered'?", Chemical Engineering Progress, pages 39-42, May 1999.
4. International Electrotechnical Commission (IEC), IEC 61511, "Functional Safety: Safety Instrumented Systems for the Process Sector," Geneva, Switzerland (expected 2002).