MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Evolutionary Themes from ISA 84 to ISA 61511

Eloise Roche*, Angela Summers
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034
*Presenter E-mail: eroche@sis-tech.com

Keywords: Safety Management System, Standards

Abstract

ANSI/ISA 84.00.01 was the second edition of ISA standard to address safety instrumented systems for the process industry sector and was recognized by OSHA as a good engineering practice within process safety management. Nevertheless, standards must evolve over time based on application experience. After a decade of international process sector experience in applying these requirements for safety instrumented systems (SIS), a new edition of the IEC 61511 international standard was published. Recently published, ANSI/ISA 61511-1 brings the ISA standard into complete alignment with IEC 61511-1. This paper will review ten major themes of change between ANSI/ISA 84.00.01 and ANSI/ISA 61511-1.

1 Introduction

The American National Standard ANSI/ISA-S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries" [1] was published just a few years after the issuance of the OSHA regulation on process safety management (PSM) [2]. Within this context, this first edition of the safety instrumented system (SIS) standard focused predominately on the design, installation and change management of the system hardware and said little about other aspects of functional safety management already addressed in the PSM regulation. This original standard also said little about application programming for programmable electronic systems, which were a relatively new logic solver technology compared to the simpler safety relays and trip amplifiers that were in common use at the time for emergency shutdown systems and other safety applications.

Of course, the need for a standard on safety instrumented systems was not limited to the United States of America. The first edition of the U.S. standard on SIS was an input to the newly formed IEC 61511 committee. Not all of the nations involved in the IEC committee had laws similar to the U.S. regulation on process safety management. Therefore, many of the changes made in the

development of IEC 61511-1:2003 [3] focused on adding the functional safety management requirements that would otherwise have been absent in the international context. Since the programmable electronic logic solver was by this time a much more established technology, IEC 61511-1:2003 also included requirements for the application programming for SIS using this technology. For the most part, the resulting set of requirements would have been very familiar to facilities subject to both OSHA PSM regulations and the ANSI/ISA-S84.01 standard. IEC 61511-1:2003 was adopted the following year as the second edition of the ISA SIS standard, retitled ANSI/ISA 84.00.01 [4], with only the addition of one clause in the scope to address existing systems that had been designed and implemented using the 1996 standard.

During the first handful of years after the publication of ANSI/ISA 84.00.01, members of the ISA 84 committee, the MT61511 team, and the broader industrial community began to note sections of the standard where systematic misunderstanding in application still seemed to be occurring relatively often. The fundamental safety instrumented system hardware and functional safety management requirements in the standard were by this time well-established process safety practice across the globe. Therefore, the major change themes for the second edition of IEC 61511-1 [5] focused on clarifying existing concepts in the requirements to improve the systematic use of the standard in these sections. Adopted by ISA without change in late 2017, the standard now known as ANSI/ISA 61511-1 [6] (retiring the ISA 84.00.01 nomenclature) can be more consistently applied around the world.

These major change themes can be grouped together into the following categories:

- Hazards and Risk Analysis (H&RA) and Specification
- Detailed Design and Engineering
- Operations and Maintenance

2 H&RA and Specification

The failure frequency claimed for initiating sources related to the basic process control system (BPCS) and the risk reduction allocated to BPCS protection layers directly impact the risk reduction target for an associated safety instrumented function (SIF). Likewise, any common causes or dependencies between functions involved in a hazardous event initiation or the responding protection strategy can affect the residual frequency of the hazardous outcome. Finally, once a SIF is required by the H&RA, the specification of performance requirements for the SIS performing the SIF must be sufficiently clear that the system is designed and implemented correctly, resulting in a demonstrated performance consistent with the safety integrity level (SIL) the H&RA assumed.

All three of these concepts were addressed in ANSI/ISA 84.00.01. However, a few years after this standard was published, comments submitted by experienced personnel revealed that further clarification would be needed in the new edition.

