Functional Safety and Explosion Protection

Fundamentals of Functional Safety in Accordance with IEC 61508 and how it is Linked to Applications in Hazardous Areas

by André Fritsch

Figure 1: Functional Safety SIL

Were we to place the Standards and regulations of these two specialist areas side by side and compare their content, we could easily conclude that these two topics have nothing to do with one another and coexist with no interrelationship whatsoever. Many operators and planners will confirm, on the basis of their own experience, that this is not the case and that both topics are even frequently inseparably linked.

Manufacturers of explosion protected apparatus recognised this interrelationship at an early stage, and the required knowledge was acquired in parallel with product developments and certifications. Consequently, many manufacturers of explosion protected apparatus now also supply the components and systems specified for functional safety circuits together with the required specialist knowledge.

Who invented it ?

How did ›Functional Safety‹ arise? One should assume that safety of personnel does not require specific legislation but, rather, is in the interests of the user and should be handled as a high priority. Unfortunately, this is not always the case and, as has frequently occurred in history, action is taken only after an actual incident. This happened approximately 29 years ago on July 10, 1976, in Seveso, northern Italy. A toxic gas accident released highly toxic dioxin (TCDD), triggered by an uncontrolled overheating reaction whose excess pressure destroyed a plant safeguard. The reactor in question featured no automatic cooling systems whatsoever. There were neither warning systems nor alarm plans in the installation. The population was informed 9 days later. Fortunately, there were no specialist personnel in the plant when the incident occurred and, by chance, the quantity of toxic substance released was limited. Nevertheless, approx. 2 kg of highly toxic dioxin was released into the environment and caused illness, death of animals, and serious environmental pollution.

As a consequence of this accident it was decided to tighten up legislation and ordinances aimed at protecting humans, living organisms and the environment.

The European Community published the Seveso I Directive in the 1980s and later the Seveso II Directive 96/82/EC ‹on the control of major-accident hazards involving dangerous substances›.

In Germany for instance, this Directive was adopted in national law with reference to DIN V 19250. This Standard also included a definition of the Requirement Classes AK 1-8 used internationally.

IEC 61508 ›Functional Safety of Safety-Related Electrically/Electronically Programmable Electronic Systems‹ which has been valid Europe-wide as EN 61508 since August 2002, was published in the year 1998. This new Safety Standard, for the first time, defined the safety requirements in automation engineering comprehensively, independently of the application, and also allowes for modern, microprocessor-based systems. IEC 61508 has now been accepted worldwide and is being or has been adopted in national law or national Standards and regulations in many countries (e.g. AS 61508 in Australia, BS IEC 61508 in Great Britain, NFPA 79 -2002 in the USA and JIS C 0508 in Japan). After adoption in a German Standard DIN EN 61508 (VDE 0803), DIN V 19250 and DIN V 19251 ceased to apply on July 31, 2004 so that there is now only one binding regulation.

While IEC 61508 is aimed primarily at manufacturers of components for protection equipment and devices, IEC 61511 ›Functional Safety – Technical Safety Systems for the Process Industry‹ is aimed at users and planners of safety devices and equipment. IEC 61511 provides recommendations and targets for assessment of the damage risk of installations and provides assistance in selection of appropriate, safety-related components. Part 3, Annex D of IEC introduces the risk graph as a method of risk assessment to assist users and planners in design. Other application-specific Standards on the basis of IEC 61508 include, for instance, IEC 61513 ›Nuclear Power Facility Control and Instrumentation Systems for Systems Important for Technical Safety‹ and DIN IEC 62061 (2005-01) Safety of machinery – Functional Safety of safety-related electrical, electronic and programmable electronic control systems.

Technical jargon?

If we consider the topic of ›Functional Safety‹ in greater detail and if, for instance, we read a corresponding test report, we quickly encounter certain terms and abbreviations that are far from self-explanatory. Consequently, we shall discuss the terminology and technical expressions which are essential for understanding the topic in brief below.

