The latest version of the General Terms of Supply for Products and Services in the Electronics Industry set out by the German Electrical and Electronic Manufacturers’ Association (ZVEI) and the „Extended Retention of Title“ clause apply to this document.
Contents

Basic Principles .................................................................................................................................................. 6

What Causes Accidents? ................................................................................................................................. 6
Risk and Risk Reduction (Risk-Based Approach) ........................................................................................... 7
    Risks Are Subjective ................................................................................................................................. 8
    Tolerable Residual Risk ........................................................................................................................... 8
    Limiting Risks .......................................................................................................................................... 9
    Reducing Risks ...................................................................................................................................... 9

Standards .......................................................................................................................................................... 10
    Approach to Risk Mitigation in Accordance with IEC/EN 61508 ............................................................. 10
    Safety Instrumented Function (SIF), Safety Instrumented System (SIS) ................................................... 12
    Safety Integrity Level (SIL) ....................................................................................................................... 12
Safety Life Cycle Concept ............................................................................................................................... 14
    Faults Resulting from Wrong Organization and Planning of the Safety Function ................................. 14
    Eliminating Planning and Organizational Risks ....................................................................................... 14
Risk Analysis for Risk Reduction ..................................................................................................................... 15
Functional Safety Management ......................................................................................................................... 15

Hazard and Risk Analysis ............................................................................................................................... 16

Identifying, Revealing, and Evaluating Risks ............................................................................................... 16
Hazard Analysis Methods .................................................................................................................................. 16
    HAZOP .................................................................................................................................................... 17
    FME(C)A .................................................................................................................................................. 17
    FTA ......................................................................................................................................................... 18
    ETA ....................................................................................................................................................... 19
Risk Analysis Methods ..................................................................................................................................... 20
    ALARP Method ...................................................................................................................................... 20
    Risk Graph ............................................................................................................................................. 21
    Risk Matrix .......................................................................................................................................... 23
    LOPA ..................................................................................................................................................... 24

Implementing Safety Equipment ..................................................................................................................... 26

Random Failures and Systematic Failures ....................................................................................................... 26
System Architecture Requirements ................................................................................................................... 27
    Redundancy Types .................................................................................................................................. 27
Low Demand/High Demand Mode .................................................................................................................... 28
    Low Demand Mode ............................................................................................................................... 28
    High Demand Mode .............................................................................................................................. 28
Basics for the Calculation .................................................................................................................................. 29
    Probability of Failure of a Safety Instrumented System ......................................................................... 29
    Failure Rates According to Failure Categories ....................................................................................... 30
Basic Principles

Risk is an integral part of our daily lives. Hazards are also present in our working environment. Thus, it is important to identify anything that could pose a risk of death or injury and to eliminate any hazards at work emanating from production processes.

Standards applied to overcome these risks are based on proven principles:

- Statutory architectures
- Exclusion of faults
- Stipulation of single and multiple fault safety measures to implement a protective function

An increasing number of programmable devices are now used when designing a plant, from a PLC to intelligent sensors. It is not possible to assess multiple fault safety measures in this form. Specific standards have therefore been devised so that the risk can be quantified, based on probability statements, and reliably reduced. This involves new concepts that require a more detailed explanation. The following summary intends to clarify these concepts and definitions.

What Causes Accidents?

The primary aim of functional safety is to prevent accidents. An accident is...

... if something unexpected happens to the unprepared.

(georges charles ellipton)

This definition can be applied to numerous disastrous industrial accidents and accidents in the private sphere. In hindsight, most accidents could have been avoided by considering the potential occurrence of the situation beforehand and taking preventive measures.

Measures for preventing industrial accidents can be found in the IEC/EN 61508 series of standards. The series of standards outlines specifications for the entire life cycle of plants and devices. The probabilistic methodology employed by these standards also analyzes the situations that arise during operation of an industrial system and evaluates the resulting risks. This analysis is used to define the safety measures required to prevent risks in the particular plant.
Risk and Risk Reduction (Risk-Based Approach)

The relevant standards define "risk" as the product of the following factors:

- Probability that an undesired (hazardous) event will occur
- Consequences resulting from the hazardous event (extent of harm)

These consequences include effects such as damage to health, as well as damage to parts of the plant and the costs incurred as a result of the event. They also cover environmental damage.

Processing plants have different operating states that can be attained during plant operation. During plant operation, the state of the plant can reach a permissible fault range in which the process does not fail dangerously yet. Safety equipment is designed to prevent the process transitioning to the impermissible fault range. The following figure shows this process in relation to a critical process variable.

For plant operation, 3 areas can be distinguished. Protective measures only need to take effect once the plant no longer operates as intended. Usually, there is a permissible fault range between the good range and the impermissible fault range. Within this permissible fault range, a control device may adjust the process variables until the safety equipment possibly stops the process.

![Figure 1. Schematic diagram of the operating ranges of a plant. Source: VDI/VDE 2180 (2007/1998), Blatt 1/Part 1](image-url)
Risks Are Subjective

Damage to health is often divided into categories ranging from minor to severe injuries, immediately followed by the assumed number of deaths. Understandably, no one wishes to dictate how many deaths should be considered acceptable. Therefore, literature on the subject is extremely vague about this.

One possible way of determining an acceptable threshold for the residual risk is via statistics based on a person's mortality during their lifetime. Because a 75-year-old is considerably more likely to die than an 18-year-old, a minimum value for this mortality is used as a comparison value. This mortality is then assessed against the residual risk and a slightly increased percentage accepted. The EN 50126 standard refers to this concept as "minimum endogenous mortality".

Tolerable Residual Risk

There can be no complete protection from risks; a residual risk will always remain. Whether the residual risk is tolerable or not depends on a number of factors:

- Country and region
- Social environment
- Legal position
- Consequential costs

One question frequently asked on this topic remains: "Who specifies the tolerable risk and how high is the tolerable risk?"

In liberal democratic legal systems, the tolerable residual risk is based on social consensus. The level of residual risk considered to be tolerable depends on how many people would be affected simultaneously by a potential undesired event. For example, if only 1 person would be affected (individual risk), a residual risk of $10^{-6}$ per year is deemed acceptable. If several people would be affected (collective risk), the tolerable residual risk decreases depending on the number of people affected. A publication from the Netherlands\(^1\) shows an example of the implementation of this concept.

Figure 2. Graph depicting the maximum tolerable collective risk\(^1\)

Note: One of the methods described in IEC/EN 61508-5 is normally used to determine a system's safety integrity level (SIL). These methods incorporate a limit for the tolerable residual risk.

---

Limiting Risks

A system must be constructed in such a way that risks are kept as low as possible right from the start of the planning phase. Risks that are not entirely avoidable can often be limited effectively. The upper limit for this should always be the tolerable residual risk. If this cannot be achieved using constructive means, risk reduction measures must be taken until the residual risk is reduced to an acceptable level. See “Reducing Risks”, p. 9.

The controlled conditions of an industrial environment in particular provide numerous ways of reducing the probability of a hazardous event and, consequently, the residual risk to an acceptable level.

To ensure that people, technical equipment, and the environment are protected from damage, potential risks must be determined first. Only then suitable protective measures can be implemented.

Protective measures can be divided into protection layers. These protection layers build upon each other hierarchically and must be viewed independently. The underlying principle is simple: If one layer of protection fails, the next higher layer is actuated automatically to prevent or limit potential damage.

Reducing Risks

If the risk is not within the acceptable limits, it must be reduced using additional measures. A risk graph is a good way of indicating what should be achieved with risk reduction methods. This graph shows the risk increasing towards the right. In the example, it is assumed that a plant without safety equipment (referred to in the standard as “equipment under control” or “EUC”) conceals a particular risk that goes beyond the socially accepted level of risk. This shows the necessary risk reduction that is derived from the identified risks.

Risk reduction equipment often features overall methods and mechanisms that can be implemented using specific devices. These requirements are then divided into individual, dedicated safety instrumented functions to solve a defined task.

In the figure, the risk arising from the EUC is reduced to a tolerable level through “necessary risk reduction.” The risk reduction does not have to be dependent on a single safety instrumented system. A combination of different devices and organizational measures can also reduce the risk.

The figure anticipates a concept from the world of standards: A SIL (safety integrity level) indicates the level of risk reduction that can be achieved using a safety equipment. SIL 2 achieves a lower risk reduction than SIL 3. In order to lower the residual risk below the tolerable risk, a safety integrity level SIL 3 is required for risk reduction in the example below.
Standards

Many areas of risk reduction, e.g., explosion protection, are subject to European regulations and requirements based on EU Directives. Safety instrumented functions are not covered by these regulations to the same extent.

Only for the mechanical engineering sector requirements can be deduced from the Machinery Directive 2006/42/EC and the related harmonized standards regarding functional safety. In the process industry, however, the application of standards is based on national legislation. In Germany, e.g., product liability and fault-based liability for device manufacturers must be stipulated in accordance with the German Civil Code (BGB). Requirements for plant operators are derived from the German Major Accidents Ordinance and the German Ordinance on Industrial Safety and Health (BetrSichV).

The first edition of the IEC/EN 61508 series was published in 2001 and quantified risk reduction for the first time. The probability of failure of a safety equipment was determined using statistical data, with the result used to evaluate the safety equipment's efficiency. Since merely calculating the probability of failure of the safety equipment does not guarantee its safety, appropriate general conditions had to be defined for the design and use of this safety equipment. This gave rise to a 7-part series of standards that specifies the basic framework for creating functional safety standards. Developed around IEC/EN 61508, this series provided additional standards that restricted the topic to actual applications, subject fields, and products. In fact, the series formed the basis for sector standards such as IEC/EN 61511 for the process industry, as well as specific product standards such as VDMA 4315 for the safety of turbo engines.

