

PROCESS AUTOMATION

**MANUAL
SAFETY INTEGRITY LEVEL**

SIL

IEC 61508/61511

With regard to the supply of products, the current issue of the following document is applicable:
The General Terms of Delivery for Products and Services of the Electrical Industry, published by
the Central Association of the "Elektrotechnik und Elektroindustrie (ZVEI) e.V.",
including the supplementary clause: "Extended reservation of title".



Structure

This manual contains the manuscripts of various contributors, each one complete in itself. The first part presents an overview of the IEC/EN 61508. The second part is based on presentations that were given as part of a series of seminars by the author. It is therefore possible that some passages in the text are repeated.

It is not the goal of the authors to reproduce excerpts from standards in their entirety, but rather to give the general meaning. If further clarification is needed, the applicable standard should be consulted.

Authors:

Andy Ingrey (part 1, section 2 to section 5)

Patrick Lerévérend (part 2, section 6 to section 9)

Dr. Andreas Hildebrandt (part 2, section 10 and section 11)

1	Introduction	4
1.1	Safety related systems in accordance with IEC/EN 61508.	4
1.2	Introduction of safety related systems	4
1.3	Symbols used.	5
1.4	Definition of terms and abbreviations	5
2	Safety life cycle	7
2.1	Safety life cycle concept	7
2.2	Risks and their reduction	11
3	Safety integrity level (SIL)	13
3.1	Probability of failure	13
3.2	The system structure.	14
4	Probability of failure	17
4.1	Overview	17
4.2	Safety loop example	18
5	Summary of the first part of the SIL manual.	21
6	Verification of the safety integrity level of a safety instrumented function	22
6.1	What is SIL?	22
6.2	Example input subsystem with 2 components	23
6.3	Hardware fault tolerance (IEC/EN 61508, part 2).	26
6.4	SIL limitation due to architectural constraints (IEC/EN 61508, part 2)	27
7	Other structures	28
7.1	MooN system (IEC/EN 61508, part 6)	28
7.2	Two sensor subsystems from our example configured as a two channel input subsystem.	28
7.3	Common cause failures.	30
8	Proven in use (IEC/EN 61508, part 2).	32

9	How to read a SIL product report?	33
10	Glossary/formulae	34
10.1	Failure rate $\lambda(t)$	34
10.2	Constant failure rate λ	35
10.3	Failure probability $F(t)$	35
10.4	Probability density function $f(t)$	36
10.5	Reliability function $R(t)$	36
10.6	Mean life MTTF	37
10.7	Mean failure probability of the function in the demand case PFD (Probability of Failure on Demand)	37
10.8	PFD calculation for multi-channel MooN structures (M out of N)	38
11	References and bibliography	39

1 Introduction

1.1 Safety related systems in accordance with IEC/EN 61508

The international standard IEC/EN 61508 has been widely accepted as the basis for the specification, design and operation of safety instrumented systems (SIS).

As the basic standard, IEC/EN 61508 uses a formulation based on risk assessment: An assessment of the risk is undertaken and on the basis of this the necessary Safety Integrity Level (SIL) is determined for components and systems with safety functions.

SIL-evaluated components and systems are intended to reduce the risk associated with a device to a justifiable level or "tolerable risk".

1.2 Introduction of safety related systems

This document explores some of the issues arising from the recently published international standards for safety systems, particularly within the process industries, and their impact upon the specifications for signal interface equipment.

When considering safety in the process industries, there are a number of relevant national, industry and company safety standards

- IEC/EN 61511 (user)
- ISA S84.01 (USA) (user)
- IEC/EN 61508 (product manufacturer)

which need to be implemented by the process owners and operators, alongside all the relevant health, energy, waste, machinery and other directives that may apply. These standards, which include terms and concepts that are well known to the specialists in the safety industry, may be unfamiliar to the general user in the process industries.

In order to interact with others involved in safety assessments and to implement safety systems within the plant it is necessary to grasp the terminology of these documents and become familiar with the concepts involved. Thus the safety life cycle, risk of accident, safe failure fraction, probability of failure on demand, safety integrity level and other terms need to be understood and used in their appropriate context.

It is not the intention of this document to explain all the technicalities or implications of the standards but rather to provide an overview of the issues covered therein to assist the general understanding of those who may be:

- involved in the definition or design of equipment with safety implications,
- supplying equipment for use in a safety application,
- just wondering what IEC/EN 61508 is all about.

For those people who are directly responsible for the specification, design, installation, operation and maintenance of electronic or programmable systems that may have safety implications, reference must be made to part 2 (section 6 to section 10) of this manual and the standards themselves.

1.3 Symbols used



Attention

This symbol warns of a possible fault. Failure to observe the instructions given in this warning may result in the device and any facilities or systems connected to it developing a fault or even failing completely.



Note

This symbol draws your attention to important information.

1.4 Definition of terms and abbreviations

Term	Description
CDF	Cumulative Distribution Function
Electrical/electronic/programmable electronic systems (E/E/PES)	A term used to embrace all possible electrical equipment that may be used to carry out a safety function. Thus simple electrical devices and programmable logic controllers (PLCs) of all forms are included.
Equipment under control (EUC)	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.
ESD	Emergency Shut-Down
ETA	Event Tree Analysis
FME(C)A	Failure Mode Effect (and Criticality) Analysis
FMEDA	Failure Mode Effect and Diagnostics Analysis
FIT	Failures in Time
FTA	Fault Tree Analysis
Hazardous event	hazardous situation which results in harm
HAZOP	HAZard and OPerability study
HFT	Hardware Failure Tolerance
IEC/EN 61508	Standard of functional safety of electrical/electronic/programmable electronic safety-related systems
IEC/EN 61511	Standard of functional safety: safety instrumented systems for the process industry sector
LDM	Low Demand Mode – where the frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof test frequency.
MooN	M out of N channels
MTBF	Mean Time between Failures
MTTF	Mean Time to Failure
MTRR	Mean Time to Repair
PDF	Probability Density Function
PFD	Probability of Failure on Demand – mean failure probability in the demand case – the probability that a safety system will not execute its function when it is required to do so.
PFD _{avg}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
Risk	Combination of the probability of occurrence of harm and the severity of that harm. Calculated as the product between incident frequency and incident severity
SFF	Safe Failure Fraction – proportion of non-dangerous failures – the ratio of the rate of safe faults plus the rate of diagnosed/recognized faults in relation to the total failure rate of the system.
SIF	Safety Instrumented Function

Term	Description
SIS	Safety Instrumented System – A SIS (Safety system) comprises one or more safety functions; for each of these safety functions there is a SIL requirement.
SIL	Safety Integrity Level – One of four discrete stages in specifying the requirements for the safety integrity of the safety functions, which are assigned to the E/E/PE safety-related system, in which the Safety Integrity Level 4 represents the highest stage and the Safety Integrity Level 1 represents the lowest stage of safety integrity.
SLC	Safety Life Cycle – Covers all aspects of safety, including the initial conception, design, implementation, installation, commissioning, validation, maintenance and decommissioning of the risk-reducing measures.
Safety	The freedom from unacceptable risk of physical injury or of damage to the health of persons, either directly or indirectly, as a result of damage to property or the environment.
Safety function	Function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.
Tolerable risk	Risk, which is accepted in a given context based upon the current values of society.

2 Safety life cycle

2.1 Safety life cycle concept

It is seldom, if ever, that an aspect of safety in any area of activity depends solely on one factor or on one piece of equipment.

Thus the safety standards concerned here, IEC/EN 61511 and IEC/EN 61508, identify an overall approach to the task of determining and applying safety within a process plant. This approach, including the concept of a safety life cycle (SLC), directs the user to consider all of the required phases of the life cycle. In order to claim compliance with the standard it ensures that all issues are taken into account and fully documented for assessment.

Essentially, the standards give the framework and direction for the application of the overall safety life cycle (SLC), covering all aspects of safety including conception, design, implementation, installation, commissioning, validation, maintenance and de-commissioning. The fact that "safety" and "life" are the key elements at the core of the standards should reinforce the purpose and scope of the documents.

For the process industries the standard IEC/EN 61511 provides relevant guidance for the user, including both hardware and software aspects of safety systems, as shown in Figure 2.1.



Note

Please consider the close relationship between the standards IEC/EN 61511 and IEC/EN 61508.

To implement their strategies within these overall safety requirements the plant operators and designers of safety systems, following the directives of IEC/EN 61511 for example, utilise equipment developed and validated according to IEC/EN 61508 to achieve their safety instrumented systems (SIS).

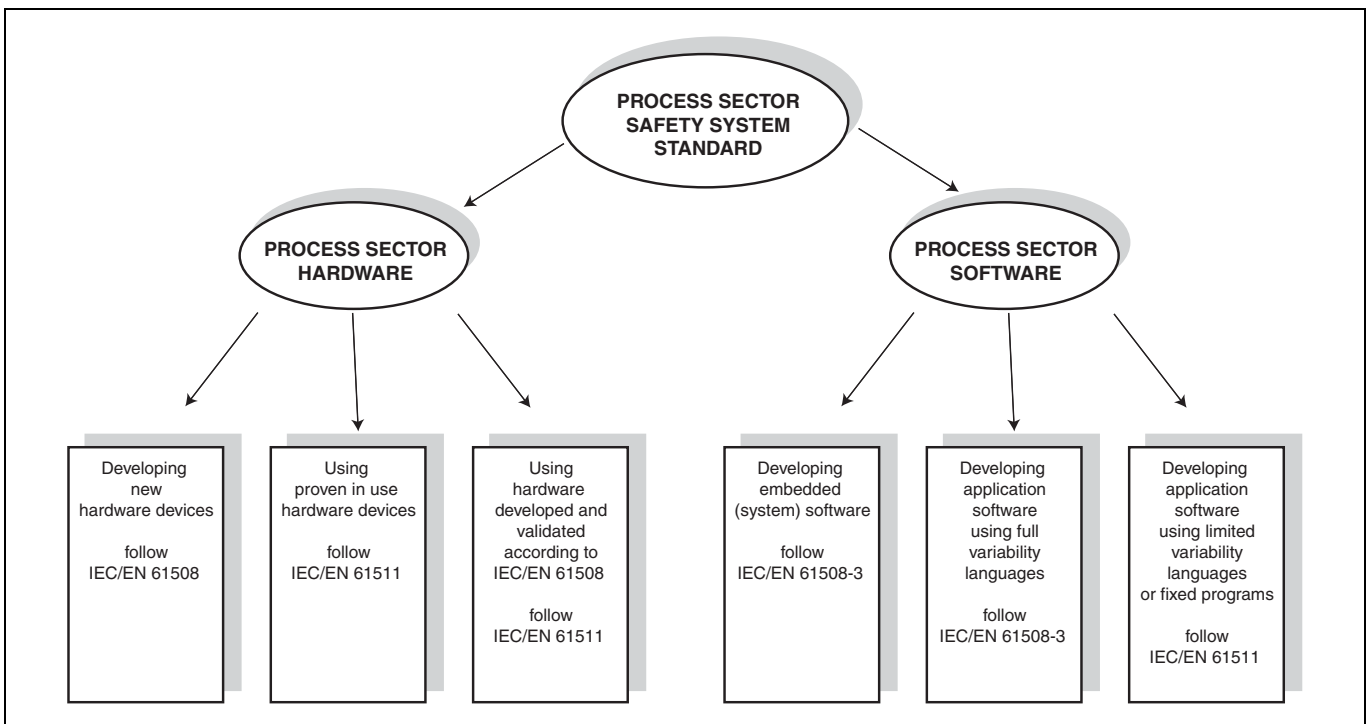


Figure 2.1 Scope IEC/EN 61508 and IEC/EN 61511

The standard IEC/EN 61508 deals specifically with "functional safety of electrical/electronic/programmable electronic safety-related systems" and thus, for a manufacturer of process instrumentation interface equipment such as Pepperl+Fuchs, the task is to develop and validate devices following the demands of IEC/EN 61508 and to provide the relevant information to enable the use of these devices by others within their SIS.

