Functional Safety
Safety Integrity Level

Dr. Thomas Reus
Matthias Garbsch

Functional Safety SIL
Safety Integrity Level

Dr. Thomas Reus
Matthias Garbsch

Note
This reference work has been created to the best knowledge and belief. We assume no liability for possible errors. The definitive source of informtion is always the operating manual for the relevant device.

Preface

Who should read this
This booklet is intended as an introductory aid to functional safety (chapter 4 “Glossary”, page 15). It is aimed at JUMO customers and staff, and its content is limited to the areas and applications where JUMO products are used.

Why JUMO offers SIL products
JUMO develops and manufactures, amongst other items, products according to the Pressure Equipment Directive, the Machinery Directive, the ATEX Directive and special safety engineering product standards, such as DIN 3440.

DIN EN 61508 is nowadays indispensible for those products that are designed for safety applications, since it defines the “state of the art” for functional safety.

Summary of products with SIL capability
For an up-to-date overview and detailed information on our SIL-certified products, visit:
www.jumo.de ➔ Products ➔ Approvals ➔ SIL.

Terminology
This booklet makes frequent reference to (DIN) EN 61508. The full title of this standard is “Functional Safety of Safety-Related E/E/PE Systems”. Its content is identical to the IEC 61508 international standard.

Dr. Thomas Reus Matthias Garbsch

JUMO GmbH & Co. KG
Moritz-Juchheim-Straße 1
36039 Fulda, Germany
Phone: +49 661 6003-0
Fax: +49 661 6003-607
Email: thomas.reus@jumo.net
matthias.garbsch@jumo.net
Internet: www.jumo.net

Reprinting permitted with source citation!

Part No.: 00476107
Book No.: FAS630
Edition: April 2016
ISBN: 978-3-935742-18-4

Contents

Contents

1 Legal foundations, significance of standards

1.1 Motivation for standards

Our everyday life is governed by machinery and equipment to which we blindly entrust our lives, e.g. automobiles, traffic lights, medical equipment and energy installations.
For this reason, the legislature has established laws and other legal regulations that define specific requirements in safety matters.

In Germany, for instance, the statutory trade insurance associations (“Berufsgenossenschaften”) set up accident prevention regulations and monitor their implementation. Throughout the European Union, EU Directives define requirements for systems and their operators, to protect and preserve health and the quality of the environment. They prescribe specific product characteristics for the preservation of consumer health and safety.

In Germany, the compliance with standards and the required safety targets is enforced through the Law on Equipment and Product Safety, in conjunction with the rights to damages prescribed by § 823 of the German Civil Code (“Bürgerliches Gesetzbuch”). Not only equipment manufacturers, such as JUMO, but also the system and plant operators, are therefore obliged to achieve the corresponding safety targets.
Similar regulations apply in other countries.

It is necessary here to distinguish between safe products in the generalized sense, and products that are specially designed for safety applications. For the latter, (DIN) EN 61508 has now become indispensable, since it defines the “state of the art” for functional safety.

1.2 Functional safety standards – development of (DIN) EN 61508

The key event was the poison gas accident in the northern Italian town of Seveso in July 1976.
Since then, the European Union Directive 96/82/EU has defined the legal conditions for plants with a high hazard potential.

The German implementation of the directive 96/82/EU is realized in the hazardous incident regulations of the Federal Law on Emission Safety (12. BImSchV).

Up to 31 July 2004, the hazardous incident regulations referred to the German Standards DIN V 19250 and DIN V 19251, in which the requirements were defined in Classes AK 1 to 8.

Since 2002, (DIN) EN 61508 provides a new method for risk assessment and the required proof of effectiveness for safety-related systems, in order to continue to fulfil the aims of the hazardous incident regulations. This defines four safety levels: SIL1 to SIL4.
(DIN) EN 61508 has thus replaced the German standards DIN V 19250 and DIN V 19251.

Ratification of the series of standards took place in July 2001. The standard was thereupon accepted by the European standards organization CENELEC. On 1 August 2002 it was incorporated into the German set of standards as (DIN) EN 61508 (VDE 0803), and thus defines the state of the art for E/E/PE (electrical, electronic and programmable electronic) systems that are involved in safety functions for safety-critical applications.

(DIN) EN 61508 is a generic standard, i. e. independent of the application. It is a fundamental standard and therefore generally valid for all E/E/PE systems.

(DIN) EN 61508 is based on the international standard IEC 61508, and thus has worldwide validity. It is the first international harmonized set of regulations that is application-independent for all E/E/PE systems.

The application-specific standards are now being derived from this, one-by-one, such as:

- (DIN) EN 61511 for functional safety in process engineering,
- (DIN) EN 62061 for functional safety in machine controls.

