

# **DIFFERENCES BETWEEN IEC 61511 AND ISA 84.01-1996**

Angela E. Summers, P.E., PhD  
President, SIS-TECH Solutions, LLC  
12621 Featherwood, Suite 120  
Houston, Texas 77034

## **KEYWORDS**

Standards, Safety Instrumented Function, Validation, Verification

## **ABSTRACT**

The international standard IEC 61511 will be released in its entirety as a final standard this year. The ISA SP84 committee has voted to accept IEC 61511 as ANSI/ISA 84.01-2003. It has also begun work on a guidance document, concerning transition to and implementation of IEC 61511 in the United States. The author of this paper is the Task Team Leader for this guidance document.

Although IEC 61511 uses a lifecycle concept, it is no mirror image of ISA 84.01-1996. An international standard must harmonize the standards of many countries. Consequently, the standard will add new requirements for management of functional safety, component selection, design, pre-startup safety reviews, operation and maintenance, and auditing. This paper will not present an overview of the IEC 61511 standard. Rather, this paper will focus on the most significant differences between IEC 61511 and ISA 84.01-1996, highlighting what end users need to consider in migrating their current ISA 84.01-1996 programs into IEC 61511 programs.

## **LIFECYCLE DIFFERENCES**

In the United States, many companies must adhere to OSHA 1910.119, Process Safety Management (PSM) for Highly Hazardous Chemicals. The ISA SP84 committee created the ISA 84.01-1996 standard to supplement PSM in the areas related to the implementation of instrumentation and controls necessary for safe operation. Rather than repeating PSM mandates, the standard references OSHA 1910 for some key PSM program elements. Specifically, ISA 84.01-1996 does not cover safety management, hazard analysis, pre-start-up safety review, or training.

Many other countries do not have a regulation similar to OSHA 1910. Therefore, IEC 61511 includes specific requirements in the areas of safety management, hazard analysis, pre-start-up safety review, and training. The inclusion of these requirements ensures that a complete safety management system, as required in the United States, is implemented worldwide. The requirements will be discussed later in this paper.

## **GRANDFATHER CLAUSE**

The US version of IEC 61511 will include a grandfather clause for existing installations that were designed in accordance with ISA 84.01-1996, which states

*For existing SIS designed and constructed in accordance with codes, standards (i.e. ANSI/ISA 84.01-1996), or practices prior to the issuance of this standard, the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.*

The grandfather clause does not protect any user from OSH Act General Duty clause, which requires that owners/operators provide a safe working environment. And, OSHA has already stated in their letter to ISA dated March 23, 2000 that “The employer may be in violation of the General Duty Clause, Section 5 (a)(1) of the OSH Act, if SIS are utilized which do not conform with S84.01 and hazards exist related to the SIS which could seriously harm employees.”

Of course, new units or retrofits must be designed and implemented according to the ISA 84.01-2003 standard.

## **TERMINOLOGY**

### **SAFETY INSTRUMENTED FUNCTION VERSUS SAFETY INSTRUMENTED SYSTEM**

ISA 84.01-1996 uses the term safety instrumented system to refer to a single instrumented loop or to the overall implementation of multiple instrumented loops in a single programmable electronic system (PES). IEC 61511 introduces a new term, safety instrumented function (SIF).

SIFs are instrumented loops that address a specific process risk and are assigned an SIL. SIFs are simply the logic that is being applied to achieve a certain amount of risk reduction, e.g. on high pressure, shut the main fuel gas valves. An SIS is used to implement the safety instrumented function. Safety instrumented systems are the actual hardware and software that is used to implement the safety instrumented function, e.g. on high pressure, transmitter PT-101 sends a trip condition to the redundant PES which de-energizes its outputs associated with solenoid XY-101A which closes valve XV-101A and solenoid XY-101B which closes valve XV-101B.

## **VERIFICATION VERSUS VALIDATION**

ISA 84.01-1996 required that the conceptual design be verified against the safety requirements specification (SRS) and the detailed design to be verified against the conceptual design and SRS. It also required that the SIL be verified. After commissioning the SIS, a pre-startup acceptance test was required that included input to output testing to ensure that the SIS works in the actual installation as intended by the design. These same activities occur in IEC 61511, but this standard makes a distinction between pre-startup acceptance testing, which IEC 61511 refers to as validation, and the earlier assessment activities, which IEC 61511 refers to as verification.

Verification is an activity in which the deliverables from any stage are compared to the specifications developed in the previous stages to ensure that the deliverables match the specifications. A verification step would be to ensure that the detail design matches the safety requirements specification.

Validation is an activity that proves that the SIS works. Validation involves a complete input to output test. In the US, this testing is performed as part of the pre-startup acceptance test.

## **MANAGEMENT OF FUNCTIONAL SAFETY**

The management of functional safety is a requirement in IEC 61511 and there is no similar requirement in ISA 84.01-1996. The intent is to identify the activities that must take place to achieve safe operation and to identify the personnel that will be responsible for conducting each activity. This is simply good project management.

Management of functional safety includes the following requirements:

- Identification of the individuals, departments or organizations that will be responsible for each of the lifecycle task
- Determination that those assigned responsibility for these activities are competent
- Define when verification, assessments, auditing and validation activities will take place
- Require procedures for evaluating the performance of the SIF after it has been installed (e.g. performance audits, tracking failures rates, etc.)
- Require at least one functional safety assessment (FSA) be performed prior to introduction of hazardous materials into the process. The FSA is similar in content to pre-startup safety review, so any OSHA 1910 compliant facility should already be fulfilling the majority of the requirements associated with the FSA. IEC 61511 does require at least one senior, competent, independent (from the project team) person take part in the FSA. This “competent” person should be able to review the hazards analysis, design, implementation, and testing to ensure that everything had been successfully completed. This “senior” person must also have the authority to prevent the start-up of the process unit, if necessary.