Let us start with a definition of terms which are frequently confused and misinterpreted: safety and availability. The essential difference can quickly be seen on the basis of an everyday example. A railway crossing is safeguarded with a barrier so that, when a train approaches, a vehicle cannot drive over the tracks at the same time. The two possible error sources in this example are the ›non-opening‹ and ›non-closing‹ of the barrier. If the barrier no longer opens after the train has passed, the availability of the road is no longer guaranteed. A parallel crossing, for instance would remedy the situation in this case as the probability of this barrier not opening is extremely low. Of course, this must be strictly rejected on the basis of safety aspects since the error probability of ›non-closing‹ is doubled from two to four barriers. Here, it is far better if we construct two barriers, one behind the other, in order to intercept an error if one of the four barriers does not close. However, in turn, this counteracts availability. How do we find a solution which avoids this dilemma and enhances both safety and availability? There is more than one solution, such as an overpass, but all these solutions have one thing in common: higher costs. We should not lose sight of the cost aspect in all applications and measures intended to enhance safety and/or availability. Consequently, it does not make sense ➔

to always demand the very highest safety level. Rather, the safety level must be determined and planned specifically to the application so as to also meet economic requirements. The above-mentioned risk graph from IEC 61511-3 is an appropriate aid, which we will describe later.

The definition of the ›safe state‹ is an important element of a safety concept. Various considerations are also possible here, depending on the application. In a process in which a fluid is heated, the safe state can be achieved by deactivating all electrical circuits, including the heater, for example, so that the fluid does not boil over. By contrast, in the case of a fault state in an aircraft, everything possible should be done to maintain the function of all systems. This example also clearly indicates that the deenergised state of a system can be achieved very simply and, consequently, should be given preference wherever possible for safety functions. Safe states on automation components may include the following: ›maintain last position‹, ›hardware deactivation‹ and ›safe shutdown‹. The definition of the safe state is an important element of the test reports for components with SIL classification. SIL itself is an abbreviation for ›Safety Integrity Level‹ and has now become a synonym for Functional Safety. SIL defines ›only‹ a measure of the safety-related performance or reliability of an electronic or electrical control device (Table 1) and says very little on its own.

Protection equipment	Installation risk reduction
SIL 1	10 ... 100
SIL 2	100 ... 1.000
SIL 3	1.000 ... 10.000
SIL 4	10.000 ... 100.000

Table 1: Interrelationship between SIL and risk reduction

IEC 61511	DIN V 19250	VDI/VDE 2180
SIL 1	AK1	Risk area I (low risk)
	AK2	
	AK3	
SIL 2	AK4	
SIL 3	AK5	Risk area II (high risk)
	AK6	
SIL 4	AK7	Not covered by PCS protection equipment alone
	AK8	

Table 2: Relationship between IEC 61511, DIN V 19250 and VDI/VDE 2180 (source: IEC 61511-3; Annex E)

Since SIL is determined and considered differently than the AK (Requirement Class) from DIN V 19250, a direct comparison is not that simple. One general rule of thumb is that an AK 3 system approximately corresponds to an SIL 1 system and an AK 5 system approximately corresponds to a SIL 3 system (Table 2).

Unlike determining the AK, the process of determining the SIL focuses on assessment of the safety chain, also referred to as SIF ›Safety Instrumented Function‹. Typically, this safety chain consists of a fail-safe control, an actuator and a sensor. The SIS ›Safety Instrumented System‹ consists of one or more safety chains.

In general, safety systems are classified in accordance with IEC 61508 as either ›low demand‹ or ›high demand‹. This defines how frequently during operation of an installation or machine the safety function cuts in. If it is be anticipated that the safety function responds several times per day or even more frequently, we speak of a ›high demand‹ system. Examples of this can be found in applications in the mechanical-engineering and machine-construction sector, e.g. if a light barrier is required to trigger the safety function when an operator intervenes and the operator works continuously on the machine. In the sector of process automation, it must be assumed that the safety function is tripped only very rarely, typically at a maximum of once per year. This is referred to as a ›low demand‹ system. Examples of these include fire alarms or emergency shut-down systems. We shall discuss only the ›low demand‹ applications below since these form the major part in the sector of automation solutions.