The further development of standardization methodology was made necessary by the ever-increasing complexity of modern safety-critical systems. Up to the mid-90s, one could say: the application of microelectronics or microcomputers in safety engineering was inconceivable or only feasible with extremely involved test equipment. At that time, many standards and regulations still expressly demanded conventional solutions with interlocks implemented by relays or contactors. The application of equipment that was more modern, more economic, and often even superior from the safety engineering aspect, was not permitted.
But the requirements that a system has to fulfill are becoming ever more complex, and can, as a rule, only be economically met by electronic solutions.
This is especially so in the sector of digital computers and automation technology, where complex digital circuits are used for the central unit.

1.3 Legal position of (DIN) EN 61508 in the sense of an EU directive

(DIN) EN 61508 describes the state of the art with regard to functional safety.
But it is not harmonized as part of an EU directive, i.e. there is no automatic assumption of fulfillment of the protective aims of a directive associated with this standard.
At present, compliance is therefore voluntary and not binding in the sense of the EU directives.

Nevertheless, the manufacturer of a safety-engineering product can apply (DIN) EN 61508 in fulfillment of basic requirements according to European directives.
This results from the new concept of the standard, e.g. in the following cases:

From a harmonized European standard (such as (DIN) EN 954 and (DIN) EN 60204-1, that harmonize the Machinery Directive) there is a referral to (DIN) EN 61508. This ensures that the relevant requirements of the standard are fulfilled (“jointly applicable standard”).
If a manufacturer applies (DIN) EN 61508 in the sense of this referral, in an expert and responsible manner, then he is making use of the assumption of fulfillment from the referring standard.

There is no harmonized standard (such as, for example, DIN 3440, DIN EN 14597) for the application concerned. In this case, the manufacturer may apply (DIN) EN 61508 (state of the art). But there is no assumption of fulfillment.

Explanation
For the process industry, (DIN) EN 61511 has already been derived from (DIN) EN 61508 as a basic standard. Likewise, (DIN) EN 62061 is available for the Machinery Directive. For combustion engineering, (DIN) EN 50156 is available as a standard.

2 Fundamental principle of (DIN) EN 61508

2.1 Changes compared with previous safety standards

In the (DIN) EN 61508 standard for functional safety, the requirements for safety-related systems are divided into Safety Integrity Levels (SIL) (see Glossary). Instruments, sensors and controls must therefore have a SIL classification according to the standard. A new understanding of safety also arises. Whereas previous safety engineering standards usually involved a purely qualitative examination, the new standard demands, for the first time, a quantitative examination of the entire system and proof that the residual risk is sufficiently small.

Furthermore, the entire safety life cycle of a system is also regulated for the first time, see chapter 2.4 *„Life cycle“, page 10*.

2.2 Risk reduction

Every application of technology represents a simultaneous safety engineering risk. The more people, property, or the environment are set at risk, the more measures must be taken to reduce that risk. The risk should at least be so far reduced that the probability of a person losing their life as a result of the failure of a technical device is less than 10^{-4} fatalities / per person and year.
This is roughly equivalent to the risk of a person losing their life as a result of natural causes in the course of a year. This risk varies with the age of the person concerned, and lies between 10^{-2} and 10^{-4}.
A summary of basic everyday risks is shown in figure 1 on page 8.

In order to achieve functional safety for a machine or plant, it is necessary to ensure that the safety-relevant parts of the control and protection equipment function correctly and, in the event of a fault, respond in such a manner that the system remains safe or is put into a safe state.

The object of (DIN) EN 61508 is to avoid faults in safety-related systems, or to have faults under control and to limit the probability of dangerous failures (risk) in a defined manner. A quantitive proof is required for the residual risk that remains.

