Functional Safety: Finding the right balance

Hervé Vaudrey[a], Managing Director EMEA Process Safety, DEKRA Insight, herve.vaudrey@dekra.com

Clive de Salis, Process Safety Specialist, DEKRA Insight, clive.desalis@dekra.com

[a] DEKRA Insight, Sunstone Bat 2A, 22 avenue Lionel Terray, 69330 Jonage, France

The different functional safety guides and standards, such as IEC61508/61511 which impose a formal scheme for the safety instrumented functions, have allowed huge improvements in process safety to be made over the last 30 years, making operations less manual and safer. It has also allowed a number of industrial disasters to be avoided by automatically triggering and activating the purposely planned and designed layers of protection.

Still, one can observe a drift in the application of those standards in the process industry which often leads to increased costs, loss of operability and more worrying to a false sense of reduction of the process incident risk.

Having too few safety instrumented functions is generally not sufficient to 'compensate' for the low reliability of human actions but having too many can compromise the operability of an over-engineered plant. A possible consequence is that operators will end up bypassing the safety instrumented function that is spuriously tripping too frequently leading to process interruption or even an emergency shutdown of the unit.

The design process assumes that the SIF is the last layer of protection and the last to operate. Often, however, safety instrumented functions can also lead to a poor overall functional safety management. Many of those functions are for instance poorly or too rarely tested leading to risk reduction factors smaller than was specified. In some cases, the safety instrumented function is used to trip before relief valves open thereby reducing emissions to the environment but simultaneously increasing the number of times the SIF trips. Similarly the SIF is made to operate the process in the 'red-zone' instead of remaining the ultimate barrier. It is not uncommon to see operators waiting for the high level trip when filling a tank. This compromises highly the reliability of the barrier which is operating outside its design frequency and which is activated too frequently and not exceptionally as designed. Having too many safety instrumented functions contributes also to an overload of information in the control room.

Several of those elements lead to smaller installed risk reduction factors and thus higher risks of major accidents than believed by management or even tolerated by corporate policies.

The causes of this situation are multi-fold and the objective of this paper is to dig further and provide insight into the drift towards sometimes over-engineered processes, not necessarily safer, and exemplify the typical pitfalls to avoid when dealing with functional safety management. From there, guidance and solutions are given to get the right balance between a plant without enough instrumented safety functions and a hypothetical unmanned plant. As with other elements of process safety management, process safety competence is critical to being able to optimise safety investments and direct them towards the barriers and measures with the greatest impact on reducing process risk.

Keywords: functional safety, safety instrumented systems, IEC61511, human factor, over-engineering, SIL.

Introduction

Functional safety standards (IEC standards 61508/61511) have already brought many improvements in the process industries as they require to focus on safety instrumented systems (SIS) with some degree of formality. However, there is some evidence to suggest that they are not always fully implemented, resulting in additional costs, lack of readiness of facilities and – more worryingly – false reductions in the risk of accidents. The objective of this article is to provide some insight into ways of establishing the right balance between an unsafe and an unmanned plant.

What is functional safety?

Functional safety, as far as the process industries are concerned, refers to the entire life cycle of safety instrumented chains or safety instrumented functions (SIF). Process plant safety is now governed by the IEC 61511 standard, a subset of the generic master IEC 61508 standard, which *de facto* represent the minimum best practices in this area. Functional safety is, at its heart, process safety rather than the more conventionally understood occupational safety.

It relates to making the process safe by using automatic protection or prevention barriers that do not require any human action when activated. A typical example is the high level trip on a storage tank which, when a pre-established threshold of level measurement is reached, will trigger a series of automatic actions such as stopping a pump and closing a series of valves. As such, these barriers can be considered as a subset of an industrial unit's protection layers.

One of the essential aspects of those standards is the *integrity levels* of the safety instrumented functions, reflecting their reliability and which is generally defined by their probability of failure on demand (PFD) range or their safety integrity level (SIL). Firstly if the risk reduction required is less than a factor of 10 then an ordinary trip is suitable, but if high reliability is required and the risk reduction needed is more than 10 then a SIL rating applies. Thus most safety trips are non-SIL, but they are still safety trips.

One of the tasks involved in establishing compliance with these standards is to determine the required SIL level to close the gap and make the process safe. This involves establishing the risk reduction factor that the safety instrumented function is required to provide to reduce the risk of an accidental scenario to an acceptable value. The subsequent task following designing a safety instrumented function is to SIL assess the SIF in order to prove that the SIF can achieve an equal or better level of protection than is required by the first SIL assessment.

