Is your current safety system compliant to today's safety standard?

Abstract

It is estimated that about 66% of the Programmable Electronic Systems (PES) running in the process industry were installed before the publication of today's commonly used safety standards (IEC 61508 and IEC 61511/ISA 84)

Some of those safety systems, particularly the ones installed between the late 1980's and early 2000, are either

1. General-purpose PLCs,
2. Not designed or certified according to the IEC 61508,
3. Might not satisfy current requirements on IEC 61508

In some cases they were not implemented according to ISA84 or IEC 61511.

This whitepaper covers the changes in the safety standards affecting those systems, a follow up whitepaper will address the safety life cycle activities involved in modifying or decommissioning an existing system to install certified Safety Systems according to today's standards.

Key words

Programmable Electronic System, Safety Instrumented System, Functional Safety Management System, Proven-in-Use

Author

Luis M. Duran

TUV FS Eng# 902/07

Product Marketing Manager Safety Systems

ABB

Houston, TX

e-mail: luis.m.duran@us.abb.com

What is the issue?

The economic growth of heavy regulated industries such as Oil & Gas and Power, increased demand for energy from BRICs economies, particularly China and India, and the increased acceptance of international functional safety standards, especially after major incidents are driving the growth of the Safety Automation Market in the Process Industries, growth estimated in 9% CAGR.

This trend is likely to continue for the process industries (which include non-nuclear power, chemical, petrochemical, refining and oil & gas production) as about 66% of the Programmable Electronic Systems used in safety applications were installed between 11 and 30 years ago; before ISA 84, IEC 61508 or IEC 61511 were issued and recognized as good engineering practices.[1] The same source indicates that many users have extended the lifespan of their system beyond their supplier's obsolescence notice.

Additionally there are many relay-based safety systems that missed the initial wave of automation or were left alone as installing a digital electronic programmable system was not economically feasible for the plant in those applications at the time.

Prescriptive vs. Performance Base Functional Safety Standards

The international Functional Safety standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems is a general standard applicable to multiple industries. In addition to IEC 61508, there are industry specific standards. For the process industries, the applicable international safety standard is IEC 61511; ISA has adopted IEC 61511 in their latest revision of ISA84. Although there are similar changes affecting the machinery safety standards, this paper will only cover the process industries and IEC 61511.

IEC 61508 and IEC 61511/ISA 84 are known as performance based safety standards, contrasting with previous standards that prescribe the type of protective functions needed to reduce risk, performance base standards require an analysis of the hazards associated to the process, the risk reduction alternatives and the determination of the performance needed to reduce risk to an acceptable level.

Grandfather clause

The concept of the "grandfather clause" in ISA-84.01-2004-1 originated with OSHA 1910.119. The grandfather clause's intent is to recognize prior good engineering practices (e.g., ANSI/ISA-84.01-1996) and to allow their continued use with regard to existing Safety Instrumented Systems.

According to ISA-TR84.00.04-2005 Part 1 Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) "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

[1] ARC, INSIGHT# 2010-53EMPH The Coming Wave of Process Safety System Migration

determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner."[2]

The Technical Report highlights two essential steps:

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

According to ISA-TR84.00.04-2005 Annex A.2.[3], if those activities have not been done, they should be scheduled for review at the "next appropriate opportunity" which mean if any of the following conditions is met:

- Modifications to the process unit that impact process risk managed by the SIS;
- Modifications to the control system that impact protection layers used to achieve safe operation;
- When an incident or near miss investigation has identified an SIS deficiency; or
- When the review of another process unit designed according to similar practice has identified an SIS deficiency.

Where are the Safety Certificates?

In reviewing project specifications during the bidding phase of a project, it is common to find ISA 84 or IEC 61511 as a requirement of mandatory compliance. Compliance to IEC 61511 implies more than a certified system, particularly at the time of design and implementation. On the subject of PES, this standard requires that components and subsystems selected for use in SIL 1 through SIL 3 shall either be designed in accordance with IEC 61508-2 and IEC 61508-3 or comply with the "Proven-in-Use" criteria. Additionally, the system programming tool should use Limited Variability Languages, defined in the standard as "software programming language, whose notation is textual or graphical or has characteristics of both, for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application"[4].