Approach to Risk Mitigation in Accordance with IEC/EN 61508

IEC/EN 61508 focuses on risk reduction through safety devices that contain E/E/PE components. Whereas the effect of organizational or structural measures cannot be calculated exactly, when using E/E/PE devices, it is possible to quantify the failure rates of devices and their safety functions. These failure rates can be used to ascertain the probability that an operating E/E/PE device will function correctly at the precise moment when the safety function is required. It is extremely important for plant operators to have this information so that they can predict the effectiveness of an implemented risk reduction measure. This is the concept behind IEC/EN 61508.
Figure 5. Correlation of existing functional safety standards
Safety Instrumented Function (SIF), Safety Instrumented System (SIS)

A safety instrumented function (SIF) in electrical and electronic devices rarely consists of a single part. Several parts are always required for a full response to excess temperature in a process or plant:

- 1 sensor
- 1 information processing unit (programmable logic controller, PLC)
- 1 actuator for intervention in the process, e.g., to interrupt the power supply, activate the brakes, actuate the valves
- Isolators for explosion-hazardous areas, where necessary
- Signal converters in the cordset, where necessary

This series of devices is known as a safety instrumented system (SIS). A safety instrumented system performs one or more safety instrumented functions. It is not necessary to know whether the safety instrumented function works correctly at all times—it is important that the safety instrumented function is performed correctly when it is needed.

The availability of SIF is quantified by the value "probability of failure on demand" (PFD). This value is calculated during the SIL evaluation. The PFD for a safety instrumented system takes into account the PFD of all modules relevant to the function in question, regardless of the probabilities of failure for these modules.

Safety Integrity Level (SIL)

The individual parts of a process plant involve different risks. The higher the risk, the more important the availability of the safety instrumented system (SIS).

The abbreviation „SIL“ refers to the safety integrity level in accordance with IEC/EN 61508 and indicates the degree of reliability with which a safety instrumented function actually operates when required (integrity). Achieving a particular level of safety integrity calls for both organizational and technical measures.

SIL is function-oriented. A SIL is assigned to a safety instrumented function (SIF) comprising different functional modules. These modules are used to describe systems.

The higher the safety integrity level of a safety instrumented function, the more comprehensive the risk reduction. The risk identified for a plant determines the risk reduction measures required. If the risk is limited through electrical and electronic devices, the devices used for this must meet the criteria specified in IEC/EN 61508. The standard divides the risk reduction measures into 4 safety levels, from SIL 1 for a low baseline risk, up to SIL 4 for a high baseline risk.

This must take the tolerability of a risk into consideration. If a foreseeable hazard with negligible consequences occurs, this could be deemed tolerable. On the other hand, even the slightest probability of a disaster occurring can pose an unacceptable risk. If the risks connected with operation of the plant cannot be tolerated based on the specified criteria, the risks must be reduced using safety instrumented functions. See „Risk and Risk Reduction (Risk-Based Approach)“, p. 7.

The SIL is therefore a measure of the probability that the safety instrumented system (SIS) can perform the required safety instrumented functions correctly for a specific period. There are various ways of ascertaining the SIL required for a safety instrumented function. IEC/EN 61508 and IEC/EN 61511 outline a number of methods for determining the SIL.
Figure 6. Example of fault distribution in a safety instrumented system
Safety Life Cycle Concept

If a device has been evaluated in accordance with IEC/EN 61508, characteristic values for the devices—and thus for the entire safety function—can be specified in the form of failure rates. Simply calculating the probabilities of failure of a SIF does not make the application safe. Calculations according to the standard quantify the failures of components (E/E/PE components). They do not provide any information on the quality of the development process though. If systematic errors were made during development of the device, there is no basis for calculating the probability of failure.

When analyzing failures that have led to accidents in the past, the calculation of the probability of failure is not of primary importance during the planning and implementation of a safety function.

Faults Resulting from Wrong Organization and Planning of the Safety Function

The Health and Safety Executive organization in the UK conducted a study on the prevention of accidents at work. In its publication „HSG238—Out of Control“ the organization came to the conclusion that the cause of most faults could be traced back to the system specifications. The cause could be that something was formulated incorrectly or ambiguously, or because attention was drawn to the wrong points. ¹

The Commission of Hazardous Incidents (SFK) at the Federal Ministry for Environment, Nature Conservation and Nuclear Safety in Germany also commissioned research into the causes of accidents, concluding that 90% of accidents were the result of organizational factors. ²

Eliminating Planning and Organizational Risks

The IEC/EN 61508-1 standard therefore attaches great importance to companies' compliance with organizational measures that are relevant to the use of devices, introducing the concept of the "safety life cycle."

The user is asked to analyze all necessary phases of the safety life cycle and to eliminate systematic faults in the execution of these phases. This ensures that all aspects are observed and fully documented for assessment purposes. This forms the basis for fulfillment of the safety-related equipment requirements. Essentially, the standards form the framework and guidance for use of the entire safety life cycle. The standards encompass all aspects of the safety life cycle for a system, including the concept, design, implementation, installation, commissioning, validation, maintenance, and decommissioning. The key elements in these standards—"safety" and "lifetime"—focus primarily on appropriate documentation in relation to this concept.

In the process industry, the IEC/EN 61511 series of standards forms the basis for the design of safety instrumented systems. The standards allow plant operators to use appropriate documentation to prove that they have designed safety functions based on state-of-the-art technology.

1 Health and Safety Executive (publisher): Out of Control (HSG238), Surrey, UK, 2003
2 Working group for technical systems, risk and communication processes, Commission of Hazardous Incidents (SFK): Risk management in accordance with the German Plant Safety Major Accidents Ordinance, SFK-GS-41, 2004
Risk Analysis for Risk Reduction

IEC/EN 61511 stipulates clear criteria for establishing the risk for a processing plant. The risk identified according to these criteria determines the required risk reduction measures. If the risk is reduced with the help of automation technology, the devices used for this must meet the criteria in accordance with IEC/EN 61508.

The safety life cycle indicates the risk analysis and hazard analysis to enable users to estimate the risk in a system. Several methods are specified for this and are explained in more detail below.

Figure 9. Safety life cycle from IEC/EN 61511

Functional Safety Management

As outlined in the section on the safety life cycle, most risks during the development of a safety instrumented system are of an organizational nature. Research has shown that the main causes of accidents are insufficient commitment to safety on the part of the management and the basic safety culture within the organization or industrial sector. The IEC/EN 61508-1 standard dedicates an entire chapter to this fact. In particular, this section emphasizes that all personnel involved in the safety life cycle should be specified and their areas of expertise should be described. These individuals must be competent to perform the function entrusted to them. The company must ensure that the relevant skills and expertise are available. Also, general requirements for the processes within a company are specified by the standard. For example, the company and its suppliers must have an appropriate level of quality management.
A hazard analysis describes the potential hazards in the operation of a plant as consistently as possible. A risk analysis also extends to the necessary risk reduction, including quantification, thereby allowing to determine the required risk reduction measures.

The step clearly identifying hazards and a risk analysis is the most difficult to implement. This is particularly true if the process to be examined is new or innovative and empirical values are not yet available.

Identifying, Revealing, and Evaluating Risks

Numerous hazard and risk analysis methods are used around the world. The IEC/EN 61508 and IEC/EN 61511 standards both provide an overview of the different methods. In addition to advanced studies, checklists, tabular methods, and grid-based methods, the following concepts are frequently selected methods:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAZOP</td>
<td>HAZard and OPerability study</td>
</tr>
<tr>
<td>FME(C)A</td>
<td>Failure Mode and Effect (and Criticality) Analysis</td>
</tr>
<tr>
<td>ETA</td>
<td>Event Tree Analysis</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
</tbody>
</table>

One phase of the safety life cycle concerns the analysis of the hazards and risks connected with operation of a plant. These analytical methods are initially intended to identify hazards from accidents in a plant. In a risk analysis, the consequences of an accident are then stated implicitly in the accident description. Literature on the subject refers to individual risk analysis measures that allow to identify risks:

- Brainstorming on the plant structure and its key elements
- Expert opinions
- Interviews and questionnaires
- Checklists
- Available data from similar applications
- Experience gained by employees and from other projects
- Testing and modeling
HAZOP

HAZOP is a well-known method of analyzing the operation of a system. It aims to identify correlations within a process and between process variables, and to categorize them on a granular scale. This can then be used to determine which correlations within the plant operation process could trigger malfunctions. A safety function can then be planned and designed at these points.

HAZOP uses a list of guide words. Although this list can be expanded, it is advisable to indicate the correlations as simply as possible at a basic level, using the default guide words.

This enables correlations to be identified and protective measures to be found at critical points in the process. The creation of a HAZOP study is described in IEC/EN 61882.

FME(C)A

An FMEA can systematically check all parts of a plant or device for potential failures and their consequences. If an appropriately detailed FMEA is performed, it provides a complete overview of potential failures.

The failure types are then assessed to determine the probability of occurrence. Thus, risk reduction measures can be defined and their effect on plant safety evaluated. This means that the effect of the measures on the overall system can be examined and a weighting can be attributed to the implementation of risk reduction measures. An FMECA can continue this process down to E/E/PE component level. Various methods can be used to estimate failure rates at electronic component level, in order to quantify the probability of undesired events occurring. These processes are covered, e. g., in the IEC/EN 60812 standard.
FTA

The FTA method provides a diagram that starts with the occurrence of an undesired event, and deductively analyzes and documents the interconnected causes that led to this event. The sequence of events resulting in the undesired event can thus be identified. An additional aim is to establish the probability of a path being followed. The paths towards the undesired event are indicated using logic operations (AND, OR, etc.). The resulting groundwork enables risk reduction measures to be defined at different levels and their effectiveness to be evaluated.

This process is described in the IEC/EN 61025 standard.

Example:

The top-level event is overpressure in a heating system, which may be attributable to a variety of causes:
- External events, e.g., fire; this is a temporary cause that is prevented as soon as it is identified
- The process control system function fails. There are a number of different possible reasons for this:
  - The process control system itself fails; this is a temporary cause that is rectified as soon as it is identified
  - A sensor fails
  - A valve jams

Figure 10. Example of a fault tree analysis
**ETA**

Beginning with a start event, ETA provides a graphical display of potential events that could occur during operation of a system. The result is an inductive analytical diagram showing event consequences that branch out based on „Fails“ and „Works“. The method is used in particular to identify the potential for serious subsequent events. ETA allows the probabilities of occurrence to be estimated and protective measures to be defined as a result. The probability of occurrence is determined on the basis of decision probabilities for individual branches depicted in the diagram.

This process is described in more detail in the IEC/EN 62502 standard.

**Example:**

The assessment focuses on 3 potential failures (fill level sensor failure, isolated barrier failure, and valve control failure) that may occur stochastically and independently of each other according to the probability indicated on the branches of the tree.

This gives a total of 8 event scenarios, which can be assigned potential probabilities if they are known. A probability result for each scenario can then be calculated.