2 Fundamental principle of (DIN) EN 61508

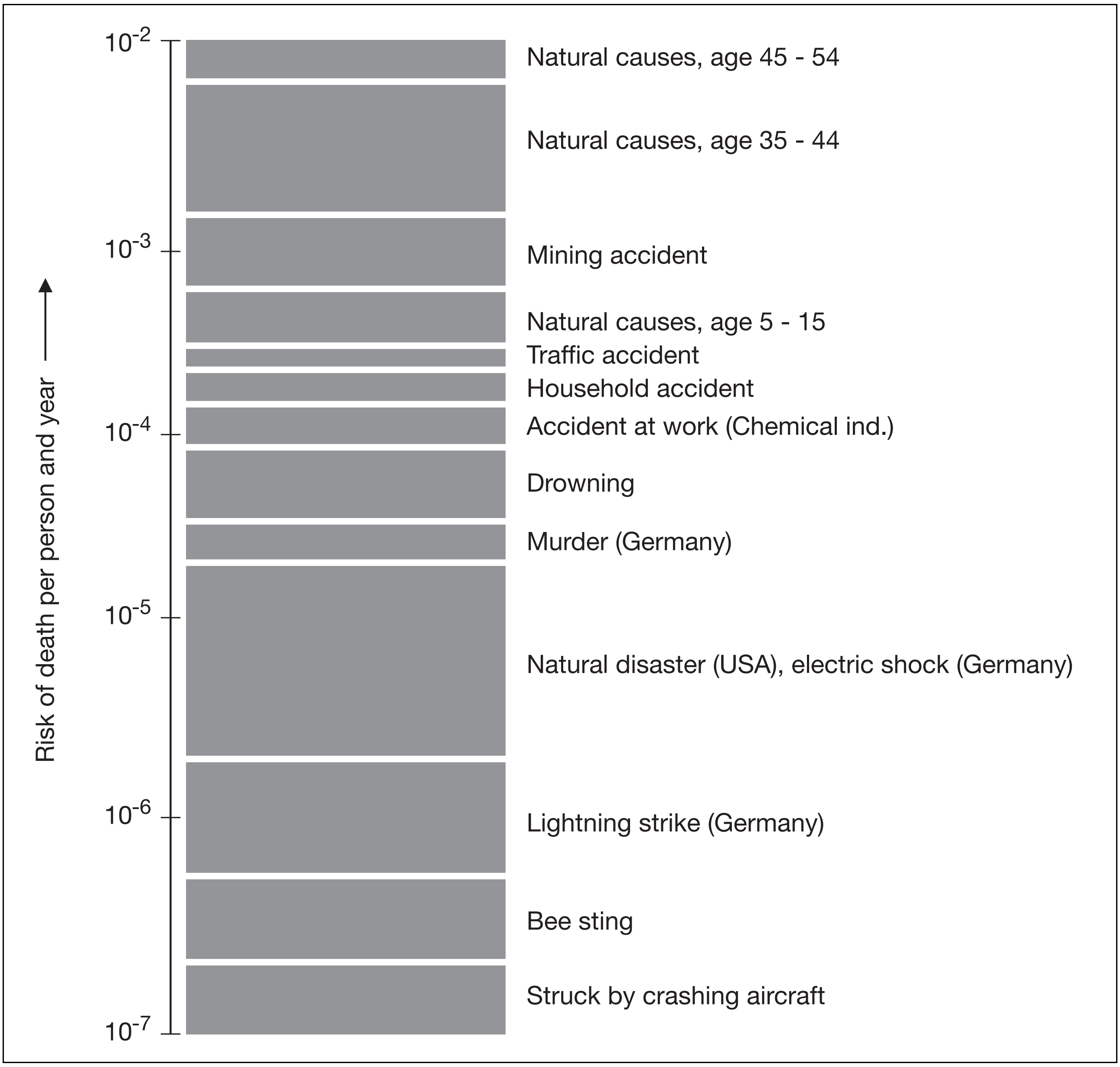


Figure 1: **Summary of basic risks**

2.3 Tolerable risk

The tolerable risk for a technology is not always clearly defined, but is basically determined by society, taking social and political factors into consideration.
If the risk attached to a technical installation is perceived to be too high, then special measures must be implemented to reduce the risk.
The necessary risk reduction is achieved by a combination of all the safety-relevant protective measures. The residual risk should be, at most, no larger than the tolerable risk.
In the end, the plant operator must accept and bear the residual risk.