For project planning of safety systems information on the SIL of the individual components is not enough. While in the past the safety chain could meet exactly the lowest AK of the individual components, with SIL a calculation on the basis of failure probability has to be made. Here, the value PFD_a (= Probability of Failure on Demand, average) has a central significance. PFD_a

Fault types	Non-fatal faults	Hazardous faults
Recognised faults	λ_{sd} (= safe detected)	λ_{dd} (= dangerous detected)
Unrecognised faults	λ_{su} (= safe undetected)	λ_{du} (= dangerous undetected)
Faults of components which are not a part of the protection system	λ_{np} (= not part)	

Table 3: Fault types on safety systems

specifies the average probability with which a safety system will fail at exactly that moment in which this safety function will be required. This value is related to a selectable period of time, typically per year. A PFD_a of $3 \cdot 10^{-3}$, for example, means that with high probability the safety function will fail once in 333 years in the moment when it is required. But that does not mean that the system will work for 333 years without failure. The safety-critical failure may occur after one year and then will not occur again for another 332 years – that is what the probability calculation means.
Determination of component PFD_a is done by a quite elaborate analytic process, the so-called FMEDA (Failure Mode Effects and Detectability Analysis), with which down to the individual components an analysis is made about what will happen with which fault and how this may be detected.

The basis of this analysis are the data collections on the failure rate of electronic components such as for example, Siemens-Standard SN 29500 or, quite conservative, the MIL-manual 217F, but also the statistics the manufacturers did themselves on the failure behaviour of their components.

Possible faults in components can be classified into five different fault types which have differing effects on the failure probability PFD_a (Table 3).

In the case of the ›low demand‹ systems considered here, only the hazardous, unrecognised fault λ_{du} plays an essential role, referred to as a defined time interval which is designated T_{proof} (inspection interval). The aim of these inspections is to detect and eliminate the hazardous fault, i.e. the fault which would lead to failure of the safety function. Conversely, a change of the inspection interval results in a change in the failure probability when the safety function is needed (If you inspect a system more frequently, there is a lower probability that it will fail when needed).

The determined PFD_a value allows assignment of the device to an SIL (Table 4). The safety quality of the device is described by two further parameters. The SFF (Safe Failure Fraction) states the magnitude of the share of non-dangerous faults in relation to the total possible faults. A non-dangerous fault is defined as a fault which is, admittedly, relevant to safety but which is neither nor sets the system to a safe state. A simple example of this would be a device fuse that sets the device to the safe Off state in the event of overvoltage – provided this state is the safe state. An SFF of 90 % for instance, states that only 10 % of the possible faults in a safety device cannot be detected and would lead to a dangerous state. The second parameter, which is relevant here, is the HFT (Hardware Failure Tolerance). The HFT describes the redundancy tolerance of the device or system. Systems without redundancy, i.e. on which the safety function is no longer guaranteed in the event of one failure, have an HFT of 0. The HFT is 1 in the case of single redundancy and it is 2 in the case of double redundancy. Linking the two parameters SFF and HFT then provides the SIL of a device. A further distinction is also made between simple Type-A devices on which all faults are known and can be described (Table 5), and more complex Type-B devices if not all faults are known and can be described, as will generally be the case in microprocessor systems or software (Table 6).

IEC 61511 defines the term ›proven in use‹. If the manufacturer is able to verify the proven operational effectiveness of his or her components or systems, the achievable SIL can be upgraded. Tables 5 and 6 refer to this with ›HFT = 0[1]‹ or ›1[1]‹. The number of devices already marketed and the systematic evaluation of safety-related faults on these devices during their lifetime form the basis for this verification. This verification of ›proven in use‹ is the only effective way of conducting a SIL assessment in the case of more complex systems frequently ➔

PFD_a Fault if system is needed; low demand Systeme	SIL
$\geq 10^{-2} \ldots < 10^{-1}$	SIL 1
$\geq 10^{-3} \ldots < 10^{-2}$	SIL 2
$\geq 10^{-4} \ldots < 10^{-3}$	SIL 3
$\geq 10^{-6} \ldots < 10^{-4}$	SIL 4

Table 4: Failure probability and achievable SIL

featuring microprocessors. The lowest value of the two, possibly differing, SIL values, resulting from the PFD_a and from the SFF and HFT, is taken as the SIL of the device or system.

