Standard devices vs IEC 61508 SIL safety devices Integration in process industry

Eric Fae, Fabrice Marcel

Standard devices vs IEC 61508 SIL safety devices Integration in process industry

Paper No. PCIC Europe EUR18_34

Mr. Eric FAÉ
INERIS
Parc Techno. ALATA - BP2
F-60550 Verneuil-en-Halatte
France

Mr. Fabrice MARCEL
KROHNE SAS company
2 Allée des Ors - BP 98
26103 Romans sur Isère cedex
France

Abstract – In process industries like in other sectors, two mains systems are working together.

- The control system and,
- The safety system

If the requirements for the control system are mostly based on the performance of the safety controller – safety PLC[1] (or other standard device), sensors and actuators in terms of :

- computation,
- response time.

depending mostly of the process that is supervised.

The answer for the safety requirements are mostly defined in IEC 61511 [1]. This standard defines the application of the other standard IEC 61508 [2] for the process industry.

End users can reach the requirements of IEC 61511, for the realization of the safety function:

- by Using "*prior use hardware devices*" or
- by Using "*hardware developed and assessed according to IEC 61508*" safety devices.

For software, there is also an additional limitation for the programming of the safety PLC with the following requirement "*developing application program using limited variability or fixed program*".

If the case for the link of safety PLC and the BPCS[2] controller seems to be solved in most applications, it is not the case with sensors and actuators.

This article will present :

1) Introduction – process & safety – regulations in Europe
2) IEC 61508 requirements for safety systems – specifics: low demand high demand & route 1H/2H
3) Process and safety IEC 61511 & IEC 61508
4) Application of safety devices & IEC 61511 - the application of the approach of security through the example of a radar.
5) Can we trust in the SIL certificates ?
6) IEC 61511 requirements : comparison with the field of ATEX, machines and processes.

Index Terms — Functional safety, safety device, IEC 61508, IEC 61511, safety applications.

[1] PLC : **P**rogrammable **L**ogic **C**ontroller

[2] BPCS : **B**asic **P**rocess **C**ontrol **S**ystem

I. INTRODUCTION – PROCESS & SAFETY – REGULATIONS IN EUROPE

In Europe, there is no European Directive that gives mandatory requirements for the use of process **PLANTS**. Some procedures exist when a manufacturer launches on the market **PRODUCTS** e.g. machines (machinery directive 2006/42/CE [3]), ATEX apparatus (ATEX directive 2014/34/UE [4])

In Europe, process industries are in the scope of the SEVESO directive [5] and mostly under the mandatory requirements of national regulations that are taken under the application of the SEVESO directive.

In France, in order to run a **PLANT** with a hazardous process two different procedures could apply :

- The authorization to run a dangerous process that is given by the authorities or,
- The declaration from the process owner

Each country defines in its regulation the way to prove that the risks are under control mainly by the presence of technical barriers for safety and by the training of the personnel that operates on the **PLANT**.

We will not go into details of the application for each country of the SEVESO directive. We will present the non-regulatory rules that are used by end users to justify the safety level of their safety barriers and layers of protection based on safety standards IEC 61508 and IEC 61511. We will also point out the possible traps that are in the SIL certificates they use.

II. IEC 61508 REQUIREMENTS FOR SAFETY SYSTEMS - specifics: low demand high demand & route 1H/2H

IEC 61508 standard comprises 7 parts. Parts 1, 2 & 3 are normative and defines several kinds of requirement including:

- **A safety lifecycle** - defined mainly in IEC 61508 parts 1, 2 and 3 together with qualitative and quantitative requirements of behavior of the safety system in case of failures (defined in terms of SIL). Safety systems are defined in two types: protection system and safety systems and operates in the following modes of operation: the low demand, high demand or continuous mode of operation.

These modes of operation described in IEC 61508 are subject to discussion even in standardization groups with experts.