Functional safety improvements

Functional safety formalisation has allowed huge improvements in process safety to be made over the years, making operations safer. It has also allowed a number of industrial disasters to be avoided by automatically activating the purposely planned and designed layers of protection[1].

The left part of the schematic graph in Figure 1 illustrates this improvement as a decrease in the risk as the number of SIFs increases. Unfortunately, this improvement is not asymptotic as, beyond a certain instrumentation and control level and complexity, the risk rises again as shown in the right part of Figure 1.

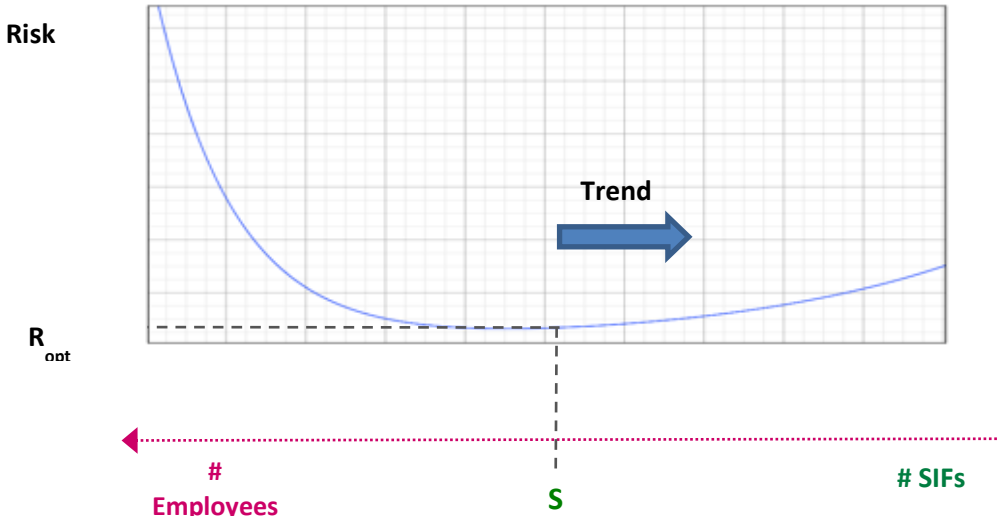

Figure 1. Optimum operability/safety

This optimum (S) can also be seen as the balance between over-simplicity and under-specification, on the left, and over-complexity and over-specification, on the right, which is detrimental to operability.

Functional safety trend

Over the last decade, there has been an escalation in the number of safety systems in industrial processes, and a trend towards over-specification. E. Marzall[2] reports that some studies indicate that close to 50% of the SIFs of refineries are over-specified.

The total costs are often very high (investment costs, operating costs and maintenance costs) and increase quickly with the complexity of such functions. The need to ensure that safety functions are not oversized can be readily understood. Figure 2 provides a visual understanding of the impact of this over-specification according the integrity level of chains and in particular the significant costs for SIL3 type of functions which are, depending on the sources, 3 to 4 times higher than a SIL1 type of function in terms of reliability.

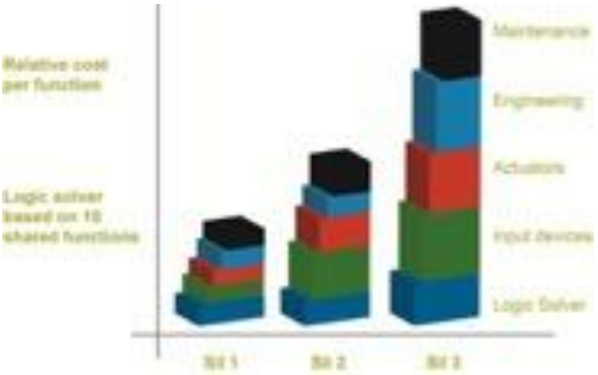

Figure 2. Cost of SIF versus their integrity level (Honeywell[3], 2011)

[1] Casal identifies 17 of the 34 cases studied in A. Casal, SIS Pitfalls, Major Incidents and Lessons Learned, Safety Control System Conference, Perth, 2011
[2] E. Marzall, Decrease Safety System Costs by Considering Existing Layers of Protection, Exida, 2001
[3] Honeywell White Paper, Planning Your Safety Instrumented System, 2011

The challenges and costs of establishing compliance with functional safety standards are high. And as is often the case, the material part of process safety costs depends crucially on the quality of the phases conducted in the front-end (understanding of hazards, risk analysis, …).

