Functional Safety is so much more than using certified hardware

A White Paper by Dave Huffman

Abstract

It does not seem to be widely understood in the process industries that IEC61511/ISA84 is a standard placing demands on the process owner and system integrators, and not the Safety Instrumented System (SIS) suppliers and their products. Suppliers and products of certified hardware and embedded software must comply with IEC61508.

This white paper is meant to serve as a brief tutorial explaining how IEC61511/ISA84 directs owner’s activities and work practices. The intent is to help process owners understand their role and responsibilities in the Functional Safety environment and allow them to create better requirements documents for the SIS so the owner can make a better informed selection of an SIS supplier.

Introduction

Although compliance to Functional Safety might not be, by itself, the primary driver of the production facility, it is directly connected to Overall Equipment Effectiveness (OEE), Total Cost of Ownership (TCO), insurance verification cost, and to limiting the exposure of companies to potential liabilities associated with the cost of an incident. Compliance with good practice equals a profitable and sustainable business.
It is not uncommon to see safety automation project specification statements such as, “System must be designed following IEC61511/ISA84”, or system must be “SIL 3 certified.” But what does either of these mean for your safety automation vendor? The first quote is almost irrelevant, and the second is fine, but can be met by any system supplier that has a TÜV, Exida, or other certification that the system hardware and software does in fact meet a certain Safety Integrity Level of compliance. But the compliance is not to IEC61511/ISA84, but rather to IEC61508.

This may come as a surprise to many, because the IEC61511/ISA84 is the common standard referenced by the process industries when discussing Safety Instrumented Systems (SIS). And it is their key standard, just not for hardware and software they select for their safety automation, but rather the one that provides the requirements for the owner’s work practices and actions.

There are several industry standards that form the foundation for the implementation of Functional Safety for any segment of the process industries.

- **IEC61508 Functional safety of electrical/electronic/programmable electronic safety-related systems … is relevant to SIS automation suppliers.**
- **IEC61511/ISA84 Functional safety - Safety Instrumented Systems for the process industry sector … is relevant to process owners.**
- **IEC62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems … not commonly used but relevant to machine safety automation suppliers.**

When specifications are issued, it would be far better if the documents made reference to meeting specific SIL requirements, according to IEC61508 that meet the owner’s requirements. These should be expressed in terms of either Probability of Failure on Demand (PFD) or Risk Reduction Factors (RRF). The specifics should be identified in a Functional Safety Requirements Specification (FSRS) that has been completed and can be included as part of the SIS specification. When this is done, the owner will receive the specific information they need to make a selection that addresses their specific requirements.

Meeting the IEC61511/ISA84 requirements

Meeting the requirements of this standard can be summed up in a simple statement. Follow the recommended lifecycle, performing each step of the lifecycle when the steps are required. Meeting the requirements is not a single point in time event, but rather is truly a lifecycle, and as the process evolves and changes, a variety of the lifecycle steps will likely be repeated many times over.

Below is a reproduction of the graphical view of the Functional Safety lifecycle from the standard:
Key:
- Typical direction of information flow.
- No detailed requirements given in this standard.
- Requirements given in this standard.

NOTE 1 Stages 1 through 5 inclusive are defined in 5.2.6.1.3.
NOTE 2 All references are to Part 1 unless otherwise noted.
As can be seen, the lifecycle consists of 12 primary phases or sets of work processes. There is a structure to the layout of the view presented. The flowchart items in the middle of the view depict a series of steps ([1]-[8]) and one that is not numbered) that, in meeting the standard, are performed at least once, and many may be repeated each time a modification is made to the process. The remaining 3 steps ([9]-[11]) are shown in boxes that extend across the entire timeframe of the lifecycle, indicating that these steps do not occur only at one instant in time, but rather are required to be performed “continuously” throughout the lifecycle.

There is much to be said for utilizing SIL certified field and system components. The reliability information published by the manufactures certainly makes performing the validation calculations required within the lifecycle easier to accomplish. They also provide a degree of certainty that the solutions created will meet the risk reduction requirements. But the hardware alone will not satisfy the Functional Safety requirements.