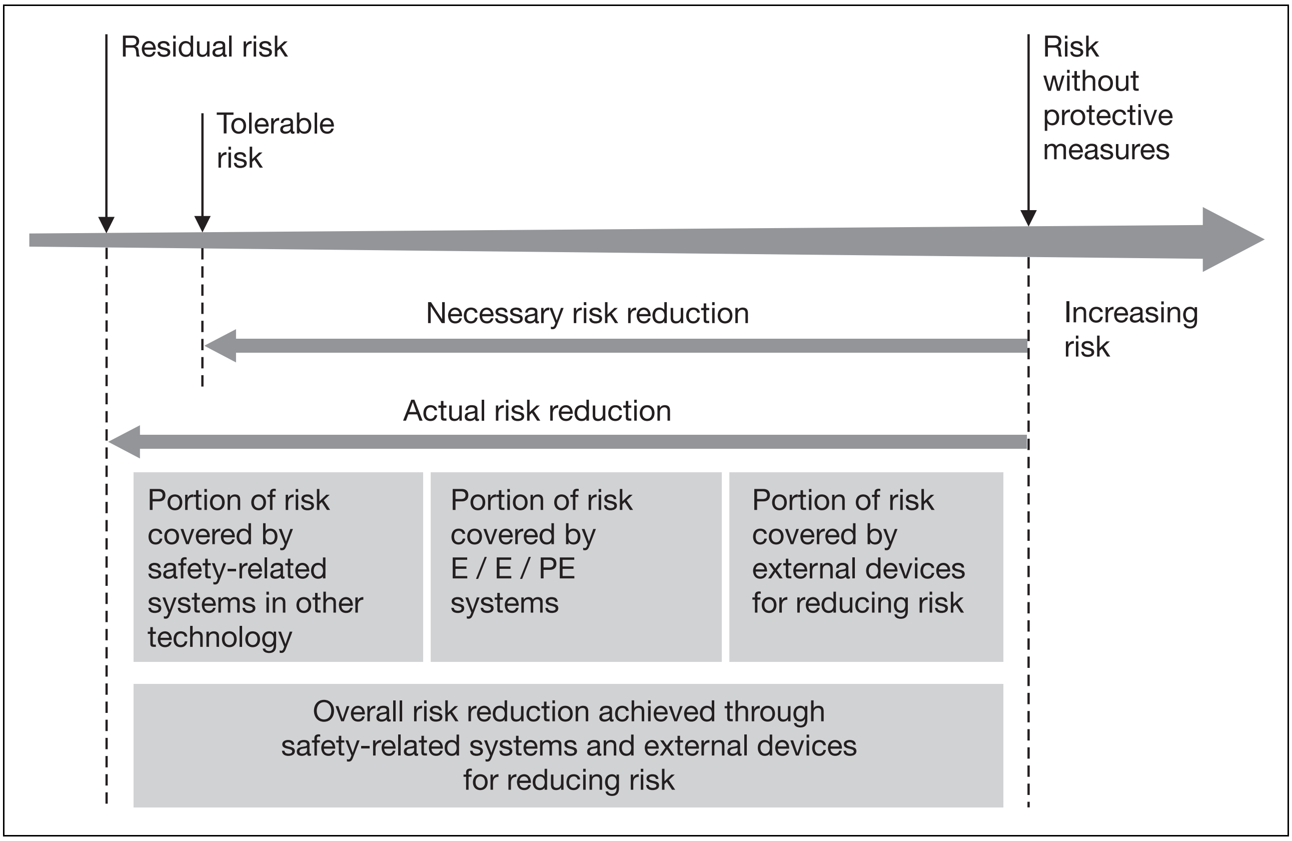

Residual risk
Tolerable risk
Risk without protective measures
Necessary risk reduction
Increasing risk
Actual risk reduction
Portion of risk covered by safety-related systems in other technology
Portion of risk covered by E / E / PE systems
Portion of risk covered by external devices for reducing risk
Overall risk reduction achieved through safety-related systems and external devices for reducing risk

Figure 2: Risk reduction: general concepts

2 Fundamental principle of (DIN) EN 61508

2.4 Life cycle

The operator of a safety engineering installation has to take suitable steps to assess and reduce risk during the complete life cycle of the installation. To this end, the (DIN) EN 61508 standard prescribes the following steps:

Risk definition and evaluation according to detailed failure probabilities - for the entire safety circuit (loop) from the point of measurement through the control system to the actuator, as well as during the entire life cycle (Overall Safety Life Cycle) of the application.
This can be done, for example, by FMEDA (Failure Mode, Effect and Diagnostics Analysis) or Hazard Analysis.

Determination and implementation of the measures (Management of Functional Safety) for reducing the residual risk.

Use of suitable (certified) equipment.

Periodic checking that regulations are correctly observed.

An overview of the systematic procedure is represented in figure 3. The first step is to carry out a failure analysis. This is followed by the selection of the measures for keeping faults under control and the implementation of these measures.