In itself, the choice to invest heavily in high-integrity safety instrumented functions is not a problem as this often corresponds to a decision of the company in seeking reassurance. Paradoxically the same decision does not always actually reduce the risk. Before examining the causes of this escalation in the number and especially in the integrity levels of safety instrumented functions, let's first justify this apparent paradox.

Why do more SIFs cause the risk to increase again?

Compromised operability

Too many SIFs decrease the operability of an industrial unit. A classic example of this is a pump's low-pressure safety trip that has to be disabled or over-ridden for a given period to be able to start the pump. Another such example is the spurious activation of SIF which is related to the design decisions of the SIF itself. Spurious activations cause more frequent shutdowns and start-up and hence deviations from normal operations. It is well known, as substantiated by accident rates, that industrial accidents occur more often during those transient phases, i.e. start-up and shutdown or similar events (as is the case for an aircraft landing or taking off). Yet in the standard EN 1127 we are reminded that start-ups and shutdowns are normal operations[4].

Beyond a certain level of nuisance to operations, the decision may even be taken to bypass the safety system, even though the standards (IEC61508 and IEC61511) are not in favour of bypasses and sometimes without any adequate management of change, which brings us back to the risk on the left side of Figure 1. A fairly typical example of such situation is the one of explosion suppressors that are disabled due to spurious activation.

Complexity

Having too many safety instrumented functions requires a good and positive overall functional safety management. Functional Safety Management is now mandated in both standards, IEC61508 and IEC61511. Yet having too many SIFs puts maintenance under pressure and many of those functions can be poorly, or too rarely, tested leading to risk reduction factors smaller than was originally specified. In some cases, the safety instrumented function is used to operate the process in the 'red-zone' instead of remaining as the ultimate barrier. It is not uncommon to see operators waiting for the high level switch tripping when filling a tank. This compromises highly the reliability of the barrier which is activated too frequently and not only exceptionally as designed, a continuous control mode (i.e. a process function) rather than an occasional safety trip.

This complexity also results in an escalation in the number of alarms in the control room. When an unwanted event happens then it is normal that several alarms are activated due to the consequences. This situation is so real that it has given rise to the growth of a new discipline called alarm management. Being flooded by alarms potentially overlooks the alarms that are actually important and critical for safety. The Public Enquiry into the Texaco Pembroke disaster (1994) noted that in the last 10.7 minutes and operator had to read, understand, acknowledge and act upon 275 alarms[5]. That is one alarm every 2 seconds for more than 10 minutes.

Cognitive biases

The mere presence of automatic SIL rated ultimate barriers gives rise to a sense of complacency about safety in the plant. Operating staff gradually build the mental idea that nothing serious can go wrong, and that the installation will automatically switch over to the failsafe position. In some cases, instrumented safety has become part of running the process plant. At Buncefield operators got used to starting off the filling of the tank with fuel knowing that the safety system would stop the fill[6].

During one of our accident investigations, involving a near-miss disaster which fortunately turned out well that evening, the operators told us that the instrumented safety barriers were "what stops us going off the road, whatever mistake in terms of process deviation we might make" (sic). This is obviously a cognitive bias that is not without echoing the video games, something we could call the Nintendo effect. To use the simplistic metaphor of a car, the situation could be compared to the mere presence of an airbag and an anti-sliding system gradually inducing the driver to drive faster even under the rain. It is well known that the time spent near safety limits, an already degraded situation, is in itself a factor contributing to major accidents.

Along the same lines, too many SIFs also create an "illusion of understanding and expertise among operating staff, including engineers"[7]. Having a fully automated unit will cause people to gradually lose sight of the normal operation of the process. It is crucial to fight this bias.

Addressing this bias is not so simple, however, one of the key actions being to train and educate operators to the ultimate layers of protection and their basis of safety. But truly fighting those cognitive biases that have pervaded the all organisation

[4] Only unplanned or emergency shutdown is not a normal operation.
[5] HSE Public Enquiry report paragraph 102, "The Explosion and Fires at the Texaco Refinery Milford Haven", page 27
[6] HSE report, "Buncefield: Why did it happen?", paragraph 12, page 11
[7] Dennis Hendershot, Process Safety and Environmental Protection 2006, 84, 1-6

is not just a matter of providing a few training sessions and often requires a wider set of activities. The operators need to value all of the layers of protection and not just the SIF.

