SIEMENS
Ingenuity for life

Choosing Functional Safety Field Instrumentation

Certified, prior use or both? - Fundamentals of VDI 2180

By: Luis M F Garcia G & Gene Cammack

Introduction

As a subscriber of the Safety List, which is an International Society for Automation – ISA - open email based forum (SAFETY@ISA-ONLINE.ORG); I was drawn to a very interesting discussion about the selection of instruments to be used in a Safety Instrumented Function (SIF) and the implications that such selection would have in the performance of such a safeguard.

As might be expected, two camps developed as soon as people started sharing their thoughts and experiences. Some colleagues claimed that certified instrumentation was just a ploy from vendors to make more money, and that field data collection and analysis is the only way to select equipment to be used in functional safety applications. Others recognized that many systematic faults could be avoided all together by using properly IEC 61508 certified equipment. One recognized international engineering firm went as far as to indicate that up to 30% of the instrumentation they had analyzed had shown design flaws that would lead to dangerous failures.

What it points out is that determining the equipment to use in safety instrumented systems (SIS) and the rules for maintaining them is one of the most difficult and controversial topics in the industrial SIS marketplace. As is usually the case, there are valid arguments in both sides, but in truth, there is a third approach where both philosophies are needed and, in fact, must be adopted in most cases. This is based on the use of certified equipment which needs to be continuously monitored to weed-out implementation systematic faults.

To get to the heart of the matter, we will look at the background of both positions, review the recent changes to the standards, and look at the recommended practices from the German Engineering Association, VDI to calculate performance of different instrument arrangements as subsystems of a Safety Instrumented Function (SIF).

Safety Integrity Level (SIL) of a Safety Instrumented Function

A SIF is a safeguard, designed to take the process to a safe condition if the process functionally exceeds safe operating conditions. As a "safeguard", it should only function when required. Therefore, equipment used in a SIF needs to reliably operate and execute its function whenever the process exceeds safe operating conditions (a demand). A failure to do that is called a "failure on demand"

The performance of a SIF and their components are expressed as Safety Integrity Levels (SIL). These are statistical estimations of average probability that they will fail on demand (PFD_{AVG}). The Average Probability of Failure on Demand (PFD_{AVG}) is a function the failure rate of the device (expressed as λfailures per time) and the time between inspections (proof test interval) since a periodic inspection will decrease such likelihood of failure (Figure 1).

SIL calculations for PFD_{AVG} are also dependent on the architecture of the SIF where redundancy and common cause (β) become factors. One out of Two (1oo2) and Two out of Three (2oo3) architectures are often used to lower the PFD_{AVG} for a subgroup (Sensors, Logic Solver or Final Elements). Failure of the SIF will occur in the event of failure of the sensors subgroup or the logic solver or the valves subgroup. Like a chain, it will fail in its weakest link.

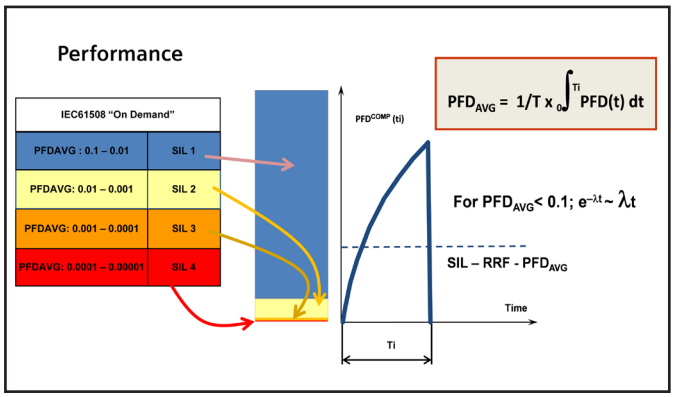

Figure 1

Performance	Risk Reduction	PFD_{AVG}
SIL 1	10 to 100	1 in 10 will fail
SIL 2	100 to 1,000	1 in a 100 will fail
SIL3	1,000 to 10,000	1 in 10,000 will fail
SIL4	10,000 to 100,000	1 in 100,000 will fail

Table – SIL for Low Demand Mode

But SIL Calculations are based on λ (failures per unit time) which only considers random failures. We must also take into account Systematic Failures which could be several orders of magnitude higher than random failures, rendering PFD_{AVG} calculations irrelevant.