Definition of the low demand mode of operation and high demand/continuous mode of operation is given on IEC 61508 standard, and clarification on the IEC web site

following page http://www.iec.ch/functionalsafety/faq-ed2/page5.htm that says [3]:

These are low demand *mode of operation and* high demand or continuous *mode of operation. Those definitions are based on the division between a* demand *mode of operation and a* continuous *mode of operation.*
A safety function operating in **demand** *mode is only performed when required (i.e. on demand) in order to transfer the equipment under control (EUC) – example a motor into a specified state. In this case, the safety device and safety system that performs the safety function has no influence on the EUC until there is a demand for the safety function to be performed.*
A safety function operating in continuous *mode operates to retain the EUC within its normal safe state, and the safety-related system continuously controls the EUC, and a dangerous failure of the safety-related system will lead to a hazardous event unless other safety-related systems or other risk reduction measures intervene (other layers of protection).*

IEC 61508 distinguishes between[4]:

- low demand mode of operation, and
- high demand or continuous mode of operation.

Modes of operation are used in IEC 61508 to describe two types of safety function carried out by the safety systems. The modes are relevant when relating the target failure measure of a safety function to be implemented by an **E**lectrical, **E**lectronic or **P**rogrammable **E**lectronic (E/E/PE) safety-related system to the safety integrity level. IEC 61508 relates the safety integrity level of a safety function to:

- the average probability of a dangerous failure on demand (in the case of low demand mode – see table 2 of IEC 61508-1), or
- the average frequency of a dangerous failure per hour (in the case of high demand or continuous mode – see table 3 of IEC 61508-1). The average frequency of a dangerous failure per hour is sometimes referred to as the dangerous failure rate (i.e. dangerous failures per hour).

Low demand mode is where the frequency of demands for operation made on a safety-related system is no greater than one per year.
High demand or continuous mode, is where the frequency of demands for operation made on a safety-related system is greater than one per year. Continuous is regarded as very high demand.
But the time is not the only criteria. IEC 61508 website present different kind of architectures for low demand and high demand / continuous mode of operation.

An example of a system architecture in which a safety-related system implements safety functions operating in **either low or high demand mode is** shown in Figure 1(a). In this example, dangerous failures of the equipment under control (EUC) or the EUC control system place demands on the E/E/PE safety-related system (see Figures 1(b) and 1(c)).

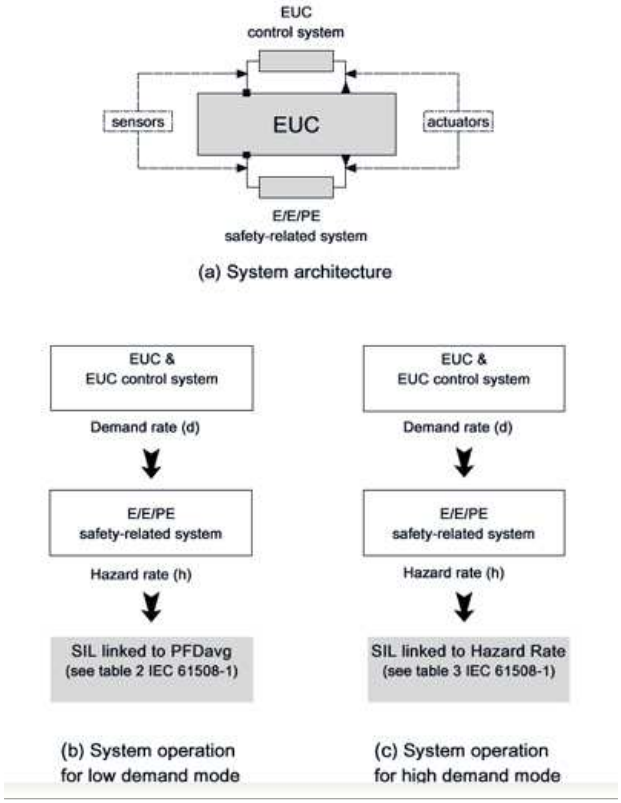

Figure 1: Example system operating in demand mode (high demand and low demand)

An example of a system architecture in which a safety-related control system implements safety functions operating in **high demand mode** is shown in Figure 1(a). The corresponding system operation is shown in Figure 1(c).
An example of a system architecture in which a safety-related control system implements safety functions operating in **continuous mode** is shown in Figure 2(a). The corresponding system operation is shown in Figure 2(b).

