Selecting "Sensors" for Safety Instrumented Systems per IEC 61511 (ISA 84.00.01 – 2004)

Dale Perry
Worldwide Pressure Marketing Manager
Emerson Process Management – Rosemount Division
Chanhassen, MN 55317 USA

Abstract:

The international standard for safety instrumented systems for the process control sector (IEC 61511) was published in 2003 and details the lifecycle requirements for Safety Instrumented Systems (SIS). The ISA Standard 84.01-1996 has migrated to the IEC 61511 standard under the name ISA 84.00.01 – 2004. New technologies and support from manufacturers are now available that will allow designers to select "sensors" that meet safety requirements in compliance with these new standards while reducing overall lifecycle costs. This paper will outline the selection of sensors for SIS applications that meet the requirements of IEC 61511 / ISA 84.00.01-2004 while minimizing lifecycle costs.

Introduction:

This paper will discuss sensor classifications of "sensors" for SIS applications that meet IEC 61511 (ISA 84.00.01-2004) requirements while minimizing lifecycle costs. The history of SIS standards is discussed followed by a discussion on the iterative process used for selecting sensors for SIS applications. The sensor selection includes an in-depth discussion of the two options, certified and prior-use. The paper then concludes by discussing other considerations when selecting sensors for SIS such as product capabilities and limitations, proof-test, safety accuracy and safety response time.

New International Standards – add value for process sector operating plants

In 1996 an international standard for safety was published under the title of IEC61508. This international standard set out a generic approach for all safety activities. The intent of the generic standard was to enable future application sector international standards.

In 2003, a process industry standard was published under the title IEC 61511. This standard was developed by end-users representing an international consortium from over 20 countries including the United States. The purpose of this standard was to develop a single set of requirements that would address the entire SIS lifecycle (identification, design, installation, operating & maintenance and decommissioning) specific for the process sector while meeting the requirements of the global process industry. The standard is organized into three parts:

IEC 61511-1	Requirements
IEC 61511-2	Informative guidance on meeting the requirements
IEC 61511-3	Informative examples of different methodologies to assist in the determination of the Safety Integrated Levels

This standard offers significant value to operators and integrators in the process industry. Since most global standard committees and/or authorities are expected to adopt this standard for their specific countries, companies can now develop standardized processes for safety instrumented systems that will meet most all global requirements. This standard also follows the "life-cycle" approach that assists users in ensuring that SIS are designed to meet the operating plant's risk reduction requirements from conception through decommissioning.

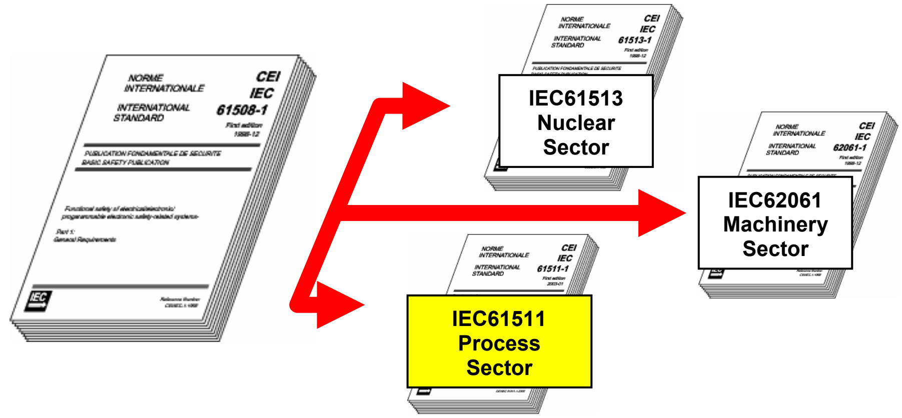


Figure 1: IEC 61508 was developed for any industry sector and also addresses the requirements for manufacturers of safety components used on SIS. IEC 61511 was developed specifically for the process sector and outlines the requirements for end-users and integrators only.