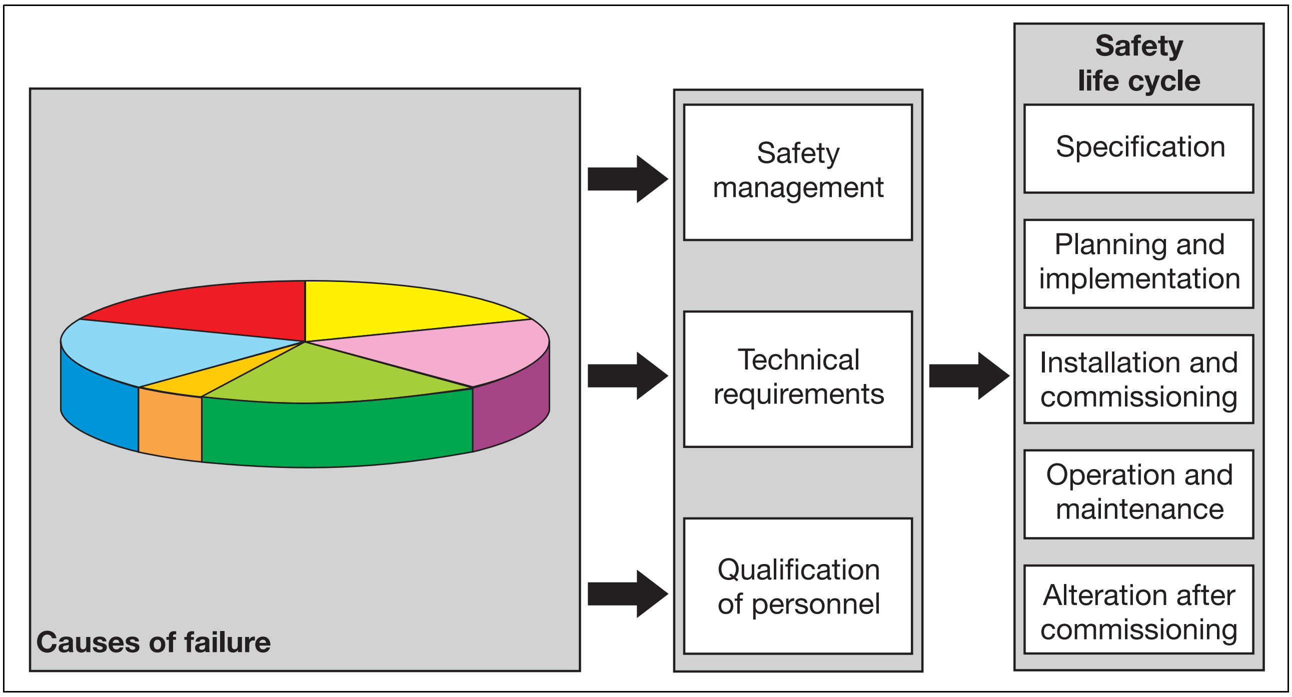

Causes of failure
Safety management
Technical requirements
Qualification of personnel
Safety life cycle
Specification
Planning and implementation
Installation and commissioning
Operation and maintenance
Alteration after commissioning

Figure 3: Procedure for implementing (DIN) EN 61508

2.5 JUMO’s task during the safety life cycle

The operator of a safety-related installation requires a quantity of technical data and information about all the equipment used, in order to be able to carry out the risk assessment for the entire safety loop and over the entire operating life of the system.

So it is naturally advantageous for the operator of the installation to be able to make use of SIL-certified equipment. In this case, the manufacturer, e. g. JUMO, has already established the necessary data for the instrument concerned, by means of a detailed hazard and risk analysis. All the relevant data and information for the customer is then presented in a safety manual. The terms that are used there are explained in the next chapter.

3.1 Safety integrity and its measurement – the Safety Integrity Level (SIL)

The **Safety Integrity Level** (safety-related reliability) of a system is “The probability that a safety-related system will perform the required safety function under all defined conditions within a defined time period according to specification.”

The **Safety Integrity Level (SIL)** is the measure for safety integrity. It is divided into four discrete levels, whereby Safety Integrity Level 4 represents the highest level of safety integrity, and Safety Integrity Level 1 represents the lowest level.

The achievable SIL is determined by the following parameters:

- the probability of the hazardous failure of a safety function (PFD or PFH),
- the hardware fault tolerance (HFT),
- the safe failure fraction (SFF),
- the type of components (Type A or Type B),
- lifetime, and
- proof-test.

3.2 PFD, PFH: operating modes and failure probabilities

A distinction is made between two modes of operation for the SIL classification: Low Demand Mode and High Demand Mode.

Low Demand Mode
For operation in Low Demand Mode, it is assumed that the safety function only has to respond once a year, on average. In this case, the SIL value is derived from the PFD (Probability of Failure on Demand).
PFD is a measure of the probability of failure of the safety function on demand, in a system operating with a low level of demand.

The Low Demand Mode is typically found in process industry installations and plant. Here there are, for instance, emergency shutdown systems that only become active if the normal process goes out of control.

High Demand Mode
For operation in High Demand Mode, it is assumed that the safety function has to respond continuously, or on average once per hour.
For a high or continuous rate of demand, the measure that is used is PFH (Probability of Failure per Hour), which expresses the probability that there will be a failure of the safety function within a one hour period.

The High Demand Mode is typically found in production installations, where continuous monitoring of the manufacturing operations is necessary.

