# What is the importance of third party certification and SIL rating of SIS devices?

Luis Duran
Triconex, Irvine, CA

## KEY WORDS

IEC 61508, IEC 61511, ANSI ISA S-84.01, Certification Process, Proven in Use, Prior Use, TÜV Technisher Überwachungs-Verien, SIS Safety Instrumented System, SIL Safety Integrity Level.

## ABSTRACT

Based on the growing number of safety certified devices or systems in the automation marketplace, these are the times of Functional Safety Certification, especially in the process industries. However as basic as it might sound, is there a “one-size-fits-all” certification process? Or how useful is that “certified equipment” for your application?

From the reasons that gave birth to third party certification agencies through the remaining fundamental need for their work today, the questions to answer are: what is the end user getting with the certification?; how can the end user benefit by utilizing certified equipment?; why this might be better than using “proven in use” equipment as defined by IEC61511?

This paper presents a practical perspective to understanding certification and selecting and applying certified devices or systems while deploying a safety instrumented system, and highlights what else remains to be done by the implementation team and end users to fulfill the requirements of current safety standards as IEC61511 and best engineering practices.

## BIO

MBA and BSEE from Universidad Simon Bolivar, Caracas, Venezuela with over 15 years experience in different industrial automation disciplines, including design and implementation of Safety Shutdown System and Critical Controllers and BPCS, Process Modeling and Design Software and Advanced Process Control for Business Improvement in the Oil & Gas Downstream industry.

**Introduction**

Based on the growing number of safety certified devices or systems in the automation marketplace, these are the times of Functional Safety Certification, especially in the process industries. However as basic as it might sound, is there a “one-size-fits-all” certification process? Or how useful is that “certified equipment” for your application?

There is no question we are witnessing significant improvements in the design and manufacturing of instrumentation and control equipment for automation. We are seeing the same trend towards better instrumentation and control for Safety Instrumented Systems. This includes improved diagnostics of measurement systems and final acting elements, along with new technologies applied to logic solvers or E/E/PES and new software capabilities.

The industry is exposed to new technology offerings that supposedly allow the user who is performing a SIL verification to take a greater credit in the SIL determination and reduce redundancy in field devices or reduce the overall requirements on the E/E/PES.

This sounds good for the project budgets but, in reality is it possible to achieve automatic compliance to safety standards? Or on the contrary, do we need to be even more concerned with the false sense of security?

Unless designers and practitioners analyze how these new technologies are applied to particular safety systems and understand their impact on process performance, it is almost impossible not to be concerned with such advertising.

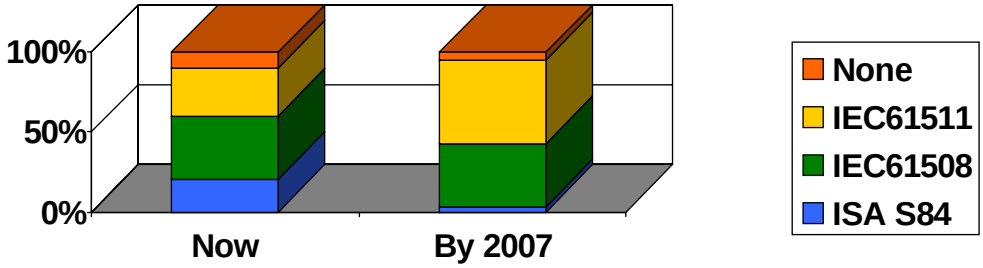
According to a recent study by the ARC Advisory Group, the process industries are aiming for:

- Improved Safety
- Prevention of Loss of Live and Limbs of Production Personnel AND People outside the Production Area
- Avoidance of Environmental Damage
- Avoidance of Production Losses
- Avoidance of Legal Liabilities

Unfortunately, we’ve all seen industrial accidents and their impact upon the community.

Best engineering practices and safety such as IEC61508 and IEC61511 are the result of expert examination of the conditions which led to these industrial accidents and a reflection of the lessons we have learn over time.

The question to us all is: Should we lower the bar on our requirements for SIS?, or on the contrary, be more concerned and analyze safety from even more angles than in the past?