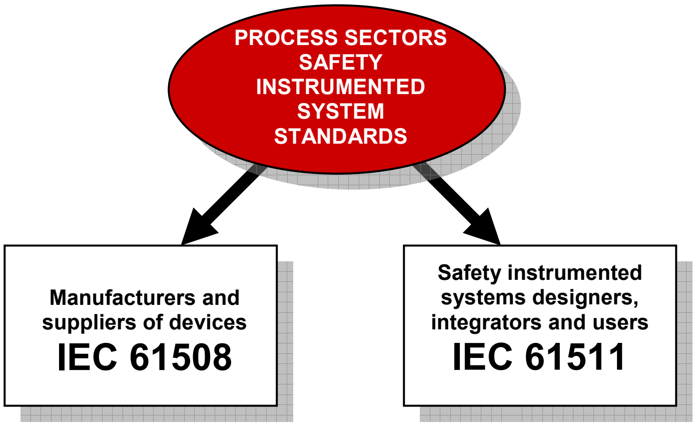


Figure 2: IEC 61511 - Relationship between IEC61511 and IEC61508

Numerous statements within IEC 61511 provide further evidence of the separation and applicable use of these two standards.

IEC 61511 lists the requirements for end-users and integrators. This standard requires manufacturers and suppliers of equipment used in SIS applications to follow the requirements outlined in IEC 61508 Section 2 (Hardware/System) and Section 3 (Software). This is a very important distinction. IEC 61511 states:

Scope (b): "(This Standard) applies when equipment meets the requirements of IEC 61508, or if Section 11.5 of IEC 61511 (Prior-Use or Proven-in-use) is integrated into an overall system that is to be used for process sector applications ***but does not apply to manufacturers wishing to claim that devices are suitable for use in SIS*** *for the process sector."*

*Scope (d): "(This Standard) applies when application software is developed**….but does not apply to manufacturers**, SIS designers, integrators and users that develop embedded software."*

IEC 61511 clearly states that manufacturers of equipment used on SIS must follow the requirements of IEC 61508 Section 2 and 3 unless the end-user has met the requirements of Section 11.5 "Prior-Use". Note, manufacturers cannot make a claim to meet "Prior-Use" per this standard, this is the responsibility of the end-user. Manufacturers would need to follow the "Prior-Use" requirements of IEC 61508.

Requirements for Sensors used in Safety Instrumented Systems

IEC 61511 documents specific requirements for hardware used in SIS. The hardware is broken up into two groups. One group consists of just the Programmable Electronic logic solver (PE logic solver). The other group consists of non PE devices, sensors and final control elements which are the focus of this paper. The two options end-users have for the selection of "Sensors" and "Final Control Elements" for SIS according to IEC61511 section 11.5.2 are:

- Components and subsystems selected for use as part of an SIS for SIL1 to SIL 3 applications shall either be in accordance with IEC61508 section 2 and section 3 or
- Meet the requirements of IEC61511 section 11.4 and sections 11.5.3 to 11.5.6, requirements for the selection of components and subsystems based on prior-use.

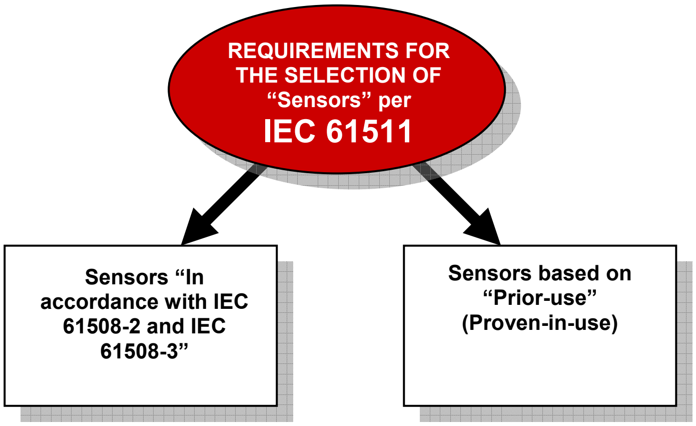

REQUIREMENTS FOR THE SELECTION OF "Sensors" per IEC 61511
Sensors "In accordance with IEC 61508-2 and IEC 61508-3"
Sensors based on "Prior-use" (Proven-in-use)