[3] E9) What is a mode of operation?

[4] E10) What is the difference between *low demand mode of operation* and *high demand or continuous mode of operation*?

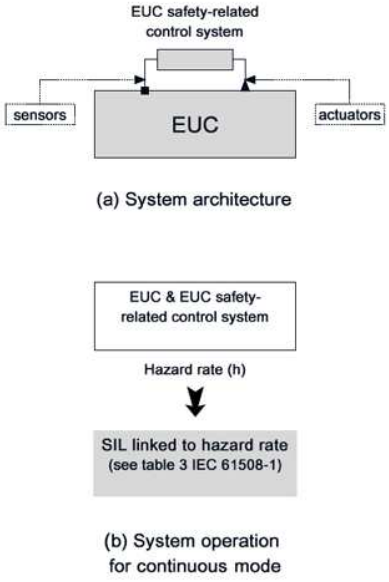

Figure 2: Example system operating in continuous mode

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFDavg)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h-1] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

- Requirements for the realization of the hardware part of safety systems with two major ways for the realization of these devices. The best way based on fault tolerance requirements (referenced in the standard as “route 1H”) and another route based on the feedback return from field (“route 2H”) with additional criteria and requirements.

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 4 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 5 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

- Requirements for the realization of software defined in part 3 of the standard.

III. PROCESS AND SAFETY IEC 61511 & IEC 61508

In most cases, functional safety in process industries starts with a hazard analysis, based on the different methods that are defined in IEC 61511 standard.

This standard is not mandatory in Europe because no European Directive requests explicitly for it.

This IEC 61511 standard presents for process industries a methodology to manage safety and is based on the principles of IEC 61508.

The first step of the safety analysis starts with an HAZOP[5] in order to identify the hazards. The results of this analysis is to define the functioning of the process with those different safety devices (breathing valve, high level sensor, ...) and to set requirements for the two main systems for risk reduction devices classified in two categories :

- Safety devices that reduce the effect of the hazard in the case the dangerous event occurs. Such safety devices are disk rupture, flame arrest, that protect against the effect of an

[5] HAZOP : **HAZ**ard and **OP**erability study

explosion. Those devices are called **protection devices**.

- Safety devices that are put in place for detecting the potential cause of hazard and for avoiding the dangerous situation to occur. Because they detect a physical phenomenon (like a level, or any other values) they are based on most cases on electronics. Those devices are called **safety related systems.**

If the definition of safety protection devices is well known in the process industries, the choice of safety devices are less simple, because end users must fulfill the requirements of IEC 61511.

We will focus on this subject:

- By defining the safety functions and safety level linked with
- The different "so called" safety devices.
- And possible traps attached in the SIL certificates of these SIL safety devices.

<u>The scope of IEC 61511, specifics : low demand, route 2H and layer of protection</u>

IEC 61511 is an application standard of IEC 61508 for process industries. The scope of EC 61511 is defined in the following figure.

Figure 3: Scope of IEC 61508 / IEC 61511

The links between IEC 61508 and IEC 61511 are also defined in the IEC 61511 standard and are limited to the scope of the boxes identified in light grey rectangles on the following figure.