A systematic failure is a failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. When designing a SIF, users need to select instrumentation with a clear understanding of their performance.

There are four factors to take into consideration when assessing the SIL an instrument could reach.

1. PFD_{AVG}: Does the instrument have low enough random failures and high enough inspection frequently to achieve the PDF_{AVG} required by the SIL level?

2. Architectural constraints: Does it meet a minimum level of redundancy?

3. Systematic Faults: Have systematic faults been controlled through good design processes and when used as instructed by the manufacturer?

4. Security: Is the device secure or hardened against threats?

So, the question is how do we evaluate, prove and document the performance of a SIF component?

SIL Determination of an Instrument – What to use?

There are three possible ways in which a device is evaluated.

Certified - Route 1H: The instrument manufacturer may follow Standard IEC 61508; 2010 Route 1H and 1S[1] ; then a third party (TÜV, exida, Risknology, FM etc.) certifies the instrument. The process involves:

a) Performing Failure Mode and Effect Diagnostic Analysis (FMEDA), a detail and lengthy analysis of all failure modes of all components of an instrument.

b) Compliance with Safe Failure Fraction (SFF) constraints tables for the level of redundant architecture where the instrument will be used.

c) Using an appropriate group of techniques and measures designed to prevent the introduction of systematic faults

during the design and development of the device. This includes evaluation of the device, the design process and the safety manual (architectures, inspection frequencies, operating conditions, etc.)

To certify an instrument, or a component following this process, might take months or years, and the certification entity has a clear incentive of finding mistakes in the instrument, resulting in an improved design.

Certified - Route 2H: The instrument manufacturer may follow Standard IEC 61508; 2010 Route 2H and 2S [2] and/or 3S; then a third party (TÜV, exida, Risknology, FM etc.) certifies the instrument. The process involves:

a) The collection of failure data, following IEC 60300-2-3

b) The analysis of the data following IEC 61649 (2H) and Proven In Use (PIU)

The goal is to demonstrate, based on an analysis of operational experience for a specific configuration of the instrument, that the likelihood of dangerous systematic and random faults is low enough so that every safety function that uses the instrument in the same conditions achieves its required safety integrity level (Route 2S). This includes pre-existing software components (Route 3S).

The process also might take months or years depending on the data available.

Prior Use: Users follow Standard IEC 61511; 2016 Prior Use evidence determination (PU). The process involves:

a) PU analysis, which consists of data collection and analysis of failure rates in the user's environment with the goal of performing a documented assessment of a device, supporting that it is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar operating environments.

b) Understanding how the equipment behaves in its specific operating environment to achieve a high degree of certainty that the planned design, inspection, testing, maintenance, and operational practices are sufficient.

c) Calculating upper bound statistical confidence limit 70%.

The process might yield too conservative values, as systematic faults are expected to dominate. Replacing by a different design instrument would only introduce different systematic faults.

Possible scenarios

Users are therefore confronted with 4 possible scenarios when selecting critical instrumentation (which was exactly what fired up these discussions in the first place);

Scenario 1 – when IEC 61508 certified instrumentation (either Route 1H or 2H) is available for the specific application. This is the ideal situation. If the user follows the safety manual of the instrument; (like type of application, installation, inspections frequencies, procedures and life of the instrument); expected performance should be achieved, and SIL Calculations, including redundant architectures will be easily performed.

Scenario 2 – when IEC 61508 certified instrumentation is available, but the user application is slightly different to what is recommended by the certification entity. In this case, evaluation of severity of the deviations needs to be analyzed.

Scenario 3 – when certified instrumentation is NOT available, yet failure rates data of instruments used for interlocks and other safeguards in similar environment is available. This scenario is similar to scenario 4, but with a lesser degree of difficulty.

Scenario 4 – when certified instrumentation is NOT available, yet failure rates data of instruments used in process control is available. Then PU evidence of suitability, although in different conditions (process control environment is not the same as functional process safety) should be performed, following IEC 61511-1; 2016. Evaluation should include analysis of:

- Manufacturer's quality management systems;
- Adequate identification and specification of the devices;
- Demonstration of the performance of the devices in similar operating environments;

Performance of redundant instruments subsystems – VDI/VDE 2180

SIL related PFD_{AVG} calculations models take into account all failure modes and how they affect the performance of equipment under study, and consider:

- Time in which each type of failure mode affects performance
- Architecture under consideration
- Influence of common cause (for redundant architectures)
- Time a component of the SIF is bypassed for maintenance.