In the case of Functional Safety, there is no mandatory certification, unlike explosion protection for instance. In accordance with IEC 61508, a manufacturer's test which, however, must be conducted by an independent department in the company suffices for SIL 2 applications. As of SIL 3, the Standard recommends that the analysis be conducted by an outside company.

What does the user do?

Fortunately, the user does not need to bother about the costly, and in some cases, complex process of determining the individual parameters. This is done by the device manufacturer and is documented in test reports and a Safety Manual. However, this does not affect the user´s responsibility to correctly classify his or her installation and to use the right components under the right boundary conditions. Field reports indicate that approximately 44 % of all faults occur as early as the specification phase.

Normally, the procedure for obtaining an approval is not stipulated by law. The user files an ›application for approval of the safety-related installation‹. The approval procedures and the responsible public authorities differ nationally.

In principle, the safety analysis of an installation or part-installation is subdivided into four steps. The basic function of the safety requirements is defined first, the ›Safety Requirement Specification‹ or SRS for short. What should or what must be achieved with the safety function? The second step is the actual risk analysis, also referred to as ›SIL a ssessment‹. The risk analysis is conducted with the aid of the risk graph from IEC 61511-3, Annex D, for instance (Figure 2).

Annex D of the aforesaid Standard only has an informative character, so application of the risk graph is not obligatory. Alternative procedures are just as reliable and, in some cases, even stipulated by the approval authority. Frequently, a so-called LOPA ›Layer Of Protection Analysis‹ is also conducted. Since the procedure in accordance with IEC 61511 has proven to be very expedient and is suitable both for analysis of the risks to people and the risk to environment, and also as a cost analysis in relation to production outage costs, this procedure will be used in the examples which follow. Regardless of the particular procedure used, it is always important to document and substantiate the assumptions and decisions made. All stipulations and results are cited in an easily understandable manner in the safety document. It is also practical to keep an eye on the cost aspect in the safety analysis: »What will a fault cost – what will avoidance of the fault cost?«.

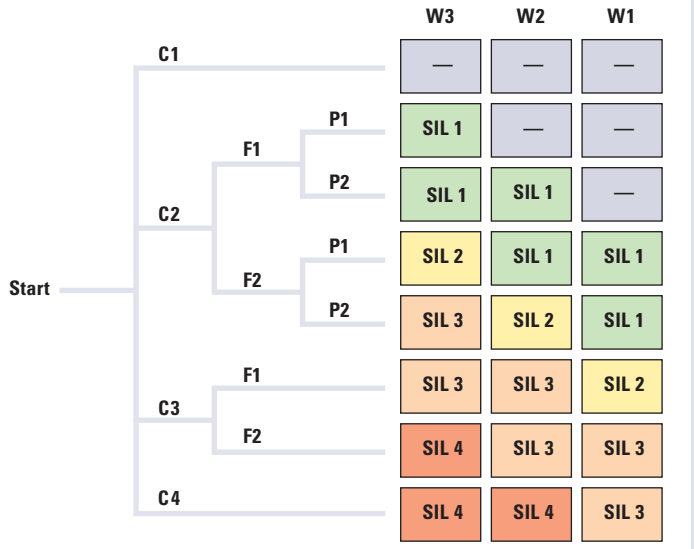
The aforesaid IEC 61511-3 provides detailed instructions on use of the risk graph so that we shall not discuss it in detail at this point. Measures to downgrade the required SIL and the resultant costs may be taken as early as when conducting the risk analysis. Organisational measures allow the presence time of people in the risk area to be shortened, for instance and, thus, make it possible to change parameter F2 to F1 (see Figure 2). In the case of parameter ›P‹, risk defence, it is possible to achieve a reduction of P2 to P1 by design measures or structural measures, such as a bursting disc or a pressure relief valve. This means that it may be possible, as early as the analysis phase, to downgrade from SIL 3 to SIL 1 which, in turn, leads to simpler, less costly solutions.