We can see that the following are under the scope of IEC 61508:

- Developing new hardware devices
- Developing embedded system software
- Developing application programs using full variability languages

Are only on the scope of IEC 61511:

- Using prior use hardware devices
- Using hardware developed and assessed according to IEC 61508
- Developing application programs using limited variability or fixed program languages

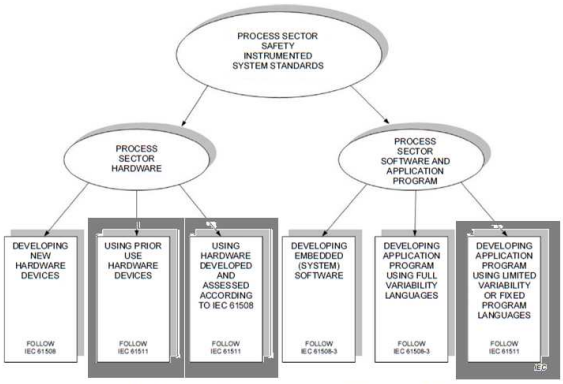

Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

Figure 4: Links and bridges IEC 61508 / IEC 61511

IEC 61511-1:2016 requires :

- Management of functional safety (chapter 5) with Organization, resources (chapter 5.2.2) and activities. Inside this chapter : Risk evaluation and risk management (chapter 5.2.3) - Functional safety assessment (FSA) 5.2.6.1
- Safety life-cycle requirements (chapter 6)

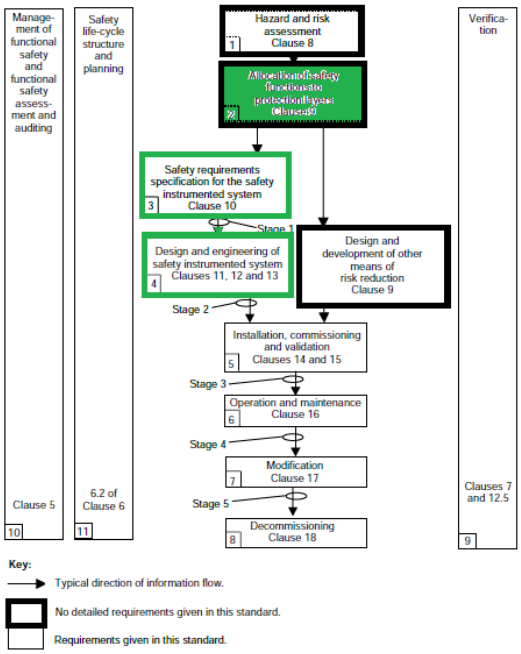

Figure 5: IEC 61511 Safety life-cycle requirements

- Objectives

Table 4 – Safety integrity requirements: PFD_{avg}

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	PFD_{avg}	Required risk reductio
4	$\geq 10^{-5}$ to $< 10^{-4}$	$>$ 10 000 to $\leq$ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	$>$ 1 000 to $\leq$ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	$>$ 100 to $\leq$ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	$>$ 10 to $\leq$ 100

Table 5 – Safety integrity requirements: average frequency of dangerous failures of SIF

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	Average frequency of dangerous failures (failures per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 6 – IEC 61511 qualitative requirements

With a limitation to SIL 3.

- Allocation of safety functions to protection layers (chapter 9)

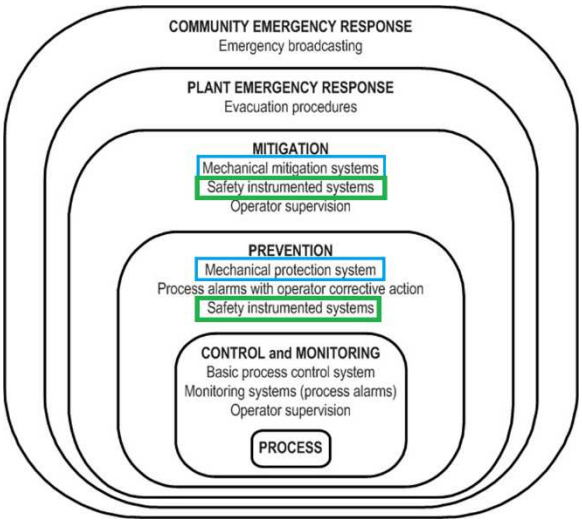

Figure 6: IEC 61511 Protection layers

IV. APPLICATION OF SAFETY DEVICES & IEC 61511 - THE APPLICATION OF THE APPROACH OF SAFETY THROUGH THE EXAMPLE OF A RADAR

- **Definition of the process**

In order to illustrate the way to select the safety devices as components of the safety loop, the following example will be followed:

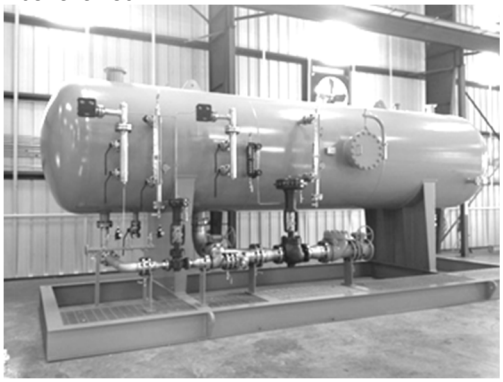

Figure 7: IEC 61511 example : tank protection

In a tank, there is a separation of multiple mediums, according to their respective physical properties. The input medium is a mix, and the outputs, after heating are the gas, the water and oil.

This tank can be represented as follows:

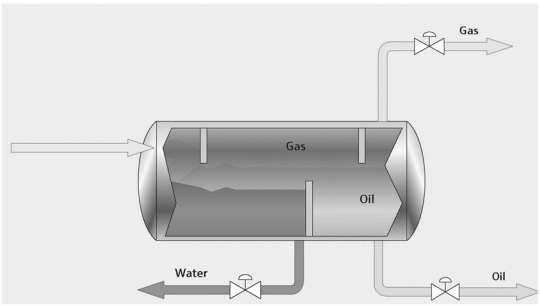

Figure 8: IEC 61511: Products & Hazards

According to the laws and regulation, the owner of such a process (the end users) should take into account the risks to humans (health and safety – covered in Europe by the machinery directive) and the environment (pollution).

- **Risk analysis**

There are multiple ways to study a process to increase its safety. In this example let's assume that a dedicated HAZOP (meaning Hazardous Operations) has been conducted. The HAZOP is a systematic technique that has to be applied by selecting "nodes" on the schematic representation of the process. Starting from each node, keywords have to be linked, asking a special question[6] that the owner of the process has to answer.

Of course each question built with these keywords and the nodes has to be adapted.

Performing a risk analysis on a process will lead to a list of problems that has to be sorted out by gravity. For each dangerous issue, the owner of the process has to define a technical solution for decreasing the risk. This technical solution is in most cases called a safety function. The set of all the safety functions represents the safety Instrumented System (SIS).

For instance, in the current example, 2 main risks are identified:

1. Risk of overfilling that can cause environmental damage
2. Risk of very high temperature that can cause an explosion, and can affect safety or life of people

- Definition of the safety function and their level of integrity

The safety function is an added function to a process with the goal of securing it. It is an additional layer of protection. This safety function must react automatically (without the need of any human intervention) and should put the process into a safe state when the probability of occurrence of the danger is too high.

Thus, each risk should be carefully studied, and according to 4 parameters (risk avoidance, proximity of people/environment, severity of potential damages and the probability of unwanted occurrence), an the integrity

[6] Keywords like the following ones: No, More than (more of, higher), Less than (less of, lower), the reverse, …

level must be allocated to each safety function, according to the following table.

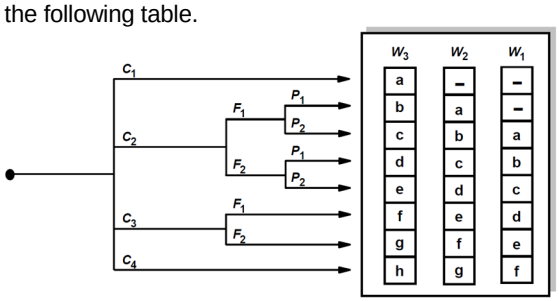

Figure 9: IEC 61511 Risk graph

With the parameters:

C: Consequence risk

C1: minor injuries of to a person; minor harmful influences on the environment

C2: serious, irreversible injuries of one or more persons or death of a person; temporary major harmful influences on the environment

C3: death of several persons; lasting major harmful influences on the environment

