BS EN 50495:2010

## BSI Standards Publication

# Safety devices required for the safe functioning of equipment with respect to explosion risks

*raising standards worldwide™*

**BSI**

**National foreword**

This British Standard is the UK implementation of EN 50495:2010.

The UK participation in its preparation was entrusted to Technical Committee GEL/31, Equipment for explosive atmospheres.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2010

ISBN 978 0 580 70994 4

ICS 13.230; 29.260.20

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2010.

**Amendments issued since publication**

| Date | Text affected |
| --- | --- |

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN 50495

February 2010

ICS 13.230; 29.260.30

English version

## Safety devices required for the safe functioning of equipment with respect to explosion risks

Dispositifs de sécurité nécessaires
pour le fonctionnement sûr d'un matériel
vis-à-vis des risques d'explosion

Sicherheitseinrichtungen
für den sicheren Betrieb von Geräten
im Hinblick auf Explosionsgefahren

This European Standard was approved by CENELEC on 2009-12-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

# CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**Central Secretariat: Avenue Marnix 17, B - 1000 Brussels**

Ref. No. EN 50495:2010 E

# Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 31, Electrical apparatus for potentially explosive atmospheres. The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50495 on 2009-12-01.

This European Standard is to be read in conjunction with the European Standards for the specific types of protection listed in EN 60079 or EN 61241 series of standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

− latest date by which the EN has to be implemented
   at national level by publication of an identical
   national standard or by endorsement       (dop)      2010-12-01

− latest date by which the national standards conflicting
   with the EN have to be withdrawn       (dow)      2012-12-01

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directive 94/9/EC. See Annex ZZ.

————————

# Contents

**Tables**

## Introduction

Safety devices, controlling devices and regulating devices which are used for the protection concept of equipment for explosive atmospheres, shall function reliably for the intended purpose. This shall be expressed in terms of some measure of confidence that the devices will be able to maintain a required level of safety at all times. This measure of confidence needs to be in conformity with [1], CENELEC standards of the series EN 60079 and EN 61241 for apparatus for use in explosive atmospheres and relevant control standards.

CENELEC identified the need for research to determine whether existing and proposed standards in the field of safety-related control systems were suitable for this purpose. Research proposals on this topic were invited under the Standardisation, Measurement and Testing (SMT) Programme of the EU-commission and the SAFEC project was selected for funding (contract SMT4-CT98-2255). The project was a 12 month project which began in January 1999. The SAFEC partners were the Health and Safety Laboratory (HSL) of the Health and Safety Executive in the UK (the project coordinator), the Deutsche Montan Technologie (DMT) in Germany, the National Institute for Industrial Environment and Risks (INERIS) in France and the Laboratorio Oficial J.M. Madariaga (LOM) in Spain. The result of this project is summarised in [2] and recommends the application of Safety Integrity Levels as specified in EN 61508-1 for safety devices. A short description of the basic concept is provided in Annex E of this standard.

## 1 Scope

This European Standard specifies the requirements of electrical safety devices, which are used to avoid potential ignition sources of equipment in explosive atmospheres.

This also includes safety devices, which are operated outside areas with explosive atmospheres, to guarantee the safe function of equipment with respect to explosion hazards.

> NOTE 1    This European Standard can also be used to design and assess safety devices for protective systems.

Electrical equipment, which is intended for use in explosive atmospheres, may rely on the correct operation of safety devices which for example maintain certain characteristics of the equipment within acceptable limits. Examples of such safety devices are motor protection devices (to limit temperature rise during stall conditions) and controlling devices for pressurisation protection.

By means of control or monitoring devices, sources of ignition can be avoided. Therefore these devices shall execute the appropriate measures in the appropriate reaction time, for example the initiation of an alarm or an automatic shut down.

> NOTE 2    Some potential ignition sources might not be controllable by safety devices, e.g. electrostatic discharges, ignition sparks caused by mechanical impact. Also some protection measures might not be controllable by safety devices, e.g. flameproof enclosures.