In the following example, the probability is calculated, for each event scenario, that the fill level control will fail completely as the result of one or more prior events. One scenario calculates the probability that none of the events will occur and the fill level control will work.

---

![Event Tree Analysis Diagram](image-url)

**Figure 11. Example of an event tree analysis**
Risk Analysis Methods

The IEC/EN 61508-5 standard specifies four risk analysis methods. The risk analysis determines the degree of risk reduction that is required. In addition to these 4 methods, a process FMEA can be used, meaning that, altogether, the following methods are available:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARP</td>
<td>As low as reasonably practicable</td>
</tr>
<tr>
<td>--</td>
<td>Risk graph</td>
</tr>
<tr>
<td>--</td>
<td>Risk matrix</td>
</tr>
<tr>
<td>LOPA</td>
<td>Layer of protection analysis</td>
</tr>
</tbody>
</table>

All methods have advantages and disadvantages, and they can also be combined. This can give rise to different requirements, which must then be discussed by the various people involved in the plant planning process to enable them to reach a viable solution.

ALARP Method

The acronym ALARP (as low as reasonably practicable) clearly describes the aim of this method: The risk must be reduced as far as can reasonably be expected. The desired level of risk reduction is in contrast to the German MGS principle (German “mindestens gleiche Sicherheit”—at least the same level of safety) used in railway engineering, which defines safety via existing safety instrumented functions: If the safety mechanism has to be replaced, the solution must at least be no worse than a previously known solution.

The ALARP method proposes safety measures and evaluates the resulting risk reducing effect. This enables an estimation of whether the measure is sufficient or whether an additional measure needs to be implemented. Once a certain point is reached, the measures cease to be economically viable. In order to spread the risk or allow other risk reduction methods to be used, a decision must be made as to whether implementation is still justifiable or if the system needs to be designed differently.

The ALARP method produces quantitative or qualitative statements on the risk. Both types allow the residual risk to be estimated. Risk is classified in 4 risk classes, ranging from I (intolerable) to IV (generally acceptable). The residual risk is classified according both to the frequency of its occurrence and to its consequences. A verbal description of these frequencies can be found in the sample matrix in the table that follows. This matrix is defined either specifically for the application or on a company-wide basis. The thresholds between risk classes can also be stipulated in more detail. These specifications are referred to as calibration.

Other methods have the advantage for the user that a risk and the necessary risk reduction measures are assessed regarding their effectiveness. Once a tolerable risk has been achieved, only such additional measures have to be considered that can be easily implemented. ALARP is based on the assumption that all economically justifiable measures will be implemented.

In some countries, e.g., the UK, jurisdiction demands to proceed in accordance with ALARP.

More information on this can be found in the IEC/EN 61508-5 standard, Annex C.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Catastrophic</th>
<th>Critical</th>
<th>Marginal</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>II</td>
</tr>
<tr>
<td>Probable</td>
<td>I</td>
<td>I</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>Occasional</td>
<td>I</td>
<td>II</td>
<td>III</td>
<td>III</td>
</tr>
<tr>
<td>Remote</td>
<td>II</td>
<td>III</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Improbable</td>
<td>III</td>
<td>III</td>
<td>IV</td>
<td>IV</td>
</tr>
<tr>
<td>Incredible</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
</tr>
</tbody>
</table>

Table 1. IEC/EN 61508-5:2010, Table C.1: Example of risk classification of accidents
Note: The actual population with risk classes I, II, III and IV are sector-dependent and also depend on what the actual frequencies are for frequent, probable, etc. Therefore, this table should be seen as an example of how such a table could be populated, rather than a specification for future use.
Risk Graph

Use of the risk graph method is described in the standard IEC/EN 61508-5, Annex E.6. The risk graph records and evaluates risk factors related to the operation of a plant without protective measures. Several risk parameters influence the level of risk reduction required. A distinction is made between the following risk parameters:

- Consequence of hazardous event (C)
- Frequency of, and exposure time in, the hazardous zone (F)
- Possibility of avoiding the hazardous event (P)
- Probability of unwanted occurrence (W)

Depending on how the graph is populated following the assessment of these parameters, this results in a necessary risk reduction as shown in the figure.

![Risk Graph Diagram]

Figure 12. Example of a risk graph based on IEC/EN 61508-5, Annex E.6

Legend:
- $W_1$: Very unlikely
- $W_2$: Unlikely
- $W_3$: Quite likely
- $a$: Safety integrity level, SIL
- -: tolerable risk, no safety requirements
- $a$: no particular safety requirements needed
- $b$: a single E/E/PE system is not sufficient

Consequence of hazardous event:
- $C_1$: Minor injury or minor damage
- $C_2$: Serious permanent injury to one or more persons; death to one person
- $C_3$: Death to several people
- $C_4$: Very many people killed

Frequency of exposure:
- $F_1$: Time spent in the hazardous zone rare to frequent
- $F_2$: Time spent in the hazardous zone frequent to permanent

Possibility of avoiding hazardous event:
- $P_1$: Possible under certain conditions
- $P_2$: Almost impossible

Probability of unwanted occurrence:
- $W_1$, $W_2$, $W_3$
The risk parameters can also be classified quantitatively by assigning numerical values to them and then multiplying these values. This enables increments to be specified and risks to be compared. The result allows the risk to be classified more precisely than with other methods and reduced more selectively.

The individual assessment of the necessary risk reduction is often referred to as calibration. This calibration is specified for a plant or for a company. The individual criteria are precisely defined so that the criteria for additional plants can be stipulated with the required clarity.

Example of a Calibrated Risk Graph

The method using a calibrated risk graph is also referred to as risk-oriented hazard analysis.\(^1\)

One drawback of the risk graph is that the assessment covers only one part or one function within a plant—the method does not provide a comprehensive estimation for the overall plant. The risk reduction measures are then specified for each single function.

It is therefore possible that interactions between single functions are not assessed appropriately. Mistakes when planning the risk graph can result in a common safety instrumented function influencing several single functions. In the event of a failure, this could have much more serious consequences than the risk graphs had initially implied.

<table>
<thead>
<tr>
<th></th>
<th>(W_1)</th>
<th>(W_2)</th>
<th>(W_3)</th>
<th>(W_4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(C_1)</td>
<td>0.002</td>
<td>0.02</td>
<td>0.16</td>
<td>1.64</td>
</tr>
<tr>
<td>(C_2)</td>
<td>2</td>
<td>0.02</td>
<td>0.16</td>
<td>1.64</td>
</tr>
<tr>
<td>(C_3)</td>
<td>20</td>
<td>0.16</td>
<td>0.16</td>
<td>1.62</td>
</tr>
<tr>
<td>(C_4)</td>
<td>200</td>
<td>0.16</td>
<td>0.16</td>
<td>1.62</td>
</tr>
<tr>
<td>(F_1)</td>
<td>0.09</td>
<td>16.56</td>
<td>16.38</td>
<td>16.38</td>
</tr>
<tr>
<td>(F_2)</td>
<td>0.91</td>
<td>16.38</td>
<td>16.38</td>
<td>16.38</td>
</tr>
<tr>
<td>(P_1)</td>
<td>0.91</td>
<td>16.38</td>
<td>16.38</td>
<td>16.38</td>
</tr>
<tr>
<td>(P_2)</td>
<td>0.09</td>
<td>16.38</td>
<td>16.38</td>
<td>16.38</td>
</tr>
<tr>
<td>(W_1)</td>
<td>0.1</td>
<td>165.62</td>
<td>165.62</td>
<td>165.62</td>
</tr>
<tr>
<td>(W_2)</td>
<td>1</td>
<td>165.62</td>
<td>165.62</td>
<td>165.62</td>
</tr>
<tr>
<td>(W_3)</td>
<td>10</td>
<td>165.62</td>
<td>165.62</td>
<td>165.62</td>
</tr>
</tbody>
</table>

Figure 13. Calibrated risk graph\(^2\)

---

1 Bock, Franz-Josef, Haferkamp, Klaus, TÜV Rheinland Industrie Services GmbH: ROGA—Methodology of the Risk Oriented Hazard Analysis (ROGA-LOPA – A Comparison), lecture at SIL Symposium 2012, TÜV Rheinland GmbH, Cologne, Germany

2 Hildebrandt, Andreas, Pepperl+Fuchs GmbH: Bedeutung der Probabilistik bei der Bewertung sicherheitstechnischer Einrichtungen [Importance of Probability in the Assessment of Safety Instrumented Equipment], lecture at SIL-Tag 2007 event, DEHEMA, Frankfurt/Main, Germany
Risk Matrix

In order to display information on the potential extent of damage and the frequency of occurrence of the hazardous event, the risk matrix has proven to be another effective way. In a risk matrix, the potential extent of harm is normally shown vertically and the frequency of occurrence horizontally. The fields of the resulting matrix combine the two aspects so that the risk can be evaluated according to its tolerability. The fields are often marked in colors. The colors are used to indicate the consequences of each combination.

Concrete hazards are frequently listed on the axes that can be subdivided as granularly as needed. The calibration is more important than with the risk graph, which always has the same basic number of branches and therefore provides fewer opportunities for detailed classification.

The risk matrix procedure is described in the IEC/EN 31010 standard.

<table>
<thead>
<tr>
<th>(Potential) consequences</th>
<th>Occurrence frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rarely</td>
</tr>
<tr>
<td>Death; severe consequences for environment/public; major property damage</td>
<td></td>
</tr>
<tr>
<td>Serious injuries; limited consequences for environment/public; property damage</td>
<td></td>
</tr>
<tr>
<td>Injuries; no consequences for environment/public; minor property damage</td>
<td></td>
</tr>
<tr>
<td>Negligible effects on humans/environment/public, or on property</td>
<td></td>
</tr>
</tbody>
</table>

Figure 14. Example of a risk matrix

Explanation of the Matrix

- Red coloring indicates that the identified risk is not justifiable and cannot be taken without implementing additional or modified risk reduction measures.

- Yellow coloring indicates that more information must be obtained. Only then will it be possible to judge whether or not a safety instrumented measure is required. Additional risk reduction measures can be added directly to avoid a complicated analysis process.

- Green coloring indicates that the residual risk is justifiable. Additional risk reduction measures are not obligatory from the plant operator's point of view. To improve plant availability and make the process even safer, however, additional risk reduction measures should be considered and added where necessary. It is mandatory to take measures into account that can be easily implemented without substantial economic expenditures.