Figure 3: Two options IEC61511 allows for selection of SIS sensors

The differences between the choices of designed per IEC61508 and IEC 61511 prior-use is who is responsible for the burden of proof, the boundaries of the proof and the assumptions of the proof for sensors or final elements to function properly upon demand in SIS applications.

Below is a simplified graphic of the burden of proof. When using a sensor designed per IEC 61508 the manufacturer proves the safety level, capabilities and limitations of the device up to and including the wetted parts. The end-user has the responsibility to prove the interface between transmitter and process does not have any undetectable failures. This evaluation has to also consider undetected failure modes the process could cause to the sensor wetted parts such as physical damage from hammering, corrosion, hydrogen permeation or hydrogen embrittlement. It is the responsibility of the user to determine the PFD to be assigned to the interface. The end-user has all the burden-of-proof responsibility when using the qualified under the prior-use clause. The end-user determines the PFD, the capabilities and the limitations of these sensors. The prior-use evaluation also includes a complete process interface evaluation for dangerous undetected failures.

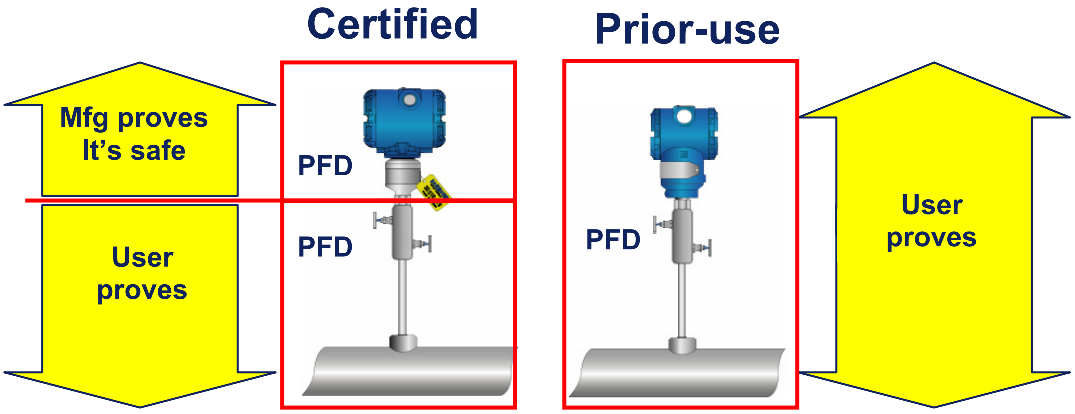


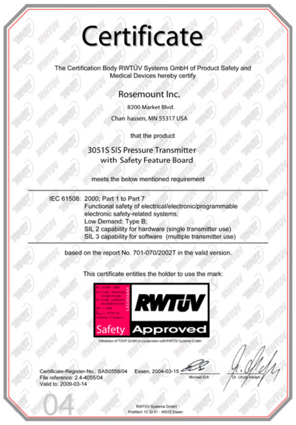
Figure 4: Responsibility of proof for SIS sensors

Sensors Selected "Designed per IEC 61508 Sections 2 and 3"

Sensors that are "designed per IEC 61508" define a field instrument design that meets the hardware, system and software requirements detailed in IEC 61508 Sections 2 and 3. The standard uses the Safety Integrated Level (SIL) table and applies it to the instrument system design as a measure of the device "safety level." The typical approach manufacturers' use to comply with IEC 61508 is as follows:

- Develop safety requirements and safety requirements specification
- Design instrument architecture and hardware per the "rules" of Section 2
- Design, verify, validate and control software and systems per the "rules" of Section 3 to the desired SIL level (level of device safety)
- Complete fault insertion testing to verify diagnostics
- Implement design control processes for management of change
- Implement manufacturing controls to ensure safety of device is not degraded
- Complete a Failure Mode Effect Diagnostic Analysis (FMEDA) to determine the failure rates, safe failure fraction (SFF) and probability of failure on demand (PFD)
- Detail the device "proof-test" requirement for the specified PFD
- Contract with a Notified Body for a third party review of the design requirements, hardware, software, system and design controls
- Notified Body issues a third party certification and report
- Manufacturer supplies a "Safety Manual" documenting for the end-user proper use of the product in SIS

Manufacturers submit products to notified bodies to certify the products meet all the requirements. If the products do meet the requirements, they will issue a certificate certifying the products meet all the requirements of IEC 61508. Below is an example of a certification certificate. The certificate indicates the product name, the product type classification and the applicable hardware and software SIL level rating.



Certificate

The Certification Body RWTÜV Systems GmbH of Product Safety and Medical Devices hereby certify

Rosemount Inc.
8200 Market Blvd.
Chan hassen, MN 55317 USA

that the product

3051S SIS Pressure Transmitter
with Safety Feature Board

meets the below mentioned requirement

IEC 61508: 2000; Part 1 to Part 7
Functional safety of electrical/electronic/programmable electronic safety-related systems;
Low Demand; Type B;
SIL 2 capability for hardware (single transmitter use)
SIL 3 capability for software (multiple transmitter use)

based on the report No. 701-070/2002T in the valid version.

This certificate entitles the holder to use the mark:

Validation of TÜViT GmbH in cooperation with RWTÜV Systems GmbH

Certificate-Register-No.: SAS0558/04
File reference: 2.4-4055/04
Valid to: 2009-03-14

Essen, 2004-03-15

Michael Eck

Dr. Ulrich Adolph

04

RWTÜV Systems GmbH
Postfach 10 32 61 - 45032 Essen

Figure 5: Certificate example for a sensor certified by TUV, the listed sensor complies to the requirements listed in IEC 61508 sections 2 & 3

Notified Bodies include RWTUV-Augsburg-Germany, TUV Sud, TUV Rhineland, Factory Mutual, USA, and many others. In certain cases, manufacturers will use industry experts to assist in meeting the requirements. These experts, such as EXIDA or Risknowledgy, are not notified bodies but have expertise in meeting IEC 61508 requirements and will assist in activities such as completing FMEDA and developing the safety requirements.

All products have limitations. These limitations need to be examined before selection. A product designed per IEC61508 limitations are listed in the Product Safety Manual. The safety manual will list at a minimum: product installation, configuration and safe operation requirements, product life and maintenance requirements such as proof-test.

Sensor failure data and PFD information can be taken directly from the product FMEDA. The PFD must be adjusted if there is a possibility the measurement can be affected by physical or environmental effects outside the bounds of the sensor certification such as impulse lines or primary elements plugging due to an unclean process or diaphragm seals.

There is significant value to end-users in specifying “designed per IEC 61508” sensors for SIS.

- Allows simple compliance to IEC 61511, supplier is responsible for documenting the safety level of the device
- Assurance that the failure rate data and PFD values are valid and correct
- Assurance that the instrument design meets good engineering practice for SIS applications defined in international standard IEC 61508 (especially important for minimizing systemic software failures)
- Assurance that the manufacturer has processes for “management of change” over the product life-cycle
- A Safety Manual and Certification Reports are available for proper implementation into an SIS

Although “Design per IEC 61508” add value for SIS designers, extreme caution must be used before specifying these sensors. Specific issues important to selecting sensors include:

- Safety review and certification does not mean a reliability review was completed – “safe” does not mean “reliable”. Therefore a thorough review of the failure rates should be completed to ensure the potential for spurious trips is reduced.
- Designs per IEC 61508 are reviewed as “white paper” analysis with no requirements for operating experience. Using untested, unproven devices in SIS application carries very high risk. Users should gain experience with the devices before installing on SIS applications.
- Failure rate data supplied by manufacturers DOES NOT INCLUDE the failure rates of the process interface. This is very important when selecting sensors. A high Safe Failure Fraction (means a low % of potential dangerous failures from the sensor) will not include dangerous failures such as line plugging, line freezing, slugs in lines, or gas permeation.
- Certification statements and the safety manual must be read carefully – many designs require significant proof-testing or have severe limitations on their use for the safety certification to be valid.