**Phase [3]: Safety requirements specification for the safety instrumented system**

This is a document(s) detailing the SIS functional requirements specification for the SIS hardware (clauses 10 & 11) and for the SIS application software (clause 12). The requirements identified in this phase cover the details related to specifics of individual Safety Instrumented Functions (SIFs). This includes the requirements pertaining to the field input and output devices and the functional and performance requirements for the logic solver and its connected I/O modules. Note that this is a “functional specification” document, not a “detailed design” document. There should be considerations for both safety reliability (probability of failure on demand [PFD] or risk reduction factor [RRF] requirements that translate into SIL requirements) and for availability requirements (uptime for the SIS, allowances for hardware failures, redundancy requirements, etc.) as not all processes have the same requirements for either of these concerns.

When developing the SRS, the writer needs to stay focused on performance-based reliability criteria of PFD and RRF, and on availability (uptime, MTBF, MTTR, as appropriate.). Doing so will avoid the specifics of an architecture (dual redundancy, triple modular redundancy [TMR], quad modular redundancy [QMR], etc.) or the design details of one particular product in order to properly define the requirements. After all, the SRS is intended to define the performance criteria against which supplier solutions are to be judged.

The requirements developed in the SRS should allow the process owner to make a selection of related functions should reside in the safety hierarchy based on the outcome of the hazard and risk assessments completed in Phase 1. Some items such as interlocks may be assigned to the Basic Process Control System (BPCS). Where SIL2/3 items have been identified, those will be allocated to the Safety Instrumented System (SIS). And if other requirements for safety relief, physical containment, etc. have been identified, those need to be addressed with other mitigation layers of the overall functional safety hierarchy. The SIL rating requirement of the SIS is identified from the work processes in Phase 1 and Phase 2, but this is the only outcome at this point.
field devices, peripheral equipment, and the SIS control platform that best meets the functional requirements for both reliability and availability. If more than one solution can meet the performance criteria, then additional "soft criteria" like lifecycle cost, services and support can enter into the decision.

Taking time to develop a sound, performance-based SRS can translate into more than optimal risk reduction based on considerations for plant operations. It may also lead to hardware cost savings, reduced configuration changes throughout the lifecycle and opportunities for reduced operational affects with options like online proof testing.

Phase [4]: Design and engineering of safety instrumented system

As is the case with all well managed projects, the functional requirements completed in the previous phase need to be converted into detail design specification based on the selected field devices, peripherals, and system hardware (clause 11) and application software (clause 12). The sequencing of this activity is critical. Too frequently, process owners make the mistake of creating a design specification in place of the functional specification that is the focus of Phase [3]. A detail design specification should result from the selection of all of the parts of the SIS and not dictate the selection of the SIS. Three examples are provided below.

Example 1: A field device requirement for an isolation valve may need to meet a risk reduction factor (RRF) of 5000 (SIL3 has a range of RRF between 1,000 and 10,000). If the specification developed in Phase 3 is written around a specific valve specification from Supplier 1 (detail design specification) based on the knowledge that it provides the required RRF. Having done so may preclude using a valve and positioner from Supplier 2 that also delivers on the RRF, but not on other specific details issued in the specification. The solution from Supplier 2 may also be less expensive and offer Partial Stroke Testing (PST) functionality that can extend the SIF full function test periods and could result in significantly more production revenue over the lifecycle of the process. Using specific design details rather than functional requirements leads to the wrong choice in suppliers and results in increased lifecycle cost.

Example 2: The safety control system hardware and software is specified in Phase 3 as needing to be a TMR architecture because TMR delivers both SIL3 and high availability that may be needed. Unfortunately, the proper analysis of each SIF was never done to find out how important one or both really are for the process. The owner believes time at this stage is more important and "just knows" the bases are covered with this specification. In many situations, had the analysis been done, the results may have shown that none of the SIFs required RRFs above 1000 (SIL2 upper limit) and the studies related to availability needs would have shown that needing high availability (redundancy) was not a concern since the process is batch and needing long, uninterrupted running cycles is not an issue. The specification leads to the purchase of a TMR system that is overly costly to the process owner when a more cost effective solution. Meeting the real requirements would have been more appropriate.

