Functional Safety for Safety-Related Systems: 10 Common Mistakes

Florent Brissaud, Didier Turcinovic

Functional Safety for Safety-Related Systems: 10 Common Mistakes

F. Brissaud
FMDS industrie (.fr) / RAMSindustry (.eu), France

D. Turcinovic
IR&IS, France

ABSTRACT: The functional safety is the part of the overall safety relating to equipment/ system/ installation and their control systems that depends on the correct functioning of the safety-related systems. Due to the critical role of safety-related systems for managing risks, international standards have been developed to provide guidelines and requirements for all their safety lifecycle activities. The IEC 61508 and IEC 61511 are now recognized all around the world and have become the references for the best practice of functional safety. However, a decade of on-the-filed functional safety experience has shown that several concepts used in these standards are still subject to common mistakes in their interpretation or implementation, which may result in significant loss of safety. This paper proposes a review of ten common mistakes in functional safety, relating to: Safety Lifecycle (SLC), Functional Safety Management (FSM), Safety Integrity Level (SIL), Safety Requirement Specification (SRS), PFDavg and PFH, System architecture "M-out-of-N" (MooN), "Safe Failure Fraction" (SFF), and Certification. This review aims at contributing to a better practice of functional safety.

1 INTRODUCTION

Safety-related systems are designed to implement safety functions in order to achieve or maintain safe states of equipment/ system/ installation, in respect to specific hazardous events. In this context, the functional safety is the part of the overall safety relating to equipment/ system/ installation and their control systems that depends on the correct functioning of the safety-related systems.

Due to the critical role of safety-related systems for managing risks, international standards have been developed to provide guidelines and requirements for all their safety lifecycle activities. Notably, the IEC 61508 functional safety standard (IEC, 2010) provides a generic approach for all the electrically-based safety-related systems. Based on the IEC 61508, product and application sector standards have then been developed, such as the IEC 61511 (IEC, 2004) for the Safety Instrumented Systems (SIS) used in the process industries.

The first edition of the IEC 61508 has been issued in the late 1990's and the second edition has been published in 2010. The first edition of the IEC 61511 has been issued in the early 2000's and the second edition should be published soon. These standards are now recognized all around the world and have become the references for the best practice of functional safety. However, a decade of on-the-filed functional safety experience has shown that several concepts used in these standards are still subject to common mistakes in their interpretation or implementation. These common mistakes cover technical, organisational, and managerial topics and may result in significant loss of safety.

This paper proposes a review of ten common mistakes in functional safety, which have been observed several times in the industry for these last years. This review aims at contributing to a better practice of functional safety.

2 TEN COMMON MISTAKES

2.1 *Safety Lifecycle (SLC)*

Both the IEC 61508 and IEC 61511 standards state the importance of the Safety Lifecycle (SLC) concept. The SLC is fundamental for the application of the standards' content because it constitutes the "technical framework" for dealing "in a systematic manner with all the activities necessary to achieve the required safety integrity for the safety functions" (IEC, 2010, Part 1: Sub-clause 7.1.1.1) of the safety-related systems. The SLC, as described in the IEC 61508 and IEC 61511, is presented in Figures 1 and 2, respectively.

The SLC can be compared to a road map or, more accurately, to a temporal map. It provides a graphical description of the itinerary to be followed, phase by phase, for the project execution.