Sensors Selected Based Upon “Prior-Use”

The international committees that developed IEC 61508 and IEC 61511 recognized that users could develop other criteria for certifying SIS loop components. Therefore, a “Prior-Use” (also referred to as Proven-in-Use) clause was included. The Prior-Use clause allows users a methodology to accept Sensors and Control Elements that were not designed per IEC 61508 Section 2 and 3 for SIS applications.

The Prior-Use clause of IEC 61511 states the following:

*IEC 61511-1, Section 11.5.3.1: “**Appropriate evidence** shall be available that the components and sub-systems are suitable for use in the safety instrumented system.”*

The “appropriate evidence” for Sensors must be a documented case that includes (Reference IEC 61511-1, Section 11.5.3.2):

- Consideration of the manufacturer’s quality, management and configuration management systems
    - This clause requires validation that the manufacturer of the device has a quality system in place for consistency of product and a management of change system that documents hardware and software modifications.
- Adequate identification and specification of the components or sub-systems
    - This clause requires hardware and software identification of the qualified prior-use products. The intent is for end-user to be aware of and evaluate the effect on the SIF when the manufacturer modifies the product.
- Demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments
    - This clause requires proof the qualified device has been operating in environmental and physical stresses similar to the intended SIS environment. The intent of this clause is to validate that the PFD calculations will be the same as in the intended installation.

- Volume of operating experience
  - This clause requires proof of continuous performance evaluation of proved products. The intent of this clause is to ensure that the end-user continues to monitor products after the initial proof.

To meet these requirements, the standard allows users to document operating experience from basic process control applications as well as SIS applications. However, the standard does require that the operating experience be the same conditions as the planned use in SIS and that the data collected have statistical significance. In addition, only the end-user can establish prior-use per IEC 61511; suppliers cannot make this claim.

Sensor contribution to the PFD for prior-use sensors has to be calculated by the end-user. The end-user can use the manufacturer's product FMEDA as a starting point and adjust it for process conditions or to confirm the calculated PFD but they are not to use the data directly from the FMEDA without other considerations.

There is significant value to end-users in specifying "designed per IEC 61508" sensors for SIS.

- Sensors have a known reliability
- Sensors are already well understood by the designers and maintenance technicians
- Sensors have same installation practices for SIS and BPCS
- No additional training is required for maintenance personnel
- Spare part inventory can be leveraged
- Sensor failure history typically includes failures of the process interface.

This is why IEC 61511 only allows the end-user to establish prior-use, not manufacturers or suppliers. End-users know more about how these sensors perform in the field.

IEC 61511-1, Scope (b): "(This Standard) applies when equipment meets the requirements of IEC 61508, or if Section 11.5 of IEC 61511 (Prior-Use or Proven-in-Use) is integrated into an overall system that is to be used for process sector applications ***but does not apply to manufacturers wishing to claim that devices are suitable for use in SIS*** *for the process sector."*

Although "Prior-Use" offers some advantages for end-users, there are many hidden costs and risks, as the end-user must:

- Maintain documentation on sensor operating hours, environments and failure rates resulting in higher maintenance expenditures (MaintEx).
- Monitor management of change effect on Prior-Use. Manufacturers continue to make changes on Sensors due to part obsolescence, added features, or cost reductions. These changes need to be evaluated for the impact on the ability of the sensor to operate as the proof documentation claims. In some cases the change of form, fit, or function could negate all previous proof and the proof process will have to start all over again (CapEx, MaintEx).