The SLC, as shown in Figure 2.2, includes a series of steps and activities to be considered and implemented.

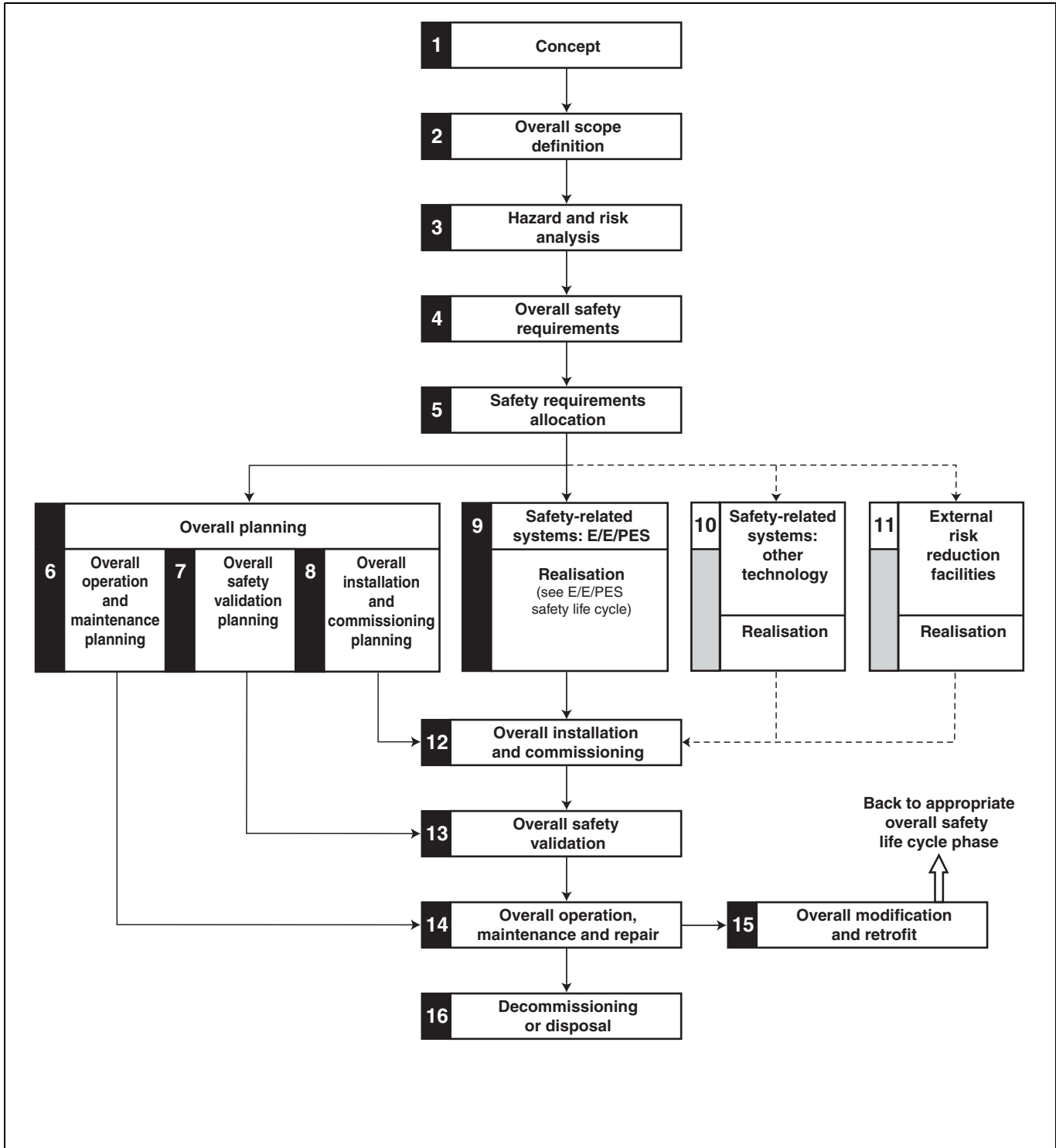


Figure 2.2 Phases of the safety life cycle

Within the SLC the various phases or steps may involve different personnel, groups, or even companies, to carry out the specific tasks. For example, the steps can be grouped together and the various responsibilities understood as identified below.

Analytical measures The first five steps can be considered as an **analytical** group of activities:

1. Concept
2. Overall scope definition
3. Hazard and risk analysis
4. Overall safety requirements
5. Safety requirements allocation

- and would be carried out by the plant owner/end user, probably working together with specialist consultants. The resulting outputs of overall definitions and requirements are the inputs to the next stages of activity.

Implementation measures The second group of **implementation** comprises the next eight steps:

6. Operation and maintenance planning
7. Validation planning
8. Installation and commissioning planning
9. Safety-related systems: E/E/PES implementation (further detailed in Figure 2.3)
10. Safety-related systems: other technology implementation
11. External risk reduction facilities implementation
12. Overall installation and commissioning
13. Overall safety validation

- and would be conducted by the end user together with chosen contractors and suppliers of equipment. It may be readily appreciated, that whilst each of these steps has a simple title, the work involved in carrying out the tasks can be complex and time-consuming!

Process operation The third group is essentially one of **operating** the process with its effective safeguards and involves the final three steps:

14. Overall operation and maintenance
15. Overall modification and retrofit
16. De-commissioning

- these normally being carried out by the plant end-user and his contractors.

Within the overall safety life cycle, we are particularly interested here in considering step 9 in greater detail, which deals with the aspects of any electrical/electronic/programmable electronic systems (E/E/PES).

To return to the standards involved for a moment: Following the directives given in IEC/EN 61511 and implementing the steps in the SLC, when the safety assessments are carried out and E/E/PES are used to carry out safety functions, IEC/EN 61508 then identifies the aspects which need to be addressed.

More details of the safety life cycle for an E/E/PES are shown in the following diagram. It can be seen that even at this overview level the integrity as well as the function of the safety systems are included in the specification. We will return to this issue later in the discussion.

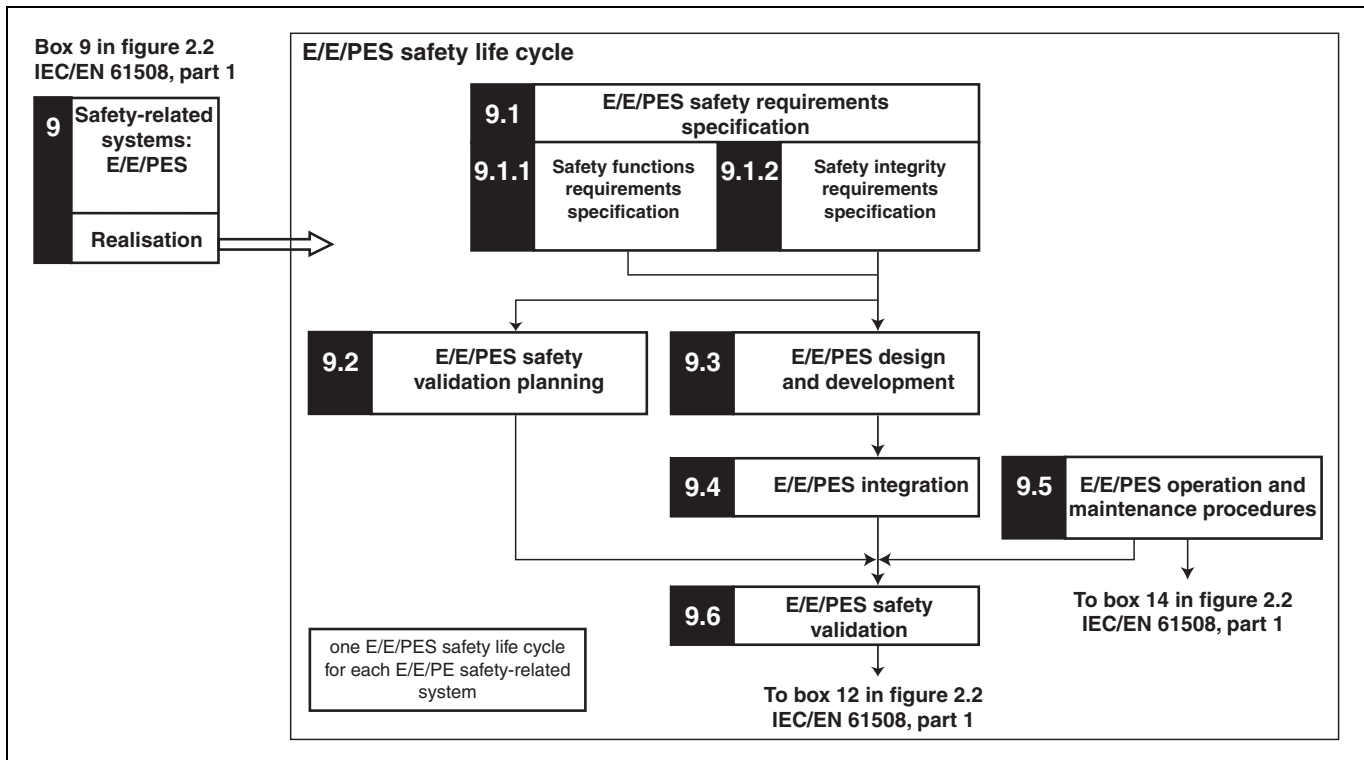


Figure 2.3 Safety life cycle of an E/E/PE System

There are essentially two groups, or types, of subsystems that are considered within the standard:

- the equipment under control (EUC) carries out the required manufacturing or process activity
- the control and protection systems implement the safety functions necessary to ensure that the EUC is suitably safe.

Fundamentally, the goal here is the achievement or maintenance of a safe state for the EUC.

You can think of the "control system" causing a **desired** EUC operation and the "protection system" responding to **undesired** EUC operation.



Note

Note that, dependent upon the risk-reduction strategies implemented, it may be that some control functions are designated as safety functions.

In other words, do not assume that all safety functions are to be performed by a separate protection system. (If you find it difficult to conceive exactly what is meant by the IEC/EN 61508 reference to EUC, it may be helpful to think in terms of "process", which is the term used in IEC/EN 61511.)

When any possible hazards are analysed and the risks arising from the EUC and its control system cannot be tolerated (see section 2.2), then a way of reducing the risks to tolerable levels must be found.

Perhaps in some cases the EUC or control system can be modified to achieve the requisite risk-reduction, but in other cases protection systems will be needed. These protection systems are designated safety-related systems, whose specific purpose is to mitigate the effects of a hazardous event or to prevent that event from occurring.

2.2 Risks and their reduction

One phase of the SLC is the analysis of hazards and risks arising from the EUC and its control system. In the standards the concept of risk is defined as the probable rate of

- occurrence of a hazard (accident) causing harm and
- the degree of severity of harm.

So risk can be seen as the product of "incident frequency" and "incident severity". Often the consequences of an accident are implicit within the description of an accident, but if not they should be made explicit.