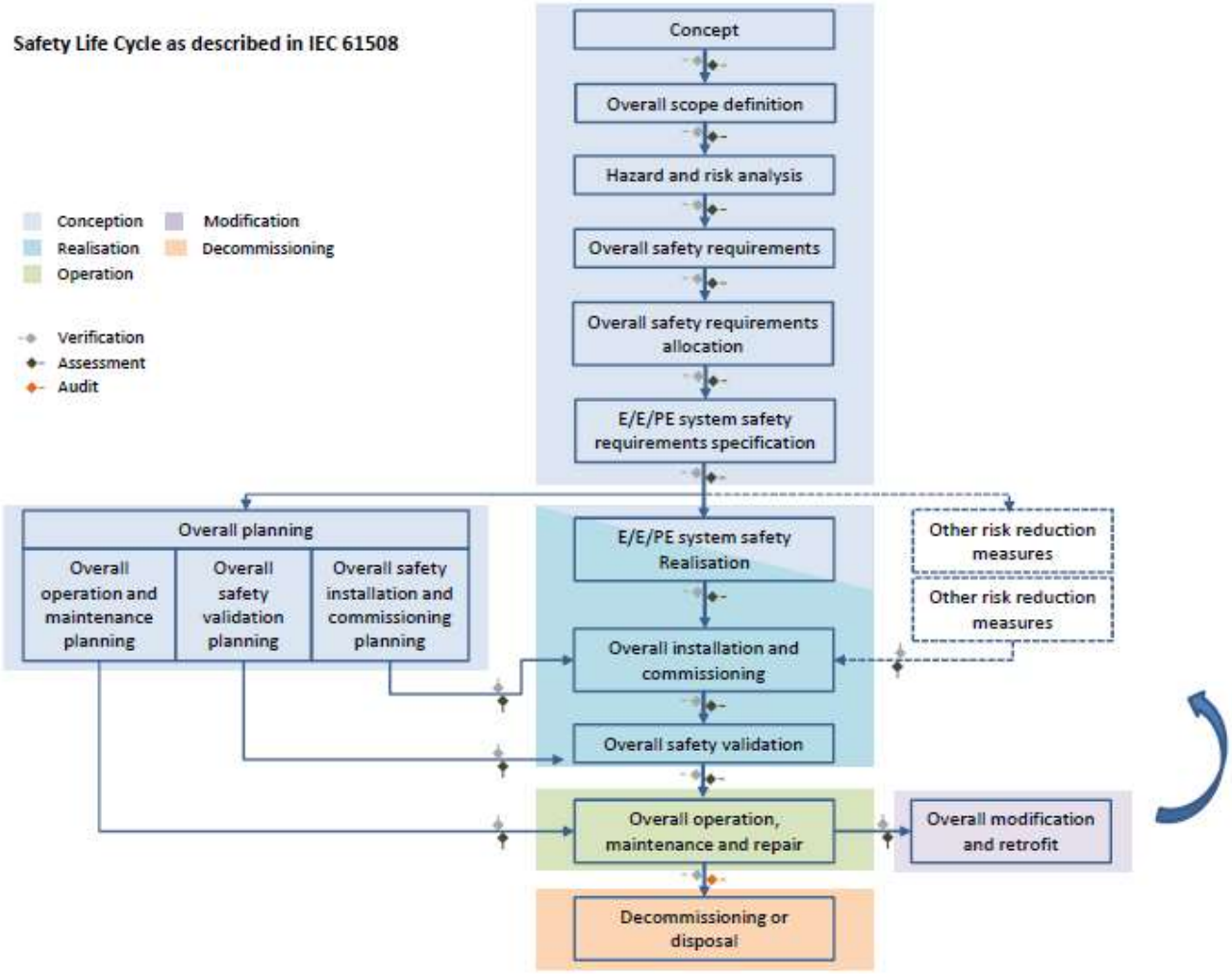

Figure 1. Safety Lifecycle (SLC) as described in IEC 61508 (IEC, 2010)