Sensor Selection and its effects on the Hardware Fault Tolerance requirement

Fault Tolerance is defined as the ability of a functional unit to continue to perform a required safety function in the presence of a fault. This ability is expressed in the minimum number of required redundant sensors. The requirement per SIL is expressed in Table 6 of IEC 61511-1. This table is read by first looking for the SIL level and then looking at the fault tolerance minimum. For example: An SIL 2 application requires one sensor and one redundant sensor. An SIL 3 application requires one sensor and two redundant sensors.

IEC 61511 Table 6: Hardware Fault Tolerance for Sensors, Final Elements and non-PE Logic Solvers

Hardware Fault Tolerance	
SIL	**FT_{min}**
1	**0**
2	**1**
3	**2**
4	See IEC 61508

The Hardware Fault Tolerance requirement is not effected by the selection of either certified or prior-use sensors.

For prior-use sensors, IEC 61511 Section 11.4.4 states that “excluding PE logic solvers, the minimum fault tolerance specified in Table 1 may be reduced by one if the devices used comply with the following:”

- The hardware of the device is selected on the basis of prior-use
- The device allows adjustment of process-related parameters only
- The device is password of jumper protected

For devices designed per IEC 61508, IEC 61511 Section 11.4.5 states that “Alternative fault tolerance requirements may be used provided an assessment is made in accordance to the requirements of IEC 61508 – 2, Tables 2 and 3.” This statement directs the user to the IEC 61508 Hardware Fault Tolerance tables for Type A or Type B devices. These tables specify the number of required redundant sensors by the sensor Safe Failure Fraction (SFF). Knowing that a device designed per IEC61508 requirement of an SFF of >90%, Table 3 (Type B device) reveals the same fault tolerance requirements as stated in IEC 61511 Table 6 with a reduction of one fault tolerance.

IEC 61508 Table 2: Hardware safety integrity: architectural constraints on type B safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60%	Not Allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL4	SIL 4

The standard next requires the designer to review any process interface effects that could lead to a dangerous failure condition. For sensors, these would include line plugging, freezing, gas permeation, etc. If any dangerous failure potentials exist, the fault tolerance must again be increased by 1.

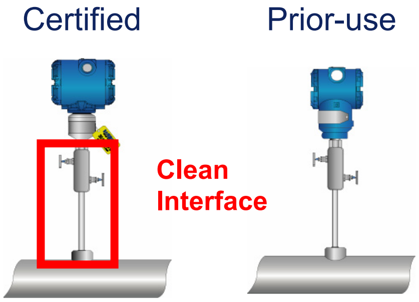


Figure 6: A clean interface is required for Fault tolerance credit for certified devices

The following table (Table 1) is an adjusted Hardware Fault Tolerance table with a reduction of one fault tolerance. It can be used when either a sensor meets the requirements of prior-use or the sensor is certified with a SFF > 90% and has a clean interface to the process.

Table 1 - Hardware Fault Tolerance table with credit taken

Hardware Fault Tolerance	
SIL	**FT_{min}**
1	**0**
2	**0**
3	**1**
4	See IEC 61508

One should be aware of the trade-offs of safety vs. availability when considering using the allowable credit.

Common Cause/Common mode/Systematic Failures

Although common cause and common mode differ slightly in definition standards, common cause and common mode are typically used synonymously. These failures are defined as failures that impact two or more channels of redundant systems. An example of this is where sensors are affected by electromagnetic disturbances. If this type of sensor is used in a 2oo3 voting scheme and these sensors get exposed to a electromagnetic field, the effect of the field may negatively affect the output of all the sensors causing the same erroneous result and possibly an unsafe condition. Other examples of common cause stressors are temperature transients, thermal or physical shock, vibration, design errors, or maintenance errors. The term assigned to common cause failures is the beta factor and is expressed as a percentage. The beta factor can be calculated by a third party or by the end-user. It is used by first calculating the PFD for the redundant system and then multiplying it by the beta factor number and then adding the result to the loop PFD.