	HFT (Hardware Failure Tolerance)		
SFF (Safe Failure Fraction)	0	1 / 0[1)]	2 / 1[1)]
< 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 5: Interrelationship between SFF and HFT on simple devices (Type A) 0[1)] or 1[1)] in the case of verification of proven operation effectiveness in accordance with IEC 61511

	HFT (Hardware Failure Tolerance)		
SFF (Safe Failure Fraction)	0	1 / 0[1)]	2 / 1[1)]
< 60%	—	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 6: Interrelationship between SFF and HFT in the case of more complex devices (Typ B) 0[1)] or 1[1)] in the case of verfification of proven operational effectiveness in accordance with IEC 61511



C = extent of damage
C1: slight injury
C2: serious irreversible injury to one or more persons, or death of a person
C3: death of several persons
C4: catastrophic consequences many fatalities

F = proportion of time of exposure to hazard
F1: low (< 0.1)
F2: high (> 0.1)

P = mitigating factors (prevention)
P1: good chance of avoiding consequence (> 50 %)
P2: poor chance of avoiding consequence (< 50 %)

W = probability or frequency of hazardous event/demand
W1: very low (F < 0.01/YR.)
W2: low (F > 0.01/YR.)
W3: relatively high (F > 0.1/YR.)

— = No safety requirements

Remarks:
SIL 4 cannot be achieved with one item of safety equipment alone

Figure 2: Risk graph for injury to persons in accordance with IEC 61508/61511

When the requirements needed have been stipulated, the first step is then to configure the safety functions, typically consisting of PLC, and input and output circuits, including selection of the components to be used.
The last step is then to analyse the safety function for their SILs. In this case, each safety circuit must be analysed separately. The analysis is conducted on the basis of the failure probabilities PFD_a of the components used which are documented in the relevant test reports.
In the case of simple, non-redundant safety circuits, these values are added and the result is compared with the permitted values shown in Table 4.

Unfortunately, the calculated value will frequently differ from the required value in practice. What options now exist for upgrading the SIL of the safety systems? Since the inspection times T_{proof} in the case of ›low demand‹ safety systems are included in the result in virtually linear manner, upgrading the SIL can be achieved by shortening inspection times. However, more frequent inspections, in turn, cause an increase in costs. One other tried and tested method is to configure redundancies. Essential improvements can be achieved, depending on the redundancy used. In this case, we talk of 1oo2 (1 out of 2) or 2oo3 (2 out of 3) redundancies. Maximum effectiveness is achieved by so-called ‹diversities‹ that work with differing measuring instruments and measuring methods. If, for instance, a temperature measurement is conducted with a temperature transmitter, a second, redundant transmitter of the same type will, admittedly, reduce the failure probability. However, this involves the possibility of what is called a Common Cause Fault (›beta factor‹), a fault which occurs simultaneously for both transmitters subjected to common loading. For example, this would be a systematic error in the transmitter software affecting both devices at the same moment in the case of a specific measurement result. In the case of ‹diversities‹, transmitters of different manufactures and, possibly, even using different measuring methods are used so as to eliminate the possibility of this Common Cause Fault and substantially reduce the failure probability. A further enhancement of the safety chain can be achieved with diagnostic methods. Early detection of failures or malfunctions by Diagnostic Coverage also improves the safety application since hazardous, unrecognised failures become hazardous, recognised failures.

