What Every Manager Should Know About The New SIS Standards

Angela E. Summers, Ph.D., P.E., President, SIS-TECH Solutions, LP

"What Every Manager Should Know About the New SIS Standards," ISA Technical Symposium 2002, Research Triangle Park, NC: Instrumentation, Systems, and Automation Society, Baltimore, Maryland.

"What Every Manager Should Know About the New SIS Standards," ISA EXPO 2002, Research Triangle Park, NC: Instrumentation, Systems, and Automation Society, Chicago, IL (2002).

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, since these standards are performance-based rather than prescriptive. However, the SIS performance is often the predominant reason for the installation of additional redundancy and the requirement for more frequent functional testing. The impact snowballs when the need for the redundancy and testing requirements are identified 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 SISs 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 the 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, will take the lifecycle concept of ANSI/ISA 84.01-1996 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, and these opinions will likely be based on potential liability. In any event, 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. "Safety instrumented system" is a term used to describe the complete system used to implement the SIF.

A simple analogy can be provided by the examining a typical DCS. Control loops are implemented to perform specific control functions, such as controlling the flow of a chemical into a vessel. The actual

implementation of the control function is performed in the DCS. The control loop provides specific functionality, while the DCS is the overall system.

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 the 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 LOPA team identifies hazardous events and determines their potential causes and consequences. The team then assesses the IPLs used to prevent or mitigate the hazardous events and assigns a target risk reduction to each based on its specific design. The IPL Analysis is not complete, until the residual risk has been reduced to the tolerable level.

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. It 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, IPL Analysis can be used at any time. The most important thing is to start the analysis as soon as possible in the project.

WHAT IS SAFETY INTEGRITY LEVEL?

During the IPL Analysis, the safety instrumented functions (SIF) are identified and each is assigned a required 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.

TABLE 1. THE RELATIONSHIP BETWEEN SIL, PFD, AND RISK REDUCTION

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

WHAT AFFECTS THE SIL OF A SIF?

The safety integrity level is affected by the following parameters:

1. Device failure rate
2. Diagnostic coverage
3. Redundancy and voting
4. Testing interval
5. Common cause

From a plant perspective, the redundancy and functional testing interval have the greatest impact on the current design and operation practices. The other parameters, device integrity, diagnostic coverage and common cause, are typically limited as soon as the user selected the device.

DEVICE FAILURE RATE

The failure rate should be based on the performance of the device in the application environment. The device failure rate should include all components required for the device to perform its design function. For a transmitter, the device failure rate should include the sensor, transmitter, process connection, and impulse line. The application failure rate can be established by examining how the specific device or a similar device has performed in other applications, such as a process control application. The selected device should be known to function well in the intended application environment. This concept is referred to as “proven-in-use” or “prior use” and is important for successful implementation of new instrumentation. Be cautious with vendor failure rate data, because it often reflects the device performance in its shelf state and therefore does not include the process impact. From a user perspective, most device problems occur because of the impact of the process environment, such as crimped impulse lines, plugged process connections, or deposition in valve seats. Additionally, vendor data often does not cover the complete device boundary, i.e. the impulse lines or process connection.

DIAGNOSTIC COVERAGE

Diagnostic coverage is provided using automatic, on-line techniques. Diagnostic coverage may consist of trending, comparisons, or tests, intended to detect various failure modes of a device. The choice of a specific device may limit the potential diagnostic coverage that can be obtained from the device. For example, if discrete inputs, such as switches, are used, very little diagnostic capability will be available. Changing to analog inputs allows signal comparison to be performed and diagnostic coverage to be obtained.

REDUNDANCY AND VOTING

Most plant managers are completely unprepared for the device redundancy requirements. For example, in SIL 2 and SIL 3 applications, dual or triple inputs and dual outputs are often required to meet the PFDavg 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 simplex SISs that achieve high safety integrity, but the required testing intervals are typically intolerable to the maintenance staff. Redundancy and testing interval are like a child's seesaw. Low redundancy generally yields frequent testing. High redundancy yields significantly lower testing frequency.

TESTING INTERVAL

In the past, most maintenance departments performed function tests at turnaround only. During turnaround, contractors were utilized to perform tests and to address non-functioning equipment. Any other testing was restricted to "round-to-it" testing. Any on-line testing was restricted to work order requests based on a specific fault alarm or an operator complaint. Now, the testing interval is an important variable in determining the PFDavg for the SIS. When the actual device failure rate is used in the PFDavg calculation, many users find that turnaround testing is insufficient. This results in the need for periodic on-line testing, which can be conducted manually or automatically.

COMMON CAUSE

Common cause is based on the concept that it is possible that redundant devices could fail due to the same fault at nearly the same time. For example, all three transmitters may be calibrated incorrectly by the same technician, resulting in the failure of the SIS to trip at the intended setpoint. The analog signal comparison would not generate a fault alarm, because the transmitters would be in agreement. Consequently, 2oo3 voting transmitters with analog signal comparison are defeated by this single calibration fault.

The only way to reduce common cause is the use of good administrative, design, procedural, and installation practices. Beyond this, the potential for common cause exists. It is usually small, but it is still there.

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, trip, 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, communications 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 communications has delayed many plant start-ups.

HOW DO THE SIS STANDARDS AFFECT OPERATIONS?

In terms of operating procedures, many procedures focus on quality control and associated operational parameters. Operating procedures should be viewed as much more than a way to get a quality product. The SIS standards require that operating procedures document specific responses to process deviations, alarms, and shutdowns. Operating procedures should also inform the operator of the process risks and the potential consequences if the alarms and shutdowns do not occur.

HOW DO THE SIS STANDARDS AFFECT MAINTENANCE?

The importance of maintenance and functional testing is well documented in the SIS standards. Maintenance procedures should provide detailed procedures and should be written from the technician perspective with sufficient detail to ensure that all SIS devices are completely tested and returned to service. Maintenance and supervisor sign-offs are essential. Well-written procedures should be viewed as the way to guarantee consistency of performance, which is the only way to achieve the desired device integrity.

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. “Functional safety of electrical/electronic/programmable electronic safety related systems,” IEC 61511, International Electrotechnical Commission, Geneva, Switzerland (expected 2oo2).
3. Summers, A.E., “Understanding Safety Integrity Levels,” Control Engineering website (February 2000).