Operating mode with a low level of demand (Low Demand Mode)	
Safety integrity level	**PFD** (average probability of failure of the safety function on demand)
SIL 4	10^{-5} to $<10^{-4}$
SIL 3	10^{-4} to $<10^{-3}$
SIL 2	10^{-3} to $<10^{-2}$
SIL 1	10^{-2} to $<10^{-1}$

Table 1: Safety integrity level: failure rate limits for a safety function operating with a low level of demand

Operating mode with a high level of demand (High Demand Mode)	
Safety integrity level	**PFH** (probability of a hazardous failure per hour)
SIL 4	10^{-9} to $<10^{-8}$
SIL 3	10^{-8} to $<10^{-7}$
SIL 2	10^{-7} to $<10^{-6}$
SIL 1	10^{-6} to $<10^{-5}$

Table 2: Safety integrity level: failure rate limits for a safety function operating with a high level of demand, or with continuous demand

3.3 HFT, SFF: Safety integrity of the hardware

The following parameters are also used for determining the SIL classification:

- the hardware fault tolerance (HFT) and
- the proportion of non-hazardous failures (SFF, Safe Failure Fraction)

Tables 3 and 4 show the relationship.
According to (DIN) EN 61508, a distinction must be made here between Type A and Type B systems.

Type A systems
A partial system can be viewed as a Type A system if, for the components that are necessary to achieve the safety function,

a) the failure modalities of all components that are used are adequately defined, and

b) the response of the partial system in fault conditions can be completely determined, and

c) reliable failure data based on field experience are available for the partial system, to demonstrate that the assumed failure rates for recognized and unrecognized hazardous failures can be achieved.

Type B systems

All other systems can be viewed as Type B, i. e. a partial system can be viewed as Type B if, for the components that are necessary in order to achieve the safety function,

a) the failure modalities of at least one component that is used are not adequately defined, or

b) the response of the partial system in fault conditions cannot be completely determined, or

c) no adequately reliable failure data based on field experience are available for the partial system, to support the assumed failure rates for recognized and unrecognized hazardous failures.

HFT (Hardware Fault Tolerance)

A fault tolerance of N for the hardware means that N+1 faults can cause a failure of the safety function.
The hardware fault tolerance is also defined by the “MooN” architecture that is used.
The expression MooN (for an architecture with M out of N channels) describes the architecture of an SIL device. For example, 1oo2 signifies an architecture with 2 channels, whereby each one of the channels can perform the safety function.
For a 1oo2 system, HFT = 1
For a 1oo1 system, HFT = 0

SFF (Safe Failure Fraction)

SFF is the proportion of non-hazardous failures, i. e. a higher SIL requires a higher SFF.
The SFF of a system is calculated from the individual failure rates (values) for the individual components, see chapter 3.5 *„Failure rate“, page 14*.

Type A systems			
Safe failure fraction (SFF)	**Hardware fault tolerance**		
	HFT = 0	HFT = 1	HFT = 2
<60%	SIL1	SIL2	SIL3
60 to <90%	SIL2	SIL3	SIL4
90 to <99%	SIL3	SIL4	SIL4
99%	SIL3	SIL4	SIL4

Table 3: Safety integrity of the hardware: limitations due to the architecture, for safety-related Type A partial systems

Type B systems			
Safe failure fraction (SFF)	**Hardware fault tolerance**		
	HFT = 0	HFT = 1	HFT = 2
<60%	not permitted	SIL1	SIL2
60 to <90%	SIL1	SIL2	SIL3
90 to <99%	SIL2	SIL3	SIL4
99%	SIL3	SIL4	SIL4

Table 4: Safety integrity of the hardware: limitations due to the architecture, for safety-related Type B partial systems

3.4 Lifetime and proof-test interval

Lifetime
When the lifetime of a device has expired, it must be replaced, since it no longer conforms to the requirements of its SIL certification.

Proof-test interval
The proof-test interval defines a repeated test to reveal faults in an SIL system, so that the system can be restored to the “as new” state, if necessary. If the proof-test interval is the same as the lifetime, then no proof-test is required.

3.5 Failure rate

After a successfully concluded hazard and risk analysis, it is necessary to implement the results in the system. An important role is played by the ability of a system to detect faults and to make an appropriate response. One must therefore distinguish between hazardous and non-hazardous faults, and the possibility of the fault being detected or not.

The failure rate is defined by the factor , and is generally divided into four groups (see Abbildung 4):

- $_{SD}$ = safe detected failure rate (faults that are detected, and not hazardous),
- $_{SU}$ = safe undetected failure rate (faults that are undetected, and not hazardous),
- $_{DD}$ = dangerous detected failure rate (faults that are detected, and hazardous),
- $_{DU}$ = dangerous undetected failure rate (faults that are not detected, and hazardous),

Usually, faults that are detected and non-hazardous will form the largest fraction. The undetected, hazardous faults $_{DU}$ are, on the other hand, a small proportion of all possible faults. But this type of fault is the most dangerous, and so appropriate measures must be taken to keep its proportion as small as possible.