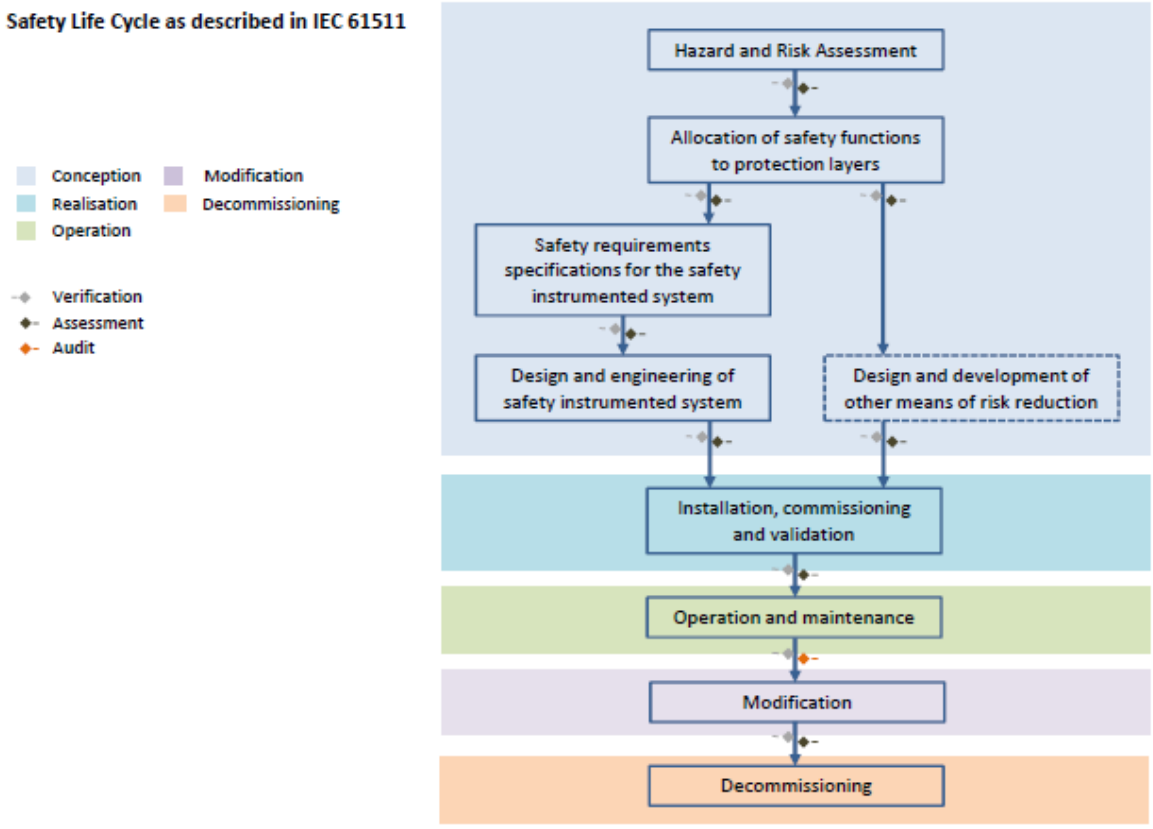

Figure 2. Safety Lifecycle (SLC) as described in IEC 61511 (IEC, 2004)

A phase corresponds to a period where specific activities take place. Each phase is fed by the previous ones in a specific order materialized by arrows (cf. Figures 1 and 2). The various phases are organised in five key categories, which reflect the lifecycle of any manmade construction: conception (including analysis), realisation, operation, modification, and decommissioning

In addition to the project flow description, the interest of having an SLC is to provide for each phase a systematic identification of: (a) the activities to be carried out; (b) the competences required to carry out the activities; (c) the distribution of the responsibilities among professional team members, services and organisations; and (d) the required documentation, including inputs, scope, procedures, templates, reports, and deliveries, to be passed on to the next phase.

The systematic approach is also strengthened by two "gates" (at the exit of each phase) that must be crossed before moving further: verification and assessment (cf. Figures 1 and 2). These activities are intended to be executed by independent parties, that is, separate and distinct from those who actually performed the task (or who is responsible for it), and who are not related through their management lines. These gates guarantee: the technical correctness of the deliveries, as originally specified; and the truthfulness of the functional safety achieved, as a result of the follow-up of the adopted procedures and plans.

Last but not least, the functional safety management (FSM, cf. below) is required across the entire SLC. This implies organisation and resources, planning, implementation, monitoring and activities coordination.

In the industry, the SLC concept is generally embraced but, when it comes to users' projects, the actual application is regularly in conflict with the overall project planning. There is a lack of an upfront integration and, as a result, the SLC is no longer interpreted as a temporal map but as a check list. Therefore, a common mistake that takes place for a given phase is that all previous activities are ticked as being duly completed, and documentation is produced as the evidence, but they have not necessarily been performed in the right sequence. Typical example is the validation phase where the activities are performed without the suitable Safety Requirement Specification (SRS, cf. below). Subsequently, the SRS is revised and, now, the remaining question is the confidence level we may have in the purpose of the project when the documentation portrays more the realisation rather than the actual needs. This case illustrates the introduction of nasty organisational systematic failures, arduous to identify when encountered.

2.2 *Functional Safety Management (FSM)*

The IEC 61508 and IEC 61511 standards call for Functional Safety Management (FSM) and clearly express the necessity of it for each phase of the SLC (cf. above). FSM requires organisation, resources and specialist activities. Yet, the figure of the functional safety manager is not explicitly mentioned.

Within any company, all activities (e.g. operations, sales, human resources, accounting, etc.) and relating resources are managed, and have a designated managerial figure that is responsible for each of them. Being responsible is usually defined as being accountable for one's actions and decisions. When a mishap occurs, this is commonly interpreted as one being amenable, answerable or liable. However, "responsible" would rather be looked at when activities follow their normal course, and interpreted using the etymology as being "capable to respond". Then, a responsible individual looks more as the figure that is capable to perform and achieve what is expected, and less the one that is liable for what is unexpected. A proper responsible professional achieves the expected when the person is competent in the given assignment, in possession of means for its accomplishment, and invested with the required authority for its execution.