2.1 Limits on BPCS failure frequency and target risk reduction

Submitted comments on IEC 61511-1:2003 and ANSI/ISA 84.00.01 revealed that the previously existing two clauses (9.4.2 and 9.4.3) were not sufficiently clear in expressing the limitations that had been intended by the committee:

a) Minimum assumed frequency of a BPCS failure (whether referring to the system as a whole or to just one part thereof) that could initiate a hazardous event
b) Maximum risk reduction that could be claimed for a protection layer within the BPCS
c) Maximum number of protection layers that could be executed within the BPCS for a given hazardous events
d) Requirements for independence for protective layers executed within the BPCS

These limitations reflect the overall performance impact associated to the less rigorous design, implementation, and management practices typically applied to the BPCS (as compared to those used to manage the SIS). The recognition that the BPCS had a limited capability to provide risk reduction for process safety incidents had been documented in the first edition of CCPS *Guidelines for Safe Automation of Chemical Processes* [7], published just after the OSHA PSM standard was issued. Further guidance was provided a few years later in CCPS *Layer of Protection Analysis: Simplified Process Risk Assessment* [8]. Reinforcing and building upon these original positions, additional technical guidance was provided in CCPS *Guidelines for Safe and Reliable Instrumented Protective Systems* [9] and *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis* [10]. The values provided in ANSI/ISA 61511 for each of limitations listed above reflect the long-standing experience of overall BPCS performance that is documented in these industry consensus publications.

2.2 Requirements for claiming RRF>10,000 in total for instrumented safeguards

The verification, validation, and change management practices documented in ANSI/ISA 84.00.01 were designed to keep the probability of systematic error relatively low for a given safeguard. However, once the overall risk reduction for the BPCS protection layer(s) and SIS(s) exceeded 10,000 (i.e., equivalent to 4 orders of magnitude in LOPA), the impact of systematic error could no longer be considered negligible in the evaluation of risk reduction achieved. ANSI/ISA 84.00.01 addressed these issues for a single function in a clause on the requirements for a SIL 4 SIF.

However, even when the risk reduction allocation is spread over multiple protection layers with independent primary safety system devices (sensors, logic solvers, final elements), common personnel are often used to program, operate and maintain the instrumented safeguards. Likewise, internal process and external environmental impacts on the reliable operation of instrumentation can impact multiple instrumented functions. ANSI/ISA 84.00.01 included requirements to address common cause and dependent cause failure between all protection layers, as well as with the BPCS that could initiate a demand on those protections. Where multiple instrumented safeguards provided an overall risk reduction of 10,000, all the issues noted in the clause on SIL 4 SIFs would

be applicable to the required common cause analysis. Making it easier to recognize the technical interaction of the ANSI/ISA 84.00.01 clauses, the SIL-4 clause in ANSI/ISA 61511-1 explicitly addresses the case where the risk reduction of 10,000 is spread across multiple instrumented safeguards.

2.3 SRS clarity and traceability

Experienced users of ANSI/ISA 84.00.01 reflected that the safety requirements specification (SRS) and the instrument selection justification for SIS are sometimes written in highly technical language that may not be maintainable, verifiable, or even understandable by operations and maintenance, but which nevertheless were considered compliant with the standard. For example, it could not always be determined that the information used in the instrument selection and system design was even relevant to the operating environment for that installation. As is the case with any other engineering document, clarity and applicability of this information is essential to achieving and maintaining the expected performance of the resulting system, including supporting nearly inevitable management of change. ANSI/ISA 61511-1 requires clarity and traceability of all the assumed parameters back to the SRS, H&RA, and operating environment, not just the application programming as was already required in ANSI/ISA 84.00.01. The requirement for clarity and traceability reflects the automation systems engineering reality described above and supports the OSHA PSM expectation that the compilation of process safety information enables "the employer and the employees involved in operating the process to identify and understand the hazards".

3 Detailed Design and Engineering

Most of the current SIS hardware requirements have origins in the original standard from over two decades ago. However, some of the design and engineering clauses in ANSI/ISA 84.00.01 were unnecessarily complex. Design and engineering change themes implemented in ANSI/ISA 61511-1 sought to relocate or reword these more complex provisions to make them easier to understand and simpler to incorporate into a design. Being a standard addressing instrumented safety systems, design and engineering provision changes also needed to be made to reflect the ongoing evolution in industrial automation and control system technology.

