ISA 84 – THE STANDARD FOR SAFETY INSTRUMENTED SYSTEMS

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

"Regulations, Standards, and Safety Instrumented Systems," Keynote Speech at European Triconex Users Group, Venice, Italy, May 1998.
"Regulations, Standards, and Safety Instrumented Systems," Plenary Speaker, ISA EXPO 1998, Houston, TX, October 1998.
"Workshop: Safety Instrumented Systems Under the New Standards," ICEX 99, Institute of Instrumentation and Control, Melbourne, Australia, May 1999.
"Regulations, Standards, and Safety Instrumented Systems," Mary Kay O'Conner Process Safety Center, Texas A&M University, College Station, Texas, October 1999.
"Path to S84 Compliance," Guest Editorial, Factory Mutual Newsletter, July 2000.
"Setting the Standard for Safety Instrumented Systems," Chemical Engineering, December 2000.

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 a response to ISA's inquiry regarding the relationship between ANSI/ISA 84.01-1996 (1) and OSHA's Process Safety Management (PSM) program (2). 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 known as interlocks, emergency shutdown systems, or safety critical systems. ISA 84 refers to these instrumented systems as safety instrumented systems (SIS).

In the letter, OSHA states that the Agency considers ANSI/ISA 84.01-1996 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 with the specific requirements of ISA 84.

While ISA 84 does contain a "grandfather clause" for existing SISs (3), which is consistent in language and content to the "grandfather clause" of OSHA PSM, engineers involved in the modification of existing process units, or design of new grass-roots facilities must implement ISA 84.

The Scope of ISA 84

The ISA 84 standard was accepted by the American National Standards Institute (ANSI) in March 1997. It specifies requirements for the SIS assessment, design, installation, operation, and maintenance of SIS. In the event of hazardous incident, involving fire, explosion, or chemical release, insurers and regulators will audit installations for compliance with ISA 84 requirements.

At the time of ANSI's acceptance of the ISA 84 standard in 1997, many process operators accepted the standard as a way of demonstrating good engineering practice per OSHA PSM and began implementing its requirements. However, those who have waited for more-specific OSHA guidance now have it, and the clock is ticking with regard to any projects underway. Since, no grandfather clause exists for modified or new SIS designed and constructed after March 23, 2000, implementation of the ISA 84 is no longer just good engineering practice --- it is now a routine OSHA-compliance issue for process operators.

Interpreting and implementing the requirements contained in ISA 84 provide a new challenge for the chemical process industries (CPI). Included in an SIS are all devices necessary to reach the desired failsafe condition for the process, including the entire instrument loop from the field sensors through the logic solver to the final elements (e.g. solenoid, valve, pump, and compressor).

ISA 84 establishes the concept of an SIS lifecycle, providing a cradle-to-grave process for managing SISs. Figure 1 shows the ISA 84 lifecycle flowchart, overlaying six major project phases: research & development, specification, design, installation, operation & maintenance, and modification. Engineers, who adhere to such a lifecycle management approach, essentially make a commitment to carefully scrutinize every decision made during the life of the SIS, to ensure compliance with ISA 84 requirements.

What does it take to comply with ISA 84?

ISA 84 was developed as a consensus standard, covering a wide range of chemical process operations. Due to its broad scope, the standard has many general requirements that were written to allow flexibility in their application to many different processes. In general, compliance with ISA 84 can be managed using this three-step process (each is discussed below):

1. Decide how much risk reduction is required
2. Design systems that can meet the desired risk reduction
3. Operate, maintain, and test the systems to ensure long-term risk reduction

Note that the key word in each of these steps is "risk reduction." Without risk assessment tools and internal risk management policies in place, compliance is impossible.

Getting Started

1. Decide how much risk reduction is required. ISA 84 implementation begins with an early process hazards analysis (PHA). An assessment team identifies potentially hazardous events, their causes, potential consequences, and the non-SIS safeguards used to prevent or mitigate them. The PHA team then determines whether existing safeguards are adequate or whether additional risk-reduction measures are required. If the existing risk is found to be unacceptable, action items are developed to guide the engineering team to an appropriate solution.

In general, risk reduction is accomplished through the use of "layers of protection," such as those shown in Figure 2. A key requirement is that each protection layer must be designed to function independently from the other protection layers to ensure protection in the event of failure of one or more layers. Cost-effective risk reduction is achieved by designing and managing each protection layer to maximize its risk-reduction capability at minimum cost. The challenge is to select protection layers that yield the best cost-to-benefit ratio, while achieving the ultimate goal of reducing process risk to a tolerable level.

Once the decision has been made to utilize an SIS for risk reduction, the requirements of ISA 84 must be implemented. The safety integrity level (SIL) is assigned by the owner/operator to the SIS. ISA 84 has three discrete SIL performance ranges, as shown in Table 1. The SIL is related to the average probability of the SIS failing on process demand (PFDavg). For example, SIL 1 must achieve a minimum PFDavg of 0.1, which means that the SIS has a probability of failing 1 in every 10 times that it is needed (6). SIL 1 represents the lowest acceptable performance. SIL 3 represents the highest recognized performance.