As the reader might anticipate, the majority of the Programmable Electronic Systems used before 1995 were not certified to the same criteria as those released to the market over the last ten years, legacy systems are likely to be general purpose systems (i.e. standard PLC) or an early version of Safety PLCs/Programmable Electronic Systems (First Generation Safety Systems).

Proven-in-Use

In order to keep using a system that is not certified according to IEC 61508, the user must demonstrate "Proven in Use" and such demonstration shall include:

1. The manufacturer's Quality Management system

[2] ISA-TR84.00.04-2005 Part 1 Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)
[3] ISA-TR84.00.04-2005 Part 1 Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)
[4] IEC 61508 – 4 Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 4: Definitions and abbreviations

2. Adequate identification and specification of the components and sub-systems
3. Demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments
4. The volume of operating experience

The documented evidence shall demonstrate that the likelihood of any failure of the subsystem is low enough so that the required safety integrity level(s) of the safety function(s) is achieved.

Certified to IEC61508

If the system has an IEC61508 certification, then it's important to understand the criteria used by the third party assessor for issuing such certification to a First Generation Safety System. The IEC 61508 standard recognizes the following four criteria in the assessment of a Safety PLCs/Programmable Electronic Systems:

- Hardware Safety Integrity
- Behavior in presence of failure
- Safe Failure Fraction
- Systematic Capabilities

Most First Generation Safety Systems were certified on the basis of the Hardware Safety Integrity which is related to redundancy and behavior in presence of failure, and these two concepts were sufficient to describe their performance that at the time included few and maybe limited software diagnostics. Many of these systems used Relay Ladder Logic as a programming language which was a representation relay based logic and useful at the transition point between said technology and the emerging digital systems.

Safe Failure Fraction (SFF) and Systematic Safety Integrity are new terms for many users, particularly Systematic Capabilities is a new concept that many of the First Generation of certified systems today do not support and is a requirement gaining more visibility in the new edition of IEC 61508 published in 2010.

To release a certified system following the new revision of the standards, the vendor needs to start by establishing a Functional Safety Management System (FSMS) and having the development organization certified by an independent assessor. The FSMS requires the design process to document and track functional requirements, review functional specifications and test against requirements and validate performance and results during the development of the product. Every step needs to be properly documented; the competence of the personnel involved in each step is also documented. It might be easier understand for the reader if the FSMS is compared to a Quality Assurance process, it will be difficult, if not impossible, to assure or even test performance if the performance criteria is not well defined and documented.

Over time it will be very challenging for a product vendor to certify a system to the latest revision of IEC61508 if their development organization was not previously certified and if their design practices lack the FSMS and the document trail explained in the previous paragraphs.

The reader is probably familiar with the discussions around the architecture of Programmable Electronic Systems used in safety applications as the majority of First Generation Safety Systems used redundancy (Hardware Safety Integrity) to satisfy the requirements of Low Demand Applications commonly found in the process industries.

Product Developers in the Safety Automation market might adopt different design methodologies, but current Functional Safety standards encourage the use of software diagnostics and diverse technologies.

Diverse Technology

As indicated by this author in previous publications[5], technology has evolved to a point in which there are multiple options to address a similar technical problem. For example, by selecting two or more of these technologies, diversity can be embedded in the system design.

Examples of diverse implementation include using different operating systems and then using different teams to develop the software on multiple cooperating modules, or combining two different technologies (such as Micro Processor (MPA) or Micro controllers and Field Programmable Gate Arrays (FPGA)) to perform the same functionality in parallel to each other. Unlike traditional redundancy, by applying diverse technologies, the design achieves a redundancy scheme with minimum or no common cause failures.

IEC 61508 Edition 2

There are other concepts added to IEC 61508 Edition 2 that might affect compliance and should be considered when choosing a PES. This paper will concentrate only on the following three areas, but the author encourages the reader to seek additional information on the topic.