FSM is due across the entire SLC. This may represent 20 to 40 years and that is more than one's average professional career duration. So, there is a necessity to perform FSM with continuity in time and athwart all stakeholders' organisation. This is a fundamental need for maintaining the functional safety over time. However, it has been observed that organisations are usually not well prepared, equipped or ready to follow up the very same project over a long period of time with continuity. The challenge is also growing when providers are involved. For example, a simple maintenance action could imply the operation and maintenance teams as well as the purchasing and logistic departments on the site end; and the technical support, shipping and repair departments on the supplier end. Theoretically, all these entities should contribute directly or indirectly for keeping the PFDavg or PFH (cf. below) as it was originally calculated. FSM then requires determining explicitly who coordinates that this information is known by all at any time and that maintenance actions are performed as designed.

A second common trouble is that project management is usually short term orientated while the FSM is long term oriented, over the entire SLC. The drives over these distinct periods of time are usually conflicting and short term is given a higher priority by higher level of authorities within organisations, leaving FSM subservient. But, who represents FSM? How many organisation charts show the functional safety manager position?

2.3 *Safety Integrity Level (SIL)*

The safety integrity is an attribute to a safety-related system with regards to safety functions. It is defined by a probability of a safety-related system satisfactorily performing specified safety functions. The Safety Integrity Levels (SIL) are classes, ranging the safety integrity from SIL 1 (for the lowest integrity level) to SIL 4 (for the highest integrity level). Depending on the applied functional safety standard, the safety integrity (and thus the SIL) concept is restricted to electrical/ electronic/ programmable electronic (E/E/PE) safety-related systems (for IEC 61508) and to Safety Instrumented Systems (SIS) (for IEC 61511). However, this concept can be easily extended to other systems.

Based on the hazard and risk analysis, the allocation phase (among the other activities defined in the SLC, cf. Figures 1 and 2) aims at determining the target SIL of the required safety functions, in order to achieve the necessary risk reduction. The SIL aims at specifying the safety integrity requirements (reported in the SRS, cf. below). Those include requirements related to systematic safety integrity, hardware safety integrity, and software safety integrity. It is then the purpose of the design/realisation phase to verify that the safety-related system meet these requirements. Notably, the hardware safety integrity requirements deal with architectural constraints (where the SFF may appear, cf. below) and quantification of the effect of random failures (PFDavg or PFH, cf. below).

If it is common to see "SIL reports" or "SIL certificates" that consider hardware safety integrity, it should be noted that other requirements are often omitted, notably those related to systematic safety integrity and software safety integrity. In the worst cases, it can be also observed that a SIL is directly deduced from a PFDavg calculation or (less often) from a simple verification of architectural constraints. This is wrong. In fact, for a given SIL, several other requirements are also requested to be met. Any "SIL report" should therefore define precisely the limitations in terms of safety requirements. Moreover, a "SIL certificate" cannot pretend that a given SIL is reached if the whole of safety requirements are not met.

Finally, it should be reminded that a SIL always refers to a safety function and, therefore, it is inappropriate to assign a SIL to a safety-related system without specifying the safety function.

2.4 *Safety Requirement Specification (SRS)*

The Safety Requirement Specification (SRS) phase follows the allocation phase in the SLC (cf. Figures 1 and 2), and provides the inputs of the design/realisation phase.

The SRS objective is to define the safety-related system requirements, in terms of safety functions and safety integrity requirements. The IEC 61511 standard provides a list of 27 requirements to be specified for Safety Instrumented Systems (SIS) in the process industry sector (IEC, 2004, Part 1: Sub-clause 10.3.1).

It is important that the SRS describe the safety functions and their required functional safety performances (which includes safety integrity) in terms not specific to the equipment. In fact, the equipment designers can use the SRS as a basis for selecting the equipment items and architectures. Then, the next SLC phases (and notably the design/realisation phase) allows verifying that the safety-related system meet all the requirements specified in the SRS. This is why the SRS should be "clear, precise, unambiguous, verifiable, testable, maintainable, feasible" and "written to aid comprehension by those who are likely to utilise the information at any stage" of the SLC (IEC, 2010, Part 1: Sub-clause 7.10.2.4).