The user documents the safety functions he or she carried out over the service life of the systems, together with all faults that occurred, in the Safety Manual. What ➔

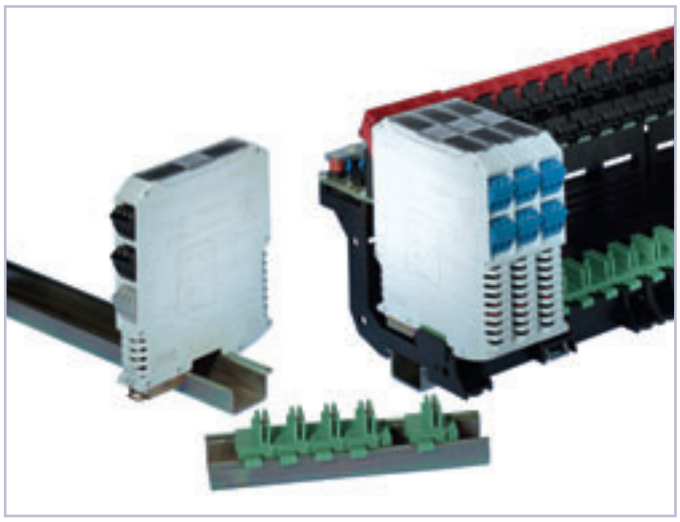


Figure 3: IS pac Ex i isolator system for SIL 2 and SIL 3 applications

might initially be seen as annoying paperwork does, however, assist in designing new safety circuits. If a safety system has been in use for several years and if no or only a few safety-critical faults have occurred during this time, it is also possible to upgrade the SIL for this application using the argumentation of proven in use. We should also point out that a subsequent change in the result of the conducted risk analysis is not recommended for downgrading the required SIL. After all, the analysis was conducted to the ›best of the knowledge and ability‹ of the analyst. If there have been no real changes in the installation there is no logical reason for a subsequent change.

As can be seen very well from the aspects described above, analysis and optimisation of safety circuits may take a great deal of time.

Fortunately, certain software tools are now available on the market offering assistance for the design of safety systems. One of the features of a good tool includes providing device databases for the user, which list as many devices as possible together with their safety characteristics (Table 8).

Some of the tools also include a risk analysis function with the risk graph, dynamic costing and a log function for saving the decisions taken with a versioning function.

Name of the software	Manufacturer	Note
SILence	HIMA	
SILver	EXIDA	Internet application
TRAC	ABB	with risk graph
TRAMS	ABB	for documentation

Table 8: Selection of available software tools with device databases

Even the relevant software tools may be good and helpful, but they do not, overall, exempt the user from his or her responsibility.

Explosion protection and SIL

Installations with hazardous areas also frequently include Functional Safety applications. Generally, all types of protection can be used here as well. However, one aspect which aggravates the situation in the case of Functional Safety is that the inspection interval is generally once per year while the inspection and maintenance interval is specifically three years in the case of explosion protection applications.

Consequently, easy inspection involving as low a cost as possible is particularly important in the case of combined applications comprising explosion protection and Functional Safety. While the inspections can be conducted only in a deenergised state and require special permits in the case of most types of protection such as Flameproof Enclosures ›d‹ or Increased Safety ›e‹, work can continue as under ›normal conditions‹ in the case of type of protection Intrinsic Safety ›i‹.

Measurements, tests and inspections can be conducted during operation in the hazardous area, this being a major advantage when testing the safety circuits. Consequently, the obvious approach is to design the circuits with type of protection Intrinsic Safety ›i‹ in the case of Functional Safety applications in hazardous areas. The principle of the type of protection Intrinsic Safety is based on limitation of current, voltage and power of the signals entering the hazardous area. In this case, one or two possible faults are also considered, thus resulting in Categories (Protection Level) ›ib‹ and ›ia‹ which, in turn,

define usability for Zone 1 or Zone 0 circuits. However, this does not automatically result in a solution suitable for Functional Safety as, in this case, no adequate statement is made on availability of quality of signal transmission. A corresponding analysis and SIL assessment must thus also be conducted here. Various solutions are possible with intrinsically safe components and systems.

The ›classic approach‹ is to use point-to-point connections with conventional isolators or safety barriers.