According to ARC Advisory Group, there is no doubt that the process industries are rapidly moving toward the adoption of safety standards, especially IEC61508 and IEC61511.

This growing adoption seems to indicate that the process industries are not ready to lower the bar in the design and implementation of safety systems. Actually the general consensus seems to be, “let’s do it better and more efficiently.”

This growing adoption of standards is affecting manufacturers and functional safety system providers alike, both are urged to adopt new processes or improve existing ones and follow additional guidelines to meet standards.

However since the standards are not prescriptive, there is some room for interpretation and not everybody takes the same approach to areas such as:

- Quality
- Validation Testing
- Functional Testing
- Maintenance
- Operation

**Functional Safety**

Understanding Functional Safety as the area of Safety that depends on the Correct Operation of a System in response to its inputs, the history shows a significant change in its implementation. The last 20 years alone, indicates a transition from simple, difficult to diagnose, technology, to the adoption of more complex systems with somehow better diagnostics.

But with these new technologies, it is difficult to fully determine every Failure Mode, difficult to fully test all Possible Behavior and difficult to predict the Safety Performance.

Periodic on-line proof testing thus becomes an essential activity to ensure correct operation of the E/E/PES over its lifecycle.

The design of these new systems, incorporating their added complexity should make them more robust and safe, reducing the number of potential dangerous failures and those so-called “safe” failures.

Some examples of dangerous failures are:

- Incorrect Hardware or Software Specifications
- Omissions in the Safety Requirements Specification
- Random Hardware Failure Mechanisms
- Systematic Hardware Failure Mechanisms
- Software Errors
- Common Cause Failures
- Human Error
- Environmental Influences – like Electromagnetic, Temperature, Mechanical
- Supply System Voltage Disturbances – such as Loss of Supply, Reduced Voltages

However, “safe” is a relative term in the context of process failures, since a safe system failure leading to a shutdown can still cause a number of dangerous conditions in addition to the adverse economic impact upon operations.

**Certification**

Certification is a formal process to identify that a product, service or process conforms to a particular set of standards, like ISO9002 certifies the quality processes. An example within the Functional Safety arena would be to demonstrate that SIS elements conform to the IEC61508 Standard.

Historically, end users or technology practitioners have tested or certified equipment for a given application. Twenty years ago each manufacturer selected products from a vendor list, in order to get into the vendor list, each vendor would endure a battery of functional test. Such testing required the appropriate resources, time, lab facilities and specialized equipment.

As the devices morphed into more complex systems, it was not practical or feasible to perform in-company tests. End users started to rely on third party agencies to demonstrate product suitability for a particular use, thus reducing the scope of user specific testing to those aspects particular to the application that were not part of a generic standard.

In the automation of safety instrumented systems, third party certification deals with the manufacturer’s compliance to industry standards, research and development best practices, electrical installation and EMC requirements among others. the main objective is to demonstrate that a given product is suitable for use in a particular industrial setting.

It is common nowadays to see application-specific testing that demonstrate suitability to demonstrate the particular requirements of a given application such as NFPA 72 for Fire & Gas Systems or NFPA 85 for Boilers.

Certification to IEC 61508 (and other applicable standards) is a substantial undertaking. Unlike a product certification that involves a specific portion of a company for a brief period, committing to IEC 61508 affects the corporate structure to a much broader extent with a change that is permanent. A new functional safety management system must be established within the company that encompasses; quality assurance, configuration management, project management, and functional safety assessment.

Many manufacturing organizations lack the staff and monetary resources to successfully obtain certification. A company that is contemplating IEC 61508 certification should be fully aware of the necessary investment. It is important to assess the organization to determine whether IEC 61508 certification would be feasible and beneficial.

From the reasons that gave birth to third party certification agencies through the remaining fundamental need for their work today, the questions to answer are: what is the end user getting with the certification?, how can the end user benefit by utilizing certified equipment? And why this might be better than using “proven in use” equipment as defined by IEC61511?

Depending on the risk associated to the process and the required risk reduction factor, the certification process can be done by different entities.