---

1 Working group for technical systems, risk and communication processes, Commission of Hazardous Incidents (SFK): Risk management in accordance with the German Plant Safety Major Accidents Ordinance, SFK-GS-41, 2004
LOPA

LOPA refers to safety functions as protection layers. These protection layers help to determine the risk reduction more precisely by different simultaneously effective safety functions.

First, all potential hazards associated with a plant are documented and the related damage is estimated. The probability of occurrence allows you to quantify the risk. The next task is to determine how protective measures should be combined for maximum effect. This way, the resulting residual risk can be determined for which a necessary electronic protective measure must be defined.

An easy way to explain this is by using the “Swiss cheese model.” This model visualizes the existence of a residual risk throughout all the protection layers. According to this model, a residual risk only exists where the holes in the overlapping “cheese slices” form a continuous hole through all the layers. None of the protective measures are effective at these points. An additional measure must therefore be defined to protect against this residual risk.

LOPA features reports that stipulate a very rigid range of protection layers with the following fixed categories (cf. IEC/EN 61508-5:2010, Table F.1):

- System design
- Control system
- Alarms
- Restricted access

This results in a probability of failure on demand (PFD) for the specific function to be monitored. In the field of process automation, a HAZOP can be used as the basis for a LOPA. The assessment is based on scenarios, the effect of which is evaluated via the simple correlations from the HAZOP. The correlation of terms is described in the IEC/EN 61511–3 standard.

<table>
<thead>
<tr>
<th>LOPA Required Information</th>
<th>HAZOP Developed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact event</td>
<td>Consequence</td>
</tr>
<tr>
<td>Severity level</td>
<td>Consequence severity</td>
</tr>
<tr>
<td>Initiating cause</td>
<td>Cause</td>
</tr>
<tr>
<td>Initiating likelihood</td>
<td>Cause frequency</td>
</tr>
<tr>
<td>Protection layers</td>
<td>Existing safeguards</td>
</tr>
<tr>
<td>Required additional mitigation</td>
<td>Recommended new safeguards</td>
</tr>
</tbody>
</table>

Table 2. HAZOP developed data for LOPA.

Although the LOPA is an accepted method in Europe, it is more commonly used in the Americas. Some aspects of the method are different compared to the previously described methods, which define protective measures based solely on the device level. For example, organizational measures can also be used as a way of reducing risk. Furthermore, standard control mechanisms can also perform a safety instrumented function. This gives rise to a potential for failure if both the control system and safety loop stop working when a device fails. In case of a defined fault behavior, this approach can, in principle, be taken into consideration, though.

The LOPA can also include measures that require human intervention: Specially trained personnel can perform a risk reduction task. In Europe, such measures are not very common in the mechanical engineering sector, where there is always a chance of human error. This is particularly true in exceptional circumstances, which are most commonly connected with undesired events.

The HSG 48 guideline issued by the UK Health and Safety Executive (HSE) allows you to include measures requiring human intervention. The LOPA method is not officially recognized by all test facilities in Germany because of these additional possibilities.¹

¹ Health and Safety Executive (publisher): Reducing Error and Influencing Behaviour (HSG48), Surrey, UK, 2007
The effectiveness of the individual measures in the LOPA can be linked graphically with the residual risk as a probability of failure after considering each independent protection layer (IPL).

The range of analysis methods described here allow a similarly extensive coverage of hazards. An additional benefit of the LOPA is that it also explicitly covers simple methods such as the requirement to wear a helmet in a plant.

Figure 16. Example of a LOPA analysis

### Implementing Safety Equipment

In a safety instrumented system (SIS), systematic and random failures can occur. Both types of failures must be considered separately to fulfill the required SIL criteria.

<table>
<thead>
<tr>
<th>Failure types</th>
<th>Characteristic of these failures</th>
<th>Measured sufficient?</th>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systematic failure</td>
<td>Possible to mitigate</td>
<td>FSM system</td>
<td>Plan fault detection / fault prevention methods</td>
</tr>
<tr>
<td>Random failure</td>
<td>Barely possible to mitigate</td>
<td>Diagnostics</td>
<td>Calculate, plan any additional measures</td>
</tr>
</tbody>
</table>

**Figure 17. Failure mechanisms**

### Random Failures and Systematic Failures

Random failures are the result of random faults that occur at a random point in time and are basically not reproducible. These include hardware defects. These faults do not exist at the time of commissioning and, in E/E/PE components, include, e.g., short circuits, open circuits, or component drift. It is possible to calculate the probability of random failures and the associated failure rate. This involves viewing the individual hardware components of a SIS separately and calculating the probability of failure on demand (PFD) from the individual failure rates thus obtained. The PFD is in turn a factor when determining the SIL value.

Systematic failures are the result of systematic faults, and, unlike random failures, are already present at the time of commissioning. They typically include development errors, installation errors, or project planning errors such as software faults, incorrect dimensioning, the wrong design for the measuring device, etc.

Failures that occur as a result of systematic faults are always reproducible. Systematic faults of this type cannot be excluded. The IEC/EN 61508 standard outlines different ways of counteracting these faults, though. For example, an appropriate hardware fault tolerance (HFT) can prevent a dangerous failure of the entire safety function through redundancies in the system architecture. It is also possible to define a property for individual devices: The higher a device's safe failure fraction (SFF)—i.e., the calculated proportion of safe system failures—the higher the probability that device failure will result in a safe situation rather than a dangerous one. An appropriate device design can therefore counteract dangerous systematic faults.

Systematic faults often originate in the device software. When systematic software faults are present, it is assumed that programming errors may also lead to a failure of the function. Specific measures must therefore be taken when designing the SIS to avoid systematic failures. A quality management system is used for this that constitutes an integral part of IEC/EN 61508 and IEC/EN 61511. The device manufacturers must provide details of the SIL rating with regard to the systematic faults. This information is normally found in the safety manual for the individual devices. An independent body must assess whether a device is suitable for use in safety loops with a particular SIL. An employee from an independent department at the manufacturer’s company is sufficient for this assessment for SIL 2, whereas an external, independent organization (TÜV, Exida, ...) must be consulted for SIL 3. To fulfill the systematic fault requirements for a particular SIL (e.g., SIL 3), the entire safety instrumented system (SIS) must be considered accordingly.
System Architecture Requirements

The IEC/EN 61508 standard also defines system architecture requirements for reducing a risk with a particular SIL. One factor for this is the hardware fault tolerance (HFT). The HFT indicates the redundancy built into the individual parts of a safety instrumented system (SIS). For example, during a safety-critical temperature measurement, a second signal converter can prevent the reading being lost due to signal converter failure. The protection of the measured value via a second measuring device is referred to as a loop with HFT = 1, indicating single redundancy.

When planning redundancies in the architecture, the design of the redundant loops and the safety function of the devices used are key factors.

For each device consider carefully which state shall represent the "safe state" in order to ensure that the plant as a whole is working safely.

Example

A valve should always close safely when it is required to do so. A valve must therefore be set up to show the "closed" state as its safe state. Some valves also retain their last position once the plant is deenergized. These valves can still be used if an external circuit can switch them to the "closed" state in the event of a loss of power. However, solutions of this type are more susceptible to malfunctions than a solution involving a basic valve design that provides for automatic closure when the power is switched off.

The way the elements are interconnected is also key to the safety of the system.

Example

The flow in a piping system should be stopped safely by 2 safely closing valves, using a redundant loop design. In a redundant design, this requires the second valve to be ordered in series rather than in parallel. In a parallel circuit, a valve that is jammed and cannot perform its "closed" safety function would render the other one completely ineffective. The combination would remain open, resulting in a dangerous failure. The "open" state requires the opposite. To ensure that failure of one of the valves in case of a demand does not lead directly to a dangerous failure, 2 safely opening valves must be connected in parallel.

Redundancy Types

When specifying redundancies, a distinction is made between diverse redundancy and homogeneous redundancy.

If the same process variable is assessed using different measuring devices or measuring principles, this is an example of diverse redundancy. This type of redundancy is most effective when designing a safety loop based on varying reactions to a malfunction. When using different types of mechanics, electronics, and software, it is reasonable to assume that, if an incorrect response is produced by one device, a failure is unlikely to occur in the other device at exactly the same time. Consequently, signal converters from different manufacturers are also frequently used. This greatly reduces the probability of common cause failures.

In contrast, homogeneous redundancy involves the redundant use of the same measuring principle and the same type of device from one manufacturer. This is often sufficient for low-value risk reduction. This method is often used for temperature measurements where extremely high temperatures are expected. In this type of measurement, the sensor element fails due to aging, generally because of a line break. The additional signal converter allows work to continue without interruption, and "flying blind" without any temperature information is avoided. When using two identical devices, the service personnel do not require extra training, and keeping replacement devices in stock is a smaller effort. In this respect, homogeneous redundancy is also useful for safety loops, depending on the application.

Using the diverse redundancy method can also overcome systematic failures. The advantage of diverse redundancy is that devices suitable for SIL 2 protective functions can be used for SIL 3 protective functions. If, for example, SIL 2 pressure monitors are to be used in a SIL 3 safety instrumented system (SIS), it is important to ensure that different device software is used for this. 2 different devices can also be used. Diverse redundancy occurs whenever different measuring principles, e.g., ultrasonics and vibration measuring technology, are used for fill levels, rather than different devices. Measuring devices originating from different manufacturers then give a high degree of independence. The use of devices based on the same measuring principle but from different manufacturers should be treated with skepticism. These days, the same devices are often supplied by different manufacturers using other names and, despite the different housings, the devices themselves are identical. In this respect, another interesting option involves setting up measurement loops based on different principles. Sometimes, for example, a differential pressure can produce information that is similar to a flow measured using different principles.
Low Demand/High Demand Mode

Depending on the area for which a safety instrumented system (SIS) is to be designed, a different basic mode of operation must be used.

**Low Demand Mode**

The process industry uses low demand mode (on demand mode). This is a mode of operation with a low demand rate in relation to the SIS. The prerequisite for this classification is that the SIS must not be demanded more than once per year.

Emergency shutdown systems are a typical example of this, as they are activated only when the process is out of control. This situation normally occurs less than once a year. Thus, in the majority of cases the high demand mode is irrelevant for process instrumentation.

**High Demand Mode**

The manufacturing technology or factory automation sectors generally use high demand mode or continuous mode.

High demand mode is a mode of operation with a high demand rate or continuous demand in relation to the SIS. In practice this means that the SIS works continuously or is demanded more often than once per year.