Safety devices, whose safety function can not adequately be specified under the existing EN 60079 or EN 61241 series of standards, shall additionally be designed according to the requirements of this standard. Generally for complex safety devices appropriate design requirements are not provided in the existing types of protection (see 3.13 for the definition of a complex device).

> NOTE 3    In general the levels of safety required by this standard are considered to be equivalent to those provided by conformity to EN 60079-0 or EN 61241-0. No increase or decrease of safety is intended or required. Similarly neither increase nor decrease of safety with respect to EN 61508 series is intended.

Safety devices can be classified in 2 types:

a)    devices, which are included as component in the equipment under control (see 3.8). The combined apparatus is considered as equipment.

> EXAMPLES
> - thermal switch or thermistor to avoid overheating,
> - temperature monitoring devices to control the surface temperature.

b)    devices, which are installed separately from the equipment under control and considered as associated apparatus exclusively for a specific type of protection or specific equipment under control. The combined apparatus is considered as a system.

> EXAMPLES
> - external control devices or safety related parts of a control system for type of protection pressurisation,
> - overload protective device for electric motors of type of protection Ex e 'Increased Safety',
> - control devices for battery charging equipment (protection against overcharging or deep discharging),
> - level detectors for the control of submersible pumps.

Exclusions from this standard:

Safety devices, where the safety function is adequately covered in the existing standards of EN 60079 and EN 61241 series do not need any additional assessment according to this standard.

> EXAMPLES    Intrinsically safe associated apparatus, fuses, electromechanical overload protection, simple thermal protection devices (e.g. thermal fuses, thermal switches).

The standard does not include devices or systems to prevent the occurrence of explosive atmospheres, e.g. inerting systems, ventilation in workplaces and containers/vessels.

Gas detectors, which are covered under EN 61779 series, EN 50271 or EN 50402 are also excluded from the scope of this standard.

This standard does not deal with protection by control of ignition source 'b' for non-electrical equipment as defined in EN 13463-6.

## 2   Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

| | |
|---|---|
| EN 13237 | *Potentially explosive atmospheres – Terms and definitions for equipment and protective systems intended for use in potentially explosive atmospheres* |
| EN 13463-6 | *Non-electrical equipment for use in potentially explosive atmospheres – Part 6: Protection by control of ignition source 'b'* |
| EN 50271 | *Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen – Requirements and tests for apparatus using software and/or digital technologies* |
| EN 50402 + A1 | *Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen – Requirements on the functional safety of fixed gas detection systems* |
| EN 60079 series | *Explosive atmospheres* (IEC 60079 series) |
| EN 60079-0 | *Electrical apparatus for explosive gas atmospheres – Part 0: General requirements* (IEC 60079-0, mod.) |
| EN 60079-10-1 | *Explosive atmospheres – Part 10-1: Classification of areas – Explosive gas atmospheres* (IEC 60079-10-1) |
| EN 60079-30-1 | *Explosive atmospheres – Part 30-1: Electrical resistance trace heating – General and testing requirements* (IEC 60079-30-1) |
| EN 60079-30-2 | *Explosive atmospheres – Part 30-2: Electrical resistance trace heating – Application guide for design, installation and maintenance* (IEC 60079-30-2) |
| EN 60812 | *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)* (IEC 60812) |
| EN 61010-1 | *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements* (IEC 61010-1) |
| EN 61025 | *Fault tree analysis (FTA)* (IEC 61025) |
| EN 61165 | *Application of Markov techniques* (IEC 61165) |
| EN 61241 series | *Electrical apparatus for use in the presence of combustible dust* (IEC 61241 series) |
| EN 61241-0 | *Electrical apparatus for use in the presence of combustible dust – Part 0: General requirements* (IEC 61241-0, mod.) |
| EN 61496-1 | *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests* (IEC 61496-1, mod.) |
| EN 61508 series | *Functional safety of electrical/electronic/programmable electronic safety-related systems* (IEC 61508 series) |