There is a wide range of methods applied to the analysis of hazards and risk around the world and an overview is provided in both IEC/EN 61511 and IEC/EN 61508. These methods include techniques such as

HAZOP	HAZard and OPerability study
FME(C)A	Failure Mode Effect (and Criticality) Analysis
FMEDA	Failure Mode Effect and Diagnostics Analysis
ETA	Event Tree Analysis
FTA	Fault Tree Analysis

and other study, checklist, graph and model methods.



Note

This step of clearly identifying hazards and analysing risk is one of the most difficult to carry out, particularly if the process being studied is new or innovative.



Note

When there is a history of plant operating data or industry-specific methods or guidelines, then the analysis may be readily structured, but is still complex.

The standards embody the principle of balancing the risks associated with the EUC (i. e. the consequences and probability of hazardous events) by relevant dependable safety functions. This balance includes the aspect of tolerability of the risk. For example, the probable occurrence of a hazard whose consequence is negligible could be considered tolerable, whereas even the occasional occurrence of a catastrophe would be an intolerable risk.

If, in order to achieve the required level of safety, the risks of the EUC cannot be tolerated according to the criteria established, then safety functions must be implemented to reduce the risk.

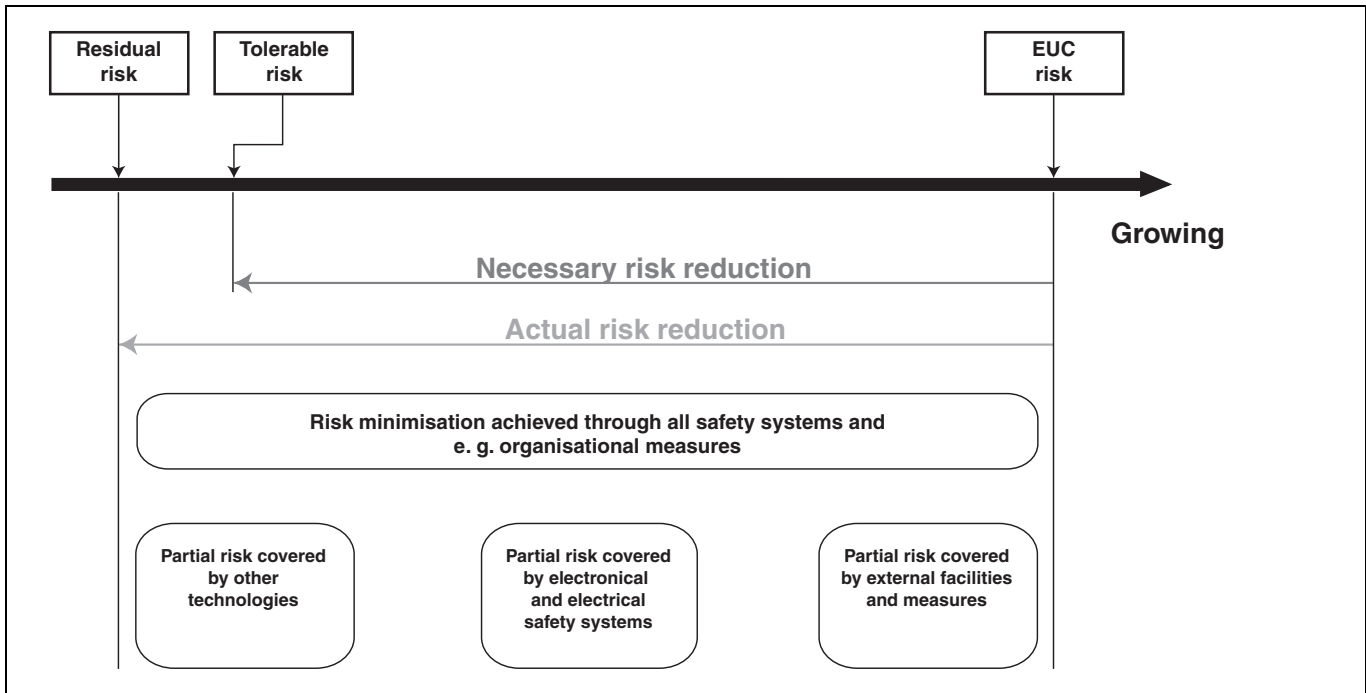


Figure 2.4 Relation between residual risk and tolerable risk

The goal is to ensure that the residual risk – the probability of a hazardous event occurring even with the safety functions in place – is less than or equal to the tolerable risk.

The diagram shows this effectively, where the risk posed by the EUC is reduced to a tolerable level by a "necessary risk reduction" strategy. The reduction of risk can be achieved by a combination of items rather than depending upon only one safety system and can comprise organisational measures as well.

The effect of these risk reduction measures and systems must be to achieve an "actual risk reduction" that is greater than or equal to the necessary risk reduction.

3 Safety integrity level (SIL)

As we have seen, analysis of hazards and risks gives rise to the need to reduce the risk and within the SLC of the standards this is identified as the derivation of the safety requirements. There may be some overall methods and mechanisms described in the safety requirements but also these requirements are then broken down into specific safety functions to achieve a defined task.

In parallel with this allocation of the overall safety requirements to specific safety functions, a measure of the dependability or integrity of those safety functions is required.

What is the confidence that the safety function will perform when called upon?

This measure is the safety integrity level or SIL. More precisely, the safety integrity of a system can be defined as

"the probability (likelihood) of a safety-related system performing the required safety function under all the stated conditions within a stated period of time."

Thus the specification of the safety function includes both the actions to be taken in response to the existence of particular conditions and also the time for that response to take place. The SIL is a measure of the reliability of the safety function performing to specification.

3.1 Probability of failure

To categorise the safety integrity of a safety function the probability of failure is considered – in effect the inverse of the SIL definition, looking at failure to perform rather than success.

It is easier to identify and quantify possible conditions and causes leading to failure of a safety function than it is to guarantee the desired action of a safety function when called upon.

Two classes of SIL are identified, depending on the service provided by the safety function.

- For safety functions that are activated when required (on demand mode) the probability of failure to perform correctly is given, whilst
- for safety functions that are in place continuously the probability of a dangerous failure is expressed in terms of a given period of time (per hour)(continuous mode).

In summary, IEC/EN 61508 requires that when safety functions are to be performed by E/E/PES the safety integrity is specified in terms of a safety integrity level. The probabilities of failure are related to one of four safety integrity levels, as shown in Table 3.1

Probability of failure		
Safety Integrity Level (SIL)	Mode of operation – on demand (average probability of failure to perform its design function upon demand)	Mode of operation – continuous (probability of dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 3.1 Probability of failure



Note

We have seen that protection functions, whether performed within the control system or a separate protection system, are referred to as safety related systems. If, after analysis of possible hazards arising from the EUC and its control system, it is decided that there is no need to designate any safety functions, then one of the requirements of IEC/EN 61508 is that the dangerous failure rate of the EUC control system shall be below the levels given as SIL1. So, even when a process may be considered as benign, with no intolerable risks, the control system must be shown to have a rate not lower than 10^{-5} dangerous failures per hour.

3.2 The system structure

3.2.1 Safe failure fraction

The safe failure fraction (SFF) is the fraction of the total failures that are assessed as either safe or diagnosed/detected (see section 6.2.3)

When analysing the various failure states and failure modes of components they can be categorised and grouped according to their effect on the safety of the device.

Failure rate definition

Thus we have the terms:

λ_{safe} = failure rate of components leading to a safe state

$\lambda_{\text{dangerous}}$ = failure rate of components leading to a potentially dangerous state

These terms are further categorised into "detected" or "undetected" to reflect the level of diagnostic ability within the device. For example:

λ_{dd} = dangerous detected failure rate

λ_{du} = dangerous undetected failure rate

The sum of all the component failure rates is expressed as:

$$\lambda_{\text{total}} = \lambda_{\text{safe}} + \lambda_{\text{dangerous}}$$

and the SFF can be calculated as

$$\text{SFF} = 1 - \lambda_{\text{du}} / \lambda_{\text{total}}$$

3.2.2 Hardware fault tolerance

One further complication in associating the SFF with a SIL is that when considering hardware safety integrity two types of subsystems are defined. For type A subsystems it is considered that all possible failure modes can be determined for all elements, while for type B subsystems it is considered that it is not possible to completely determine the behaviour under fault conditions.

Subsystem type A (e. g. a field transmitter)

- failure mode of all components well defined, and
- behaviour of the subsystem under fault conditions can be completely determined, and
- sufficient dependable failure data from field experience show that the claimed rates of failure for detected and undetected dangerous failures are met.

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % ... 90 %	SIL2	SIL3	SIL4
90 % ... 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Table 3.2 Hardware safety integrity: architectural constraints on type A safety-related subsystems (IEC/EN 61508-2, part 2)

Subsystem type B (e. g. a logic solver)

- the failure mode of at least one component is not well defined, or
- behaviour of the subsystem under fault conditions cannot be completely determined, or
- insufficient dependable failure data from field experience show that the claimed rates of failure for detected and undetected dangerous failures are met.

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % ... 90 %	SIL1	SIL2	SIL3
90 % ... 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

Table 3.3 Hardware safety integrity: architectural constraints on type B safety-related subsystems (IEC/EN 61508-2, part 3)

These definitions, in combination with the fault tolerance of the hardware, are part of the "architectural constraints" for the hardware safety integrity as shown in Table 3.2 and Table 3.3.



Note

Note that although mathematically a higher reliability might be calculated for a subsystem it is this "hardware safety integrity" that defines the maximum SIL that can be claimed.

In the tables above, a hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function. For example, if a subsystem has a hardware fault tolerance of 1 then 2 faults need to occur before the safety function is lost.

3.2.3 Connecting risk and safety integrity level

Already we have briefly met the concepts of risk, the need to reduce these risks by safety functions and the requirement for integrity of these safety functions.

One of the problems faced by process owners and users is how to associate the relevant safety integrity level with the safety function that is being applied to balance a particular risk. The risk graph shown in the Figure 3.1, based upon IEC/EN 61508, is a way of achieving the linkage between the risk parameters and the SIL for the safety function.