Continuous monitoring of work processes is necessary to guarantee the safety of personnel and the environment, e.g., for punch presses with a safety circuit, saws with a protective cover, etc.

It makes sense to differentiate between the 2 modes of operation for mechanical components in particular, since these components vary considerably in terms of their failure behavior. For example, weathering or other environmental factors are responsible for the majority of failures in low demand mode due to infrequent use, whereas wear plays a more prominent role in high demand mode.

In some cases, the option of treating a low demand system as a high demand system may be considered. This idea may appear convenient because it can be advantageous for the calculation, but it is sometimes actually a requirement due to specific guidelines and standards. At first it seems that the idea will be easy to implement, e.g., by triggering the safety instrumented function more frequently than planned.

The function is normally designed so that repeated triggering is not possible. An example of this is a bursting disk that protects part of the process against damage.

For devices that can be used in both modes of operation, wear or environmental factors in the event of failures must be evaluated. Valves in high demand mode can reach the end of their life cycle, which is highly unlikely in low demand mode.
Basics for the Calculation

Probability of Failure of a Safety Instrumented System

Information on the SIL of the individual devices is not sufficient when planning safety instrumented functions (SIF). In the past, the safety loop needed to be capable only of achieving the lowest requirement class for the individual devices in accordance with DIN V 19250. Nowadays the probabilities of failure based on the random failures must also be calculated for SILs. The aforementioned probability of failure on demand (PFD) is the basic parameter for low demand mode in this respect. See „Faults Resulting from Wrong Organization and Planning of the Safety Function“, p. 14.

The PFD is the average probability that a SIF will be unavailable at the exact moment when this safety function is required. The probability of failure is expressed in hours for high demand mode/continuous mode and is referred to as the average frequency of dangerous failure per hour, or PFH.

The PFD/PFH of devices is determined in a complex analytical procedure called failure mode, effect and diagnostic analysis (FMEDA). This analysis examines the individual E/E/PE components' faults and their consequences, and determines whether these faults can be detected.

For the assessment of electronic circuits many widely known sources exist that examine the failure rate of individual components:

- SN 29500, by Siemens
- MIL-HDBK 217, by the US Department of Defense, focusing particularly on the determination of environmental conditions
- OREDA Offshore Reliability Database established by companies in the oil industry

All these data sources assume that the failure rates of components follow the principle of a bathtub curve. Increased failure rates are only recorded in 2 cases: For early failures at the start of operation or when a component has almost reached the end of its useful life. Otherwise the components' failure rate remains constant. For the constant phase, the failure rate of devices can be determined.

For devices with a safety function it is not merely the overall failure rate of the device that is important. IEC/EN 61508 also wants to ascertain the following:

- Does the effect lead to a safe or dangerous situation?
- Does the effect have any impact on the safety function?
- Are failures detected by an appropriate diagnostic function or not?

A safe failure by definition sets the system to a safe state. A dangerous failure causes the safety function to cease running correctly. The system can no longer be set to a safe state.

With both failure types, a distinction can be made between detected and undetected failures, but only a dangerous undetected failure actually leads to a dangerous failure of the safety function. This categorization allows users of a device to determine the probability of a dangerous failure if this device is used in a safety loop. The surrounding system is unable only to cope with dangerous undetectable failures. This failure rate for dangerous undetected failures can then be used to derive the PFD values for low demand mode or the PFH values for high demand mode/continuous mode.
In accordance with the new 2010 edition of the IEC/EN 61508-2 standard, a distinction between detected and undetected failures is no longer made for safe failures.

Another aspect is important for low demand mode. In order to ensure that dangerous undetected failures do not “lie dormant” in the system for a long time, the safety function must be tested regularly. Based on the degree of reliability required, the intervals at which a proof test must be performed are specified in accordance with IEC/EN 61508. This ensures that the safety loop is checked regularly for correct operation and that dangerous undetected failures are identified and fixed in the proof test. This test plays a key role for the safety function. Shortening the interval between these tests reduces the probability of failure on demand, but also increases the cost. Any car driver can imagine this when thinking of the (often biennial) general inspection, their car is supposed to pass to ensure it is still running safely. An annual or even 6-monthly inspection would increase the vehicle’s safety but would increase the cost at the same time.

The regular proof test must detect and fix all faults. In practice, however, this cannot always be guaranteed. An additional parameter has been introduced to take this into account, known as the proof test coverage, or PTC for short. The PTC indicates how high the relative proportion of detected faults is.

The failure rate \( \lambda(t) \) indicates the relative number of failures during a specific monitoring period. The failure rate \( \lambda \) is used to obtain the probability of failure for a component (E/E/PE device or component) during the specified monitoring period.

The following applies:

\[
\lambda(t) = \frac{\text{Number of failures during a specific observation time}}{\text{Number of monitored components} \times \text{observation time}}
\]

Therefore:

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

\( \Delta t \) = observation time

\( n(t) \) = number of functioning components at time \( t \)

The unit for the failure rate \( \lambda \) is 1/time. In this case the failure rate of \( 10^{-9} \) t/h is often referred to as “failure in time” (FIT).

If the PTC is < 1, complex formulas must be used for the PFD calculation that also take the PTC into consideration. Suitable formulas can be found e.g., in version 2 of IEC/EN 61508-6.

If the PFD or PFH values are too high, this can prevent or at least limit achievement of a SIL through risk reduction measures.

### Failure Rate \( \lambda(t) \) – Concepts and Formulas

The failure rate \( \lambda(t) \) indicates the relative number of failures during a specific monitoring period. The failure rate \( \lambda \) is used to obtain the probability of failure for a component (E/E/PE device or component) during the specified monitoring period.

The following applies:

\[
\lambda(t) = \frac{\text{Number of failures during a specific observation time}}{\text{Number of monitored components} \times \text{observation time}}
\]

Therefore:

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

\( \Delta t \) = observation time

\( n(t) \) = number of functioning components at time \( t \)

The unit for the failure rate \( \lambda \) is 1/time. In this case the failure rate of \( 10^{-9} \) t/h is often referred to as “failure in time” (FIT).

**Example:**

A service life test is performed on 10 000 E/E/PE components. Within a week, 3 components fail.

The failure rate is determined as follows:

\[
\lambda = \frac{10 000 - 9997}{10 000 \times 7 \times 24 \text{ h}} = \frac{3}{1 680 000 \text{ h}} = 1.8 \times 10^{-6} \text{ t/h} = 1 800 \text{ FIT}
\]

In service life tests of this type, only the part of the bathtub curve where the failure rate is constant is considered. See „Probability of Failure of a Safety Instrumented System“, p. 29. Early failures and higher failure rates at the end of a component’s service life are not taken into account.

Calculation results that assume a constant failure rate are only valid as long as no wear occurs. Electronic devices are expected to have a service life of 8 … 12 years. The service life also depends on operational conditions such as environmental influences, useful working period, and the sensitivity of the components used. For example, some components are known for being prone to accelerated aging, e.g., electrolytic capacitors. Further details on this can be found in IEC/EN 61508-2.
Probability of Failure, \( F(t) \)

The probability of failure of a component (E/E/PE device or component) can be determined, provided that the failure rate \( \lambda(t) \) is constant. As a general rule:

\[
F(t) = 1 - e^{-\lambda \times t}
\]

This means the probability of failure moves closer to 1 as time progresses.

In practice, the exponent of the "e" function in the amount is always considerably lower than 1 \((\lambda \times t < 1)\), which means that the equation can be simplified.

The probability of failure \( F(t) \) results in the basic term:

\[
F(t) = \lambda \times t
\]

This approximation ceases to be valid if high \( \lambda \) values or long time intervals are involved.

---

Mean Probability of Failure on Demand

The probability of failure on demand (PFD) is important for safety functions that are only rarely demanded as risk reduction measure (low demand mode). In order to simplify the calculation, as outlined in IEC/EN 61508, the time dependence can be eliminated by averaging (PFDavg).

There are 2 different failure types:

- Dangerous undetected failures (failure rate \( \lambda_{du} \))
- Dangerous detected failures (failure rate \( \lambda_{dd} \))

The failure rate \( \lambda_{du} \) influences the PFD insofar as a device in which a failure has been detected must be repaired from this point. The safety function is not available during the repair time (mean time to repair, MTTR) and fails on demand. If the failure is fixed within a few hours and the failure rate \( \lambda_{dd} \) of the dangerous detected failures is not unusually high, this risk can be disregarded. This simplifies the PFD calculation.

Example:

The failure rate of a sensor is

\[
\lambda = 30 \text{ FIT} \\
\lambda = 30 \times 10^{-9} \times \text{h}^{-1}
\]

The probability that the sensor will fail within the first year of operation can be calculated using the simplified formula for the probability of failure \( F(t) \) (1 year = 8760 h). This leads to:

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

If a 1-channel structure (1oo1) regularly undergoes a full proof test in the time interval \( T_1 \), the simplified formula for the PFD calculation is as follows:

\[
PFD_{1oo1} = \lambda_{du} \times \frac{T_1}{2}
\]

The PFH is needed for frequently required safety functions (high demand mode). The PFH value matches the failure rate \( \lambda_{du} \) for 1-channel systems.
Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT)

Definitions

The parameters SFF and HFT can influence or even reduce the SIL of a risk reduction measure.

The HFT is a factor relating to redundancy in the structure of a safety function. If an individual safety function evaluates an input variable via two paths, the HFT = 1, i.e., 1 fault is tolerable.

In order to describe redundancies and redundant architectures, the notation "MooN" (M out of N) is often used. The variables M and N are defined as follows:

- M = number of channels that must operate correctly to perform the safety function correctly.
- N = total number of redundant channels within a safety-related architecture (or safety loop).

Example of 2oo3 Fill Level Measurement:

A fill level measurement system of this type works as follows: At least 2 out of 3 parallel fill level sensors must indicate that a fill level has been exceeded. Only after that the system indicates that the specified limit is reached.

Possible MooN Structures

The HFT provides more information on the structure of the safety loop. Consequently, the HFT can also influence the safety function's probability of failure on demand (PFD). The PFD is determined based on the proportion of dangerous undetected failures of devices and the intervals between proof tests on a safety function. Since the PFDs of devices connected in series must be added up for the calculation, an overall PFD can be obtained for a safety function. The formulas indicated here are taken from the VDI/VDE 2180 guideline, which uses much simpler formulas than the formulas in IEC/EN 61508. If repair times can be disregarded, these simplified formulas are sufficiently precise.