The simplest solution in this case is to use safety barriers as simple, passive networks since they do not make an active contribution to the safety chain and, in principle, can be considered in the same way as a passive component. However, circuits with safety barriers entail potential functional risks owing to the series resistance and the fact that the equipotential bonding system is connected to earth reference, besides other aspects. Consequently, electrical isolators have been given preference for some years now (Figure 3). Since they generally have an external power supply and feature more complex internal electronic circuitry, they are required to have a corresponding SIL analysis. The parameters such as PFD_a or inspection intervals T_{proof}, required for project planning, are documented in the test reports or Safety Manuals.

Use of the isolators may result in a problem in designing the safety function. Since there is now a further element interconnected both in the sensor circuit and in the actuator circuit, the PFD_a of the safety function is,of course, downgraded by these values A circuit which just meets the requirements of SIL 2 circuit for instance may thus now only be useable for SIL 1 circuit. It is thus recommended that maximum 10 % of the entire PFD_a be attributable to an isolator which can be used for safety circuits for the required safety level. Thus, for instance, while a value of $5 \cdot 10^{-3}$ suffices for an SIL 2, only a maximum of $5 \cdot 10^{-4}$ of this should be attributable to the corresponding isolator. Figure 4 shows how the typical distribution of the failure probabilities in a safety function with isolators should look.

If this is not possible or if no corresponding isolator is available, one remaining alternative is redundancy, as already described above. One other alternative consists in using additional diagnostics. One interesting solution in this case is the HART communication signal which supplies a wide variety of parameters that can also be used for early detection of faults, among other uses. Special HART Management Systems, for example, which read in and evaluate the HART signals collectively via a HART multiplexer are available for evaluation of the HART information. The HART multiplexer must, of course, also have SIL assessment since it does, after all, intervene in the safety circuit and could falsify the relevant analogue process signals (Figure 5). Consequently, the SIL assessment of the HART multiplexers does not include use of the HART information for control and monitoring of the safety chain but, rather, a verification that the HART multiplexer has no safety-related influence on the analogue signal.

Modern bus technology has been used to an increasing extent in recent years on many new installations. Solution concepts and products are also available for configuring safety systems. Bus protocols configured specifically for safety applications include PROFISafe or INTERBUS-Safety. Universal usability and, thus, acceptance does, however, frequently fail owing to the narrow selection of field devices available for this. In this case, Remote I/O Technology offers more selection options. Conventional analogue field devices with SIL classification can be operated easily on the Remote I/O. However, the most important requirement for this is, of course, that the Remote I/O System also be assessed on the basis of the SIL criteria. The only system currently on the market, R. STAHL's Remote I/O System IS1, complies with the requirements of SIL 1 (Figure 6).

In order to prevent users from having to deal with the relatively complex structure of this safety function, it is advisable to consider the overall system as one component. On IS1, the fieldbus isolating repeaters for the intrinsically safe Profibus DP (Profibus RS485-IS), the intrinsically safe Profibus DP itself, the CPU module of the system and the analogue and digital input/output modules are allowed for jointly in the SIL assessment, i.e. the user can take only one value for the failure probability of his or her safety function, and then add the corresponding values of the field devices and the automation system to this. Unfortunately, only a few automation systems with SIL assessment have been available to date. Consequently, an empirical value of 0.001 for the failure probability is taken in practice when designing systems without SIL.

Summary and Outlook

Even though the topic of Functional Safety has become extremely complex, or because of this fact, the user must deal with this topic. It must not be the case that the safety of installations and, above all, that the safety of personnel suffers owing to complex or unmanageable regulations and procedures. Fortunately, there have recently been frequent reports in the technical ➔

press on this topic so that users can already gain a good general view of the subject. It is no wonder that manufacturers of explosion protected apparatus in particular have taken up the cause of ›Functional Safety‹ and offer both products and training courses for it. The many years of experience in explosion protection which is, after all, very similar, together with the required high-quality production methods and development procedures, offer a solid basis for this. Explosion Protection and Functional Safety Standards are still developing mutually and independently. However, ›Functional Safety‹ will already be included in a revised Low-Voltage Directive (RL 73/23/EEC). A new European Standard on ›Safety Equipment in Explosion Protection‹ (CENELEC TC31-WG9) is currently in preparation, containing a reference to IEC 61508.