3.1 Application programming provision relocation

When they were added to IEC 61511-1:2003, the set of new provisions related to SIS application programming were gathered together in clause 12. For simplicity of adoption into ISA, this structure was unchanged in ANSI/ISA 84.00.01. With the rest of the document being structured in the order of the safety lifecycle, however, this separation let to confusion regarding when the application programming activities were to take place during the execution of a project. In addition, some of these activities would typically impact both the hardware and application program design or implementation, requiring careful coordination. In ANSI/ISA 61511-1, a significant number of application programming provisions were relocated from clause 12 to provide clearer guidance on when the activity should be executed. For example, application program safety requirements have been incorporated into the main SRS requirements to emphasize

the need for a close relationship between the SIS SRS and the application program safety requirement development.

3.2 Hardware fault tolerance

Prescriptive hardware fault tolerance (HFT) limits were added in the previous edition of the standard to mitigate some of the more common design and implementation systematic failures:

a) Using overly optimistic reliability parameter assumptions
b) Maintenance error such as leaving a root valve closed or a bypass jumper in place

However, the complex rules, which had been derived from the original edition of IEC 61508-2 [11], were themselves subject to systematic error and differences of interpretation. The basic HFT requirements in ANSI/ISA 61511-1 are simplified, adapting one of the second edition IEC 61508-2 [12] approaches in a manner that better supports implementation using prior use justification of SIS field devices within the process sector.

3.3 Fault detection, bypassing, and compensating measures

One common underlying SIS design assumption is that a SIS device will be out of service due to bypass or detected failure for a limited time and that compensating measures will be used to manage any gap in risk reduction during that time. This expectation is closely aligned to the OSHA PSM requirement that the employer "correct deficiencies in equipment that are outside acceptable limits…before further use or in a safe and timely manner when necessary means are taken to assure safe operation." ANSI/ISA 84.00.01 addressed this concept in a series of provisions that stated the requirement in a different way depending on the architecture of the subsystem that was degraded. User observations from a decade of application of this standard exposed a lack of clarity regarding the requirement of managing known periods of SIS unavailability or degraded performance while the equipment the SIS was designed to protect remained in operation. The two clauses in ANSI/ISA 61511-1 that require compensating measures to maintain safe operation when a dangerous fault in the SIS is detected or when the SIS is bypassed are stated in a simpler manner than in the prior edition.

3.4 Cybersecurity for SIS

With continued occurrences of successful cyber security attacks against industrial control systems and more frequent installations of SIS with digital communication to other devices, cybersecurity needed to be incorporated into the updated SIS standard. To avoid unnecessary overlap with the ANSI/ISA 62443 [13] series of standards on network and system security for industrial communication networks, ANSI/ISA 61511 contains only two new clauses on this topic. The first requires a security risk assessment to be performed that included the SIS. The second clause requires the SIS be designed to provide the necessary resilience against the identified security risks. Located in the risk analysis and detailed design sections of ANSI/ISA 61511-1, these two clauses are "anchors" that can help the user understand how the ANSI/ISA 62443 activities should fit into the functional safety lifecycle.

4 Operations and Maintenance

As noted above, a primary change theme behind the new content in ANSI/ISA 84.00.01 was the incorporation of functional safety management requirements. Most of these have very clear relationships to OSHA PSM requirements, with technical details added appropriate to the nature of instrumented safety systems. However, over time it became evident that the topics of existing systems, change management, and periodic performance assessment were still systematically confusing to some users of the standard.

4.1 Existing systems

Addressing systems that predated the standard has been incorporated into all editions of the SIS standard. This concept is sometimes referred to as "grandfathering". In ANSI/ISA 84.00.01, the provision on existing systems had been located in the scope section of the document. This led to a misunderstanding that none of the functional safety management requirements would apply to such systems. Such a misunderstanding would have also been inconsistent with the expectations of OSHA PSM as well. In ANSI/ISA 61511-1, the clause on existing systems is relocated into clause 5, to clarify that the ongoing management of systems that predated the standard is part of functional safety management and that only the hardware and application programming (i.e., the SIS) were intended to be "grandfathered".