When the SRS is performed while a specific safety-related system is already intended or implemented, a common mistake consists in describing the current technological choice without impartial consideration for the safety requirements. For example, the response time requirement is sometimes wrongly defined by the actual respond time of safety function instead of "the time within which it is necessary for the safety function to be completed" (IEC, 2010, Part 1: Sub-clause 7.10.2.6). In that case, the SRS is useless and dangerous systematic failures cannot be prevented. Regarding the safety integrity requirements, it is also curious to see that some SRS specify a "target contribution to the PFDavg" (cf. below) for each subsystem of the safety-related system (for example, 30% for sensors, 20% for logic solver, and 50% for final elements). Even if these contributions could be observed in practise, what would be the safety reason for specifying them in the SRS?

2.5 *Average Probability of dangerous Failure on Demand (PFDavg)*

The computation of the average probability of a dangerous failure on demand (PFDavg) is required for safety functions operating in a low demand mode (only performed on demand, with a frequency of demands that is no greater than one per year). This takes part of the hardware safety integrity requirements, and more precisely of the quantification of the effect of random hardware failures. The PFDavg is the achieved safety integrity of the safety-related system due to random failures, and shall be below the target value specified in the SRS (cf. above).

The PFDavg is computed as a mean unavailability and takes several characteristics into account: system architecture, failure rates[1], common cause failures, intervals and effectiveness of tests, repair times, and random human errors. Several methods can be used, including approximate equations, reliability block diagrams, fault trees, (multi-phase) Markov models, (stochastic) Petri nets (with predicates). Under conditions, all these methods are able to provide "good" results, taking the characteristics required by the IEC 61508 standard into account. However, it is required to know the method that is used well (notably in terms of intrinsic assumptions) and to use an appropriate and efficient software tool. The choice of a method should therefore not be determined by dogmatic assumptions, but should result of a balance between modelling effort and objectives, given the properties of the system to be modelled (Brissaud & Oliveira, 2012).

Notably, it should be noted that if approximate equations provide a fast and simple way to assess many simple/basic systems, it is also, by nature, the least flexible approach. Unfortunately, some users then apply such formulas without the required cautions on the predefined assumptions. In particular, hazardous situations may occur when "non-conservative" assumptions are done. Actually, when approximate equations are used, it is even seldom to see a proper description of all the assumptions that have been considered.

2.6 *Average, maximum, and on-demand values*

Fundamentally, the safety-related systems are designed to reduce the frequency (or probability) of a hazardous event and/or its severity. This risk reduction then aims at meeting the tolerable risk for this specific hazardous event.

The PFDavg (cf. above) provides an interesting indicator for the risk reduction, even so, this indicator is not exhaustive. In fact, the PFDavg is based on an average value of the unavailability of the safety-related system to perform the specified safety function when a demand occurs. The PFDavg makes fully sense when the demand for the safety function occurs uniformly. If there are intervals of time (e.g. start-up, maintenance, manual mode, etc.) where demands are assumed more frequent, then specific mean unavailabilities (computed within these intervals) should be also considered. For example, if there is a very short interval of time within the system lifetime (e.g. 30 seconds over 4 years) where, due to specific conditions, the probability that a demand occur is very close to one and the unavailability of the safety-related system is also very close to one, therefore the risk will be very high. However, as an average value, the PFDavg can still show a "very good" result (the order of magnitude of 30 seconds over 4 years is 10^{-7}, which can fit SIL 4).

As a complementary indicator, it is therefore often very useful to consider the maximum value of the unavailability of the safety-related system to perform the specified safety function when a demand occurs (usually denoted PFDmax).

Finally, it should be also noted that it may exist dependencies between the unavailability values (PFDavg or PFDmax) and the demands themselves. Notably, the IEC 61508 standard specifies that, in addition to the time dependent failures characterised by failure rates, there also exists on demand failures caused by the demands of the safety function (IEC, 2010, Part 4: Sub-clause 3.6.18). The latter can be characterised by a "probability of failure per demand (denoted by γ)".

2.7 *Average frequency of a dangerous failure per hour (PFH)*

The term "Probability of dangerous Failure per Hour" (PFH) has been introduced in the first edition of the IEC 61508 standard. This term was inappropriate because a probability is always unitless and, therefore, cannot be "per hour". Actually, the PFH is not a probability but a frequency. This is why in the second edition of the IEC 61508 standard, the PFH has been redefined by the "average frequency of a dangerous failure per hour". The acronym PFH is still in use for the continuity, but the term "Probability of dangerous Failure per Hour" has not to be used anymore.