There are different types of certification possible depending on the object of certification:

- Product certification (according to particular technical standards)
- Process certification (according to ISO 9000 or similar)
- Personnel certification
- Accreditation of certification bodies (certification of certifiers)

The level of independence required of the assessor ranges from an independent person in the same organization for Safety Integrity Level 1, to an independent organization for Safety Integrity Level 4.

The required level of independence for Safety Integrity Levels 2 and 3 is affected by additional factors including:

- System complexity
- Novelty of design
- Previous experience of the developers

These elements are obviously present in emerging technologies being applied to SIS. As mentioned above devices used in E/E/PES are more complex, some of

them include innovations which are unfamiliar to everybody in the industry but their designers. This drives a bigger concern about the resources required to assess these technologies.

There is also a specific requirement that the assessor shall be competent for the activities to be undertaken. A Safety Integrity Level (SIL) is not directly applicable to individual subsystems or components. SIL applies to a safety function carried out by the E/E/PE safety-related systems. Depending on the risk associated to the process and the required risk reduction factor, the certification process can be done by different entities.

**Assessors and Third Party Certification**
The main requirements qualities of the assessor are:

- Integrity
- Transparency
- Consistency
- Independence
- Credibility
- Competency

All those are easier to find in an independent assessor.

As mentioned earlier system complexity, novelty of design and previous experience of the developers (or lack of) in relation to a process whose risk have been rated as safety integrity levels 2 and 3 will require an assessment from an independent organization. Notified Bodies have acted as assessors in the past, they meet the integrity, transparency and independency criteria

As implied in the name “Notified Bodies”, these organizations must have fulfilled or demonstrated competency for the activities they perform.

In order to achieve consistency notified bodies can meet regularly to align processes or common principles and best practices.

An example of an independent assessor is TÜV Technisher Uberwachungs-Verien (TÜV) or translated to Technical Supervisory Association out of Germany and approved by the German Government. Their function is to evaluate and certify equipment for functional safety applications.

There are a number of independent organizations denominated as TÜV all in Germany but based out of different locations, run under different rules and each with specific expertise in particular areas of Functional Safety. Some of these organizations meet periodically to define common practices and certification criteria, which is fundamental to deliver a consistent outcome from the

certification process. It is important that users understand the rigor of the tests performed by these independent assessors, they might differ in scope.

It is important to notice that the certification is for the application of Functional Safety. Areas such as False Trips or the impact or post-effect of Detected Safe failures are not part of the scope of certification.

**Value of Certification**
If we have to state the value of certification in ten words or less, it should be *Independent documentation to support a Safe Implementation*

Basically the Certification Agency performs an evaluation of the manufacturer's design and test processes. Since the evaluation is objective and independent there shouldn't be safety issues written in fine or small print. This allows the user to review these test reports and assessments, and clearly understand the best way to deploy a given technology, and its limitations of use for a safe implementation in a particular application or industry and according to the pre-assessed risk.

Certification is also a significant saving in time and resources for the user (implementer). This time and these resources can be better spent by selecting the appropriate technology for the application, or designing peripheral interfaces, or improving operational practices.

The experienced user or those aware of the process safety issues should be able to design the SIS around those safety aspects or limitations. By defining a functional test frequency, adding redundancy, or defining an impulse line cleaning schedule if such is required.

**Proven in Use**
The IEC61511 standard allows installation of "proven in use" technologies as part of a Safety Instrumented System.

"Proven in Use" is one alternative for users that have been using a particular technology for a number of years. Proven in Use assumes that over time, users have developed an understanding of what works and what doesn't, documented their installation, operation and maintenance practices, and possess testing and tracking experience.

In some cases it's considered extremely useful, even vital because of the scarce number of certified elements, i.e. certified field devices. At the same time Proven in Use is not a *Free for All One Size Fits All.* Users must be cautious about when and how, since there are criteria in its application.

Proven in uses, relies upon the following:

- Availability of historical data for systematic failure and random hardware faults
- Analytical techniques and testing

It cannot be used for quantification of dangerous failures due to random hardware faults, or system behavior upon detection of faults

A particular application, because of SIL or a given SIF might have architectural constrains on hardware safety integrity, that need to be evaluated separately.