Table 1: SIL and Probability to Fail on Demand (PFD) Average

SIL	PFDavg
1	0.1 to 0.01
2	0.01 to 0.001
3	0.001 to 0.0001

A number of methods (6) are available for assigning the SIL. All of the methods relate the perceived risk, as measured by incident frequency and consequence, to the SIL. Qualitative methods, such as risk matrices and risk graphs, are often used when the risk is well understood, such as process furnaces and boilers. Quantitative methods, such as fault tree analysis or event tree analysis, are used when simple qualitative assessment is difficult. For instance, many specialty chemical companies do not have sufficient process history or process knowledge to make good qualitative estimates of incident frequency. Of course, semi-quantitative methods are also available, such as layer of protection analysis (LOPA) and ALARP (which stands for "as low as reasonably practicable"). Whatever method is selected, the assignment of the SIL must be carefully performed and thoroughly documented (7). In general, the task of assigning the SIL links the design integrity of the SIS to the required level of risk reduction, thereby closing the loop between process design, hazard analysis, and instrumentation and electrical design.

2. Design systems that can meet the risk reduction. SIL establishes a minimum required performance for the SIS, as measured by the PFDavg. The SIL is affected by the following:

1. Device integrity (i.e. failure rate)
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 frequency (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)

These five factors represent the major design decisions, which have typically been the provenance of the instrumentation and electrical (I&E) department. In a sense, these parameters can be considered "degrees of freedom" in the design of the SIS, while the SIL is the design constraint established by ISA 84. The owner/operator is free to design the SIS using any device, redundancy and voting, functional testing frequency, or diagnostic coverage. The sum of these choices must achieve the PFDavg, related to the assigned SIL.

Furthermore, although ISA 84 is a performance-based standard (i.e. SIL-based) rather than a prescriptive standard, there are a few specific requirements, which will impact the current design philosophy of many operating companies. These include the following:

- Process control and SIS components and functions must be separated.
- Minimum hardware redundancy must be provided.
- Personnel access to SIS components and functions must be controlled.
- The use of digitally communicated information is prohibited.
- Information transfer between process control system and SIS must be restricted.

The quantitative verification of the SIL at each step in the design process is important to ensure that the design can achieve the PFDavg. Reliability Block Diagrams, Markov models and Fault Tree Analysis are acceptable techniques for SIL verification.

The SIL should be verified at the end of conceptual design, detailed design, and prior to startup. Sometimes, the design team wants to wait until the design is complete before verifying the SIL. Unfortunately, this is the most expensive point to be making design modifications. For instance, when design is declared as complete, the piping and instrumentation diagrams (P&IDs) have been finished, long-delivery items have been ordered, and field installation drawings are nearing completion. This is not the time to determine that the SIS will require on-line testing in order to achieve the SIL, necessitating the installation of isolation valves, bypass valves, and limit switches.

3. Operate, maintain, and test the systems to ensure long-term risk reduction. Thorough risk assessment and proper design constitute half the battle to ISA 84 compliance. Long-term preservation of the SIL through operation, maintenance, and management of change activities is the other half and, for many companies, is the most difficult part of compliance. Most codes and standards focus solely on design. Once the piece of equipment is “certified” for compliance, the requirements for the code or standard are fulfilled. However, SIL is not just a design parameter. It is also an operational parameter. The choices made during design, including voting, diagnostics, and testing, must be preserved throughout the facility’s life. Once the SIS is designed and installed, and a testing frequency is chosen, the SIL is fixed and can only be changed by modification of one of the major design parameters. Consequently, SIL serves as a “management of change” checkpoint.

The commitment

ANSI/ISA 84.01-1996 is an important standard that establishes specific requirements for the assessment, design, installation, operation, and maintenance of Safety Instrumented Systems. For some process facilities, implementation of the standard will require a paradigm shift in their approach to SIS design. No longer is it acceptable to simply put instrumentation on P&IDs and assume that the instrumentation is sufficient. Documentation must be created to clearly state what is required to mitigate the risk, to demonstrate that the SIS was designed to meet those requirements, and to show that the operation and maintenance practices are established to maintain the SIS.

Some may feel that the ISA 84 requirements are excessive, and may find it a struggle to successfully integrate the standard into their policies and procedures. However, ISA 84 is a standard that OSHA has officially recognized, not only as good engineering practice for PSM facilities but also as demonstration of an Owner/operator's commitment to provide a safe working environment. By its recent letter to ISA, OSHA has now made it clear to everyone --- *ISA 84 is the standard for safety instrumented system design*.

Viva La Difference – IEC 61511

Under the direction of the International Electrotechnical Commission (IEC), an international committee is working to create an 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 (ISA 84) worldwide. As a result, in the future, the 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 consistency will become more important as International companies increasingly execute projects involving multiple countries. A global standard ensures that everyone is following the same criteria, thereby reducing front-end loading and detailed design costs associated with process hazards management.

Although the draft version of 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. Draft 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.