The dominant factors of the equations are the rates of dangerous failures which cannot be detected by automatic diagnostics (λ_{DU}), as well as the common cause (β) in redundant architectures. Therefore, basic reliability formulas could be simplified by considering just these two parameters and the time between manual inspections. The values of PFD_{AVG} would be more conservative, but by less than 10%.

This is exactly what VDI 2180 proposes. (VDI is a German Engineers association)[3] . VDI recently published "Safeguarding of industrial process plants by means of process control engineering (PCE) Recommendations for practical use" [VDI 2180].

In summary it proposes:
A - If devices are either; not certified, operating in different conditions as originally designed for, or there is not experience to determine optimal operating conditions.

Then:
a) Collect failure rates data
b) Classify for a clear taxonomy
c) Evaluate for systematic failures,
d) Calculate expected values
e) Apply following equations for different architectures;

a. $PFD_{avg\ 1oo1} = ½\ \lambda_{DU}\ Ti$

b. $PFD_{avg\ 1oo2} = 1/3\ (\lambda_{DU}\ Ti)2 + ½\ \beta\ \lambda_{DU}\ Ti$

c. $PFD_{avg\ 2oo2} = \lambda_{DU}\ Ti$

d. $PFD_{avg\ 2oo3} = (\lambda_{DU.}\ Ti)2 + ½\ \beta\ \lambda_{DU}\ Ti$

e. $PFD_{avg\ 1oo3} = 1/4\ (\lambda_{DU.}\ Ti)3 + ½\ \beta\ \lambda_{DU}\ Ti$

B - If devices are both:
A - Certified
B - Are going to operate as indicated in their safety manual

Then the PFD_{AVG} of a single device is given in the Safety Manual (nothing to calculate) and for other architectures:

a. $PFD_{avg\ 1oo2} = 4/3\ (PFD_{avg\ 1oo1})^2 + \beta\ PFD_{avg\ 1oo1}$

b. $PFD_{avg\ 2oo2} = 2\ PFD_{av\ 1oo1}$

c. $PFD_{avg\ 2oo3} = 4\ (PFD_{avg}\ 1oo1)^2 + \beta\ PFD_{avg\ 1oo1}$

d. $PFD_{avg\ 1oo3} = 2\ (PFD_{avg}\ 1oo1)^3 + \beta\ PFD_{avg\ 1oo1}$

Conclusions
There is a natural simplification in the evaluation of performance of instruments which are used in a SIF if such instruments are certified as per IEC 61508 and if the user follows the recommended operation and maintenance practices as stated in the instrument safety manual. Alternatively, instruments with PU evidence of suitability might be used but analyzing such data could be challenging, forcing very conservative application designs.

VDI 2180 offers a simplified recommended way to calculate performance for both paths.

[1]H denotes Hardware and S denotes Systematic
[2]IEC 61508;2010 part 7
[3]VDI represents all disciplines of the engineering spectrum in Germany going from Agroindustry to Biotechnology applications. VDI organizes conferences, symposiums, exhibitions, subscribes standards and promotes young talents. Founded in 1856, it is the oldest association in Germany with more than 135,000 members.

Luis M. F. Garcia G. is the Siemens Industry Inc. Senior Process Safety Consultant for The Americas (Phone: +1 281-687-8369); Email: luisgarcia@siemens.com). He has been certified as a Functional Safety Expert by TÜV SÜD and the CFSE Governing board since 2005. He is an ISA 84 safety and security committee voting member representing Siemens. Luis has taught and developed Functional Safety courses in Spanish and English as well as published numerous articles and papers in the Americas, Europe and Australia. Mr. Garcia has a Mechanical Tech. degree from Rosario-Argentina, in 1972 and a BEng in Metallurgy and material Science from Liverpool University-UK in 1981.

Gene Cammack is the Sales Manager for the Safety Consulting Practice of Siemens. Gene has 30+ years of experience in safety systems, automation and control systems in the process industries including Power, Refining, Chemicals, Pipelines and upstream Oil & Gas. Before joining Siemens, Gene worked for end users, engineering companies and manufacturers in roles ranging from system design and solution development to business development and marketing. Most recently, Gene directed The systems product marketing for North America for Yokogawa, including safety systems and previously, was responsible for Business Development for the US Gulf Coast for exida Consulting.