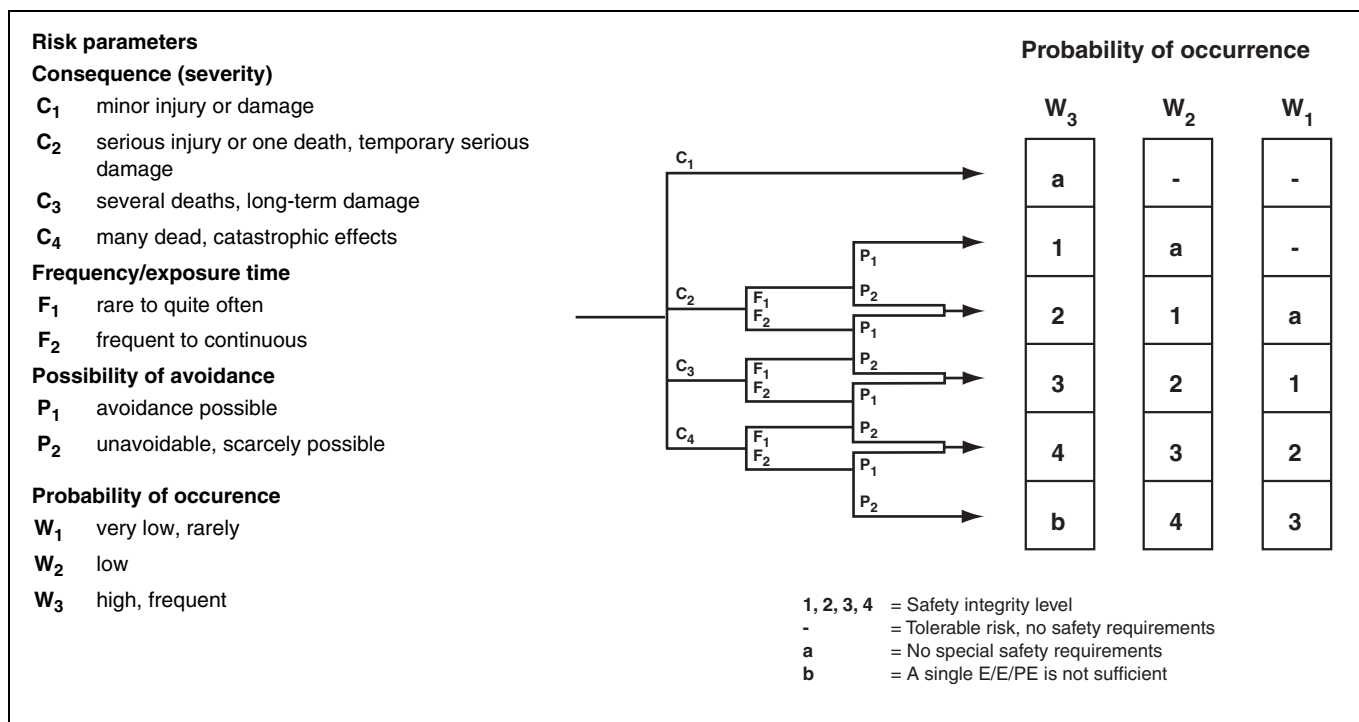


Figure 3.1 Risk assessment

For example, with the particular process being studied, the low or rare probability of minor injury is considered a tolerable risk, whilst if it is highly probable that there is frequent risk of serious injury then the safety function to reduce that risk would require an integrity level of three.

There are two further concepts related to the safety functions and safety systems that need to be explained before considering an example. These are the safe failure fraction and the probability of failure.

4 Probability of failure

4.1 Overview

An important consideration for any safety related system or equipment is the level of certainty that the required safe response or action will take place when it is needed. This is normally determined as the likelihood that the safety loop will fail to act as and when it is required to and is expressed as a probability.

The standards apply both to safety systems operating on demand, such as an emergency shut-down (ESD) system, and to systems operating "continuously" or in high demand, such as the process control system. For a safety loop operating in the demand mode of operation the relevant factor is the PFD_{avg} , which is the average probability of failure on demand. For a continuous or high demand mode of operation the probability of a dangerous failure per hour (PFH) is considered rather than PFD_{avg} .

Obviously the aspect of risk that was discussed earlier and the probability of failure on demand of a safety function are closely related.

Using the definitions

F_{np} = frequency of accident/event in the absence of protection functions

F_t = tolerable frequency of accident/event

then the risk reduction factor (ΔR) is defined as:

$$\Delta R = F_{np}/F_t$$

whereas PFD is the inverse:

$$PFD_{avg} = F_t/F_{np}$$

Since the concepts are closely linked, similar methods and tools are used to evaluate risk and to assess the PFD_{avg} .

As particular tools are used FMEDA and Markov models. Failure modes and effects analysis (FMEA) is a way to document the system being considered using a systematic approach to identify and evaluate the effects of component failures and to determine what could reduce or eliminate the chance of failure. An FMEDA extends the FMEA techniques to include on-line diagnostic techniques and identify failure modes relevant to safety instrumented system design.

Once the possible failures and their consequence have been evaluated, the various operational states of the subsystem can be associated using the Markov models, for example. One other factor that needs to be applied to the calculation is that of the interval between tests, which is known as the "proof time" or the "proof test interval". This is a variable that may depend not only upon the practical implementation of testing and maintenance within the system, subsystem or component concerned, but also upon the desired end result. By varying the proof time within the model it can result that the subsystem or safety loop may be suitable for use with a different SIL. Practical and operational considerations are often the guide.



Note also that "low demand mode" is defined as one where the frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof test frequency.

In the related area of application that most readers may be familiar with one can consider the fire alarm system in a commercial premises. Here, the legal or insurance driven need to frequently test the system must be balanced with the practicality and cost to organise the tests. Maybe the insurance premiums would be lower if the system were to be tested more frequently but the cost and disruption to organise and implement them may not be worth it.

With all the factors taken into consideration the PFD_{avg} can be calculated. Once the PFD_{avg} for each component part of the system has been calculated the PFD_{avg} of the whole system is simply the sum of the component PFD_{avg} , see also section 6.2.2 in part 2. To satisfy the requirements of a particular SIL both the PFD_{avg} and the SFF figures have to meet the specific limits.

4.2 Safety loop example

Let us summarise these points in a simple example from the processing industry.

The IEC/EN 61508 standard states that a safety integrity level can be properly associated only with a specific safety function – as implemented by the related safety loop – and not with a stand alone instrument or piece of equipment.

In our context, this means that – strictly speaking – it is only possible to state the compliance with the requirements of a specific SIL level after having analysed the whole safety loop.

It is however possible – and sensible – to analyse a single building block of a typical safety loop and to provide evidence that this can be used to finally obtain a SIL-rated safety loop. Since all the elements of a safety loop are interdependent in achieving the goal it is relevant to check that each piece is suitable for the purpose. For our example we will consider a single electronic isolator component.

Within the context of this example, the safety loop is a control system intended to implement a safety function. In the Figure 4.1 a typical safety loop is shown, including Intrinsically Safe signal input and output isolators for explosion protection, and let us assume that the safety integrity level required has been determined as SIL2. This is for reference only, and doesn't imply that a full safety loop assessment has been performed.

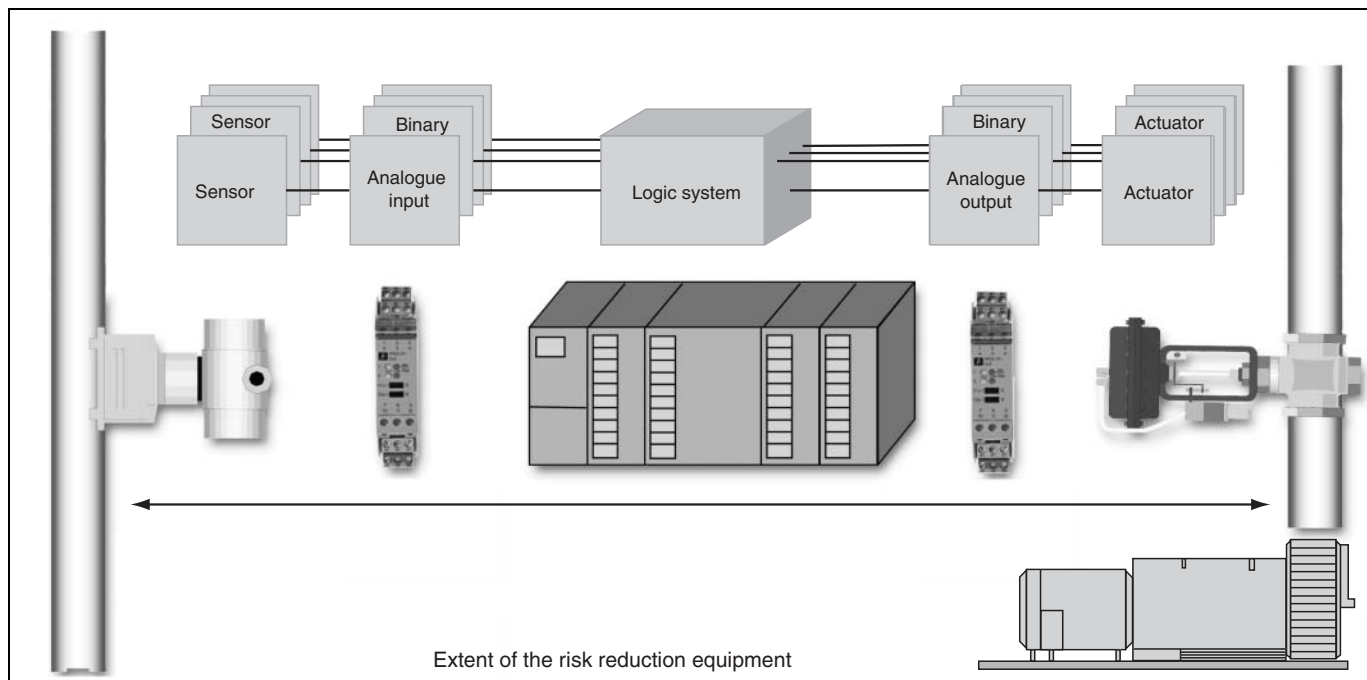


Figure 4.1 Safety instrumented system, example

You can identify in Figure 4.1 the various elements of the process loop

- Input sensor,
- Input line/input isolator block,
- Logic system (Logic solver, required to trigger the safety function),
- Output line/output isolator block (safe out) and finally
- Control valve (required to implement the safety function)

Considering that the typical safety loop as shown is made of many serially connected blocks, all of which are required to implement the safety function, the available PFD budget ($< 10^{-2}$ as for SIL2) has to be shared among all the relevant blocks.

For example, a reasonable, rather conservative, goal is to assign to the isolator no more than around 10 % of the available PFD budget, resulting in a PFD limit – at the isolator level – of around 10^{-3} , that is to say, 0.1 %. It should be clear, however, that this figure is only a reasonable guess, and doesn't imply that there is no need to evaluate the PFD at the safety loop level or that the isolator contribution can be neglected.