<table>
<thead>
<tr>
<th>HFT</th>
<th>Reliability Block Diagram</th>
<th>Plant Safety</th>
<th>Plant Availability</th>
<th>PFDavg</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><img src="image" alt="Reliability Block Diagram 0" /></td>
<td>○</td>
<td>○</td>
<td>(\lambda_{du} \times \frac{T_1}{2})</td>
</tr>
<tr>
<td>0</td>
<td><img src="image" alt="Reliability Block Diagram 0" /></td>
<td>-</td>
<td>+</td>
<td>(\lambda_{du} \times T_1)</td>
</tr>
<tr>
<td>1</td>
<td><img src="image" alt="Reliability Block Diagram 1" /></td>
<td>+</td>
<td>-</td>
<td>(\frac{\lambda_{du}^2 \times T_1^2}{3} + \beta \times \lambda_{du} \times \frac{T_1}{2})</td>
</tr>
<tr>
<td>1</td>
<td><img src="image" alt="Reliability Block Diagram 1" /></td>
<td>+</td>
<td>+</td>
<td>(\lambda_{du}^2 \times T_1^2 + \beta \times \lambda_{du} \times \frac{T_1}{2})</td>
</tr>
<tr>
<td>2</td>
<td><img src="image" alt="Reliability Block Diagram 2" /></td>
<td>++</td>
<td>-</td>
<td>(\frac{\lambda_{du}^3 \times T_1^3}{4} + \beta \times \lambda_{du} \times \frac{T_1}{2})</td>
</tr>
</tbody>
</table>

Figure 20. Potential MooN structures resulting from the HFT as the basis for the PFD calculation
The SFF indicates what fraction of the total potential failures are safe failures. In principle, the higher the SIL and the lower the HFT of a safety function, the more the SFF must be increased. The following table from IEC/EN 61511 is applicable to programmable electronic systems:

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance of PE Logic Systems</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFF &lt; 60 %</td>
<td>60% ≤ SFF &lt; 90%</td>
</tr>
<tr>
<td>SIL 1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>SIL 2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>SIL 3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>SIL 4</td>
<td>Specific requirements are applicable. See IEC/EN 61508.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5. Minimum hardware fault tolerance of PE logic systems

The following table is applicable to field devices:

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance of Sensors, Actuators, and Non-Programmable Logic Systems</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prior Use</td>
<td>Standard Requirement</td>
</tr>
<tr>
<td>SIL 1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SIL 2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>SIL 3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SIL 4</td>
<td>Specific requirements are applicable. See IEC/EN 61508.</td>
<td></td>
</tr>
</tbody>
</table>

Table 6. Minimum hardware fault tolerance of sensors, actuators, and non-programmable logic systems

IEC Device Classification for Planning Safety-Related Systems

To ensure that safety-related architectures are set up and assessed correctly, IEC/EN 61508 stipulates that E/E/PE devices must be classified. The standard differentiates between type A and type B devices. The definition of a type A device is that the failure rates and failure modes of all components are clearly known in all cases so that the device behavior in the event of fault is explicitly known.

If a device contains only discrete components, it will normally meet the requirement for a type A device. If not, it is a type B device. In this case, the device behavior in the event of a fault cannot be predicted. Programmable or configurable devices are therefore type B devices.

To create an additional safety buffer for devices with failure rates that are not easily defined, the SFF for type B devices must therefore be set one level higher than for type A devices.

If it can be demonstrated that apparatus or devices have already proven acceptable during prior use, the left column of Table 6 may be used. The HFT may therefore be decreased by one level compared with the standard requirement. In this case, appropriate proof must be provided in accordance with the requirements of IEC/EN 61511.

At the time of writing, there is no further the SFF is no longer mentioned in the upcoming new version of IEC/EN 61511. For device manufacturers, however, it remains an important variable for determining a device's SIL rating.
Multichannel MooN Architectures – Concepts and Formulas

PFD Calculation

To reduce the probability of failure of a safety instrumented function, systems can have built-in redundancy. The PFD of this redundant system can be calculated from the failure rates of the individual channels. In accordance with IEC/EN 61508, the distinguishing feature is that some of the potential failures affect all channels equally, making any redundancy ineffective for these failure types. This is represented by the β factor in the PFD calculation. The β factor indicates the failure fraction that triggers the same effect on all channels simultaneously.

Example:

If 5% of potential failures on a channel affect the other channels, then \( \beta = 0.05 \).

The β factor is determined via a tabular evaluation system, which can be found in IEC/EN 61508-6. The evaluation system takes into account factors such as the device properties, the ambient conditions at the installation location, and the scope of the quality management system. The reliability block diagram shows a 1-channel structure connected downstream of the multichannel (redundant) structure. The failure rate of this 1-channel structure corresponds to the "common cause failures".

If the influence of the repair time is disregarded, this results in the following simplified formulas for calculating the PFD for various multichannel structures (see VDI/VDE 2180):

\[
\begin{align*}
PFD_{1oo1} & = \lambda_{du} \times \frac{T_1}{2} \\
PFD_{2oo2} & = \lambda_{du} \times T_1 = 2 \times PFD_{1oo1} \\
PFD_{1oo2} & = \frac{\lambda_{du}^2 \times T_1^2}{3} + \beta \times \lambda_{du} \times \frac{T_1}{2} = \frac{4}{3} \times PFD_{1oo1}^2 + \beta \times PFD_{1oo1} \\
PFD_{2oo3} & = \lambda_{du}^2 \times T_1^2 + \beta \times \lambda_{du} \times \frac{T_1}{2} = 4 \times PFD_{1oo1}^2 + \beta \times PFD_{1oo1} \\
PFD_{1oo3} & = \frac{\lambda_{du}^3 \times T_1^3}{4} + \beta \times \lambda_{du} \times \frac{T_1}{2} = 2 \times PFD_{1oo1}^3 + \beta \times PFD_{1oo1} \\
PFD_{2oo4} & = \lambda_{du}^3 \times T_1^3 + \beta \times \lambda_{du} \times \frac{T_1}{2} = 8 \times PFD_{1oo1}^3 + \beta \times PFD_{1oo1}
\end{align*}
\]
Reiability Characteristics

A key variable for assessing device failures is the mean time to failure (MTTF). The MTTF indicates the average operating time without failures for devices of a certain type. However, this does not mean that a device is guaranteed to fail once it reaches its MTTF. Similarly, not all devices are guaranteed to operate reliably for the entire MTTF. However, the MTTF is a useful variable to help plant operators establish replacement requirements.

Note: The term “MTTF” can have 2 meanings, which often gives rise to misunderstandings.

- MTTF = mean time to failure (as used in this publication), i.e., the average operating time without failures for a type of device or a person. This gives an “average service life” of approximately 75 years for a human.

- MTTF = inverse of the failure rate λ, i.e., the probability that a device will fail during a specific time interval in the flat section of the bathtub curve. When using the term as a synonym for the inverse of the failure rate λ, the value obtained for a human is over 1000 years! EN ISO 13849-1 actually uses the term “MTTF” in this sense.

For information on the failure rate λ, see „Failure Rate λ(t) – Concepts and Formulas“, p. 30.

The term mean time between failures (MTBF) is often used as a synonym for MTTF. MTBF also includes a repair time, provided a system is repairable. This repair time can normally be disregarded.

The mean repair time (MRT) denotes the time taken to overhaul a device and is required if a device is repaired during the proof test. The very similar mean time to repair (MTTR) also considers the time that elapses before the defect in the device is identified during ongoing operation of the system. MTTR is key to the repair time for dangerous detected failures. In practice, the MRT is frequently considered to be equivalent to the MTTR for pragmatic reasons. Since repair times are usually negligible, they are disregarded in the formulas in VDI/VDE 2180.

The last time-related term that we will explain here is mean down time (MDT). The MDT denotes the average time during which a device is not operational.¹

Probability Density Function f(t) – Concepts and Formulas

The density function f(t) for the probability of failure is obtained from the derivation of the distribution function F(t). The probability density can be used to calculate the expected value of a random variable, in this case the service life (mean time to failure, MTTF).

At the start of the operating period (in the graphic e.g., up to around 8 years), the probability of failure increases approximately linearly with the time.

The time derivative of the formula for the probability of failure F(t) gives:

\[ f(t) = \lambda \times e^{-\lambda t} \]

Figure 22. Probability of failure and density function at constant failure rate

¹ DIN EN 61703:2002: Mathematical Expressions for Reliability, Availability, Maintainability, and Maintenance Support Terms
Reliability Function, \( R(t) \)

The reliability function \( R(t) \) indicates the probability that a device will perform its function successfully up to a point \( t \) in time.

Because the reliability function \( R(t) \) variable complements the probability of failure \( F(t) \), the reliability function can be calculated by subtracting the probability of failure \( F(t) \) from 1.

\[
R(t) = 1 - F(t) = 1 - (1 - e^{-\lambda t})
\]

Mean Time to Failure, \( MTTF \)

The density function for the probability of failure can be used to calculate the expected service life as follows:

\[
MTTF(t) = \int_0^\infty t \times f(t) \, dt = \int_0^\infty t \times \lambda e^{-\lambda t} \, dt = \frac{1}{\lambda}
\]

Alternatively, the mean time to failure can be calculated using the reliability function \( R(t) \), as follows:

\[
MTTF(t) = \int_0^\infty R(t) \, dt = \int_0^\infty e^{-\lambda t} \, dt = \frac{1}{\lambda}
\]

"Proven in Use" and "Prior Use"

In order to evaluate whether a device can be used in a safety instrumented system the "proven-in-use" is a key principle. In the process industry this principle has become increasingly important over recent years. Whereas theoretical device properties such as the SFF used to be required, it is now quicker and easier to assess whether a device has proved to be suitable for specific similar applications. This assessment then allows devices to be qualified for safety instrumented loops.

The process industry develops NAMUR recommendations that define properties of devices for use in processing plants. The proven-in-use concept for use of devices in safety loops up to SIL 2 is covered by NE 130. The NE 130 outlines a process for the qualification of devices. This approach can also be found under "prior use" in the IEC/EN 61511 user standard.