The dimension for the values is FIT (Failures In Time, in 1 x 10^{-9} per hour).

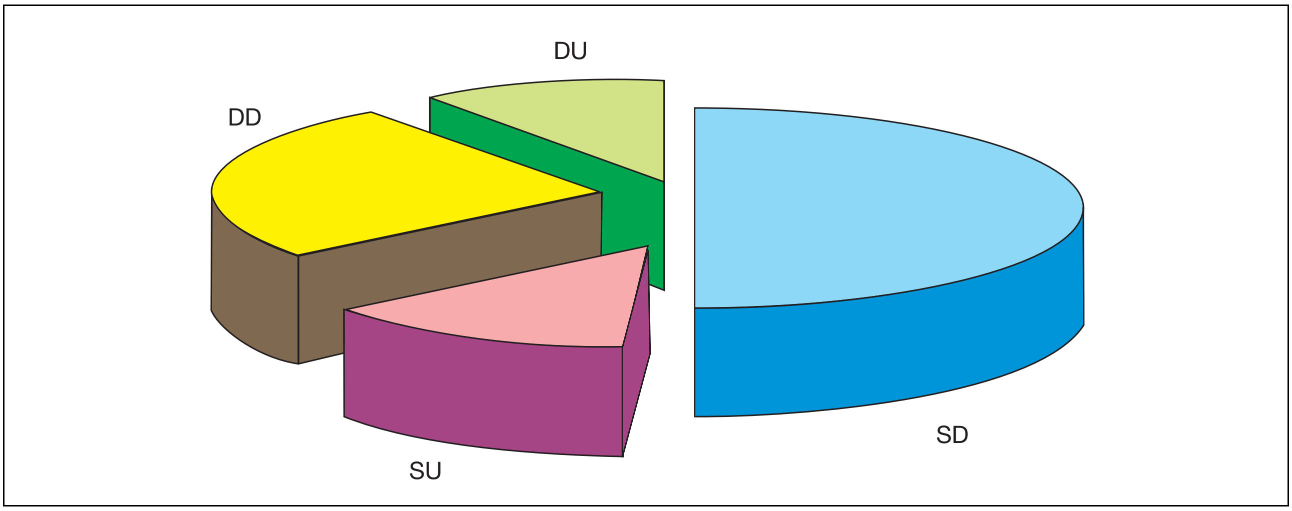


Figure 4: Failures in detail

4 Glossary

Failure rate I = The failure rate of a system (I) as a result of a fault is generally divided into four groups:

I_{SD} = safe detected failure rate
(detected, non-hazardous faults),

I_{SU} = safe undetected failure rate
(undetected, non-hazardous faults),

I_{DD} = dangerous detected failure rate
(detected, hazardous faults),

I_{DU} = dangerous undetected failure rate
(undetected, hazardous faults),

E/E/PE systems = Electrical, electronic and programmable electronic (E/E/EP) systems

FIT
(Failures in Time) = Failures in time (1 × 10^{-9} per hr)

Functional Safety = The ability of a system to perform the necessary actions in order to achieve or maintain a defined safe state for installations under control of that system.

HFT
(Hardware Fault Tolerance) = A fault tolerance of N for the hardware means that N+1 faults can cause a failure of the safety function.

Lifetime = When the lifetime of a device has expired, it must be replaced, since it no longer conforms to the requirements of its SIL certification.

MooN
(M out of N) = Safety architecture with M out of N channels.
For example, 1oo2 signifies an architecture with 2 channels, whereby each one of the channels can perform the safety function.

PFD
(Probability of Failure on Demand)

PFH
(Probability of Failure per Hour) = PFD is a measure of the probability of failure of the safety function on demand, in a system operating with a low level of demand (the probability of a dangerous failure of the system on demand).
For a high or continuous rate of demand, the measure that is used is PFH, which expresses the probability that there will be a failure of the safety function within a one hour period (dangerous failure rate).

Proof-check interval = The proof-check interval defines a repeated test to reveal faults in an SIL system, so that the system can be restored to the “as new” state, if necessary.

SFF
(Safe Failure Fraction) = The proportion of non-hazardous failures

SIL
(Safety Integrity Level) = The **Safety Integrity Level (SIL)** is a measure of the safety integrity of a system.
The safety integrity of a system is the probability that the system will perform the required safety function under all defined conditions within a defined time period.
The SIL is divided into four discrete levels, whereby Safety Integrity Level 4 represents the highest level of safety integrity, and Safety Integrity Level 1 represents the lowest level.