Causes of and solutions to the trend

The causes of the trend that we have briefly attempted to illustrate are multiple and of a varying nature. In the remainder of this section, we have tried to describe their principles and provide potential solutions to prevent them.

Systemic cause

The mere fact that the functional safety standards come from the instrumentation and control specialists' world has led many organisations to allocate their implementation to automation specialists and the maintenance department, company departments which are directly at the interface with integrated solution providers or vendors of safety equipment (sensors, actuators and instrumentation and control systems, etc.). This too often leads to functional safety discipline being disconnected from the process safety discipline. In reality it is process engineers and process safety engineers that should assess the hazard and risk of the unwanted event and determine if a SIF is needed, not the instrument engineer on their own.

To address this, the solution lies, as for Risk-Based Inspection studies, in providing a better connection between process safety and maintenance, and education of multidisciplinary teams. Moreover, it is preferable for the functional safety exercises to be process safety driven as it is primarily a wider topic of safety management rather than simply control engineering.

Formalism

The very formalism of the functional safety standards is in itself responsible for some of the observed trends. The formalism of the standard as illustrated in Figure 3 sometimes leads analysts to think in terms of safety instrumented chains at the expense of other barriers.

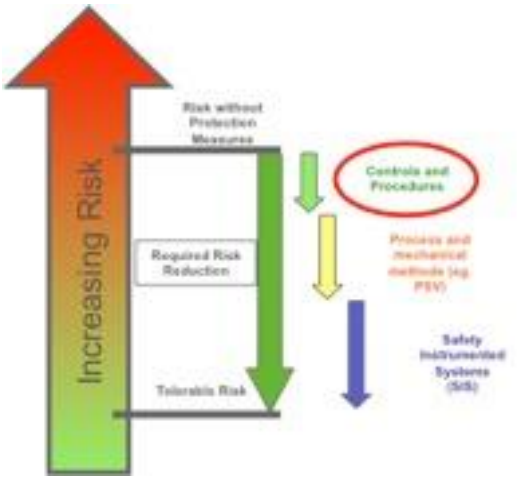

Figure 3. SIS approach as per IEC 61511

Indeed, the approach itself includes a bias as instrumented functions are isolated, and wrongly held and seen to be the ultimate way of bringing the risk of the scenario under consideration to an acceptable level. One of the direct consequences of this is that too much focus being placed on SIS at the expense of other barriers. Situations are all too often seen where the working group determining SIL levels mitigates risks by adding SIFs without giving enough consideration to other possible options, starting with the application of inherent safety concepts and questioning the assessment of the potential risk of the scenario considered. By contrast, a SIF should not become a sticking-plaster over poor process design.

The other bias is that the rationale of standards takes protection barriers (e.g. valves) into account before preventive barriers, which a SIF actually is. Consideration of the LIOPA process in the standard reveals that the SIF is the last layer of protection in the mathematics. Any risk analysis exercise must obviously first and foremost focus on barriers preventing the occurrence of a dangerous phenomenon. It is ironic that the HAZOP (or any HAZID) process has used a risk graph that is not calibrated the same as LOPA and yet the team knew that LOPA was going to be used. That whole approach makes no sense.[8]

The list of limitations and pitfalls in the exercise of determining SIL levels is fairly long. Baybutt[9] goes further in this important area and includes:

[8] The IEC committees always understood that more than one technique for assessment can be used. Others came up with the stange language of "Either risk graphs or LOPA" when it was never an either/or issue, there are simply advantages and disadvantages to both.

[9] P. Baybutt, The Interface of Functional Safety with Process Safety and Risk Analysis, Process Safety Progress, 2013

- The importance of the calibration of risk acceptability matrices
- The method selection (LOPA, Risk Graph etc)
- The importance of failure data sources
- The taking into account of common failure causes (e.g. Fukushima)

The solution to address these formalism biases is obviously to focus first on reducing the risk at the source and only then on mitigating the risk, starting with preventive barriers. One of the best examples in the chemical industry is to "work on the reaction chemistry" to make the reaction intrinsically safe and de facto limit the likelihood and consequences of a thermal runaway. More generally, it involves going back to basics and focusing on simple and reliable passive systems as can be safety valves or rupture discs.