Device Classification according to NE 130

The process starts with device qualification in accordance with NE 95, which involves a range of measuring criteria. These measuring criteria encompass, e.g., the following general information on device properties:

- Measuring accuracy, temperature drift, failure behavior, etc.
- Electromagnetic compatibility in accordance with NE 21
- Completeness and plausibility of device documentation (e.g., warnings, certifications, installation documentation, instruction manual)
- Operability
- Structural design
- Findings from maintenance
- Version history

Other measuring criteria include the following safety instrumented aspects:

- Availability of a manufacturer's declaration (e.g., form B.1); test for completeness and plausibility
- Availability of a safety manual
- Quality and practical suitability of the contents
- Non-interaction of unused device functions in safety mode
- Complexity of configuration, manual testability
- Identification of potential faults that impair functionality
- Evaluation of diagnostics suitable for safety-related use
- Assessment of safety-related parameters

Finally, the devices are tested in operation. 10 devices are tested for correct operation over 1 year, which equals 87,600 hours' operation of the system and provides initial statistical data. This must not be used to derive a blanket statement for the device. Instead, similar application types must be sought. This should not pose a problem, as most devices used in the process industry are exposed to harsh environmental conditions and aggressive media in the field.

This process makes it considerably easier to provide safety verification. Users can obtain evidence of safety themselves without having to rely on the accuracy of data provided by suppliers.
The operation of devices rated as proven in use and used for safety instrumented functions in the field must be closely monitored in accordance with NE 93. Particular attention must be paid to the following variables:

- SIL requirement of the respective safety function
- Number of dangerous failures of a device
- Number of active failures: Actual activation of a protective function resulting from a device failure

Ways of ascertaining proven-in-use state can also be found in the IEC/EN 61511 standard. However, these approaches are much less specific, which is why proceeding in accordance with NE 130 can be deemed adequate.\(^1\)

Another method of establishing proven-in-use state from the SIL standards is described in IEC/EN 61508 itself. If the development of a device did not involve "functional safety management" in accordance with IEC/EN 61508, a statement regarding its systematic suitability can still be made. The prerequisite that in the manufacturer's experience, the device has not shown any systematic failures in specific applications over a number of years. The device is then considered to be "proven in use".

This procedure is particularly justified for devices that were suitable for safety applications in accordance with older standards. Such devices do not suddenly become unsafe because the standards have changed. An assessment of "proven in use" means that devices of this type can also be used in SIL-rated safety instrumented functions.

Failure rates can be determined in the following two ways:

- Standard FMEDA: Determined via evaluation of failure rates at component level
- Failure rate based on evaluation of returns

The second option leads to the question of whether the manufacturer is really aware of all defects. Evaluation of returns is not sufficient if devices are exchanged due to wear or are inexpensive to buy. Customer surveys or contractual arrangements with users can help to ensure that failures are actually reported to valid statistical information.

The assessment of devices via proven-in-use state is invariably useful since, no matter how good a new development is, faults can never be completely ruled out. If experience of a device is available, this will always have more informative value than a mere prediction for the future based on IEC/EN 61508.

New developments cannot be assessed on the basis of the proven-in-use principle. These devices can only be assigned a confirmed SIL rating if they are developed in accordance with IEC/EN 61508.

---

\(^1\) Hablawetz, Dirk, BASF SE: Gerätequalifikation aufgrund "früherer Verwendung" (Betriebsbewährung) [Device qualification based on "prior use" (proven-in-use state)], lecture at SIL-Tag 2012 event, Automatisierungstechnische Praxis (ATP) and Pepperl+Fuchs GmbH, Mannheim, Germany
The following simplified example of an overfill prevention system shows how a safety integrity level (SIL) can be determined for a safety loop.

The overfill prevention system has diverse 1oo2 redundancy in the sensor and actuator circuits. The 1oo2 redundancy is selected by the user program in the safety PLC for the sensors, and by an appropriate topology in which both valves are connected in series for the actuators. The SIL achieved can often be assessed as follows:

1. Determining the safety function based on risk analysis
   The safety function for this safety loop is to shut off an inlet when a particular fill level is exceeded. This function must be performed at SIL 3.

2. Proving the suitability of devices
   The suitability for use in safety functions can be found in the manufacturer's specifications, e.g., as provided in safety manuals. Qualification based on prior use is also possible.

3. Checking the structural suitability
   Check if the hardware fault tolerance (HFT) required for the desired SIL has been achieved. From this, the required architecture can be derived, e.g., 1oo2 as 2-channel redundancy.

4. Determining probability of failure (PFD calculation)
   - Define boundary conditions and assumptions
   - Generate reliability block diagram
   - Simplify block diagram iteratively

5. Evaluating and documenting the result

1. Determining the Safety Function Based on the Risk Analysis
   The safety function for this safety loop is to shut off an inlet when a particular fill level is exceeded. This shutoff function must be performed at SIL 3.

2. Proving the Suitability of Devices
   The fail-safe control system is SIL-3-rated. The other devices are SIL-2-rated (manufacturer's specifications). Since SIL 3 needs to be reached for the safety function, this can be achieved only by increasing the HFT in the sensor and actuator circuit (redundancy). If the devices used are controlled by software, this requires diverse redundancy unless the device manufacturer confirms that the software is suitable for SIL 3 in the safety manual. Proven-in-use state has also been established for the field devices that come into direct contact with media, in accordance with NE 130. The failure rates for individual devices are indicated in the manufacturers' safety manuals.
3. Checking the Structural Suitability

If the devices have been selected based on prior use, a hardware fault tolerance of 1 is required in accordance with the table of hardware fault tolerances for SIL 3. This results in the 1oo2 architecture.

Note: The 2 valves in the plant (actuator 1, actuator 2) are connected in series.

The switching logic plays a significant role in a safety loop together with the plant logic. This gives rise to the following questions:

- When is which state defined as safe:
  - Actuator open or closed?
  - Actuator active/inactive?
- When does it make most sense to design a redundancy in series or in parallel?

Table 7. Minimum hardware fault tolerance

<table>
<thead>
<tr>
<th>SIL</th>
<th>SFF ≤ 60%</th>
<th>Standard Requirement</th>
<th>Prior Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SIL 2</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>SIL 3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>SIL 4</td>
<td>Specific requirements are applicable. See IEC/EN 61508.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 24. Example of systematic suitability in a safety loop up to SIL 3
The example uses valves that close when they are de-energized. Depending on whether valves in the inlet or the outlet are intended to limit the fill level in a container, the valves must be ordered in parallel or in series.

- The flow must be stopped safely at the inlet to the container. This is achieved by valves connected in series. This means that if one valve fails to close, the other valve will still achieve the desired effect.

- The opposite applies in the outlet: The valve must open safely to reduce the fill level. If one valve does not perform this task due to a failure, the objective can be achieved only by a parallel valve.

The following figures show a safety loop with diverse redundancy for a fill level limitation system.
The devices in the sensor and actuator circuit are SIL-2-rated as outlined in point 2. This means diverse redundancy is still needed to increase the HFT, and this requirement is fulfilled.

**Note:** Even if all the devices were SIL-3-rated, the minimum HFT requirement in accordance with IEC/EN 61511 would have to be met.

---

**Figure 26.** Variant 2: Opening the outlet
4. Calculating the PFD

Annual proof test $T_1 = 8760$ hours
Fraction of common cause failures is 10% ($\beta = 0.1$).

Generate a reliability block diagram (RBD) for the system. The block diagram ensures that all the involved devices are taken into account for the subsequent calculations.

Figure 27. Reliability block diagram of a safety function; all $\lambda_u$ values in 1/h
Simplify the RBD iteratively as follows

- Add up the failure rates or PFD values: In 1-channel systems or subsystems that are not redundant (1oo1), all known failure values ($\lambda_{in}$) can be added together.

- In the event of redundancy, use the appropriate formulas. If systems or subsystems are redundant (e.g., 1oo2), apply the following formula to simplify the calculation:

$$\text{PFD}_{\text{total}} = \frac{1}{3} \left( \lambda_{\text{In subsystems}} \times T_1^3 + \beta \times \lambda_{\text{In subsystems}} \times \frac{T_1}{2} \right)$$

**Figure 28. PFD calculation from the reliability block diagram**
5. Assessing the Result

Evaluate the final result based on the IEC/EN 61508-1 standard. In the example here, a comparison with the standard results in SIL 3.

### Demand Mode

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Target Value for the Average Probability of Failure (Target Failure Measure) on Demand</th>
<th>Target Value for Risk reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>$\geq 10^{-4}$ to $10^{-3}$</td>
<td>$&gt; 10000$ to $\leq 100 000$</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^{-4}$ to $10^{-3}$</td>
<td>$&gt; 1000$ to $\leq 10 000$</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^{-3}$ to $10^{-2}$</td>
<td>$&gt; 100$ to $\leq 1000$</td>
</tr>
<tr>
<td>SIL 1</td>
<td>$\geq 10^{-2}$ to $10^{-1}$</td>
<td>$&gt; 10$ to $\leq 100$</td>
</tr>
</tbody>
</table>

Table 8. Safety integrity level: probability of failure on demand

### Continuous Mode

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Target Value for the Frequency of Dangerous Failures of the Safety Instrumented Function per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>$\geq 10^{-5}$ to $10^{-4}$</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^{-6}$ to $10^{-5}$</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^{-7}$ to $10^{-6}$</td>
</tr>
<tr>
<td>SIL 1</td>
<td>$\geq 10^{-8}$ to $10^{-7}$</td>
</tr>
</tbody>
</table>