1. Systematic Capabilities
2. Competence
3. Security

Systematic Capabilities

Today, it's well understood that a system can be designed following a very strict development process, using a rock-solid Functional Safety Management System and even certified by the best independent

---

[5] Johnson, Duran Providing Independent Layers of Protection with Integrated Safety Systems

authority, yet the system can be programmed in a way that disables its safe action under some conditions. Systematic Capabilities should assist in the assessment of the programming tools to avoid this kind of situation.

Systematic Capabilities is a concept developed to replaces the term: “effectiveness against systematic failure” and is a measure (on a scale of 1-4) that the systematic safety integrity of an element fulfills the given safety function, considering the instructions stated in the product safety manual.

Competence

Competence has been recommended in the previous edition of the standard, however it is now of mandatory compliance (normative). The following are the requirements:

1. Organizations involved on safety system projects or activities shall appoint one or more persons with responsibility for one or more phases of the Safety Lifecycle (per IEC61511)
2. All persons, departments or organizations shall be identified, the responsibilities clearly defined and communicated
3. Activities related to management of functional safety shall be applied at the relevant phases
4. All persons undertaking specific activities shall have the appropriate competence
5. The competence shall be documented

Competence is particularly critical in the Management of Functional Safety and in the case of a Functional Safety Assessment which in addition to competence may require independent individuals or departments depending on the consequence of the hazard.

As concerning as the competence requirements may sound, it’s important to highlight that there are competent resources available worldwide, either as independent consultants or associated to product vendors and available to support throughout the implementation of the safety lifecycle.

Security

Infrastructure Security and Network Security have been the subject of several papers and blogs. The targeted attack of the Stuxtnet worm in 2010[6], confirmed the industry concerns. The subject is recognized in the revision of the standard, not in the application specifics or to specify the requirements needed to meet a security policy that may be required, but consider potential security threats to be added to the safety requirements.

Section 7.4. (Hazard Analysis) of the IEC 61508 standard, requires that in the case the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, is reasonably foreseeable, then a security threats analysis should be carried out, followed by section 7.5. (Overall

[6] Byres, Howard Analysis of the Siemens WinCC / PCS 7 “Stuxnet”Malware for Industrial Control System Professionals

Safety Requirements) where it recommends that a vulnerability analysis should be undertaken in order to specify security requirements.

Summary

This whitepaper explains some of the changes in the Functional Safety standards IEC 61508 and IEC 61511/ISA 84 and identifies the key elements to assess if a safety system installed the late 1980's and early 2000 meet the certification requirements for applications in the process industries.

An existing installation is only covered by the ISA84 “Grandfather Clause” if the owner/operator can demonstrate that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

Some of the systems running today might not be certified according to IEC61508, if that is the case and according to IEC 61511 those systems should comply with the “Proven-in-Use” criteria, which requires the user to demonstrate using documented evidence that the likelihood of any failure of the system is low enough so that the required safety integrity level(s) of the safety function(s) is achieved.

For those systems certified to the first edition of IEC 61508 only on the basis of Hardware Fault Tolerance (i.e. redundancy and architecture), there are technical challenges that might limit the ability of those system to retain that certification when the industry moves to IEC61508 Edition 2, this will occur on the next product release cycle for those vendors.

In addition to criteria such as Hardware Safety Integrity, behavior in presence of failure, Safe Failure Fraction (SFF) and Systematic Capabilities; the latest revision of IEC 61508 (Edition 2) introduce additional criteria such as security and increased the importance of systematic capabilities and competence.

Competence was made normative in the latest revision of the standard, this requires organizations involved on safety system projects or activities to appoint one or more persons with responsibility for one or more phases of the Safety Lifecycle (per IEC61511) and the adoption of a Functional Safety Management System.

The follow up whitepaper will address how to start an assessment of your existing safety instrumented system and the safety life cycle activities involved in modifying or decommissioning an existing system to install certified Safety Systems according to today’s standards.