Draft IEC 61511 consists of three parts. Part 1 contains the mandatory requirements while Parts 2 and 3 provide guidance information. Parts 1 and 3 have already been released as committee draft with vote (CDV), moving these parts within two administrative steps of being final. Committee members have committed to reaching final agreement and acceptance of the entire standard by the end of 2002.

Literature Cited

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. Summers, A.E. and K. Dejmek, "Is Your SIS 'Grandfathered'?," Chemical Engineering Progress, pages 39-42 (May 1999).

4. "Control systems: Why things went wrong, and how they could have been prevented," Health & Safety Executive Books, Sudbury, Suffolk, United Kingdom.

5. Summers, A.E., "Understanding Safety Integrity Levels," Control Engineering website (February 2000).

6. Summers, A.E., "Techniques for assigning a target safety integrity level," *ISA Transactions*, 37, pp. 95-104 (1998).

7. Summers, A.E., "Safety Requirements Specifications in a Capital Project Environment," Control Engineering, website publication (May 2000).

8. "Functional Safety: Safety Instrumented Systems for the process industry sector: Part 1 Framework, definitions, system, hardware, and software requirements," IEC 61511-1, International Electrotechnical Commission, CDV (2000).

Figure 1. ANSI/ISA 84.01-1996 Safety Lifecycle Model Showing Phases

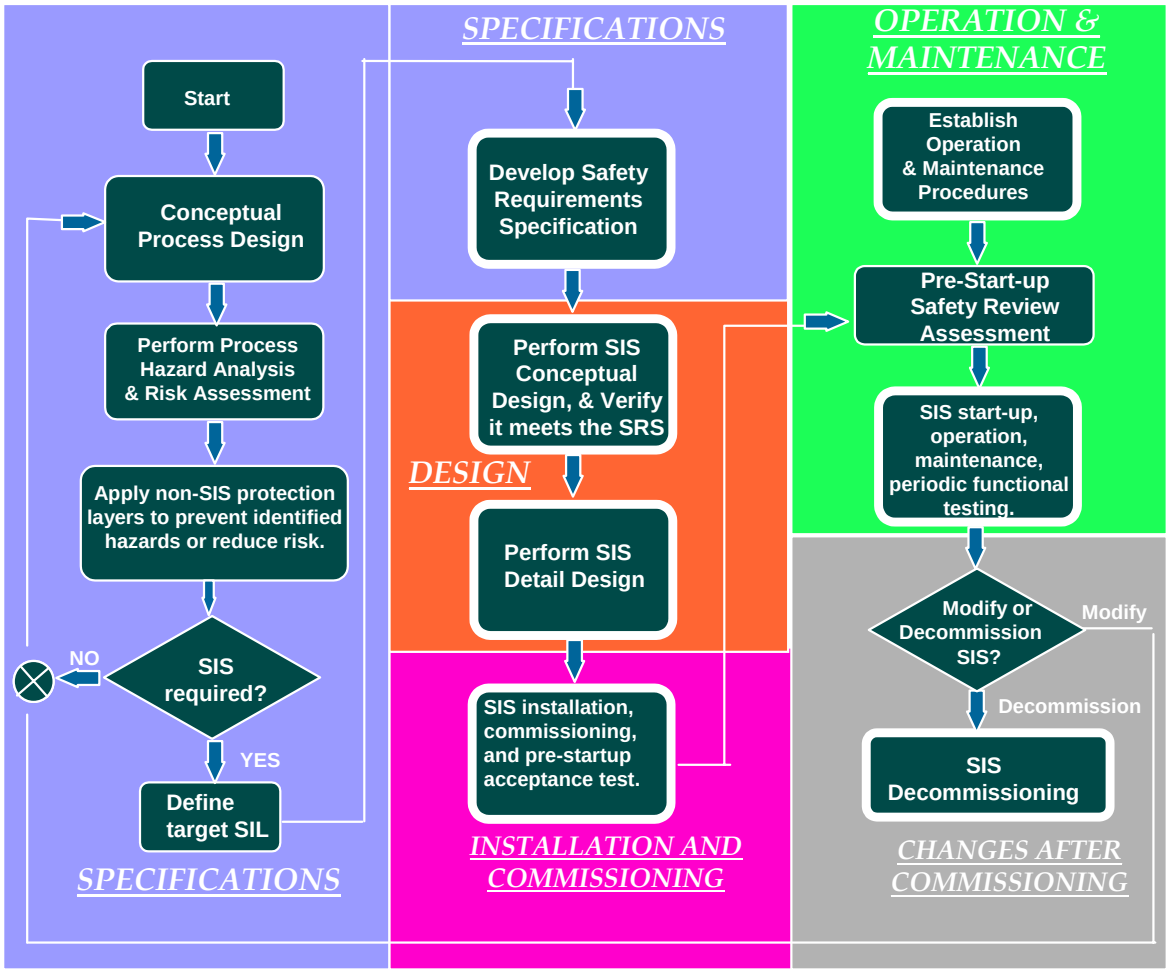

Figure 2. Protection Layers (draft IEC 61511)