Table 9. Safety integrity level: frequency of dangerous failures of the safety instrumented function
### Glossary and List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation/Term</th>
<th>Full Expression</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARP</td>
<td>as low as reasonably practicable</td>
<td>Risk reduction method that involves reducing the risk until the practicable level of safety is achieved.</td>
</tr>
<tr>
<td>E/E/PE</td>
<td>electrical/electronic/programmable electronic</td>
<td>Term relating to electrical components or devices that can be used for a safety instrumented function.</td>
</tr>
<tr>
<td>E/E/PES</td>
<td>electrical/electronic/programmable electronic systems</td>
<td>Term relating to all electrical devices or systems that can be used for a safety instrumented function. These can be basic electrical devices and programmable logic controllers (PLC).</td>
</tr>
<tr>
<td>EUC</td>
<td>equipment under control</td>
<td>Equipment, machinery, apparatus, or systems used for production, material processing, or transportation, or for medical or other tasks.</td>
</tr>
<tr>
<td>ETA</td>
<td>event tree analysis</td>
<td>Method for generating an event tree diagram. The method begins with a starting event and analyzes all events that could potentially occur during operation of the system.</td>
</tr>
<tr>
<td>FME(C)A</td>
<td>failure mode effect (and criticality) analysis</td>
<td>Method of systematically testing all components for undesired effects that increase the probability of failures. The FMECA takes this method right down to component level.</td>
</tr>
<tr>
<td>FMEDA</td>
<td>failure mode effect and diagnostic analysis</td>
<td>Analysis for examining the failure of individual components and their consequences, and determining whether these failures can be detected.</td>
</tr>
<tr>
<td>λ_d</td>
<td>dangerous detected failure</td>
<td>Overall failure rate for dangerous detected failures.</td>
</tr>
<tr>
<td>λ_u</td>
<td>dangerous undetected failure</td>
<td>Overall failure rate for dangerous undetected failures.</td>
</tr>
<tr>
<td>λ_s</td>
<td>safe detected failure</td>
<td>Overall failure rate for safe detected failures.</td>
</tr>
<tr>
<td>λ_s</td>
<td>safe undetected failure</td>
<td>Overall failure rate for safe undetected failures.</td>
</tr>
<tr>
<td>failure</td>
<td></td>
<td>Loss of a functional unit's ability to perform a required function.</td>
</tr>
<tr>
<td>FIT</td>
<td>failure in time</td>
<td>Specific type of failure rate for predicting the probability of failure of components and devices based on the design. Unit: “failures per 10^9 hours”.</td>
</tr>
<tr>
<td>FTA</td>
<td>fault tree analysis</td>
<td>Method for generating a fault tree diagram. The method begins with an undesired event and analyzes the paths leading to this event.</td>
</tr>
<tr>
<td>hazardous event</td>
<td></td>
<td>Dangerous situation leading to damage.</td>
</tr>
<tr>
<td>HAZOP</td>
<td>hazard and operability study</td>
<td>A procedure used in safety technology for testing plant safety.</td>
</tr>
<tr>
<td>HDM</td>
<td>high demand mode</td>
<td>Mode of operation with a high demand rate in relation to the safety system (&gt; 1 × per year). Example: safety cover on a saw.</td>
</tr>
<tr>
<td>HFT</td>
<td>hardware fault tolerance</td>
<td>Ability of a hardware device to continue performing a required function despite faults or deviations.</td>
</tr>
<tr>
<td>LDM</td>
<td>low demand mode</td>
<td>Mode of operation with a low demand rate in relation to the safety system (&lt; 1 × per year). Example: emergency shutdown system in the process industry.</td>
</tr>
<tr>
<td>MooN</td>
<td>M out of N</td>
<td>Classification of a safety-related system based on redundancy and the relevant selection procedure. M: Number of redundant safety functions available N: Number of failure-free channels operating Example: Fill level measurement in a 1oo2 system. A safety-related system determines that a specific fill volume is exceeded if 1 out of 2 threshold value sensors reaches this limit.</td>
</tr>
</tbody>
</table>
| MRT               | mean repair time | Expectation of the repair time. Period that follows a component failure, including:  
  - Time until repair  
  - Repair time  
  - Time until the component is recommissioned |
### Glossary and List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation/Term</th>
<th>Full Expression</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MTBF</strong></td>
<td>mean operating time between failures</td>
<td>Expected duration of the operating time between failures. The MTBF is equivalent to the MTTF + MTTR.</td>
</tr>
<tr>
<td><strong>MTTF</strong></td>
<td>mean operating time to failure</td>
<td>1. Expectation of operating time to failure. &lt;br&gt; 2. MTTF for non-repairable items or repairable items that after repair can be considered to be &quot;as-good-as-new&quot;: The distribution of operating times to failure is exponential, i.e., it is a constant failure rate. Thus, the MTTF is numerically equal to the reciprocal of the failure rate ( \lambda ).</td>
</tr>
<tr>
<td><strong>MTTR</strong></td>
<td>mean time to restoration</td>
<td>Expectation of the time to restoration. Period that follows a component failure, encompassing: &lt;br&gt; ▪ Fault identification &lt;br&gt; ▪ Time until repair &lt;br&gt; ▪ Repair time &lt;br&gt; ▪ Time until the component is recommissioned</td>
</tr>
<tr>
<td><strong>PDF</strong></td>
<td>probability density function</td>
<td>Mathematical function referring to the distribution of probabilities.</td>
</tr>
<tr>
<td><strong>PFH</strong></td>
<td>average frequency of dangerous failure per hour</td>
<td>Average frequency of a dangerous failure of an E/E/PE safety-related system to perform the specified safety function over a given period of time.</td>
</tr>
<tr>
<td><strong>PFD</strong></td>
<td>probability of dangerous failure on demand</td>
<td>Probability that a safety instrumented system will fail to perform its function when it is required. Parameter for safety functions that have a low demand rate and are rarely activated, i.e., low demand mode.</td>
</tr>
<tr>
<td><strong>PFD_{avg}</strong></td>
<td>average probability of dangerous failure on demand</td>
<td>Average probability of a dangerous failure of the safety function in case of a demand.</td>
</tr>
<tr>
<td><strong>reliability</strong></td>
<td></td>
<td>Probability that an item can perform a required function under given conditions for a given time interval.</td>
</tr>
<tr>
<td><strong>risk</strong></td>
<td></td>
<td>Combination of the probability of damage occurring and the extent of this damage, calculated from frequency and extent of damage.</td>
</tr>
<tr>
<td><strong>safety</strong></td>
<td></td>
<td>Absence of unjustifiable risks that would cause physical injury or damage to health as a direct or indirect result of property damage or damage to the environment.</td>
</tr>
<tr>
<td><strong>safety function</strong></td>
<td></td>
<td>Function of a machine whereby a failure of this function can lead to a direct increase in the risk(s). Source: EN ISO 12100:2011.</td>
</tr>
<tr>
<td><strong>SFF</strong></td>
<td>safe failure fraction</td>
<td>Proportion of safe system failures. The SFF is determined from the rate of safe failures plus the rate of diagnosed/detected failures in relation to the system's overall failure rate.</td>
</tr>
<tr>
<td><strong>SIF</strong></td>
<td>safety instrumented function</td>
<td>Risk reduction function performed by an E/E/PE safety instrumented system, a safety instrumented system using other technology, or external equipment. The function's objectives include achieving or maintaining safe state for the EUC, taking a specific hazardous incident into consideration.</td>
</tr>
<tr>
<td><strong>SIS</strong></td>
<td>safety instrumented system</td>
<td>System consisting of 1 or more safety instrumented functions, each of which is subject to a SIL requirement.</td>
</tr>
<tr>
<td><strong>SIL</strong></td>
<td>safety integrity level</td>
<td>Discrete levels ranging from 1 ... 4, for specifying the requirements for the safety integrity of safety instrumented functions assigned to the E/E/PE safety instrumented system. SIL 4 is the highest safety integrity level and SIL 1 is the lowest level.</td>
</tr>
<tr>
<td><strong>SLC</strong></td>
<td>safety life cycle</td>
<td>Activities required for the implementation of safety systems and performed over a period that starts with the design of a project and ends when all E/E/PE safety-related systems and other risk reduction measures are no longer in use.</td>
</tr>
<tr>
<td><strong>tolerable risk</strong></td>
<td></td>
<td>Acceptable risk, based on the social values currently applicable to a given context.</td>
</tr>
<tr>
<td><strong>XooY</strong></td>
<td>X out of Y Channel architecture; see MooN</td>
<td>German term relating to channel architecture. For explanation, see MooN.</td>
</tr>
</tbody>
</table>
List of Sources


Hablawetz, Dirk, BASF SE: Gerätequalifikation aufgrund "früherer Verwendung" (Betriebsbewährung) [Device qualification based on "prior use" (proven-in-use state)], lecture at SIL-Tag 2012 event, Automatisierungstechnische Praxis (ATP) and Pepperl+Fuchs GmbH, Mannheim, Germany

Hildebrandt, Andreas, Pepperl+Fuchs GmbH: Bedeutung der Probabilistik bei der Bewertung sicherheitstechnischer Einrichtungen [Importance of probability in the assessment of safety instrumented equipment], lecture at SIL-Tag 2007 event, DECHEMA, Frankfurt/Main, Germany


Bock, Franz-Josef, Haferkamp, Klaus, TÜV Rheinland Industrie Services GmbH: ROGA—Methodology of the Risk Oriented Hazard Analysis (ROGA-LORA – A Comparison), lecture at SIL Symposium 2012, TÜV Rheinland GmbH, Cologne, Germany

Working group for technical systems, risk and communication processes, Commission of Hazardous Incidents (SFK): Risk management in accordance with the German Plant Safety Major Accidents Ordinance, SFK-GS-41, 2004


Bibliography (Standards)

DIN V 19250:1994—Control Technology; Fundamental Safety Aspects to Be Considered for Measurement and Control Equipment, pre-standard, withdrawn

DIN EN 61703:2002—Mathematical Expressions for Reliability, Availability, Maintainability, and Maintenance Support Terms

EN 31010:2010—Risk Management. Risk Assessment Techniques

EN 50126:1999—Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)

EN 61025:2007—Fault Tree Analysis (FTA)


IEC/EN 62502:2010—Analysis Techniques for Dependability. Event Tree Analysis (ETA)


NE 21:2011—Electromagnetic Compatibility

NE 93:2001—Verification of the Safety-Related Reliability of PCT Safety Instruments

NE 95:2013—Basic Principles of Homologation

NE 130:2011—“Proven-In-Use" Devices for Safety Instrumented Systems


VDMA 4315:2013—Turbomachinery and Generators—Application of the Principles of Functional Safety
Index

SIF ................................................. 12, 29
SIL .................................................. 8, 12
SIL rating ........................................ 26
SIL result ......................................... 44
SIS ................................................... 12, 26
SN 29500 (Siemens) ......................... 29
structural suitability ......................... 39
Swiss cheese model ......................... 24
system architecture: examples ........... 27
systematic failure ............................. 26
systematic fault ............................... 14

target failure measures: high demand mode ........... 28
target failure measures: low demand mode ........... 28
tolerable risk ................................. 8, 20
TÜV ............................................... 26
type A device ................................. 33
type B device ................................. 33

VDI/VDE 2180 ................................. 7, 32
VDMA 4315 ................................. 10