Consequently, it can be assumed that Functional Safety will be with us in the future as well and will not disappear again some day as a passing fad like many other topics.

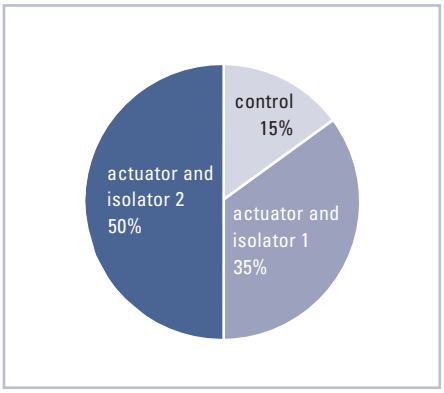


Figure 4: Typical distribution of the PFD_a values in a safety chain with isolators

Figure 5: HART multiplexer with HART connector circuit board for applications up to SIL 3

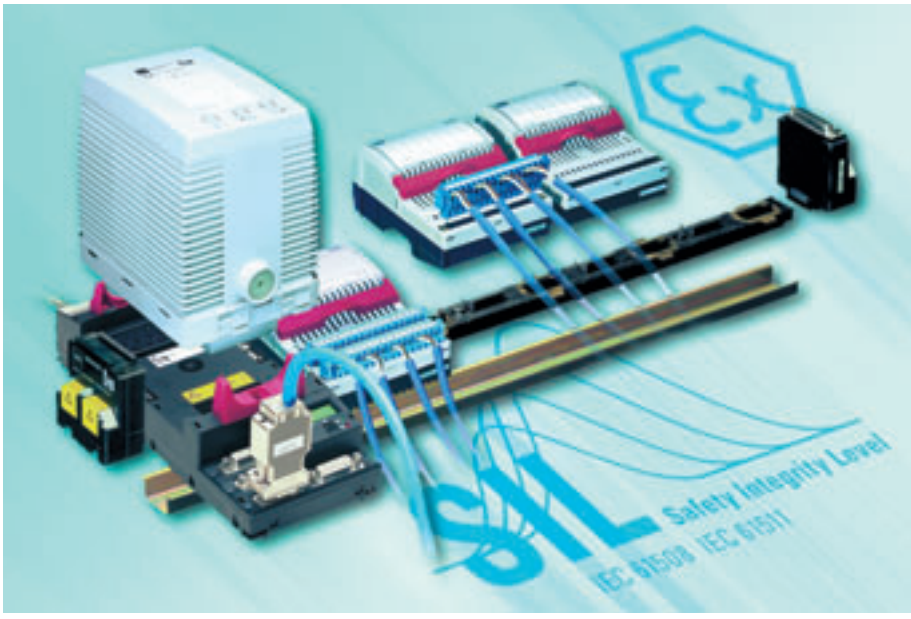


Figure 6: Remote I/O System IS1 for safety requirements up to SIL 1

Bibliography

1. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances (SEVESO II)
   Official Journal of the European Communities 1996
2. DIN V 19250 ›Grundlegende Sicherheitsbetrachtung für MSR-Schutzeinrichtungen‹
   (Fundamental Safety Consideration for Control and Instrumentation System Safety Facilities)
   (withdrawn on 31 July 2004)
3. IEC 61508:1998 Functional safety of electrical/electronical/programmable electronic safety related systems Part 1 – Part 6
4. IEC 61511 12/2003 Functional safety-Safety instrumented systems for the process industry sector
5. IEC 62061 (2005-01) Safety of machinery – Functional safety of safety-related electrical, electronical and programmable electronic control systems
6. Siemens Safety Integrated ›Safety Systems Application Manual‹, available at www.siemens.de/safety
7. Homepage of the IEC (FAQ lists and brochures etc.) available at http://www.iec.ch/zone/fsafety
8. Homepage of the EXIDA company – www.exida.com – with information publications, specialist articles and specialist literature