| EN 61508-1 | *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements* (IEC 61508-1) |
| --- | --- |
| EN 61508-2:2001 | *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems* (IEC 61508-2:2000) |
| EN 61508-3 | *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements* (IEC 61508-3) |
| EN 61508-4 | *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations* (IEC 61508-4) |
| EN 61508-7:2001 | *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* (IEC 61508-7:2000) |
| EN 61511 series | *Functional safety – Safety instrumented systems for the process industry sector* (IEC 61511 series) |
| EN 61511-1:2004 | *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements* (IEC 61511-1:2003) |
| EN 61779 series | *Electrical apparatus for the detection and measurement of flammable gases* (IEC 61779 series, mod.) |
| EN 62061 | *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems* (IEC 62061) |
| EN ISO 13849-1 | *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design* (ISO 13849-1) |
| EN ISO 13849-2 | *Safety of machinery – Safety-related parts of control systems – Part 2: Validation* (ISO 13849-2) |

## 3   Terms and definitions

For the purposes of this document, the terms and definitions given in EN 60079-0 and the following apply.

**3.1**
**types of protection**
the types of protection, as referred to in this standard, are the explosion protection measures for electrical equipment

NOTE    The protection measures are defined in EN 60079-0 or EN 61241-0.

**3.2**
**equipment category**
classification of equipment into different levels of safety with respect to the ignition risk

[EN 13237, EN 60079-0, [1] ]

NOTE    The equipment category is equivalent to the appropriate Equipment Protection Levels (EPLs), defined in the EN 60079-0. This standard may be applied for EPLs correspondingly.

**3.3**
**functional safety**
part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the safety-related systems and external risk reduction facilities

[EN 61508-4]

**3.4**
**safety device**
safety devices, controlling devices and regulating devices required for or contributing to the safe functioning of equipment with respect to the risks of explosion

Safety devices provide explosion protection by executing a safety function that works independently of the normal functions of the equipment under its control. A safety device may consist of one or more safety components, forming a Safety Instrumented System (SIS)

NOTE       A regulating device which is controlling an ignition risk is also considered as a safety device.

**3.5**
**Safety Instrumented System (SIS)**
instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final elements(s) [see EN 61511-1:2004, 3.2.72]. A safety instrumented system is equivalent to a safety-related system, which is defined under EN 61508-4

NOTE       Safety device is a term of [EN 13237], [1] and can also be a safety related system.

**3.6**
**safety component**
one of the parts of a system or device performing a specific safety function

[EN 61511-1]

**3.7**
**safety function**
a function to be implemented by a safety device, which is intended to achieve or maintain a safe state for the EUC, in respect of ignition hazards

[EN 61508-4]

**3.8**
**Equipment Under Control (EUC)**
equipment, machines, apparatus or components which contain a potential ignition source, which is controlled by a safety device

[EN 61508-4]

**3.9**
**safe state**
state of the safety device which leads to a safe condition of the EUC

[EN 61508-4]

**3.10**
**safe condition**
the safe condition of an Equipment Under Control (EUC) defines the operating mode in which an acceptable ignition risk according to the category of the protected equipment is provided by the equipment. The safe condition of the EUC is intended to be ensured by activating the safety function of the safety device

**3.11**
**combined equipment**
combination of a safety device and the Equipment Under Control (EUC). It may be physically combined in one unit or as separate units. In both cases the combination is considered as equipment according to [1]

**3.12**
**simple safety device**
safety devices where the safety function does not depend on complex technology (e.g. microprocessor technology)

**3.13**
**complex safety device**
safety devices where the safety function depends on complex technology, e.g. microprocessor technology

**3.14**
**Safety Integrity Level (SIL)**
discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety function(s) to be performed by the safety device, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest [EN 61508-4]. If the safety device consists of several safety components the Safety Integrity Level is defined for the complete safety instrumented system

NOTE    SIL 4 is not applied in this standard.