C4: catastrophic effects, many dead persons

F: Frequency and exposure time risk

F1: Rare to more often exposure in the hazardous zone

F2: frequently to permanently exposure in the hazardous zone

P: Risk avoidance

P1: possible under special conditions

P2: Almost impossible

W: Probability of the unwanted occurrence

W1: very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely

W2: slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely

W3: relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely

Then, the given letter should bring the safety integrity level to be implemented by the safety function according to the following table:

Necessary minimum risk reduction	Safety integrity level
-	No safety requirements
A	No special safety requirements
b,c	1
d	2
e,f	3
g	4
h	An E/E/PE safety-related system is not sufficient

Table 7 – IEC 61511 Risk graph and SIL

For instance, in the current example, there are two safety functions that have to be implemented in the process. Let us assume that the study has been performed and gives the following classification:

1. The overfill protection safety function should have a safety integrity of level 3 (SIL3)
2. The temperature regulation safety function should have a safety integrity of level 1 (SIL1)

- **Realization of the safety functions**

A safety function is generally composed of 3 main functional systems:

1) A sensor to detect the danger
2) A logic solver for the calculation of the information given by the sensor, and take a decision accordingly
3) An actuator, driven by the information sent by the logic solver, whose goal is to set the safe state of the process

The linear construction of sensor/logic solver/actuator implements a safety function, but according to the level of integrity, there can be more than one device in a functional system.

For instance, in the current example, SIL3 for the overfill protection needs a kind of redundancy if the device representing a sensor is only SIL2. Than would schematically be represented by the following figure:

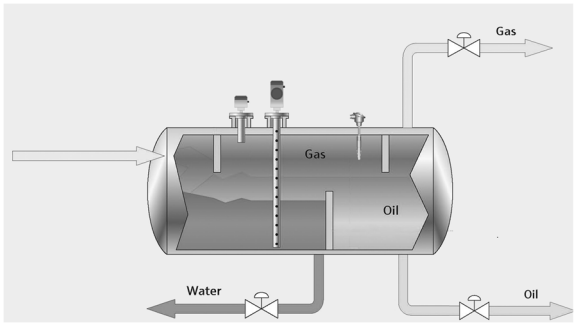

Figure 10: IEC 61511 example : safety devices

There are two SIL2 level devices to detect the maximum level in the tank, and one SIL2 temperature sensor for controlling the temperature inside the tank. (Logic solvers and actuators are not represented here.)

The choice of these devices for the implementation of the safety functions, can sometimes be difficult according to all the information (right or wrong) that end users are confronted with.

The first criteria is the function of the device: it should obviously fits with the process and other linked devices in the safety loop.

Then, the second criteria is the selection of a certified device / not certified device. A certified device is a device where some information required by IEC 61508 standard is available. After bringing in those justifications, the manufacturer of the safety device has 2 solutions: a self-certification that is possible according to the standard, or an certification by a third party (notified bodies or certification bodies in Europe), and of course, the last solution is preferable as the information given is checked by an external independent person.

The confidence and the value of certificates is given hereafter.

V. Can we trust on the SIL certificates

End users must be aware of the way the safety devices they use are assessed or certified. In some cases, SIL assessed or certified products may not comply with the end users applications. In addition, the instructions sheets and sometimes the certificates give restrictions for the use of these safety devices / safety function.

And here comes the problems !

In a lot of SIL certificates for safety devices, and their compliance to IEC 61508 and/or IEC 61511, the **prior use** [7]is used for the classification and justifications in a lot certificates.

Proven in use is often used instead of [8] **Prior use.**

In process industries, the standard reference for safety is IEC 61511.

If for a safety logic solver (e.g. safety PLC in grey color on the following figure) the definition of what is authorized is clear, what is possible with sensors and actuators devices (in dark color on the following figure) is not so clear and is subject for discussion/interpretation.

So the answer for this question : What we can find in SIL certificates ? EVERITHING.