It is important to highlight again that it is the User who assumes full responsibility for demonstration and documentation of compliance.

**The need for Functional Testing**

Certified or not, Functional Testing is still a key element of the implementation, operation and maintenance of the SIS.

As explained before not all system faults are self revealing, this means that faults that prevent or inhibit the actions of the SIS upon a demand can be hidden in the system, or “Covert”. These Faults can only be detected by testing. Periodical Functional Tests shall use a documented procedure to Detect Covert Faults. In general, Functional Testing should Record and Analyze activation of SIS functions.

The entire SIS shall be tested, though not necessarily all at once. Depending on process conditions; some elements of the SIS can have a different Test Plan or Test Schedule than others. The SIS shall be tested at specific Intervals according to its design (Safety Requirement Specifications). Elements of the SIS may require different Test Intervals; the Test Frequency of the SIS (or its elements) shall be evaluated based on:

- Historical data
- Installation Experience
- Hardware Degradation
- Software Reliability

Any Change of Test Frequency is a Modification of SIS, and all Management of Change Criteria applicable to the SIF or SIS shall be enforced. This includes any Change to the Application Logic. If the SIL has not been compromised then a Partial Testing is acceptable

**Responsibility**

Certified or not, the responsibility lies more in the hands of the users (plant operators, designers, system integrators) than on the manufacturers. Users should follow the safety lifecycle documented in IEC61511, which explains the activities that need to be performed from Design to Installation, Operation, Maintenance and eventually decommissioning.

The Safety Requirements Specification, explains what are the considerations, operational drivers and constraints imposed on the SIS and all its elements.

In addition, if “Proven in Use” criteria were the case, the documentation should include operating experience in safety applications to be used as evidence of such technology. It should also include probability of failure required to meet the SIL for that SIF, and enough detail in accordance with the complexity of the component to characterize its behavior.

In the particular case of field devices a list of Approved Field Devices can be used to claim Experience in Operation. This list needs to be Updated and Monitored Regularly, and devices can be added ONLY when Sufficient Operating Experience is available. Similarly Field Devices are removed when they show unsatisfactory performance. Last but not least The Process Application that the devices are use for is included in the List where relevant.

The manufacturers, system integrators and end users are responsible for publication and information on how to apply the devices safely.

**Critical Safety Instrumented Systems and Failure Mode Analysis**

Safety Instrumented Systems are critical to operations in the process industries. As a minimum they must be reliable, meaning able to provide a correct operation without failure and fail safe. As mentioned before the use of complex elements has extended rapidly, the design must be fail safe which assures that a potential failure will not affect safety. It is important to distinguish that Fail Safe does not mean Safe from Failure, but rather failing to a safe state.

Failures can be minimized in the design by making it fault tolerant or by testing the effect of probable failures on the performance of the elements. This can be done by Fault Insertion testing, which in some cases would use automatic schemes to randomly insert thousands of probable failure scenarios into a component. Few companies approach design this way, since it implies additional cost during the validation and verification stages of the IEC61508. More often the option is to use statistical analysis of returned elements during the warranty period.

One of the goals is to be able to calculate the probability of failure on demand of process equipment, acting as safeguards, this allows the user to:

- Determine the level of risk associated with the hazardous event
- Identify the level of reliability for that system.

The DATA required for the informed decision making process should be provided by the manufacturer, or at least documented in a Failure Mode Analysis (FMEDA). Again it is more than a statistical evaluation, since actual test cases or

potential failure modes under realistic operating conditions should be part of the analysis.

In the case where the system or components do not meet the required safety integrity level, the user or operator should take appropriate actions to increase the reliability of the system. Such actions can be:

- Adding redundant equipment,
- Increasing the diagnostic coverage
- Choosing more reliable equipment (equipment with a lower failure rate)

A typical Failure Mode Analysis would evaluate

- Detected Failures (those identified by unit diagnostics)
- Undetected or Covert Failures (those that diagnostics cannot discern)

Failures can be Safe or Dangerous. Typically Safe Failures are those detected or diagnosed failures that take the SIS to a Safe State or a Fail Safe condition. The detection or diagnosis can take place within the device or by evaluation by other elements on the SIS.