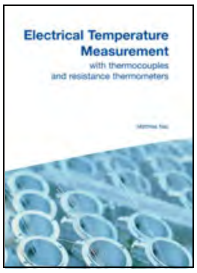
4 Glossary

Informative material from JUMO – for beginners and those with some practical experience

Know-how is not just needed to create JUMO products, but also for their later application.
That is why we offer several publications on aspects of measurement and control engineering for our users.

The publications are intended to provide step-by-step familiarization with a wide range of applications, for both beginners and those with some practical experience. They primarily illustrate general topics with JUMO-specific applications to some extent.

In addition to JUMO technical literature and our new software downloads we also offer the possibility to order our brochures and CD-ROM catalogs online.


Electrical Temperature Measurement
with thermocouples
and resistance thermometers

Electrical Temperature Measurement

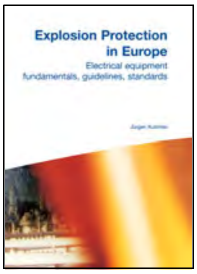
with thermocouples
and resistance thermometers
Matthias Nau

FAS 146
Sales no.: 00085081
ISBN: 978-3-935742-07-X
Free of charge

Control Engineering

Basic principles and tips for practitioners
Manfred Schleicher

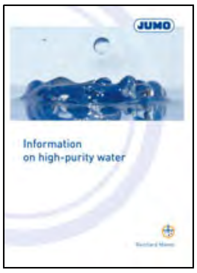
FAS 525
Sales no.: 00323761
ISBN: 978-935742-01-6
Free of charge



Explosion Protection in Europe

Electrical equipment
fundamentals, guidelines, standards
Jürgen Kuhlmei

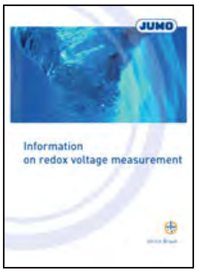
FAS 547
Sales no.: 000414312
ISBN: 978-3-935742-10-X
Free of charge



Information on high-purity water

Reinhard Manns

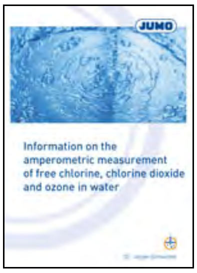
FAS 614
Sales no.: 00403834
Free of charge



Information on redox voltage measurement

Ulrich Braun

FAS 615
Sales no.: 00398237
Free of charge



Information on the amperometric measurement of free chlorine, chlorine dioxide and ozone in water

Dr. Jürgen Schleicher

FAS 619
Sales no.: 00398147
Free of charge

SCR Power Controllers

Basic principles and tips for professionals
Manfred Schleicher, Winfried Schneider

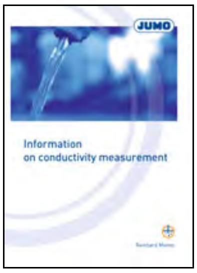
FAS 620
Sales no.: 00400481
ISBN: 978-3-935742-05-4
Free of charge

Information on pH measurement

Matthias Kremer

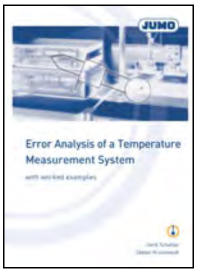
FAS 622
Sales no.: 00403233
Free of charge

Informative material from JUMO –
for beginners and those with some practical experience



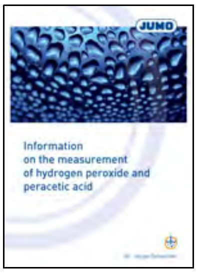
Information
on Conductivity Measurement
Reinhard Manns

FAS 624
Sales no.: 00411341
Free of charge



Error Analysis of a
Temperature Measurement System
with worked examples
Gerd Scheller, Stefan Krummeck

FAS 625
Sales no.: 00415704
ISBN-13: 978-3-935742-13-4
Free of charge

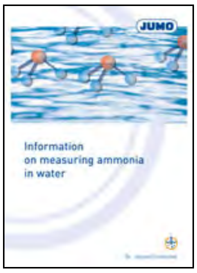


Information on the Measurement
of Hydrogen Peroxide
and Peracetic Acid
Dr. Jürgen Schleicher

FAS 628
Sales no.: 00420697
Free of charge

Functional Safety
Safety Integrity Level
Dr. Thomas Reus, Matthias Garbsch

FAS 630
Sales no.: 00476107
Free of charge



Information
on measuring ammonia in water
Dr. Jürgen Schleicher

FAS 631
Sales no.: 00485097
Free of charge

Please visit our website **www.jumo.net** and familiarize yourselves with the wide variety of JUMO products for different application fields. Our website provides you with more details and information concerning the contact persons for your requirements, questions, and orders.

JUMO

More than sensors + automation

ISBN: 978-3-935742-18-4

www.jumo.net