Everything is possible because :

1) anyone can write a certificate because there are no regulation for issuing such certificates
2) anyone can avoid hardware fault tolerance constraint on architectures requirements (defined in IEC 61508) and can claim that a general purpose sensor / actuator can reach SIL2 or SIL3 level only on the basis of calculations based on prior use.

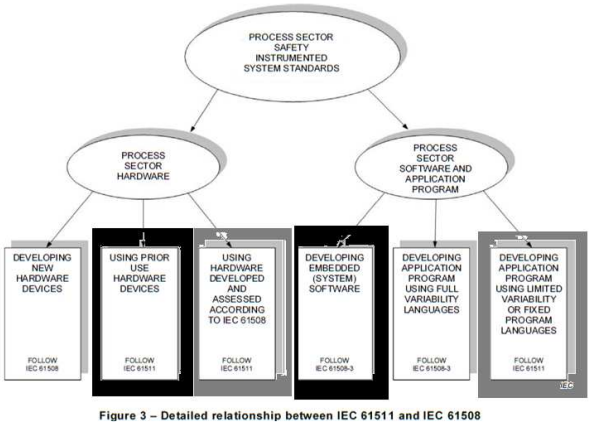

Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

Figure 11: IEC 61511 : scope & interpretation

Because sensors and actuators are subject for discussion/interpretation in different ways, never end discussions can appears and sometimes (every times) only the calculations remains and the HFT requirements defined in IEC 61511 are forgotten e.g;

- chapter **11.4.2** When the SIS can be split into independent SIS subsystems (e.g. sensors, logic solvers and final elements), then the HFT can be assigned at the SIS subsystem level.
- chapter 11.4.3 (…) The HFT of the SIS or its SIS subsystems should be in accordance with;
  - 11.4.5 to 11.4.9 of clause 11 or,
  - the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
  - the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

  NOTE The route developed in IEC 61511 is derived from route 2H of IEC 61508-2:2010.

  Even if there are restrictions for devices or architectures both in IEC 61511 and IEC 61508 (see table 2 & 3 of the standard), you can find in the market devices that do not comply to the requirements of both IEC 61508 and IEC 61511.

SIL	Minimum required HFT
1 (any mode)	0
2 (Low demand mode)	0
2 (High demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

Table 8 – Minimum HFT requirements according to SIL (from IEC 61511 Table 6)

[7] Defined in IEC 61511-1:2016

3.2.51 : **prior use** : documented assessment by a user that a device 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.

[8] **3.2.51** : Note 2 to entry: **Proven in use** is based on the manufacturer's design basis (e.g., temperature limit, vibration limit, corrosion limit, desired maintenance support) for his device. Prior use deals with device's installed performance within a process sector application in a specific operating environment which is often different than the manufacturer's design basis

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2 C[9]	SIL 3
60 % – < 90 %	SIL 2 LD	SIL 3 HD, C	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 9 – IEC 61508 Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2 C	SIL 3
90 % – <99 %	SIL 2 LD	SIL 3 HD, C	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 10 – IEC 61508 Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Requirements for the selection of devices based on prior use (chapter 11.5.3).

VI. IEC 61511 requirements : comparison with the field of ATEX, machines and processes

Depending on different industrial sectors, the way to accept routes and architecture constraint of IEC 61508, is different :

- In the **machinery sector**, covered in Europe by the machinery directive 2006/42/EC
  - a standard, based on IEC 61508 give requirements for the realization of the machines & safety control system : The IEC 62061 standard [6],
  - an other standard for machinery (ISO 13849-1/2 [7]) can also be used.

  In both standards for machinery only route 1H is allowed that means that **prior use** is strictly forbidden (see provisions of the standards).
- For **ATEX sector**, safety devices are defined according to EN 50495. In this standard not all architectures of IEC 61508 are possible for the realization of the safety function, and if **prior use** is not strictly forbidden, it is not mentioned in the standard. Only route 1H is described.