Of biggest concern are those Undetected Dangerous Failures that might lead to a hazardous situation. However, although those so-called safe failures that normally would take the plant to a safe condition, typically transition the process through a dangerous phase. It is commonly said that at least 40% of plant incidents occur during startup or shutdown

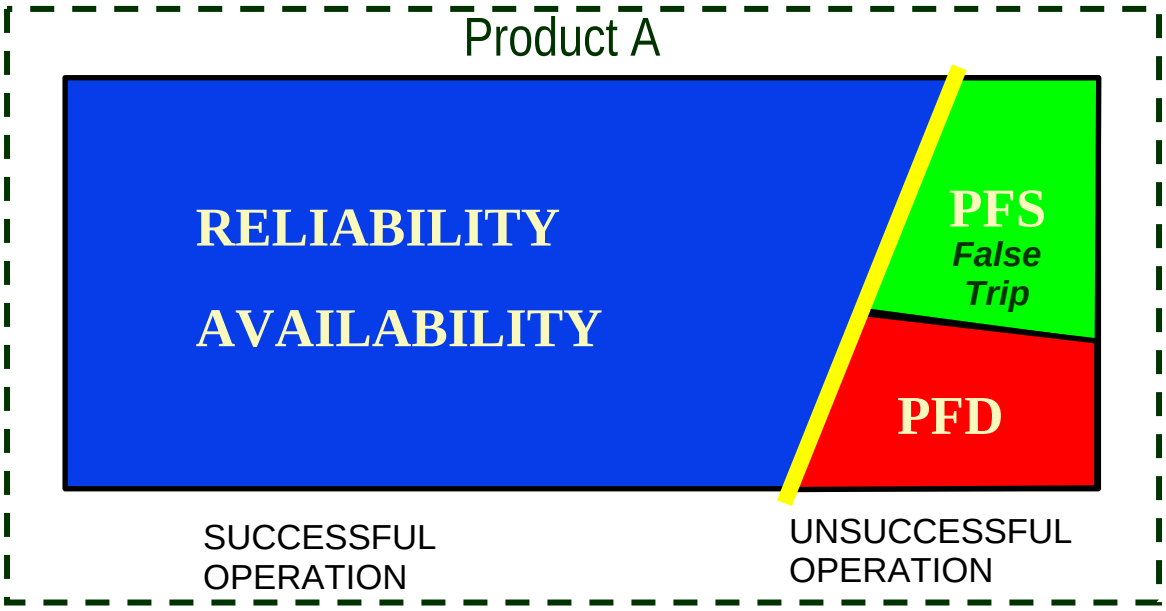
**To Be or Not to Be (Certified) FMEDA Examples**

Using a Best in Class field device, like a standard smart transmitters (not safety certified), an analysis of the Failure Mode Analysis would indicate compliance to IEC 61508, and would define these transmitters as Complex devices (Type B). This means that they are based on a microprocessor and have numerous unknown fail scenarios. HART communications are clearly out of the scope of the FMEDA, therefore HART diagnostics - which are very important for device maintenance - are not part of the safety evaluation of the element.

In order to rate the Safe Failure Fraction of the devices the FMEDA clearly assumes that a Logic Solver is programmed to detect out of range performance. Therefore the Logic Solver should have a better Safe Failure Fraction. Otherwise there are greater chances of falling into an undetected failure scenario. Typical installations will have a significant number of SIF,s on the same Logic Solver, which only makes the case for a better logic solver regardless of how good the field device is.

