WWW.CHEMICALPROCESSING.COM

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

Can you safely "grandfather" your SIS?

Several factors determine if an existing safety instrumented system satisfies a new standard

By Angela E. Summers, SIS-TECH Solutions, LP

SAFETY INSTRUMENTED SYSTEMS (SISs) — THE instrumentation and controls intended for handling process risks — play a vital role in ensuring plant safety. In September 2004, the European Committee for Electrotechnical Standardization and the American National Standards Institute (ANSI) adopted a new standard related to such systems. This standard, called IEC 61511, EN IEC 61511 or ANSI/ISA 84.00.01-2004 Parts 1-3 (IEC 61511 Mod), now becomes the primary driving force behind the work processes that should be followed to design and manage SISs. It applies to any new or expanded process unit and to the upgrade of an existing SIS.

The U.S. version, which will be referred to in this article as S84.01-2004, is identical to IEC 61511 with one exception. The United States added a "grandfather clause" for existing SISs.

The standard integrates the various process safety management (PSM) approaches used successfully throughout the world. The SIS lifecycle provides a framework for the various activities that are considered essential to the assessment, design, maintenance, inspection, testing and operation of SISs. A quality management system also is defined to minimize the systematic errors during major project phases, such as:

- hazard assessment;
- design;
- engineering, installation, commissioning and validation; and
- operations and maintenance.

The standard uses a performance metric, the safety integrity level (SIL), to indicate the risk reduction necessary to keep a specific process risk at a tolerable level. The SIL establishes order-of-magnitude bases for analysis, design, diagnostics, testing and management rigor.

The SP84 committee of Instrumentation, Systems and Automation (ISA), Research Triangle Park, N. C., will soon release a two-part technical report, ISA TR84.00.04, "Guideline on the Implementation of ANSI/ISA 84.00.01-2004 Parts 1-3 (IEC 61511 Mod)." Part 1 details the differences between the 1996 version of the standard, S84.01-1996, and S84.01-2004 and addresses a variety of topics in a series of annexes. Part 2 provides an example

of the implementation of the new standard on a hypothetical SIS project.

Some topics of particular interest in TR84.04 are:

- evaluation of the applicability of the grandfather clause;
- management of functional safety (e.g., identification of worker roles and responsibilities);
- selection of SIS devices;
- relationship of the basic process control system to the SIS; and
- human error considerations.

This article focuses on the grandfather clause and its implications for existing instrumentation and controls.

The grandfather clause

S84.01-2004 Part 1 Clause 1y states:

"For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance 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."

This grandfather clause is similar to the one contained in S84.01-1996, which was developed by the ISA SP84 committee to document the instrumentation-and-controls lifecycle associated with the U.S. Occupational Safety and Health Administration's 1910.119 Process Safety Management regulation. OSHA specifically requested a grandfather clause be included in S84.01-1996.

However, making a claim that an existing system meets the intent of the grandfather clause should not be taken lightly. When investigating incidents, OSHA looks to current good engineering practices to benchmark the owner/operator's design and management practices.

As an example, consider an OSHA citation issued on Oct. 22, 2004, to Formosa Plastics Corporation, Illiopolis, Ill. It relates to an April 23, 2004, explosion in which five workers were killed, three workers were seriously injured and the facility was heavily damaged. Numerous items were cited but three are particularly notable.

First, OSHA specifically cited the company for failing to document compliance to the S84.01-1996 standard, which the agency said represented "recognized generally accepted good engineering practices."

When an owner/operator has an incident, its practices are compared to published good engineering practices. The owner/operator is responsible for determining that existing SISs meet the intent of the grandfather clause and documenting the operating, testing, inspection and maintenance conditions under which this will remain true.

It is important to recognize that the grandfather clause only addresses the SIS devices that were installed and commissioned prior to the issuance of S84.01-2004. It does not cover the management system aspects of the standard.

All SISs, whether existing, modified or new, require the following:

- documentation (e.g., the safety requirements specification);
- procedures (e.g., operation, maintenance, bypassing and testing);
- training;
- failure tracking (e.g., process demands and dangerous failures);
- management of change (MOC); and
- auditing.

Changes that potentially impact the SIS requirements should be evaluated through a MOC process. The need to make changes in the process, its control system, its non-SIS protection layers and its SIS often defines when the grandfather clause is no longer applicable.

Second, OSHA cited Formosa for failing to determine "the required safety integrity levels, as per ANSI/ISA 84.01, of its PLCs [programmable logic controllers] and DCS [distributed control systems], critical control and safety-instrumented systems."

The new standard includes specific requirements for the assessment of the instrumented systems used to mitigate process risk. A work process provides the key steps in defining the required functionality and risk reduction for the safety functions allocated to the SIS. The risk reduction requirements are compared to order-of-magnitude ranges provided in tables in S84.01-2004 to assign the SIL to the SIS.

Third, the agency faulted the company's MOC process. Formosa was cited for not implementing a process "to address the technical impact, as well as the safety and health impact of… changes made in the staffing level of the plant in 2002 and 2003 to the maintenance staff as it impacted the ability to perform necessary inspections and tests to meet the requirements of the company's mechanical integrity program."