## **RISK ASSESSMENT AND ALLOCATION**

As mentioned previously, ISA 84.01-1996 did not provide any requirements related to the hazard and risk analysis, since this analysis was already required by OSHA 1910. Further, significant guidance on risk assessment and protection layer analysis is provided by the Center for Chemical Process Safety books, “Guidelines for Safe Automation of Chemical Process Safety” and “Guidelines for Chemical Process Quantitative Risk Analysis.”

IEC 61511 does include requirements for the risk assessment and risk allocation, including the following:

- Hazard analysis scope:
  - All protection layers, including critical control loops, safety critical alarms, and pressure safety devices, must be identified.
  - Risk reduction must be allocated to these protection layers.
  - Justification must be provided for the allocated risk reduction.
- BPCS limitations (when not designed to meet the requirements of the IEC 61511 standard):
  - Initiating cause frequency - no less than  $10^{-5}$ /hr – regardless of the BPCS technology.
  - Maximum credit as risk reduction layer – assumed risk reduction must be less than 10.

## **DESIGN RESTRICTIONS**

There are a number of new design requirements in IEC 61511, which cover everything from the selection of devices to proving that the SIS has been adequately designed.

## **DEVICE SELECTION JUSTIFICATION**

ISA 84.01-1996 left the choice of SIS devices to the discretion of the user. IEC 61511 provides two means for selecting devices for SIS applications:

1. Proven-in-use. The selection is based on the prior use of the device. There must be sufficient operating experience for the device in a similar operating profile. For field devices, this could include the use of the device in a process control system application, as long as the operating profile, including the process application environment, is similar.
2. Compliance with IEC 61508. The selection is based on the device being designed for compliance with IEC 61508. The user can make this determination or use evidence provided by the vendor or third party certification body.

## **FAULT TOLERANCE**

In ISA 84.01-1996, the design was considered adequate as long as the PFDavg was achieved by the SIS design. In addition to the PFDavg, IEC 61511 requires that the SIS demonstrate a minimum fault tolerance. The fault tolerance requirements in IEC 61511 have been highly simplified from those contained in IEC 61508. For field devices, the redundancy requirements essentially increase as the SIL is increased. For PES, the fault tolerance is based on the PES safe failure fraction. The safe failure fraction is the fraction of the overall random hardware failure rate of the PES that results in either a safe failure or dangerous detected failure. The safe failure fraction is simply a measure of the PES's tendency to go to the safe state when there is a fault within the system. The standard lowers the redundancy requirements as the safe failure fraction increases.<sup>1</sup>

## **QUANTITATIVE SIL VERIFICATION**

---

<sup>1</sup> Please note that this means that low redundancy, high diagnostic PES will meet SIL 3 requirements. And, the vendors have been proclaiming the capital cost savings of these PES. However, these PES come with another price – online operation. The very high safe failure fraction required for SIL 3 means that most PES faults take the PES to the fail safe condition. IEC 61511 is not concerned with online performance, only safe operation. So, make sure that reliability requirements are included in specifications for new SIS, so the plant does not wind up with a very safe but highly unreliable SIS.

ISA 84.01-1996 did not require a quantitative assessment of PFDavg. Instead, it stated that the user could rely on past performance of an existing SIS design as the basis for justification of its continued use. The SP84 committee issued a technical report, ISA TR84.00.02, to illustrate how to calculate the PFDavg, including simplified equations, fault tree analysis, and Markov modeling.

IEC 61511 requires quantitative assessment of the PFDavg and devotes Clause 11.9 to listing the specific information that should be included in the assessment. The PFDavg is a major checkpoint for all design, implementation, maintenance, and management of change activities.

## **OPERATION AND MAINTENANCE REQUIREMENTS**

Both ISA 84.01-1996 and IEC 61511 contain requirements for operator and maintenance procedures. ISA 84.01-1996 did not provide any requirements for training, since this was already an OSHA 1910 requirement. IEC 61511 provides specific requirements for what should be covered during training, including the following:

- SIF set points and actions
- hazard that the SIF is trying to prevent
- when bypasses can be used
- compensating measures when the SIF is in bypass
- response to diagnostic alarms
- when manual shutdown should be executed

## **AUDITING**

IEC 61511 also emphasizes the importance of auditing activities to ensure long-term performance:

1. the SIS operation must be audited to determine the actual demand rate, i.e., process excursions resulting in SIS action.
2. the SIS device failures should be recorded and the actual failure rates determined, i.e., maintenance tracking of device safe and dangerous failures.

Essentially, long-term performance is compared to the design assumptions. If plant operation is having more demands than assumed during the hazard and risk analysis, the analysis must be reviewed to determine whether the target SIL should be revised. If the maintenance data indicates that SIS devices

have a higher failure rate than used in the design calculation, the PFDavg must be reassessed based on the new data.

## REFERENCES

1. "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA-ISA 84.01-1996.01-1996, 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. International Electrotechnical Commission (IEC), IEC 61511, "Functional Safety: Safety Instrumented Systems for the Process Sector," Geneva, Switzerland (expected 2003).
4. International Electrotechnical Commission (IEC), IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems," Geneva, Switzerland (1999).
5. "Is Your SIS 'Grandfathered'?" Chemical Engineering Progress, pages 39-42, May 1999.
6. "Guidelines for Chemical Process Quantitative Risk Analysis," 2<sup>nd</sup> edition, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York (2000).
7. "Guidelines for Safe Automation of Chemical Processes," Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York (1993).

This paper was previously presented as a workshop at ISA Chicago, October 2002 and as a paper at TAMU Instrumentation Symposium 2003. **This paper has been updated to reflect the current status of IEC 61511.**