The PFH is used instead of the PFDavg (cf. above) when the safety functions operate in a high demand or continuous mode of operation (when the frequency of demands is greater than one per year). The PFH is defined as an average frequency of (dangerous) failure. A frequency of failure is equivalent to an "unconditional failure intensity" and should not be confused with a "failure rate". Simply, the unconditional failure intensity[2] is linked to the unavailability[3] while the failure rate[4] is linked to the unreliability[5]. That is, the first takes the repair times into account, contrarily to the second.

[1] The selection of the failure rates is an issue that has been discussed several times in the literature. For example, refer to (Hauptmanns, 2008).

[2] The unconditional failure intensity is the conditional probability per unit of time that the item fails between t and t + dt, provided that it was working at time 0 (ISO, 2013).

[3] The unavailability is the probability for an item not to be in a state to perform as required at a given instant (ISO, 2013).

[4] The failure rate is the conditional probability per unit of time that the item fails between t and t + dt, provided that it has working over {0, t} (ISO, 2013).

[5] The unreliability is the probability for an item to fail to perform a required function under given conditions over a given time interval {0,t} (ISO, 2013).

When the failure rate is constant and when failures are quickly detected and repaired, these two measures are close together. Moreover, the average failure rate is basically greater than the average failure intensity. Therefore, it is not really "dangerous" to consider that the PFH is an average failure rate instead of an average unconditional failure intensity. However, it is curious to observe that several references (including some "official" handbooks) use a wrong definition. Nevertheless, it is always regrettable that references feed confusions such as probability (unitless) versus frequency (per time unit), and frequency (which considers repairs) versus failure rate (which only refers to reliability).

2.8 *System architecture "M-out-of-N" (MooN)*

The system architecture has to be taken into account for the quantification of the effect of random hardware failures (PFDavg or PFH, cf. above). Usually, a safety (instrumented) system is considered as a serial system of three subsystems: sensor(s), logic solver(s), and final element(s). That is, the system is able to perform its safety function if and only if all these subsystems are able to perform their safety sub-functions. Moreover, each subsystem is basically defined by an "M-out-of-N" (MooN) architecture. That is, it is composed of N elements (i.e. channels) and is able to perform its safety sub-function if any M or more elements (of N) are not in a dangerous failure state. By definition, a 1ooN architecture corresponds to a parallel subsystem (the "safest" architecture) and a NooN architecture corresponds to a serial subsystem (the "least safe" architecture).

It should be highlighted that the success criteria of a MooN architecture is "any M or more elements of N". The word "any" is very important. Notably, this implies that all the N elements have to be solicited by the demand scenarios of the safety sub-function. As a first example, let consider 8 sensors that measure the vibrations of a compressor: 4 in part A and 4 in part B. The instrumentation logic is defined such as 2 measures of excess vibrations command the compressor trip. Would this subsystem architecture be 2oo8? The answer is yes only if the possible vibration scenarios always imply excess vibrations in both part A and part B of the compressor (based on the vibration limits defined for each sensor). If there exists a scenario where only one part is subject to excess vibrations, then the subsystem architecture would be 2oo4 (because only 4 sensors would be solicited). As a second example, let consider 4 sensors that detect smoke at different places in a room. The instrumentation logic is defined such as a single detection of smoke commands the alarm. In case of fire, if the smoke reaches all the 4 sensors, then the subsystem architecture would be 1oo4. However, it could be too late to wait that all the sensors are solicited and, in most cases, the alarm has to be activated as soon as one sensor detects smoke. Therefore, the subsystem architecture would be, in that case, 1oo1 (even if there are 4 sensors installed).

Depending on the (real) subsystem architecture, it could be required to use a method such as fault trees or Petri nets to quantify the effect of random hardware failures. However, mistakes in the subsystem architectures could lead to dangerous underestimations of the PFDavg or PFH (cf. above examples). Moreover, it should be noted that approximate equations provided by the IEC 61508 standard (Part 6) is also limited to MooN architectures where all the N elements have identical failure rates, testing and repair policy. In other cases, a method such as fault trees is more appropriate.