**3.15**
**SIL capability**
if a safety component is provided separately, its specified SIL capability is the maximum SIL that can be achieved by a safety device using this component in single channel mode

**3.16**
**Failure Mode and Effect Analysis (FMEA)**
analysis of possible failures of any component of the safety device and determination of their consequences for the overall safety function. Allows to classify any failure as safe, dangerous, detected or undetected with respect to the safety function

**3.17**
**Probability of a Failure on Demand (PFD)**
specifies the average probability of a failure to perform the safety function on demand. In the low demand mode the frequency of demands for operation made on a safety related system is not greater than one per year and no greater than twice the proof-test frequency

[EN 61508-4]

EXAMPLES FOR LOW DEMAND SYSTEMS    Running dry protection, circuit breaker, thermistor relay

**3.18**
**Probability of a dangerous Failure per Hour (PFH)**
specifies the failure rate (e.g. per hour) to perform the safety function continuously. This value shall be considered if the safety device is operated in high demand or continuous mode of operation, where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-test frequency

[EN 61508-4]

EXAMPLE FOR HIGH DEMAND SYSTEM    Continuous flow control of pressurisation

**3.19**
**Safe Failure Fraction (SFF)**
the ratio, expressed as a percentage, of the average rate of safe and detected failures to the total average failure rate of a safety device. A safe failure is a failure which does not put the safety device into a fail-to-function state (see EN 61508-4 and EN 61508-2:2001, Annex C). A detected failure is a failure which is detected by the automatic diagnostic tests, or through normal operation

**3.20**
**Hardware Fault Tolerance (HFT)**
ability of a safety device to continue to perform a required function in the presence of faults [EN 61508-4]

EXAMPLE    HFT = 1 means, the required function is still performed in the presence of 1 arbitrary fault of the safety device

Regarding the equipment under control, the requisite level of protection is assured in the event of faults occurring independently of each other.

EXAMPLE    Category 1 equipment is characterised by HFT=2, which means
– either, in the event of failure of one means of protection, at least an independent second means provides the requisite level of protection,
– or the requisite level of protection is assured in the event of two faults occurring independently of each other.

**3.21**
**trip level**
a threshold for a safety critical parameter pre-adjusted in the safety device. When exceeding this threshold the safety device activates the safety function

**3.22**
**architecture**
specific configuration of hardware and software elements in a system

[EN 61508-4]

**3.23**
**channel**
element or group of elements that independently performs a function

[EN 61508-4]

EXAMPLE        A two channel (or dual channel) configuration is one with two channels that independently perform the same function

**3.24**
**confidence level**
the confidence level is the probability, that the confidence interval around the mean value of a statistical distribution of test results includes the real value. It indicates the significance of a statistical evaluation. A specified confidence level for a probabilistic proven-in-use evaluation allows to determine the minimum number of treated demands (low demand mode) or the minimum hours of operation (continuous mode)

[see EN 61508-7:2001, Annex D]

**3.25**
**average ambient temperature**
the average ambient temperature is the mean value of the ambient temperature of the components in comparable applications. This may involve averaging temperature fluctuations with time ([5])

## 4   Ignition prevention by safety devices

### 4.1   General concept of ignition risk reduction

The ignition risk analysis of electrical apparatus starts with the evaluation of potential ignition sources even under the presumption of faults related to the equipment. If appropriate types of protection (EN 60079 or EN 61241 series of standards) are applied the ignition risk of the protected equipment is reduced to comply with the required equipment category. E.g. if equipment shall be classified in Category 1, even rare incidents related to the equipment must be considered. Hence, the equipment must

- either be safe with 2 faults occurring independently in the equipment. If a type of protection is only safe up to one fault, the fault tolerance of the equipment may be enhanced by the control with an appropriate safety device,
- or, in the event of one means of protection fails, provide at least an independent second means to ensure the requisite the level of protection. For this purpose also a suitable safety device can be used.

For category 2 equipment frequently occurring disturbances or single equipment faults must be considered with respect to potential ignition sources. If equipment would only be safe in normal operation, those disturbances or equipment faults can be controlled with a suitable safety device and the ignition risk reduced correspondingly.

If equipment contains several potential ignition sources, for each ignition source the same consideration must be performed and the ignition risk decreased by appropriate measures. The controlled equipment shall comply with the relevant standards EN 60079-0 and/or EN 61241-0 with respect to the final equipment category.