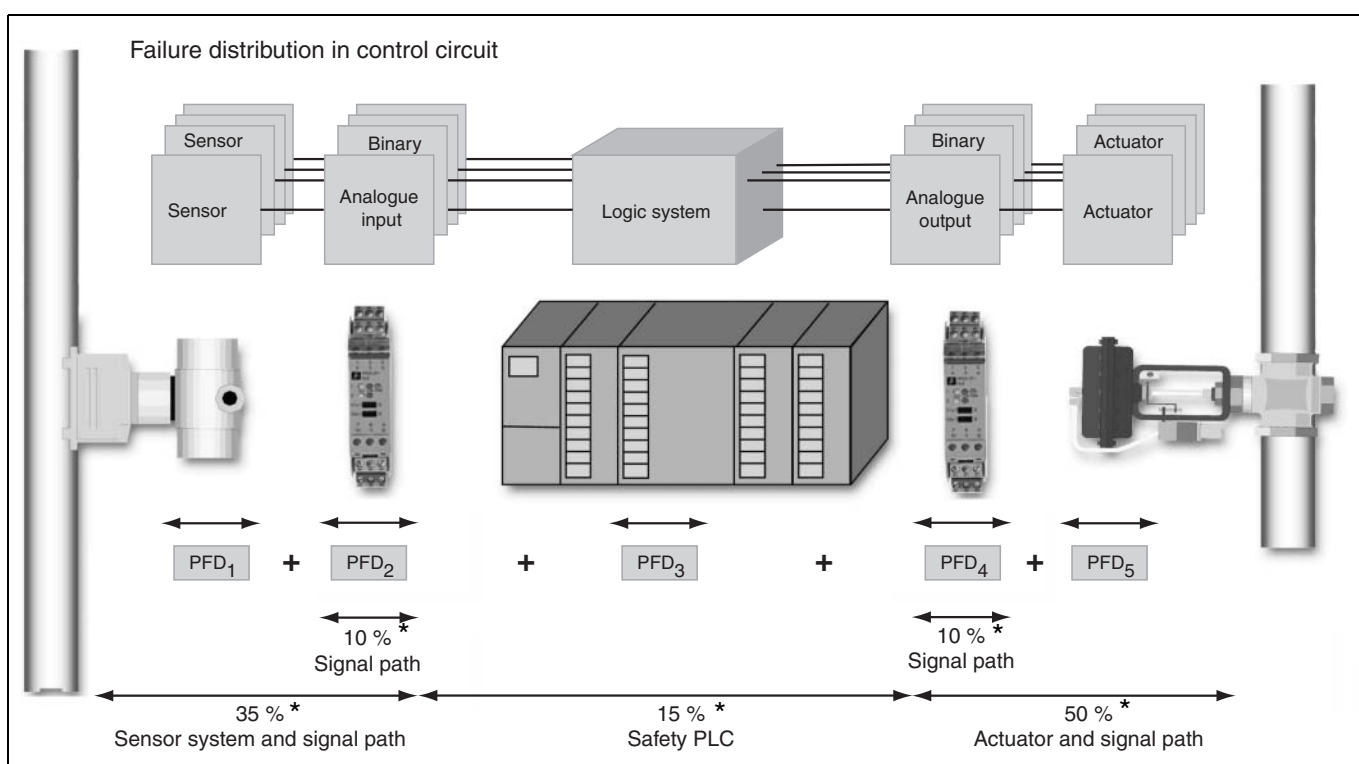


Figure 4.2 Verification of the safety instrumented system

* Numerical values depend on the application

The PFD value for the complete safety device is calculated from the values of the individual components. Since sensors and actuators are installed in the field, these are exposed to chemical and physical loading (Process medium, pressure, temperature, vibration, etc.). Accordingly, the risk of faults is high for these components. For this reason 25 % of the overall PFD is assigned to the sensors and 40 % to the actuators. Thus 15 % remains for the fault tolerant control system and 10 % each for the interface modules (the interface modules and control system have no contact with the process medium and are housed in the protected control room).

FMEA assessment

In this example, to demonstrate that the relevant isolators are suitable to be used within a SIL2 safety loop, a comprehensive FMEA analysis was carried out. The FMEA covered 100 % of the components and took into account, for each component, the different applicable failure modes including, when required, also intermittent and "derating" failures. This is the recommended procedure, according to IEC/EN 61508, with respect to other non-quantitative or semi-quantitative approaches.

As a result of the FMEA, the PFD_{avg} can be calculated for each of the relevant isolators and is shown to be less than 10^{-3} , thus enabling their possible use within this specific application.



Note

*Pepperl+Fuchs contract the specialist organisation **EXIDA** to carry out these assessments for their products.*

In summary can be determined for section 4.2:

1. IEC/EN 61508 considers the total instrumentation loop. Much like "a chain is only as strong as its weakest link" so, too, all the elements in the instrumentation loop play their part. Duplication of a particular block function may need to be applied to achieve the objectives.
2. Don't neglect any steps in assessing the life cycle. The instrumentation elements identified within this document are just one part of an SIS.
3. Unless specifically stated, it is not permitted to use more than one channel of a multi-channel interface device in the **same** safety loop. The remaining channels of the device can however be used in other independent safety loops.
4. It is false to assume that all safety functions are to be implemented in a separate protection system – some safety functions may be included in the control system.
5. To prove their satisfactory operation, safety functions may need to be exercised and the frequency of conducting these tests is a factor in calculating the probability of failure on demand. Thus different PFD_{avg} values for components such as our isolators are calculated for relevant intervals between tests, for example $T_{[proof]}$ of 1 year, 5 years and 10 years.

5 Summary of the first part of the SIL manual

1. The concept of the safety life cycle introduces a structured statement for risk analysis, for the implementation of safety systems and for the operation of a safe process.
2. If safety systems are employed in order to reduce risks to a tolerable level, then these safety systems must exhibit a specified safety integrity level.
3. The calculation of the safety integrity level for a safety system embraces the factors "safe failure fraction" and "failure probability of the safety function".

6 Verification of the safety integrity level of a safety instrumented function



This short introduction covers only the technical aspects related to the implementation of a safety related function according to the requirements of the IEC/EN 61508/61511. See also part 1.

6.1 What is SIL?

6.1.1 Basics

SIL means safety integrity level according to IEC/EN 61508 and describes the integrity of a safety related function. **Management** and **technical measures** are necessary to achieve a given integrity. A SIL is attributed to a safety function, which includes different function blocks describing systems (such as sensors, logic systems (logic solvers) and actuators).

A safety instrumented system (SIS) consists of one or more safety related functions, each of which have a SIL requirement. A component, subsystem and system do not have SILs in their own right.

Systems have "SIL limitation effect". For example the following function (Figure 6.1) can only claim SIL2 because of the limitation of the sensor system:

- Sensor system: max. SIL2
- Logic system (logic solver): max. SIL3
- Output element: max. SIL3

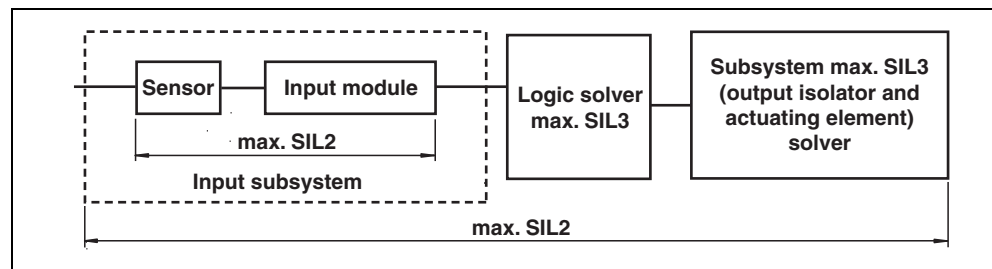


Figure 6.1 System structure

Within a system, components or subsystems can be combined (in parallel for example) in order to modify the SIL limitation.

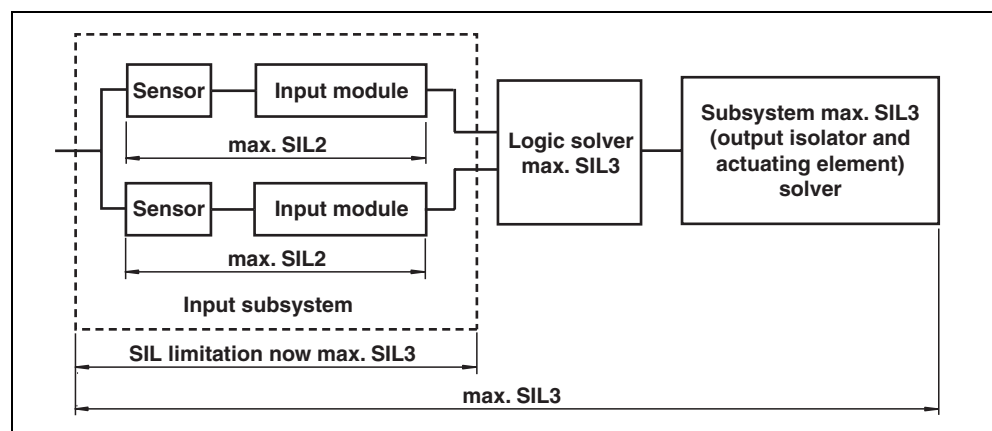


Figure 6.2 Example configuration for redundant sensor channels

6.1.2 Management requirements

Studies have found that the most important factor in the occurrence of accidents is management commitment to safety and the basic safety culture in the organisation or industry. For that reason, the relevant standards (IEC/EN 61508 or IEC/EN 61511 in the process sector) describe a lifecycle of the safety related function and its components and require also the implementation of management measures.

6.1.3 How to achieve the selected safety integrity level?

A SIL assessed product presents some specific parameters. The SIL limitation created by this product is directly affected by these parameters:

- Hardware fault tolerance
- Safe failure fraction
- Architectural constraints (see section 6.4)
- Probability of failure on demand
 - PFD (probability of failure on demand)
 - low demand mode
 - PFH (probability of dangerous failure per hour)
 - continuous mode
- Maintenance intervals.

All of these parameters are numerical values, which have to be combined with the corresponding values of the other components of the safety related function and then checked with the values of the target SIL in the relevant standard (IEC/EN 61508 or IEC/EN 61511).

In order to combine or verify different systems or subsystems, it is necessary to know how the different parameters are acting together.

6.2 Example input subsystem with 2 components

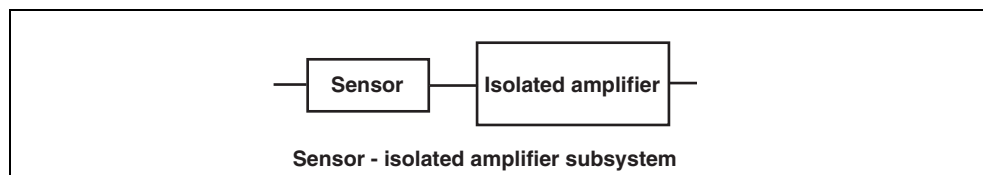


Figure 6.3 Input subsystem

6.2.1 Failure mode and effect analysis (IEC/EN 61508, part 2)

The different failure rates of the subsystem were calculated using FMEDA. Then the values of PDF_{avg} and safe failure fraction (SFF) were calculated and are stated in the manufacturer's documentation.

In our example **Sensor component:** NAMUR proximity switch NJ2-12GM-N (SJ2-N*)

$T_{[proof]}$	$PFD_{avg s}$	SFF
1 year	3.02×10^{-5}	> 76 %
2 years	6.05×10^{-5}	> 76 %
5 years	1.51×10^{-4}	> 76 %

$$\lambda_{total} = 2.90 \times 10^{-8} \text{ 1/h}$$

$$\lambda_{safe} = 1.77 \times 10^{-8} \text{ 1/h}$$

$$\lambda_{dangerous} = 6.91 \times 10^{-9} \text{ 1/h}$$

$$\lambda_{don't \text{ care}} = 4.42 \times 10^{-9} \text{ 1/h}$$

Isolated amplifier component: isolated switching amplifier KFD2-SOT2-Ex1.N

$T_{[proof]}$	$PFD_{avg I}$	SFF
1 year	9.21×10^{-5}	> 89 %
2 years	1.84×10^{-4}	> 89 %
5 years	4.60×10^{-4}	> 89 %

$$\lambda_{total} = 2.07 \times 10^{-7} \text{ 1/h}$$

$$\lambda_{safe} = 7.83 \times 10^{-8} \text{ 1/h}$$

$$\lambda_{dangerous} = 2.10 \times 10^{-8} \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1.08 \times 10^{-7} \text{ 1/h}$$

6.2.2 Average probability of failure on demand (PFD_{avg}) of the input subsystem (IEC/EN 61508, part 2 und part 6, annex B)

Failure rate λ_d is the dangerous (detected and undetected) failure rate of a channel in a subsystem. For the PFD calculation (low demand mode) it is stated as failures per year.

Target failure measure PFD_{avg} is the average probability of failure on demand of a safety function or subsystem, also called average probability of failure on demand. The probability of a failure is time dependant:

$$\text{PFD: } Q(t) = 1 - e^{-\lambda dt}$$

It is a function of the failure rate λ and the time t between proof tests.



Note

That means that you cannot find out the maximum SIL of your (sub)system if you do not know if a test procedure is implemented by the user and what the test intervals are!

The maximum SIL according to the failure probability requirements is then read out from table 3 of IEC/EN 61508 part 1 (low demand mode):

Safety integrity level (SIL)	Low demand mode of operation (average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 6.1 Safety integrity level: target failure measures for a safety function in the low demand mode of operation

These values are required for the whole safety function, usually including different systems or subsystems. The average probability of failure on demand of a safety function is determined by calculating and combining the average probability of failure on demand for all the subsystems, which together provide the safety function.