Example 3: A process is analyzed and SIL3 is required along with high availability so the specification is written as TMR rather than performance requirements. After the plant is up and running, there are problems of spurious trips (false shutdowns). When the root cause analysis is completed, the results point to improper application programming and a failure to properly validate the applications to SIL requirements. By simply specifying TMR, the owner failed to include the proper specifications for systematic safeguards that should have been identified in a proper set of performance requirements. Systems with advanced diagnostic capabilities will now test for code compliance to appropriate SIL2 or SIL3 functionality and prevent implementation of non-compliant code to help avoid a wide myriad of problems that can arise when the validity of the application is left to the code designer.
Phase Unnumbered: Design and development of other means of risk reduction

This is the phase in the lifecycle that has no relationship to the details of the SIS. As with Phases 1-2, the standard includes this phase within the lifecycle because of its overall importance, but provides very little detail on the work processes involved in the execution of the phase. The work processes are mandated either by other standards, industry best practices, or corporate standards and work processes. It is shown in parallel to Phases [3]-[4] to provide positioning within the overall functional safety lifecycle. It is also shown in this manner as it is the one phase in the entire lifecycle that may not be required if other means of risk reduction, outside of an SIS, are not identified any time Phase [1] of the lifecycle is executed.

Phase [5]: Installation, commissioning, and validation

Clause 14 deals with installation and commissioning work processes. These two work processes are generic in nature and again have almost nothing to do with the specific field equipment and safety system hardware and software that is selected, other than following proper procedures to install the equipment and commission it according to the vendors’ recommendations and the owner’s procedures and best practices.

Validation is covered in clause 15 and also has little to do with specifics other than the tools provided in the selected system are used to perform the validation and will be different in look and fall between different suppliers’ systems. Validation is often considered the site acceptance test phase of the project and should adhere to the owners specific procedures and workflows to execute the testing. Clause 15 contains specific requirements for both the execution of this phase and the documentation requirements that need to be maintained as proof of the validation.

Phase [6]: Operation and maintenance

Clause 16 of the standard deals with the requirements of operations and maintenance with the objectives:

- Ensure that the required SIL of each safety instrumented function is maintained during operation and maintenance, and
- Operate and maintain the SIS so that designed functional safety is maintained.

Again, this phase of the lifecycle has little to do with actual hardware and software that is applied for the SIS other than the specific requirements the manufacturer may recommend for maintenance practices. Also keep in mind that the requirements apply to field devices and all included peripherals, not just to the SIS logic solver and software.

This section outlines the requirements that proper procedures be followed for both operations and maintenance. It also requires that operators and maintenance personnel must be properly trained in their roles to interface with the SIS and that adherence to the proper procedures and behaviors be monitored and adjusted throughout the lifecycle as necessary to properly maintain the integrity of the SIS.

This section also contains the requirements for the execution and documentation of proof testing and inspection of the SIS as determined to meet the proper PFD_{avg} determined in Phase [1].

Phase [7]: Modification:

Clause 17 places requirements on the owner to execute a proper management of change process for any modifications and that the process of making changes ensure the integrity of the SIS with proper procedures and work processes.

Not only are changes to the SIS at issue here, but the owner has an obligation to ensure that changes made to the BPCS do not impact the integrity of the SIS or are accounted for and appropriate SIS modifications are made in parallel.

As part of the considerations around modifications, we now find ourselves at a point in time where this is especially critical. Many owners have long relied on a philosophy of “replacement in kind” to keep them in compliance with the standards and not have to evaluate the need to make large scale changes to their systems. With
the latest updates to the standards, especially to IEC61508, older system hardware and software may no longer be considered sufficiently safe to maintain appropriate performance requirements. The bar has been raised significantly on diagnostics requirements for the hardware, and many currently installed systems no longer meet the requirements.

So as part of establishing the programs focused on managing change to the SIS, considerations need to be made to periodically re-evaluate whether or not the entire SIS solution is compliant with current standards.

Phase [8]: Decommissioning:

As with any lifecycle, there is a beginning and an end, and decommissioning (clause 18) deals with end of useful life, perhaps for a single SIF, but potentially and eventually for the entire SIS.

Once again, this is a work process that is regulated not only by the owner’s management of change processes and procedures, but also by the hardware and software of the SIS as explained in the latter paragraphs of the previous section.