NOTE    Residual risks, which cannot be eliminated by a safety device, may be addressed by safety instructions for installation and use. Such ignition sources may be for example:

– electrostatic discharge of chargeable surfaces,

– mechanical impact or friction sparks on light metal alloys.

EXAMPLE    Equipment complying with Category 3G requirements contains electrical circuits and an enclosure with Mg > 7,5 %. To comply with Category 2G the electrical circuits can be protected by pressurising the enclosure (Ex p) using a programmable control system as a safety device. The potential ignition risk created by the enclosure surface can be addressed by a safety instruction.

## 4.2   Safety characteristics of a safety device

A safety device shall meet a level of reliability depending on the reduction of the ignition risk of the equipment under control. The required safety integrity level of the safety device can be assessed and classified according to 5.3. Table 1 shows the required safety characteristics for a safety device when used to control equipment (EUC) with a potential ignition source and initial fault tolerance to achieve the final equipment category of the combined equipment

**Table 1 – Minimum requirements for Safety Integrity Level and Fault Tolerance of a safety device**

| **EUC**  Hardware Fault Tolerance | 2 | 1 | 0 | 1 | 0 | 0 |
|---|---|---|---|---|---|---|
| **Safety device** | | | | | | |
| Hardware Fault Tolerance | - | 0 | 1 | - | 0 | - |
| Safety Integrity Level | - | SIL 1 | SIL 2 | - | SIL 1 | - |
| **Combined equipment** | | | | | | |
| Group I        Category | M1 | | | M2 | | - |
| Group II, III   Category | 1 | | | 2 | | 3 |

NOTE 1   Fault tolerance:

"0" indicates that the EUC is safe in normal operation. One single fault may cause the apparatus to fail.

"1" indicates that the apparatus is safe with one single fault. Two independent faults may cause the apparatus to fail.

"2" indicates that the apparatus is safe with two independent faults. Three faults may cause the apparatus to fail.

NOTE 2   SIL1 or SIL2 indicates the Safety Integrity Level of the Safety device according to EN 61508 series.

NOTE 3   Category 1 or 2 or 3: the appropriate categories are defined in EN 13237, [1]

NOTE 4   "-" means, that no safety device is required

NOTE 5   Equipment which contains a potential ignition source under normal operation is not included in Table 1, because this equipment is already covered under the types of protection.

Examples of combined equipment are listed in Annex D.

# 5   Functional requirements for a safety device

## 5.1   General requirements

A safety device shall be specified taking into account the equipment under control including the ignition source which shall be controlled. If applicable, the type of protection the safety device is designed for, shall be considered. The safety function and all required components for the safety instrumented system shall be determined.

The safety function shall be performed reliably under the specified ambient and the operational conditions of the safety device. To avoid operation errors, the setting of the safety device shall be fail-safe as far as possible and/or be reduced to the minimum.

In case of power supply or interconnection failures the safety device shall go into a well defined state. Hence, the safe state of the safety device shall be defined (e.g. off state, on state, maintain last value, etc.). After a fault has been remedied, the safety device can be reset automatically if it can be ensured that the EUC remains in the safe state until it will be restarted under safe conditions.   The safety device and control devices shall operate independently from each other. The interfaces of the safety components shall be clearly specified.

### 5.1.1  Ambient and operational conditions

The safety device shall be designed in such a manner that a safe and accurate functioning under the specified ambient conditions is provided. The ambient and operational conditions shall be specified by the manufacturer, e.g.:

- supply voltage range;

- electromagnetic environment;

- ambient temperature range, average ambient temperature (see 5.3.4, Note);

- degree of pollution;

- humidity range;

- maximum vibration values;

- maximum shock values.

### 5.1.2  Demands on the safety function

The demand of the safety device shall bring the EUC into a safe condition and/or start suitable risk reduction measures, before an ignition risk occurs. The ignition threshold (maximum and/or minimum) of the potential source of ignition shall be considered (e.g. temperature class, max. surface temperature). The measuring range, accuracy and the reaction time as well as the reaction thresholds of the safety device have to be defined in such a way, that no risk occurs from the potential ignition source. For combined equipment the ignition threshold and the reaction time of the EUC have to be considered as well. If a safety margin is required by the applied standard (EN 60079-x and/or EN 61241-x), this shall be taken into account additionally.