If the probabilities are small, this can be expressed by the following:

$$PFD_{sys} = PFD_s + PFD_l + PFD_{fe}$$

where

- PFD_{sys} is the average probability of failure on demand of a safety function safety-related system;
- PFD_s is the average probability of failure on demand for the sensor subsystem;
- PFD_l is the average probability of failure on demand for the logic subsystem; and
- PFD_{fe} is the average probability of failure on demand for the final element subsystem.



Note

This means that a subsystem or component cannot claim the whole PFD value for a given SIL! Usually, isolators have a PFD, which claims 10 % of the total PFD value of the required SIL.

In our example

$$PFD_{subsys} = PFD_s + PFD_l$$

where

- PFD_{subsys} is the average probability of failure on demand for the input subsystem;
- PFD_s is the average probability of failure on demand for the sensor;
- PFD_l is the average probability of failure on demand for the isolated amplifier.

The maximum SIL limit of the input subsystem, according to the target failure measure for low demand mode (PFD_{subsys} less than 10 % PFD_{max}), will be:

$T_{[proof]}$	PFD_{subsys}	SIL
1 year	1.22×10^{-4}	2
2 years	2.45×10^{-4}	2
5 years	6.11×10^{-4}	2

6.2.3 Safe failure fraction (SFF) (IEC/EN 61508, part 2, annex C)

Fraction of the failure rate, which does not have the potential to put the safety related system in a hazardous state.

$$SFF = (\Sigma\lambda_s + \Sigma\lambda_{dd}) / (\Sigma\lambda_s + \Sigma\lambda_d) = 1 - \Sigma\lambda_{du} / (\Sigma\lambda_s + \Sigma\lambda_d)$$

where $\Sigma\lambda_s = \Sigma\lambda_{su} + \Sigma\lambda_{sd}$ und $\Sigma\lambda_d = \Sigma\lambda_{du} + \Sigma\lambda_{dd}$

Dangerous detected failures are also considered as safe.

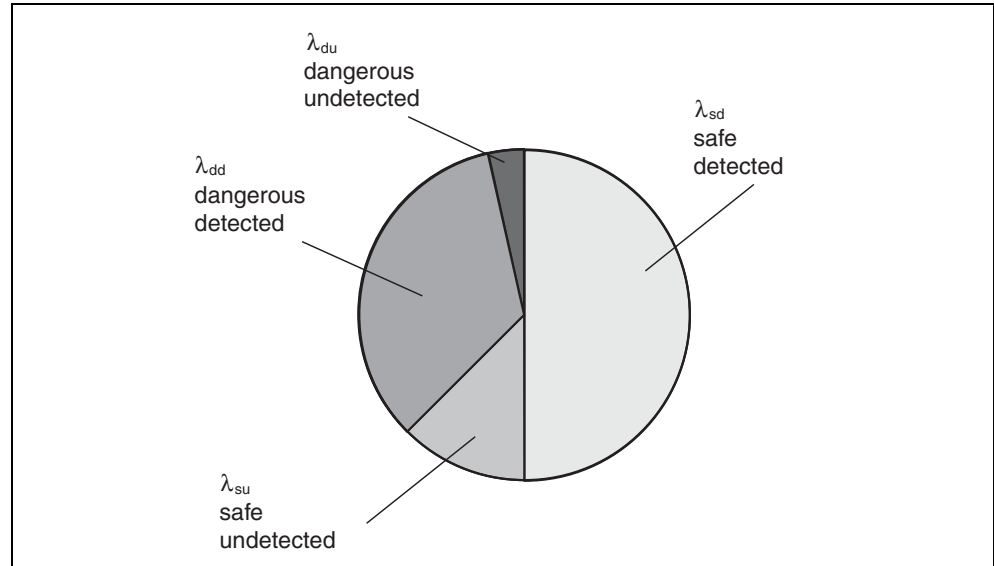


Figure 6.4 Safe failure fraction (SFF)

In our example

$$SFF = \frac{(1.77 + 0.442 + 7.83 + 10.8) \times 10^{-8}}{(1.77 + 0.442 + 7.83 + 10.8 + 0.691 + 2.1) \times 10^{-8}}$$

SFF of the input subsystem > 88 %

6.3 Hardware fault tolerance (IEC/EN 61508, part 2)

This is the ability of a functional unit to perform a required function in the presence of faults. A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

A one-channel system will not be able to perform its function if it is defective! A two-channel architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be a dangerous failure in both channels before a safety function failed on demand.

In our example The input subsystem has one channel; the

Hardware fault tolerance of the input subsystem = 0

6.4 SIL limitation due to architectural constraints (IEC/EN 61508, part 2)

The combination of safe failure fraction and hardware fault tolerance limits the maximum SIL of our device.

The standard distinguishes between two types of subsystems:

Subsystem type A A subsystem can be regarded as type A if, for the components required to achieve the safety function

- the failure modes of all constituent components are well defined; and
- the behaviour of the subsystem under fault conditions can be completely determined; and
- there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % ... 90 %	SIL2	SIL3	SIL4
90 % ... 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Table 6.2 Safety integrity of the hardware: architectural constraints on type A safety-related subsystems (IEC/EN 61508, part 2)

Subsystem type B A subsystem shall be regarded as type B, if for the components required to achieve the safety function

- the failure mode of at least one constituent component is not well defined; or
- the behaviour of the subsystem under fault conditions cannot be completely determined; or
- there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.

Simplifying, one can say that as long as programmable or highly integrated electronic components are used, a subsystem must be considered as type B.

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % ... 90 %	SIL1	SIL2	SIL3
90 % ... 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

Table 6.3 Safety integrity of the hardware: architectural constraints on type B safety-related subsystems (IEC/EN 61508, part 2)

In our example Both components of the subsystem are type A with a SFF of max. 88 % and a hardware fault tolerance of 0. The subsystem achieves the requirements for maximum SIL2.

Results of our example assessment (PFD_{subsys} less than 10 % PFD_{max}):

$T_{[\text{proof}]}$	PFD	Architectural constraints	SIL of the subsystem
1 year	SIL2	SIL2	2
2 years	SIL2	SIL2	2
5 years	SIL2	SIL2	2

7 Other structures

7.1 MooN system (IEC/EN 61508, part 6)

Safety system, or part thereof, made up of N independent channels, which are so connected, that M channel(s) is (are) sufficient to perform the safety function (M out of N). The architecture of the following example is called 1oo2 (one out of two).

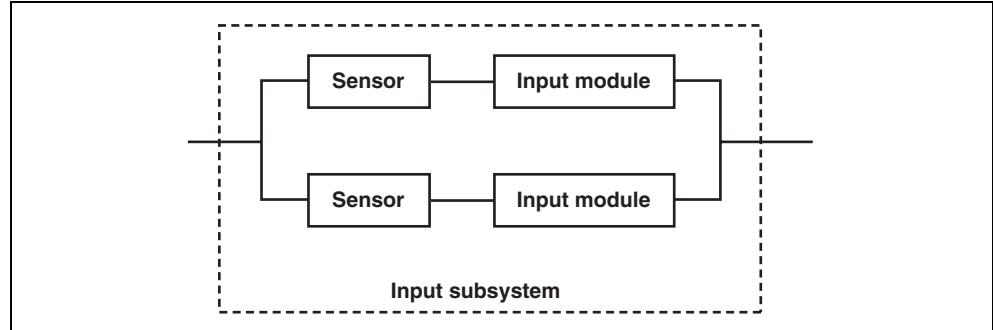


Figure 7.1 Configuration for two sensor subsystems, 1oo2-structure

7.2 Two sensor subsystems from our example configured as a two channel input subsystem



The calculations use simplified formulae (for example, the time to repair is not considered here) and may not be suitable for your application. See IEC/EN 61508, part 6 for more information.

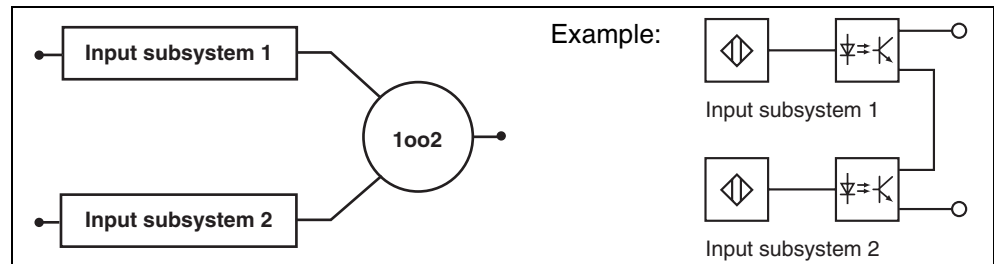


Figure 7.2 Example redundant input subsystem

The two outputs of the isolated switching amplifier are connected in series.

SIL assessment of the redundant input subsystem consisting of NJ2-12GM-N and KFD2-SOT2-Ex.N.

$PDF_{channel}$ (see section 6.2.2)

$T_{[proof]}$	PFD_{sys}
1 year	1.22×10^{-4}
2 years	2.45×10^{-4}
5 years	6.11×10^{-4}

PDF of the redundant input subsystem

$$PDF_{sys} = 4/3 \times PDF_{channel}^2$$

$T_{[proof]}$	PFD_{sys}
1 year	1.98×10^{-8}
2 years	8.00×10^{-8}
5 years	4.98×10^{-7}

SFF of the new redundant input subsystem

Both channels are identical, the safe failure fraction does not change.

SFF of the new redundant input subsystem > 88 %

Hardware fault tolerance

The new input subsystem is now redundant (1oo2)

Hardware fault tolerance = 1

Results of the new redundant input subsystem SIL assessment (PDF_{sys} less than 10 % PDF_{max}):

$T_{[proof]}$	PDF_{sys}	Architectural constraints	SIL of the new redundant input subsystem
1 year	SIL4	SIL3	SIL3
2 years	SIL4	SIL3	SIL3
5 years	SIL4	SIL3	SIL3



Attention

The calculation does not take account of any faults due to common causes (see section 7.3).