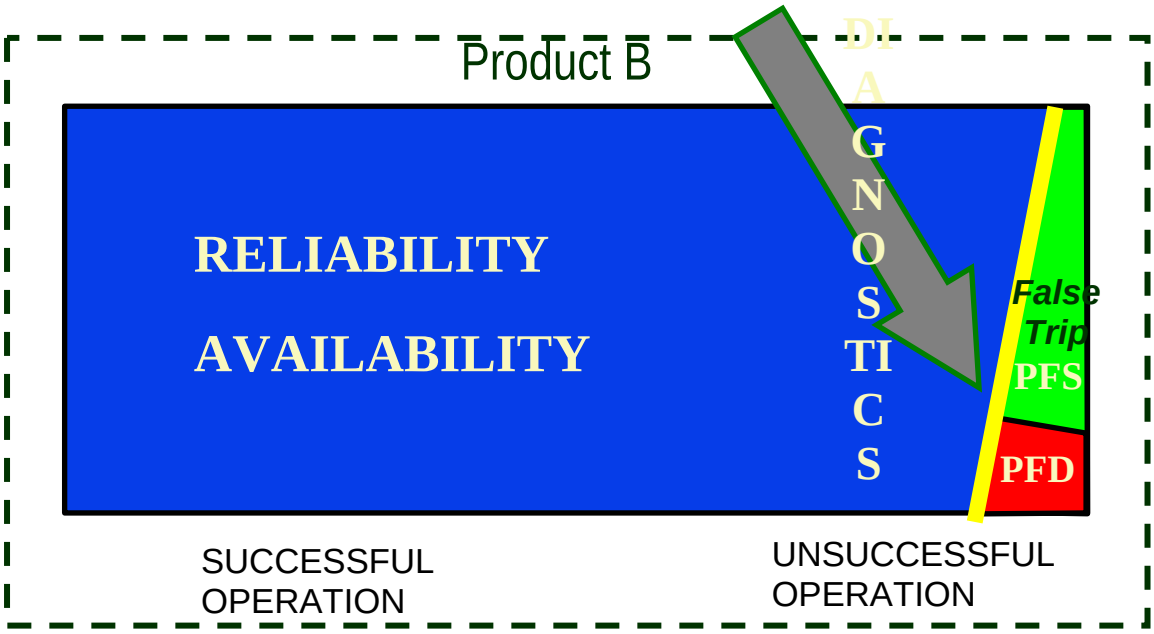
When performing a FMEDA the potential effect of the process interface is not accounted for either. Therefore, it is the responsibility of the user to identify and account for such effect while designing the application.

The FMEDA of a safety certified device is very similar to that of the non-certified. The most important difference is that the additional diagnostics implemented in the design allow a better Safe Failure Fraction than the conventional equivalent. These diagnostics are not HART or communication specific, but are built into the core of the device, and account for a reduction of almost half of the undetected dangerous failures.




PFS - Probability of Failure Safe
PFD - Probability of Failure Dangerous

Click **www.triconex.com/10truths** to read all the truths!




PFS - Probability of Failure Safe
PFD - Probability of Failure Dangerous

So, by using safety certified instruments, is it possible to reduce the redundancy of the field devices and final elements? or the requirements on the logic solver?

Again, there is not a *One Size Fits All* solution. But in critical applications where even safe failures can lead to a dangerous scenario and where plants have fewer and shorter turnaround, redundancy enables a timely functional safety with minimum effect on process uptime.

**The SMART Effect On Safety**

Without question the value of HART device diagnostics for maintenance and its positive effect in planning repairs can minimize unplanned shutdowns. However, these diagnostics are not the ones that improve the Safe Failure Fraction or reduce the susceptibility to plant false trips; in consequence we can not reduce the redundancy in ALL cases

Furthermore, though safety fieldbuses are readily available and used in the machine automation or factory floor, the process industries do not yet have certified safety fieldbus devices with any credible track record to be used in a SIF or the variety of certified devices.

The standards and guidelines used for implementing field bus today do not meet ALL the requirements of field bus for safety applications, i.e. Bus speed (3-5 sec) will not accommodate most industry process safety times such as those of Reactors or Burner Management Systems, among others.

Additional Management of Change measurements needs to be added to address or fulfill the requirements of IEC61511.

**Summary**

Safe Operation is founded upon solid design principles and best engineering practices.

A “One Size Fits All” Certification Process for SIS Does Not Exist.

Third Party Certification is the foundation for a subsequent application-specific evaluation.

A Detailed Evaluation of how the equipment fits the application is still required.

False or Spurious Trips should be minimized to prevent unsafe conditions in the plant.

The User Responsibility is Key in achieving Safety and Availability.