4.2 Change management

As part of the process safety information defined in OSHA PSM, the SIS and other safeguard systems and all documentation related to it were already subject to change management in the U.S, inclusive of the H&RA itself. Since existing SIS tend to be changed piece by piece, however, further clarity was needed in clauses 5 and 17 on how to handle such changes using the functional safety management activities, such as system verification and validation. This includes changes that affect the requirements on an existing SIS.

4.3 Performance metrics and quality assurance

A common concern in SIS design is the use of overly optimistic data or data that is not applicable to the operating environment the SIS will be used in. However, even if data and assumptions appropriate to a given operating environment are used in the initial SIS design, variations in the performance of the process, operations, maintenance, and automation management systems over time can result in poor system performance and inadequate risk reduction. The only way to correct for these systematic errors and restore the necessary performance is to collect performance data on an ongoing basis, periodically assess for conformance to the H&RA and SRS requirements, and correct deviations as needed. The expectations of performance monitoring and quality assurance are consistent with basic process safety management practices (e.g., USA CFR 1910.119(j), COMAH, DSEAR).

5 Conclusion

The SIS standard began alongside the origination of process safety management regulation. ISA S84.01 evolved from a document focused primarily on hardware management to the well-rounded ANSI/ISA 84.00.01 standard addressing both the hardware and human side of functional safety management. ANSI/ISA 61511-1, the third stage of evolution of the SIS standard, strives for continuous improvement in the global use of its long-established requirements. The changes between ANSI/ISA 61511-1 and the previous edition contains updates primarily intended to create more consistent understanding and application of previously existing provisions. The major themes of change address topics such as risk reduction allocation between instrumented safeguards, prescriptive design requirements for HFT, managing risk during bypass or failure of safety system devices, and the need to "close the loop" on functional safety performance to ensure the overall control and safety systems are delivering the performance assumed in the H&RA and SIS design. Finally, in keeping with the technological advances in automation systems, ANSI/ISA 61511-1 includes crucial cross-ties to cybersecurity requirements that make the SIS more resilient to malicious attack.

6 References

[1] ISA. 1996. Application of Safety Instrumented Systems (SIS) for the Process Industry. ANSI/ISA S84.01-1996. Research Triangle Park, NC: ISA.

[2] U.S. OSHA. 1992-2018. Occupational Safety and Health Standards: Process safety management of highly hazardous chemicals, 29 CFR 1910.119. Washington D.C.: OSHA.

[3] IEC. 2003. Functional safety: Safety instrumented systems for the process industry sector - Part 1. IEC 61511. Geneva: IEC.

[4] ISA. 2004. Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1. ANSI/ ISA-84.00.01-2004. Research Triangle Park, NC: ISA.

[5] IEC. 2016 + AMD1:2017. Functional safety: Safety instrumented systems for the process industry sector - Part 1. IEC 61511. Geneva: IEC.

[6] ISA. 2018. Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1. ANSI/ISA-61511-1-2018. Research Triangle Park, NC: ISA.

[7] CCPS. 1993. Guidelines for Safe Automation of Chemical Processes. New York: AIChE.

[8] CCPS. 2001. Layer of Protection Analysis: Simplified Process Risk Assessment, Concept Series. New York: AIChE.

[9] CCPS. 2007. Guidelines for Safe and Reliable Instrumented Protective Systems. New York: AIChE.

[10] CCPS. 2014. Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis. New York: AIChE.

[11] IEC. 2000. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems - Part 2. IEC 61508. Geneva: IEC.

[12] IEC. 2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems - Part 2. IEC 61508. Geneva: IEC.

[13] ISA. 2009. Security for Industrial Automation and Control Systems. ANSI/ISA-62443. Research Triangle Park, NC: ISA.