7.3 Common cause failures

Common cause failures must be taken into consideration in safety instrumented systems. If, for example, both channels of a 1oo2 structure are powered by the same power supply, the safety function will not be performed if a failure occurs in this power supply. This "channel separation" is described by a parameter (β), which is obtained by checking the quality of the channel diversity or separation with a table in annex D of part 6 of IEC/EN 61508 (scoring system). Table 7.1 shows an extract of this annex D table

Item	Logic subsystem		Sensors and final elements	
	X _{LS}	Y _{LS}	X _{SF}	Y _{SF}
Separation/segregation				
Are all signal cables for the channels routed separately at all positions?	1.5	1.5	1.0	2.0
Are the logic subsystem channels on separate printed-circuit boards?	3.0	1.0		
Are the logic subsystem channels in separate cabinets?	2.5	0.5		
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?			2.5	1.5
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?			2.5	0.5
Diversity/redundancy				
Do the channels employ different electrical technologies – for example, one electronic or programmable electronic and the other relay?	7.0			
Do the channels employ different electronic technologies – for example, one electronic, the other programmable electronic?	5.0			
Do the devices employ different physical principles for the sensing elements – for example, pressure and temperature, vane anemometer and Doppler transducer, etc?			7.5	
Do the devices employ different electrical principles/designs – for example, digital and analogue, different manufacturer (not re-badged) or different technology?			5.5	
Do the channels employ enhanced redundancy with MooN architecture, where $N > M + 2$?	2.0	0.5	2.0	0.5
Do the channels employ enhanced redundancy with MooN architecture, where $N = M + 2$?	1.0	0.5	1.0	0.5
Is low diversity used, for example hardware diagnostic tests using same technology?	2.0	1.0		
Is medium diversity used, for example hardware diagnostic tests using different technology?	3.0	1.5		
Were the channels designed by different designers with no communication between them during the design activities?	1.0	1.0		
Are separate test methods and people used for each channel during commissioning?	1.0	0.5	1.0	1.0
Is maintenance on each channel carried out by different people at different times?	2.5		2.5	

Table 7.1 Scoring programmable electronics or sensors/final elements (extract)

The usual values are:

- Field devices together with their cabling: between 5 % and 10 %
- Safety PLC: 1 %

In our example What is the influence of common cause failures β

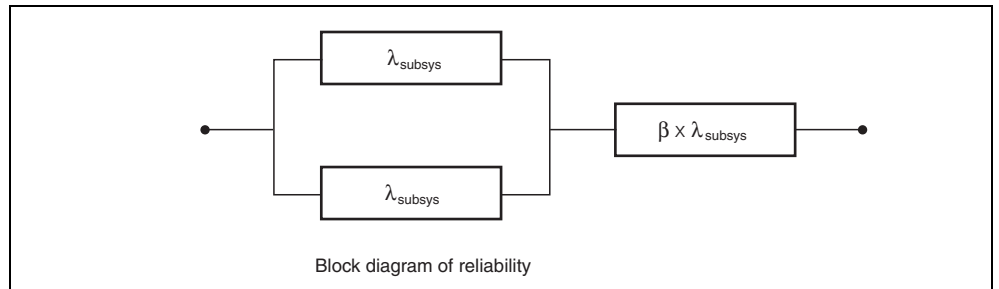


Figure 7.3 Assessment of the quality of the channel separation

As a simplification, we consider a β factor of 5 %.

$$PFD_{sys} = PFD_{red} + \beta \times PFD_{subsys}$$

where

PFD_{subsys} is the PFD of a single input subsystem and

PFD_{red} is the PFD of the redundant input subsystem without the common cause failures

PFD_{sys} is the PFD of the redundant input subsystem with the common cause failures

$$PFD_{red} = 4/3 \times PFD_{subsys}^2$$

$$PFD_{sys} = 4/3 \times PFD_{subsys}^2 + \beta \times PFD_{subsys}$$

$T_{[proof]}$	PFD_{subsys}	PFD_{red}	PFD_{sys}
1 year	1.22×10^{-4}	1.98×10^{-8}	6.11×10^{-6}
2 years	2.45×10^{-4}	8.00×10^{-8}	1.23×10^{-5}
5 years	6.11×10^{-4}	4.98×10^{-7}	3.10×10^{-5}

Results of the new redundant input subsystem SIL assessment with common cause failures (PFD_{sys} less than 10 % PFD_{max}):

$T_{[proof]}$	PFD_{sys}	Architecture	SIL_{sys}
1 year	SIL4	SIL3	SIL3
2 years	SIL3	SIL3	SIL3
5 years	SIL3	SIL3	SIL3

These results show clearly the huge influence of the quality of the separation between channels on the probability of dangerous failures.

8 Proven in use (IEC/EN 61508, part 2)

A component or subsystem may be considered as proven in use when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system.

The volume of operating experience shall be sufficient to support the claimed rates of failure due to random hardware faults on a statistical basis. Only previous operation where failures of the component have been effectively detected and reported shall be taken into account in the analysis.



Note

Further information you can find in the EN 61511.

9 How to read a SIL product report?

SIL qualified products are useless if the required data for the overall safety function SIL verification are not supplied. Usually the PFD and SFF are represented in the form of tables and calculated for different proof intervals. The calculations are based on a list of assumptions, which represent the common field of application of the device (which may not correspond with yours). In this case, some of the calculations are invalid and must be reviewed or other actions must be taken, such as safe shut-down of the process.

Assumptions:

- Failure rates are constant; mechanisms subject to "wear and tear" are not included
- Propagation of failures is not relevant
- All component failure modes are known
- The repair time after a safe failure is 8 hours
- The average temperature over a long period of time is 40 °C
- The stress levels are average for an industrial environment
- All modules are operated at low demand

Failure categories	T _[proof] = 1 year	T _[proof] = 2 years	T _[proof] = 5 years	SFF
Fail low (L) = safe Fail high (H) = safe	PFD _{avg} = 1.6 x 10.	PFD _{avg} = 3.2 x 10.	PFD _{avg} = 8.0 x 10.	> 91 %
Fail low (L) = safe Fail high (H) = dangerous	PFD _{avg} = 2.2 x 10.	PFD _{avg} = 4.5 x 10.	PFD _{avg} = 1.1 x 10.	> 87 %
Fail low (L) = dangerous Fail high (H) = safe	PFD _{avg} = 7.9 x 10.	PFD _{avg} = 1.6 x 10.	PFD _{avg} = 3.9 x 10.	> 56 %
Fail low (L) = dangerous Fail high (H) = dangerous	PFD _{avg} = 8.6 x 10.	PFD _{avg} = 1.7 x 10.	PFD _{avg} = 4.3 x 10.	> 52 %

Table 9.1 Example of the report of a SMART transmitter isolator




Column failure categories

The PFD and SFF of this device depend of the overall safety function and its fault reaction function. If, for example, a "fail low" failure will bring the system into a safe state and the "fail high" failure will be detected by the logic solver input circuitry, then these component faults are considered as safe and line 1 can be used.

If, on the other hand, a "fail low" failure will bring the system into a safe state and the "fail high" failure will not be detected and could lead to a dangerous state of the system, then this fault is a dangerous fault and the values of line 2 have to be used.

Column T_[proof] and SFF

Pepperl+Fuchs have limited the maximum PFD of an isolator to 10 % of the maximum allowed value for a given SIL (in this case SIL2).

-  Green means a PFD part smaller than 10 % of total value of SIL2.
-  Yellow means a PFD part greater than 10 % of total value of SIL2.
-  The red values in the SFF column are not compatible with the architecture constraints of the given SIL (in this case SIL2). A SFF < 60 % limits a system with a hardware fault tolerance of 0 to SIL1.

10 Glossary/formulae

10.1 Failure rate $\lambda(t)$

The failure rate $\lambda(t)$ indicates the magnitude of the relative number of failures during a specified observation period. Therefore for an individual component the failure rate λ is a direct indication of the failure probability during the above-mentioned observation period. The following applies:

Formula 1

$$\lambda(t) = \frac{\text{Number of failures during a specified observation period}}{\text{Number of observed components} \times \text{observation period}}$$

Thus, together with the two following definitions it follows that:

Definitions:

Δt = Observation period

$n(t)$ = Number of functioning components at the point in time t

Formula 2

$$\lambda(t) = \frac{n(t) - n(t + \Delta t)}{n(t) \times \Delta t}$$

The unit for the failure rate λ is 1/time. Here the failure rate of 10^{-9} h^{-1} is frequently abbreviated with the letters FIT (**F**ailures **I**n **T**ime).

Normally components and systems have an increased failure rate at the start of their lives, which however quickly reduces (so-called early failures). After a short period of operation the failure rate reaches a value, which remains substantially constant over a long period of time. As a rule, after a very long period of operation an increase in the failure rate is observed, which is usually due to wear. Because of this behavior of the failure rate with time, reference is sometimes made to a "bathtub curve".

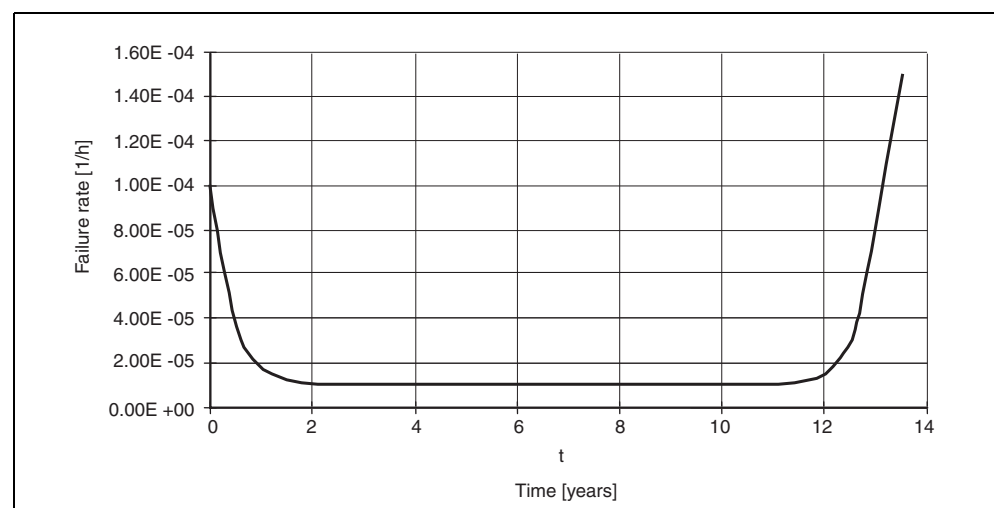


Figure 10.1 Behavior of the failure rate over a long period of time

Example:

10,000 components are subjected to a life test. Three components fail within one week. Thus, for the failure rate:

$$\lambda = \frac{10000 - 9997}{10000 \times 7 \times 24 \text{ h}} = \frac{3}{1680000 \text{ h}} \approx 1.8 \times 10^{-6} \frac{1}{\text{h}} = 1800 \text{ FIT}$$

10.2 Constant failure rate λ

In order to simplify calculations, it is normally only the part of the bathtub curve, in which the failure rate is constant, that is used. The usual argument for this is that early failures need not be considered, since these will have already occurred before or during commissioning (i. e. with the manufacturer or during commissioning). Another consideration, is that all calculated results, which have been obtained under the assumption of a constant failure rate, are only applicable so long as no wear has taken place. In the case of electronic equipment the usual assumption is that under normal operating conditions signs of wear should not be observed for between 8 to 12 years from new (EN 61508, part 2, chapter 7.4.7.4, remark 3).

Formula 3 $\lambda(t) = \text{constant} = \lambda$ for $t = 0 \dots \approx 10 \text{ years}$

10.3 Failure probability $F(t)$

Under the assumption, that the failure rate $\lambda(t)$ is constant ("bottom of the bathtub curve"), the failure probability of a component can be easily determined. The following applies:

Formula 4 $F(t) = 1 - e^{-\lambda \times t}$

Since in practice the exponent of the e-function is always significantly less than 1 ($\lambda \times t \ll 1$), equation (formula 4) can be further simplified. One then obtains for the failure probability $F(t)$ the simple expression:

Formula 5 $F(t) \approx \lambda \times t$



This approximation loses validity at large values of λ and/or long time intervals.

Example:

The failure rate of a sensor is $\lambda = 30 \text{ FIT}$ or $\lambda = 30 \times 10^{-9} \text{ h}^{-1}$

The probability, that the sensor could fail within its first year of operation, can be easily calculated from Formula 5 (1 year = 8760 h). One obtains:

$$F(1 \text{ year}) = 30 \times 10^{-9} \text{ h}^{-1} \times 8760 \text{ h} = 2.63 \times 10^{-4}$$

10.4 Probability density function f(t)

The density function f(t) of the probability is given by the derivative of the distribution function F(t). The expectation value of a variate can be calculated using the probability density (here: expectation value of life MTTF, **Mean Time To Failure**).