Another consideration for system architecture is that all the elements defined as part of a sub-system have to refer to a specific safety function. Since a functional safety assessment always refers to a safety function, it is required to limit the scope to elements that contribute to this function. The most common case concerns the "cascading" final elements that sometimes appear in a subsystem architecture while they should not be. For example, it is obvious that tripping a compressor or closing the upstream of a vessel require other actions to be performed, such as unit isolation, depressurisation, venting or flaring, in order to prevent collateral effects. However, these collateral effects have to be covered by (other) specific safety functions (with dedicated safety requirements) that should be assessed as such.

2.9 *"Safe Failure Fraction" (SFF)*

The "Safe Failure Fraction" (SFF) has been introduced in the first edition of the IEC 61508 standard, as a criteria to be used for the architectural constraints, taking part of the hardware safety integrity requirements. The SFF is defined by the sum of the average failure rates relating to safe failures (detected or undetected online) and dangerous failures detected online, divided by the sum of the average failure rates relating to safe failures (detected or undetected online) and dangerous failures (detected or undetected online). By definition, only the dangerous failures prevent the safety function from (or decrease its probability of) operating when required; while the safe failures result in the spurious operation of the safety function (or increase its probability). Other kinds of failures, such as "no part" and "no effect" failures, are not used for the SFF calculation – Refer to (IEC, 2010, Part 4) for all definitions.

In practice, a high SFF can "justify" (according to the IEC 61508 standard) a lower redundancy (i.e. hardware fault tolerance) for a given SIL. The SFF has therefore become a commercial argument for

vendors because, to perform a safety function in accordance with a given SIL, a user selecting a product with a higher SFF can avoid adding redundancies (and therefore additional items). However, the use of the SFF as a safety criteria is a lack of discernment. In fact, it is easy to see that the SFF can be artificially increased just by adding (or overestimating) safe failures. To make it clearer, if a vendor adds within its element a kind of "box" that creates random spurious operations of the safety function, therefore the SFF will be higher. For a given rate of dangerous failures (detected and undetected online), it is not opportune to consider that an element is "better" (with a lower requirements on redundancies) if the rate of safe failures is higher, which is an intrinsic assumption of the SFF. A practical issue is that "safe" failures occurring too frequently can even be dangerous for two reasons: additional maintenance operations are required, with human exposure and possible human errors; and when equipment items provoke too much spurious operations, it is tempting to bypass them. To sum-up, to give credence to the SFF is at best useless and at worst counterproductive and then dangerous. (Note that the SFF should not be confused with the diagnostic coverage (DC), which is not challenged.)

The use of the SFF has been questioned several times in the literature (Langeron *et al.*, 2007; Innal *et al.*, 2006). Then, the second edition of the IEC 61508 standard has developed an alternative "route" (the so-called "2H", "based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified SIL"), where the architectural constraints can be achieved without regard for the SFF. However, a major restriction for using this "route" is that "the reliability data used when quantifying the effect of random hardware failures" (PFDavg or PFH, cf. above) shall be based on "field feedback for elements in use in a similar application and environment" and "data collected in accordance with international standards" in order to "estimate the average and the uncertainty level[6]" (IEC, 2010, Part 2: Subclause 7.4.4.3.3). This alternative is therefore only applicable to systems already in use and with proper feedback data available. As a consequence, the SFF is still frequently used because of the most common "route" (the so-called "1H," "based on hardware fault tolerance and safe failure fraction concepts"). One reason for keeping the concept of SFF is probably the continuity with the first edition of the IEC 61508, however, commercial lobbies could also play a role. Anyway, "Route 2H" shall be preferred than "Route 1H" as far as possible, and a safety objective should be to reduce the use of the SFF until it is fully removed.

[6] For discussions on uncertainty analyses, refer for example to (Brissaud et al., 2010).

2.10 *Certification*

Today, in the industry, almost everything is certified or certifiable: components, equipment, systems, professionals, organisations and, in some instances, even plants. However, it should be noted that certification is not a requirement of the IEC 61508 or IEC 61511 standards. As a matter of fact, the terms "certificate" or "certification" cannot be found within these texts, except in the forewords mentioning that: "Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity" and that "IEC is not responsible for any services carried out by independent certification bodies" (IEC, 2010, Foreword). These standards simply provide references for the current state-of-the-art or good engineering practices in functional safety. The certification is a process through which a sufficiently independent, qualified and trustworthy entity attests that the claimed features or functionalities of a good or a person conforms to these references, at a given time and at a verifiable level of dependability.