Taking human barriers into account

Table 1 also illustrates the wide disparity in crediting the risk reduction factors of human controls (of the type alarm/analysis/action) into account, based on data from a sample of 225 companies. This means that more than a quarter of the respondents only give very little credit – less than 2 – to this type of barrier. It is therefore highly likely that the safety function allowing the scenario to be brought to an acceptable risk is over-specified. The value of 10 is used by half of the surveyed companies. While the objective of this article is not to discuss an operator's reliability when faced with an alarm, this value of 10 is usually the accepted value used by the practitioners[10].

Risk reduction factor	%
1	10.4
1 to 2	14.8
2 to 10	20
10	43
>10	3

Table 1. Distribution of typical risk reduction factors for an alarm/action type human barrier, based on a sample of 225 companies (as per Stauffer[11]).

Competency

Another fundamental cause of this drift is also the lack of order of magnitude culture amongst analysts; this could even often be referred to as a lack of competency in process safety. One important aspect being the source of the failure data. It is easy to understand that a conservative estimation (higher than real) of a potential risk will lead directly to defining a high integrity level SIF; the opposite being also true and indeed just as worrying as shown by Summers[12].

The solution to this, and it can never be repeated enough, is to increase the process safety competency of those involved, from upstream to downstream: risk analysts, instrumentation and control specialists, maintenance, operators, etc. And, in our opinion, this does not mean attending a few training courses but rather a real competency development program.

Functional Safety Management

Functional Safety Management is now mandated in both standards, IEC61508 and IEC61511. It is in IEC61511 Part 1 Clause 5 and in IEC61508 Part 1 Clause 6. In both cases is any compliance to IEC61511 is going to be claimed at all then compliance with Part 1 is essential. It is the one function that many do not want to be bothered by. Noticeably, in IEC61511, all suppliers of any service for the SIF must also show FSM to both IEC61511 and IEC61508[13]. All suppliers includes those who design the SIF, as well as those who build the panel, as well as those who install the system ….and so on.

Safety Management is an essential and can no longer be just good QA as that has led to too many abuses. At the same time the need for it is obvious: What is the point of having the SIF specified by a competent team but designed by an idiot, assembled by a moron and installed by a fool?

[10] J. M. Haight and V. Kecojevic, "Automation vs. human intervention: What is the best fit for the best performance?," Process safety progress, vol. 24, No. 1, pp. 45–51, 2005.
[11] T. Stauffer, P. Clarke, Benchmarking Industry Practices for the Use of Alarms As Safeguards and Layers of Protection, Global Congress on Process Safety, 2013.
[12] A. Summers, "Overfill Protective Systems - Complex Problem, Simple Solution", SIS-Tech, 2008
[13] Technically the supplier's IEC61511 Functional Safety Management has to show compliance to IEC61511 based upon IEC61508. It is not good enough for a supplier to claim IEC61511 FSM compliance when it is not based upon IEC61508.

Other recommendations

Several of the considerations mentioned in this article lead to smaller risk reduction factors or installed SILs than was thought or specified. This therefore implies a higher real risk of a possible major accident than believed by the management. What should be done to remedy this situation more generally?

- First of all, use some common sense. It must be fairly unusual to have more than 2 or 3 SIL3 type safety instrumented functions in an industrial unit: if not, the process itself should first perhaps be looked at again.
- Systematically consider the increase in safety compared to the cost of instrumental barriers, carrying out techno-economic analysis if needed. Resources are limited and the barriers making the highest contribution in terms of risk reduction should be favoured, using SIFs as a last resort.
- Focus on barriers with a large risk reduction factor as well as the simplest barriers which are often less expensive.
- Audit the performance of the important safeguards and of the critical layers of protection, including the SIFs, at regular intervals. This generally makes it possible to ensure that barriers which, by definition and even by design, are never or very rarely called on, will work as expected when they are actually needed.

Conclusion

Process safety performance is the result of an optimum between man, systems and machines. Instrumented safety functions are one of its key elements as they make it possible to reduce risk levels very significantly or, in other words, to provide reliability which is generally higher than that of the actions performed by a plant operator.

The various guides, norms and standards that structure their design, installation, operation and their reliability requirement have, over the last 30 years, contributed to their huge development and have greatly reduced the risk of accidents in our factories. This has also led companies to reduce operating staff, with some safety-related tasks being taken over by the safety instrumented system. It should be kept in mind, however, that there is a limit to automatic systems and that over-instrumentation can compromise the overall performance.

As with other aspects of process safety, safety management and competency in functional safety is crucial to being able to optimise safety investments and direct them towards the safeguards and layers of protection with the greatest impact on reducing process risks.