So in machinery sector, devices must reach the architecture constraints defined in IEC 61508 and the devices covered in most cases under the wording "*Logic unit*" to ensure safety functions defined in annex IV item n°21 of machinery directive 2006/42/EC. These safety devices are under the scope of specific assessment by a notified body that delivers an EC type examination certificate, that allows the device manufacturer to put the product on the market.

VI. CONCLUSION

Today, end users are lost to choose SIL safety devices assessed or certified because.

- of safety standards that are written by specialists for specialists with an alien strange language, a lot of complicated calculations.
- Of no regulation for the certification of these safety devices that allows huge consultants to issue so-called certificates.
- Of an increasing market of safety devices that do not comply all the time with the requirements of the safety standards IEC 61511 & IEC 61508.

End users that are not specialists in functional safety, rely on certificates and are happy when they find a value that reaches the requirements they have to fulfill or they have to justify.

IEC 61508 and IEC 61511 identify two routes for the classification of the safety devices.

- Route 1H and
- Route 2H

If route 1H is the royal way, with a lot of constraint that is strict and for which the safety device has to fulfill a huge number of technical requirements, route 2H is the simplest and is based mainly on data field return.

With the justification based on statistics and calculations, a lot of SIL certificates are based on route 2H approach mainly to give an answer for process industries where IEC 61511 allows the classify of these products.

So all requirements, defined in route 1H, in terms of additional features to build safety e.g. :

- Architecture
- Internal self tests
- Additional requirements for software
- Additional requirements for EMC compliance through IEC 61326-3-1 [3] specific requirements
- …

Are not fulfilled and some SIL certificates can claims a SIL level for general purpose devices.

In other industrial sectors e.g. machinery and ATEX, the route 2H is not allowed. A full demonstration of compliance to all requirements of IEC 61508 / IEC 62061 is requested. In addition in Europe, the certification of the safety devices used in machines are under the regulation of machinery directive 2006/42/EC, and only a limited number of notified bodies can issue certificates.

[9] **C** : continuous, **HD** High Demand, **LD** : Low Demand

My advice :

SIL Certificates must be read with rigid and cautious attention, especially for the limitation of the scope of the certification and the route that has been used for the certification !!

Do not believe in all shown certificates. Verify the content, limitations and the “certification body”.

VII. REFERENCES

[1] IEC 61511 : FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR

[2] IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems

[3] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)

[4] DIRECTIVE 2014/34/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (recast)

[5] DIRECTIVE 2012/18/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC

[6] IEC 62061 2005 + A1 & A2 :2015 : Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

[7] ISO 13849-1:2015 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
ISO 13849-2:2012 : Safety of machinery - Safety-related parts of control systems - Part 2 : validation

[8] IEC 61326-3-1: 2017 : Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1 : immunity requirements for safety-related systems and for equipment intended to perform safety - related functions (functional safety) - General industrial applications

VIII VITA

Eric FAE – INERIS Notified Body For ATEX 2014/34/EU directive and ExCB for IECEx certification Scheme – Member of standardization groups for the machinery sector (IEC 62061, ISO 13849) and drive systems (IEC 61800-5-2). Mr. FAE was born in France and has an Engineering education in the field of Electrotechnics (Master). He is an MBA graduated from PANTHEON SORBONNE University. He has worked for 25 years in the field of functional safety in Space, Avionics and Military Industries and since 1995 at INERIS in Machinery and Processes sector for functional safety certification. He is in charge of mandatory and voluntary certification for Machinery directive 2006/42/EC, Functional Safety (IEC 61508, IEC 61511, IEC 62061, EN 13849-1/2, ...) and for safety devices in ATEX.
eric.fae@ineris.fr

Fabrice MARCEL – KROHNE SAS – Functional Safety Professional in charge of functional safety assessment for level division (divisional level). Mr. MARCEL was born in France and has an Engineering qualification in the field of Computer Sciences. He has worked for 20 years as a software development and software quality engineer for the safety environmental markets such as railway transport, aeronautics and military industries. He is in charge of the application of IEC/EN 61508 standard an is responsible for safety for Krohne level devices.
F.Marcel@krohne.com