The SIL (cf. above) stated on a certificate should be considered only as a simple visa of entry on a business passport. This would grant the right for a device to be counted as potentially eligible in a project. A common industrial error is that, too often, we are satisfied with the assertions provided on the certificate and do not necessarily investigate further more. This business passport is often reckoned as sufficient and, therefore, thought the certificate is a shield to protect oneself. Negotiations on commercial terms are then initiated and follow their due course. However, in case of an unfit detail, the user is usually doomed to find about it during integration, validation, or worse during operation along with its potential critical consequences.

A second technical passport should be considered, revealing the actual technical fitness of the selected device for the project. This means a check on compliance with the criteria of the standards, including hardware, software, FSM (cf. above), and documentation requirements. This means a careful analysis on coherence and compliance of the information provided in the certificate, as well as the practical impact, throughout the SLC (cf. above), of all the possible assumptions considered to elaborate it.

In addition, the technical passport ought to include information that can be found in the certificate report and the manufacturer's safety manual. The certificate report provides details on the certification activities and could point out valuable data on limits and conditions used for asserting the device compliance. These data should be compared to the actual project limits and conditions. The manufacturer's safety manual covers both hardware and software aspects and gives information on functional specifi-

cation, configuration management, constrains and/or assumptions on the device. Notably, it is interesting to see that the safety manual concept became a requirement in the second edition of the IEC 61508 standard. This outlines the trend in the industry: we ought to delivery and comprehend sound information to demonstrate the integrity of the safety functions planned to protect an operation.

3 CONCLUSION

This review of selected ten common mistakes in functional safety, met in the industry, reveals that they could result from misreading of standards, missed defined targets, or misalignment between existing and required practices. Now, the question of interest that springs in mind is how could it be possible to correct this situation?

In 2010, when the second edition of the IEC 61508 was released, it was among the 10 top bestselling of the IEC standards[7]. There is therefore no doubt that functional safety is of interest in the industry and that professionals are eager to know the content of these standards. However, once the books are opened, their content appears dense, with a high level of complexity, and performance orientated. All stakeholders in a project are designated in the standard, by means of procedures, as contributors to achieve the expected performance and to keep it over time. This is a major challenge as all parties in a project do not necessarily have aligned interests. Moreover, their due contribution level is not necessarily aligned with their own business focus.

Today, some equipment and technology have suitable design and performance levels, complying with functional safety requirements of the IEC standards. This is a great success achieved in the industry and this is also what most players retain. However, this is only a first step. Much more is due to insure proper functional safety of equipment. The common mistakes reviewed in this paper show where weaknesses are. They lay in the foundations of functional safety, notably regarding to safety lifecycle, management, and safety integrity level. In addition, each project application is unique, subsequently distinct and specific measures are to be elaborated, followed and supported case by case. Readily available recipes can be useful but certainly not a panacea. Sole competent professionals who received formal education in the field, who have knowledge and experience, and who have means and authority can insure that functional safety performance is safeguarded and adequate. This is all what matters from the point of view of the standards and should for all people involved in running a plant.

[7] www.iec.ch/about/annual_report/2010/financial/sales.htm

4 REFERENCES

Brissaud, F., Barros, A. & Bérenguer, C. 2007. Handling parameter and model uncertainties by continuous gates in fault tree analyses. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 224(4): 253-265.

Brissaud, F. & Oliveira, L.F. 2012. Average probability of a dangerous failure on demand: Different modelling methods, similar results. *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012* 8: 6073-6082.

Hauptmanns, U. 2008. The impact of reliability data on probabilistic safety calculations. *Journal of Loss Prevention in the Process Industries* 21(1): 38-49.

IEC, 2010. *IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, 2nd edition.* Geneva: International Electrotechnical Commission.

IEC, 2004. *IEC 61511, Functional safety – Safety instrumented systems for the process industry sector, 1st edition*. Geneva: International Electrotechnical Commission.

Innal F., Dutuit Y., Rauzy A., Signoret J.P., 2006. An attempt to understand better and apply some recommendations of IEC 61508 standard. *Proceedings of the 30th ESReDA seminar*: 1-16.

ISO, 2013. *ISO/TR 12489, Petroleum, petrochemical and natural gas industries -- Reliability modelling and calculation of safety systems*.

Langeron, Y., Barros, A., Grall, A. & Bérenguer, C. 2007. Safe failure impact on safety instrumented systems. *Proceedings of the European Safety and Reliability Conference 2007, ESREL 2007 - Risk, Reliability and Societal Safety* 1: 641-648.