The derivative with respect to time of Formula 4 is:

Formula 6 $f(t) = \lambda \times e^{-\lambda \times t}$

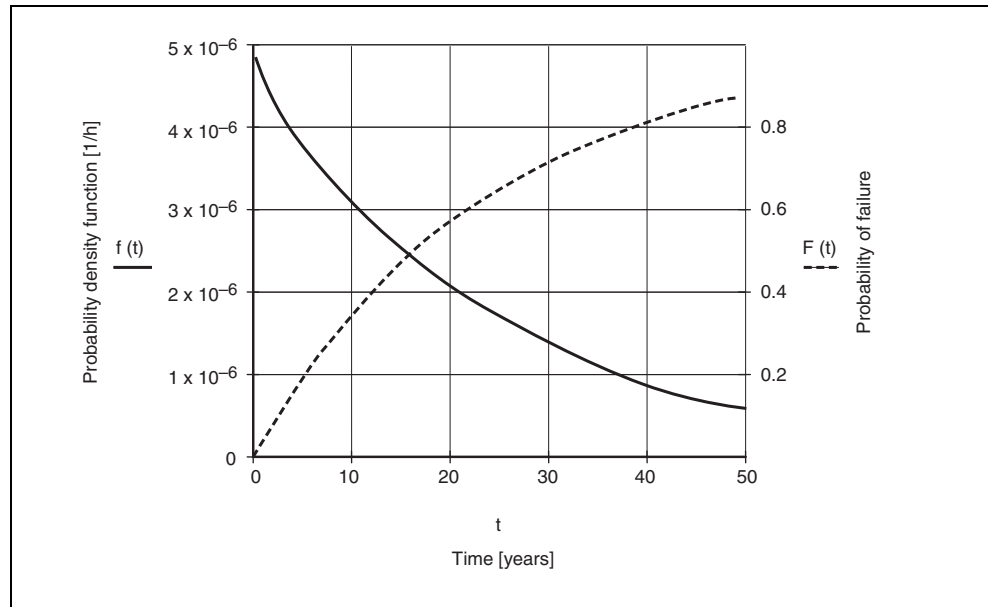


Figure 10.2 Failure probability and density function



Note

It is recognized, that at the start of the operating time (here, for example up to approx. 8 years) the failure probability increases approximately linearly with time.

10.5 Reliability function R(t)

The reliability function R(t) represents the probability, that a component will successfully carry out its function up to the point in time t.

Since the reliability function R(t) involves the complementary parameters for the failure probability F(t), these can be easily calculated, in that the failure probability F(t) is subtracted from 1. One obtains:

Formula 7 $R(t) = 1 - F(t) = 1 - (1 - e^{-\lambda \times t})$
 $R(t) = e^{-\lambda \times t}$

10.6 Mean life MTTF

The expected life can be calculated as follows from the density function of the failure probability:

Formula 8

$$\text{MTTF}(t) = \int_0^{\infty} t \times f(t) dt = \int_0^{\infty} t \times \lambda \times e^{-\lambda \times t} dt = \frac{1}{\lambda}$$

Alternatively, the mean life can also be calculated, as follows, using the reliability function R(t):

Formula 9

$$\text{MTTF}(t) = \int_0^{\infty} R(t) dt = \int_0^{\infty} e^{-\lambda \times t} dt = \frac{1}{\lambda}$$



The relationship $\text{MTTF} = 1/\lambda$ only applies to systems free from wear. Since electronic devices and components are subject to wear, it is in general not permissible to designate the reciprocal of the (constant) failure rate λ as the MTTF.

10.7 Mean failure probability of the function in the demand case PFD (Probability of Failure on Demand)

For safety functions, which are only required in the case of a fault, the **Probability of Failure on Demand**, PFD is of interest. This probability of failure represents an important criterion in the context of IEC/EN 61508 for the qualitative evaluation of a safety function.

Fundamentally, the above-mentioned failure probability involves a time-dependant parameter. That is to say, when the safety function is required, the probability of its failure is more or less high. In order to obtain the simplest possible statement in respect of the reliability of a safety function and in order to simplify the corresponding calculations, in the context of IEC/EN 61508 the mentioned time dependency is eliminated by the generation of mean values (PFD_{avg}). Therefore, when in the following "PFD" is mentioned, this always implies its mean value (strictly speaking, the PFD_{avg}).

Two different types of failure have to be considered in the calculation of the PFD. On the one hand these are the dangerous unrecognized failures (Failure rate λ_{du}) and on the other hand the dangerous recognized failures (Failure rate λ_{dd}). The latter therefore influence the PFD, since in the case of the occurrence of a failure of this type the device involved must be repaired. During the repair time (**Mean Time To Repair**, MTTR) the safety function is not available, so that in the demand case this fails. However, if one assumes, that a repair can be made within a few hours (e.g. by replacing the defective device) and the failure rate λ_{dd} of the dangerous recognized failure is not unusually high, then this risk can be neglected. The calculation formulae for the PFD are simplified by this. For a single-channel (1oo1), which is regularly subjected to a complete examination in the time interval T_1 , the simplified formula for the PFD calculation is as follows:

Formula 10

$$\text{PFD}_{1oo1} = \lambda_{du} \times \frac{T_1}{2}$$

10.8 PFD calculation for multi-channel Moon structures (M out of N)

In order to reduce the failure probability of a safety function, systems are often redundantly constructed. In these cases the PFD of the redundant system can be calculated from the failure rates of the individual channels. A special case is given in respect of IEC/EN 61508, in that for a part of the possible failure it is assumed that this has the same effect on all channels and thus for this type of failures any redundancy is ineffective. Account is taken of this circumstance in the PFD calculation by the introduction of a factor (β). The factor β takes account of the magnitude of the proportion of failures, which has a simultaneous effect on all channels. For example, if 3 % of the possible failures on a channel also has an effect on the remaining channels, then: $\beta = 0.03$.

The determination of the factor β takes place using a tabular evaluation system, in which the device characteristics as well as the type of installation and the scope of the quality management system play a part.

In the reliability block diagram the situation is then represented, in which the multi-channel (redundant) structure is connected in series with a single-channel structure, whose failure rate is equal to the "Failure rate with common cause".

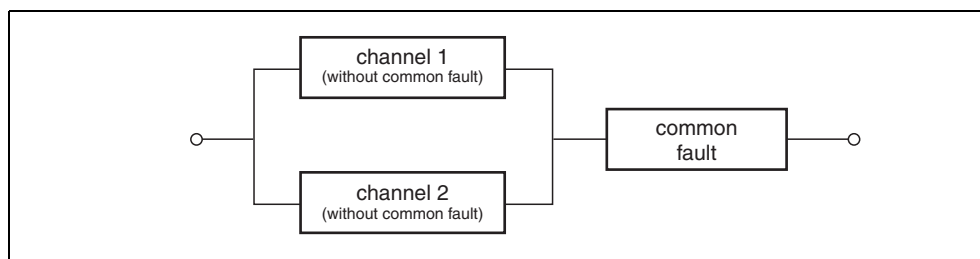


Figure 10.3 Reliability block diagram

If again here – as in the case of the above-mentioned single-channel structure – the influence of the repair time is neglected, then one obtains the following simplified formulae for the calculation of the PFD for various multi-channel structures (see also VDI/VDE 2180):

Formula 11

$$PFD_{1001} \approx \lambda_{du} \times \frac{T_1}{2}$$

Formula 12

$$PFD_{2002} \approx \lambda_{du} \times T_1 = 2 \times PFD_{1001}$$

Formula 13

$$PFD_{1002} \approx \frac{\lambda_{du}^2 \times T_1^2}{3} + \beta \times \lambda_{du} \times \frac{T_1}{2} = 4/3 \times PFD_{1001}^2 + \beta \times PFD_{1001}$$

Formula 14

$$PFD_{2003} \approx \lambda_{du}^2 \times T_1^2 + \beta \times \lambda_{du} \times \frac{T_1}{2} = 4 \times PFD_{1001}^2 + \beta \times PFD_{1001}$$

Formula 15

$$PFD_{1003} \approx \frac{\lambda_{du}^3 \times T_1^3}{4} + \beta \times \lambda_{du} \times \frac{T_1}{2} = 2 \times PFD_{1001}^3 + \beta \times PFD_{1001}$$

Formula 16

$$PFD_{2004} \approx \lambda_{du}^3 \times T_1^3 + \beta \times \lambda_{du} \times \frac{T_1}{2} = 8 \times PFD_{1001}^3 + \beta \times PFD_{1001}$$

11 References and bibliography

IEC/EN 61508, part 1 to 7

IEC/EN 61511, part 1 to 3

VDI/VDE 2180

Wahrscheinlichkeitstheorie für Ingenieure (Probability theory for engineers)

Lothar Litz

Hüthig

Zuverlässigkeitstechnik (Reliability technology)

Balbir S. Dhillon

VCH

Control system safety evaluation and reliability

Williams M. Goble

ISA

Reliability Engineering, Theory and Practice

A. Birolini

Springer



With regard to the supply of products, the current issue of the following document is applicable:
The General Terms of Delivery for Products and Services of the Electrical Industry, published by
the Central Association of the "Elektrotechnik und Elektroindustrie (ZVEI) e.V.",
including the supplementary clause: "Extended reservation of title".

PROCESS AUTOMATION – PROTECTING YOUR PROCESS



For over a half century, Pepperl+Fuchs has been continually providing new concepts for the world of process automation. Our company sets standards in quality and innovative technology. We develop, produce and distribute electronic interface modules, Human-Machine Interfaces and hazardous location protection equipment on a global scale, meeting the most demanding needs of industry. Resulting from our world-wide presence and our high flexibility in production and customer service, we are able to individually offer complete solutions – wherever and whenever you need us. We are the recognized experts in our technologies – Pepperl+Fuchs has earned a strong reputation by supplying the world's largest process industry companies with the broadest line of proven components for a diverse range of applications.

1 Worldwide/German Headquarters
Pepperl+Fuchs GmbH
Mannheim · Germany
Tel. +49 621 776 2222
E-Mail: pa-info@de.pepperl-fuchs.com

2 Asia Pacific Headquarters
Pepperl+Fuchs PTE Ltd.
Singapore
Company Registration No. 199003130E
Tel. +65 6779 9091
E-Mail: pa-info@sg.pepperl-fuchs.com

3 Western Europe & Africa Headquarters
Pepperl+Fuchs N.V.
Schoten/Antwerp · Belgium
Tel. +32 3 6442500
E-Mail: pa-info@be.pepperl-fuchs.com

4 Middle East/India Headquarters
Pepperl+Fuchs M.E (FZE)
Dubai · UAE
Tel. +971 4 883 8378
E-Mail: pa-info@ae.pepperl-fuchs.com

5 North/Central America Headquarters
Pepperl+Fuchs Inc.
Twinsburg · Ohio · USA
Tel. +1 330 486 0002
E-Mail: pa-info@us.pepperl-fuchs.com

6 Northern Europe Headquarters
Pepperl+Fuchs GB Ltd.
Oldham · England
Tel. +44 161 6336431
E-Mail: pa-info@gb.pepperl-fuchs.com

7 Southern/Eastern Europe Headquarters
Pepperl+Fuchs Elcon srl
Sulbiate · Italy
Tel. +39 039 62921
E-Mail: pa-info@it.pepperl-fuchs.com

8 Southern America Headquarters
Pepperl+Fuchs Ltda.
São Bernado do Campo · SP · Brazil
Tel. +55 11 4339 9935
E-Mail: pa-info@br.pepperl-fuchs.com

www.pepperl-fuchs.com

 **PEPPERL+FUCHS**
PROTECTING YOUR PROCESS