Phase [9]: Verification

The first of complete lifecycle timeframe phases. Verification is identified within clause 7 and clause 12, parts 12.4 and 12.7. The emphasis of this phase of the lifecycle is to call attention to the need to constantly verify that the SIS is performing properly and maintaining the required protection. For example, clause 15 deals with the site acceptance test where a first validation occurs. But then clause 16 presents the requirements for proof testing and other validation items that need to be completed throughout the lifecycle. Verification is a work process that creates the need for constant vigilance.

Phase [10]: Management of functional safety and functional safety assessment and auditing

Another of the total lifecycle timeframe phases that is solely a mandate on the owner to instantiate, execute and maintain:

- The policy and strategy for achieving safety that is identified together with the means of evaluating its achievement and shall be communicated within the organization, and
- A safety management system that shall be in place so as to ensure that where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state.

The details of these two items are extensive and cover requirements including:

- Organization and resources
- Risk evaluation and risk management planning.
- Implementation and monitoring
- Assessment, auditing, and revisions
- SIS configuration management

Phase [11]: Safety lifecycle structure and planning

Perhaps the most critical phase (should have been “Phase 1” instead of 11). The requirements are identified as occurring in clause 6.2. Simply stated, the requirement is to take the generic lifecycle we have been discussing here and make it specific to your project, site, or enterprise by identifying those pertinent inputs, outputs and verification activities that fall within the owner’s specific work processes.

Meeting the requirements of IEC61511/ISA84 is a lot of work

As should be clear at this point, meeting the requirements of this standard is a lot of work; for the owner and system integrator, not for the SIS automation suppliers. From the supplier perspective, it frequently seems that the owners do not recognize this distinction as frequently what the owner provides as a functional specification for qualifying a SIS tries to place much of the responsibilities identified in this standard onto the automation supplier. We can certainly deliver on hardware and software that meets risk reduction requirements according to IEC61508 (and a couple paragraphs with the same requirements in this standard), but beyond that, there is little we can do from our products that help with the owner’s meeting IEC61511/ISA84.
On the services side, there is much more your supplier may be able to do to assist if the owner does not have the staff or the expertise to perform:

- SIL evaluations and identify the appropriate PFD or RRF to design SIFs
- Field and peripheral hardware evaluations and selections performed by certified individuals
- Site acceptance validation or lifecycle validation services and documentation
- Detailed designs for SIFs
- Maintenance, proof testing, documentation, etc.
- Training and/or coaching assistance for:
  - Hazard and risk assessment
  - Creating and maintaining a Functional Safety Requirements Specification
  - Creating and maintaining a Safety Lifecycle structure and planning process

Any or all of these services may be available from your automation supplier. If they are required, they should be clearly identified within the functional specification of the SIS when it is issued to perspective suppliers. In some cases, to stay within the lifecycle recommended sequence, it may be appropriate to issue a request for services to start and develop within the lifecycle just so a good FSRS can be created.

**ABB as a partner in functional safety**

Ultimately, the Plant Owners and Operational Management must drive the requirements to meet stakeholder and legislative conditions. Operators must specify, design, and build plants to appropriate technical standards and good practices and operate and maintain those plants using appropriate safety and quality management systems.

To be successful accomplish this goal, the requirements need to be replicated within the supply chain and in doing so provide the plant owner with additional safety assurance that reliability, integrity and systematic errors are addressed during the design and engineering of protective systems. Following a recognized functional safety lifecycle management approach, utilizing fit for purpose technology and competent delivery resources, results in delivery of a world class corporate safety, performance & sustainability model.

ABB is able to assist Plant Owners and Operational Management to design, engineer, integrate, configure, operate and maintain up to SIL 3 capable safety instrumented systems implemented by using an accredited TÜV certified safety lifecycle model, applying subsystems and elements which are themselves third-party certified to meet all the relevant requirements of IEC61508 and IEC61511/ISA84.

For more information please contact:

Process Automation
Chemical, Oil & Gas (COG)
Industry Business Unit

**Note:**

We reserve the right to make technical changes or modify the contents of this document without prior notice. We do not accept any responsibility whatsoever for potential errors or lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained throughout. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in part – is forbidden without prior written consent of ABB Inc.