Some end-users use a variety of sensors (different technology or different vendors) to lower the beta factor. This is typically referred to as using sensor diversity. Although in theory this practice sounds good, consideration has to be taken for maintenance and operations to maintain such systems.

Sensor capabilities and limitations

There are many other considerations that must be taken into account when selecting sensors beyond the required discussed thus far, the most important being capabilities and limitations of the product and capabilities and limitations of the maintenance and operations staff to maintain the "as designed" functional safety of the SIS.

Capabilities and limitations of the sensor designed per IEC 61508 will be documented in the required product safety manual. Important topics include proof-test, safety accuracy, safety response time and unsafe modes of operation.

Proof-test:

IEC 61511 Clause 16.2.2 requires maintenance procedures to be developed to insure SIL compliance. A major component of the plan is determining the proof-test and setting the proof-test intervals. Proof-tests are a required component of the IEC 61511 for the SIS and the IEC 61508 certification process for loop components. The manufacturer develops tests to prove the sensor is not in a dangerous undetected failure mode. Proof-tests are located in the product safety manual and are expressed in percent of coverage. This percentage is part of the calculation used to maintain SIL level PFD compliance.

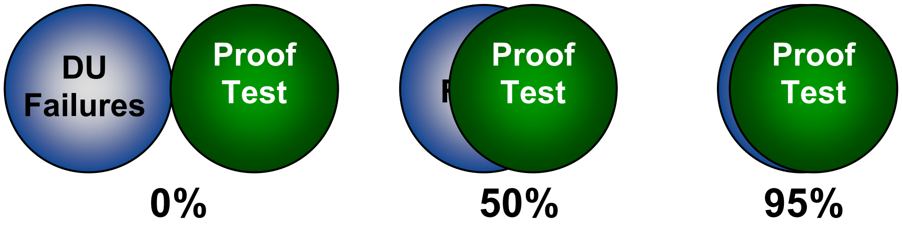


Figure 7: Proof-tests are designed to discover Dangerous Undetected failures

Things to consider are the complexity of the test, the actions required to bypass the SIS during the testing, consequences of a hazardous event during test and how often the test needs to be performed. All of these are critical as the possibility for a false trip by a maintenance action can trip the SIS and shut down all or part of the plant. The ideal sensor would have a simple test with proof-test intervals equal to or greater than normal plant shut down intervals. This allows the testing of sensors with the plant off-line.

Proof-tests for prior-use sensors are developed by the end-user. Prior-use proof-tests are also not specifically designed to detect sensor specific undetected dangerous faults as this analysis is not part of qualifying a prior-use sensor. They are generally the routine maintenance used when qualifying the sensor. The tests are easy and familiar such as a simple calibration. The simplicity of this is attractive but the issue is that you don't know if you are testing too often, not often enough, or not even testing for the right failures. Fortunately, some manufacturers are realizing this and are having the FMEDA analysis extended to include proof-tests.

Safety Accuracy:
Safety accuracy is different than sensor accuracy. Some smart safety sensors certified to meet IEC 61508 sections 2 and 3 have a feedback mechanism within the sensor to compare the actual mA output to digital output. Others have set a threshold on the amount of drift they will allow critical components before they consider the output dangerous undetected or unsafe. The precision of safety accuracy of a sensor is typically 2-5%.