S84.01-2004 includes a management system that requires, among other things, the identification of the resources responsible for carrying out each lifecycle phase, such as operation, testing and maintenance.

The way forward

According to draft ISA TR84.04, there are two essential steps in assessing the applicability of the grandfather clause:

1. Confirm that a hazard and risk analysis has been done to determine qualitatively or quantitatively the level of risk reduction needed for each safety instrumented function (SIF) in the SIS.
2. Verify that an assessment of the existing SIF has been performed to establish that it delivers the needed level of risk reduction.

TR84.04 states that these activities, if not already done, should be scheduled for review at the next appropriate opportunity. The evaluation of the SIF should take into account factors such as device failure rates and associated design, operation, maintenance, testing, inspection and change-management practices. TR84.04 Annex

A provides examples of eight grandfather clause methods submitted by SP84 committee members.

The first step in addressing the grandfather clause is the development of a method for "determining" the applicability of the grandfather status of the SIS. Local regulations, applicable codes and insurance practices sometimes require that specific standards be followed. In all cases, the owner/operator ultimately is responsible for establishing the policies that support safe operation, including the evaluation of existing infrastructure against good engineering practices such as S84.01-2004.

It is crucial that the method integrates with the existing PSM program. Work processes and procedures developed for PSM should be leveraged. MOC and process hazards analysis drive the evaluation of process risk and could challenge the appropriateness of a grandfather claim. Various study findings will require prioritization and actions plans.

When deciding the priority of evaluations or the aggressiveness of a facility review, it is important to consider, among other factors, the risk potential and anticipated gaps with the new standard. Companies which complied with the intent of the 1996 version of the standard or with other recognized standards should find very few gaps. However, firms which have not kept pace may identify significant deviations.

If an owner/operator determines that the existing SIS *does not meet* the intent of the grandfather clause (i.e., "…the equipment is designed, maintained, inspected, tested and operating in a safe manner"), a defined decision-making process should address the identified gaps between the requirements and reality. This often involves a risk-ranking matrix based on the size of the deviation and the nature of process risk (e.g., frequency and consequence) associated with the potential event. Similar work processes can be used to develop actions plans for closing the gaps.

The challenge

Many owner/operators have not previously classified their automatically initiated shutdowns, so they do not know which ones fall under the umbrella of the standard and which ones do not. At many facilities, shutdowns are grouped under categories such as emergency shutdown systems, interlocks, critical instruments, etc. No distinction is made between safety, environmental, asset or business-interruption risks. In general, asset and economic protection account for a large percentage of the automatically initiated shutdowns.

However, S84.01-2004 only applies to the mitigation of safety risks and catastrophic environmental events. It does not cover instrumented systems to mitigate economic or asset risks. A hazard and risk analysis can be used to identify those functions that are required for safety and to define their functionality and risk-reduction requirements. Once the SIFs have been defined, the performance of the installed SIFs can be compared to the requirements to identify gaps.

A safe approach

The grandfather clause of S84.01-2004 does not offer an indefinite shield against the requirements of the standard. It provides the essential criteria that should be considered in the evaluation of existing SIFs. Good engineering practice, as outlined in ISA TR84.00.04, requires two key actions for each SIF to establish the applicability of the grandfather clause:

1. Determine the risk reduction required in the SIS using hazard and risk analysis.
2. Verify that the design and operating basis used delivers the required risk reduction.

Upgrading existing facilities to meet the intent of S84.01-2004 should be accelerated when existing devices are found to no longer meet the required risk reduction. This determination may be made through hazard and risk analysis, test and inspection findings and reports, operation reports of SIS demands and failures, and audits of the performance of personnel and systems against procedures and expectations. In existing facilities, the hazard and risk analysis often serves as the trigger for the periodic re-evaluation of protection layer adequacy and conformance to the latest standard. **CP**

Angela E. Summers, Ph.D., P.E., is president of SIS-TECH Solutions, LP Houston, Texas. She is the recipient of ISA's 2005 Albert F. Sperry Award "for outstanding contributions and leadership in the specification, development, and implementation of safety instrumented systems for the process automation industry." E-mail her at asummers@sis-tech.com.

REFERENCES

1. "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," 29 CFR Part 1910, U.S. Occupational Safety and Health Administration, Washington, D.C. (1992).
2. "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA 84.01-1996, Instrumentation, Systems, and Automation (ISA), Research Triangle Park, N.C. (1996).
3. "Functional Safety: Safety Instrumented Systems for the Process Industry Sector," International Electrotechnical Commission (IEC), IEC 61511 Geneva, Switz. (2003).
4. "Functional Safety: Safety Instrumented Systems for the Process Industry Sector," ANSI/ISA 84.00.01-2004 Parts 1-3 (IEC 61511 Mod), Instrumentation, Systems, and Automation (ISA), Research Triangle Park, N.C. (1996 and 2004).
5. U.S. Department of Labor, OSHA, Formosa Plastics Corp., Inspection No. 305893679, Inspection Dates 4/24/2004 through 10/20/2004 (2004).