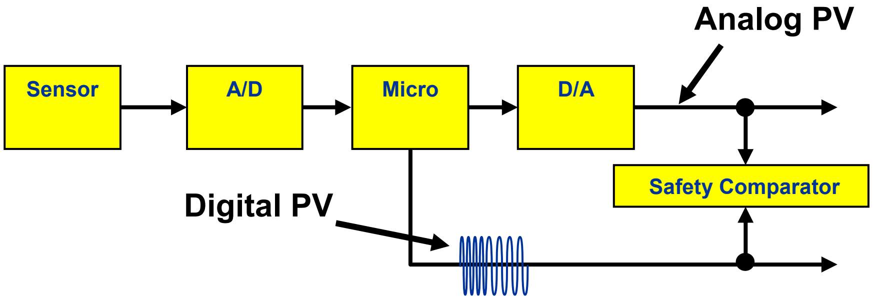


Figure 8: Smart sensor basic block diagram with output comparator

Safety Response Time:
Similar to safety accuracy, safety response time is commonly different than sensor response time. Sensor response time is the time it takes from when the input to the sensor changes to when the output responds to the change. Safety response time is the sensor response time plus the time it takes to run all the diagnostics. Typical safety response times are 1 – 5 seconds.

Capabilities and limitations of a sensor qualified under the prior-use clause are defined by the end-user. This could pose a potential safety issue as the end-user may not know all the capabilities, limitations, or failure modes of the sensor. Fortunately some manufacturers have seen this need to inform end-users of capabilities and limitations for safe operations of specific sensors and are issuing safety manuals for products that are not designed per IEC 61508.

Other Considerations for Selecting Sensors for SIS
There are other considerations a designer of SIS should review when making a selection of a specific Sensor type and manufacturer. There are other papers written on this topic so it will be covered in only a high level. (See Reference 4). The main considerations when selecting Sensors for any process application but of special importance in SIS:

Use of Process Industry Grade SMART Transmitters over Other Technologies:
Process sector grade Pressure and Temperature Transmitters are the best sensor type for SIS applications. These devices are designed for high reliability in process grade applications and environments, have good installed performance and response times and have a short Mean-Time-to-Restoration (MTTR). SMART transmitters also deliver a continuous electronic signal and therefore can be detected by SIS logic solvers if no signal is received or if internal transmitter alarms are initiated.

Installation Practices:
Proper design and installation of the sensor is critical to ensure safety. For example, process related affects on the sensor, such as process line plugging, corrosion or gas

permeation can all lead to a dangerous failure condition of the sensor. Proper installation practices can reduce or eliminate these systematic effects.

Summary and Conclusions:

In summary, there are two international standards for SIS. IEC 61508 is to be used by manufacturers of equipment for use in SIS. IEC61511 is to be used by SIS system integrators and end-users.

IEC 61511 requires users to select sensors either based on "Designed per IEC 61508" or based upon "Prior-Use". There are advantages and disadvantages to either approach.

The "Best Practice" approach is one that combines both "Designed per IEC 61508" with the elements of "Prior-Use".

- SIS sensors should have commonality between BPCS and SIS
- Prior-use or designed per IEC61508 sensors should have a significant history of proven installation performance
- Manufacturers should provide significant documentation to support prior-use sensor claims
    - Proof of a quality and management of change system
    - FMEDA
    - Reliability and performance data
    - Hardware and software change notifications
    - Proof-test requirements
- Sensors should have proof-test intervals equal to or greater than the plant shutdown schedule
- Supplier should impose no additional installation, commissioning, or testing requirements for using the sensor on SIS than required for basic process control.

Suppliers meeting these requirements will allow you to implement the "Best Practice" for selecting sensors for SIS. A practice that ensures the safety requirements are met while minimizing lifecycle costs.

References:

1. IEC 61511 (2003) *Functional safety: Safety Instrumented Systems for the process industry sector – Part 1*
2. dISA 84.00.01 (2004) *Functional safety: Safety Instrumented Systems for the process industry sector – Part 1(USA version of IEC 61511)*
3. IEC 61508 (1997-2000) *Functional safety of electrical/electronic/ programmable electronic safety-related systems*
4. *Measurement Best Practices for Safety Instrumented Systems*, May 2003, Menezes and Brown
5. *Guidelines for Safe Automation of Chemical Processes, published by the Center for Chemical Process Safety of the AICHE*