NOTE 1  The specified testing conditions of the applied standard should be the base for safety parameters e.g. the reduction of maximum surface temperature according to the standards for gas and/or dust atmosphere.

NOTE 2   In the specific application the reaction time of the complete safety instrumented system should be considered with respect to the ignition mechanism of the equipment under control (EUC). The user should take into account the total reaction time of the safety instrumented system including the reaction time of the equipment under control, to ensure, that no ignition risk may occur.

### 5.1.3  Serviceability

Any setting and operational modes of the safety device shall be restricted to a minimum and if necessary protected against unauthorised changes. All safety relevant setting modes shall be marked significantly and described in detail in a way that any effect of these modes on the EUC shall be clearly comprehensible to the user of the equipment. If required, measures shall be provided to enable the user to perform regular functional proof tests or the device provides a self testing routine.

## 5.2 Special requirements for safety components

Where applicable,

−   the sensor,

−   the actuator,

−   control unit,

−   display unit

shall comply with the relevant product standards.

NOTE    In order to obtain a maximum of safety during the operation, control and display units shall be designed in compliance with ergonomic principles:

−   ergonomic arrangement of actuators and display devices;

−   minimised number of actuators and display devices required for safety measures.

For combined equipment the interconnections, sensor, control unit and actuator shall meet the requirements of the standard series EN 60079 and/or EN 61241.

Where possible the control unit shall recognise any dangerous failure of the safety device and its associated interconnection and shall initiate appropriate risk reduction measures.

The measuring and recording units shall be designed in such a manner that any calibrations necessary can be carried out onsite. The manufacturer shall provide the intervals at which calibrations shall be carried out as part of the instruction manual.

EXAMPLE    A 4 mA to 20 mA current loop is a suitable interconnection, if a short circuit or circuit break is detected by the connected logic unit. In the case of using a bus system it shall comply with the required SIL.

## 5.3 Requirements for achieving the Safety Integrity Level (SIL)

### 5.3.1 General

The safety integrity of a complex safety device shall be derived

•   either according to EN 61508 series or related standards (e.g. EN 62061, EN ISO 13849-1);

The safety requirements shall be specified in a systematic risk-based manner in accordance with the mentioned standards. The safety function shall be described clearly in the requirement specification. Hard- and software measures shall be considered in the design process to control the occurrence of random hardware faults and to achieve an appropriate diagnostic coverage. The probability of random hardware faults shall be assessed e.g. by a systematic failure mode and effect analysis (FMEA). Design test requirements shall be systematically derived from the requirement specifications. A safety management system shall be applied during the whole life-cycle of the equipment, to minimise the probability of systematic faults (e.g. software errors).

NOTE    The detailed requirements for the management of functional safety, hardware safety integrity and software safety integrity are specified in e.g. EN 61508 Parts 1, 2 and 3 respectively.

- or based on proven-in-use experience according to EN 61508/EN 61511 series. The safety integrity is assessed by a statistical failure analysis of an appropriate number of devices used in an appropriate number of typical applications.

The failure rates can be determined from valid field reliability data records from prior use. To exclude systematic faults a statistical basis with a confidence level of at least 70 % shall be used. The statistical determination of the confidence level is defined in EN 61508-7.

### 5.3.2 General hardware requirements

Any components shall be used within their specifications. Automated diagnostic measures (e.g. a watchdog) shall be provided to detect hardware failures as far as possible. If the safety function relies on stored data, all relevant information shall be retained in the safety device. Even after an interruption of the power supply (e.g. power off) this information shall be available at the restart. If the safety function relies on the use of any battery modules or similar modules, their lifetime shall be stated in the instruction manual.

### 5.3.3 General software requirements

The user shall be able to identify the software version, e.g. by marking the installed memory module, by showing the software version on the display during power up or on user request.

Safety parameter modifications by unauthorised persons shall be prevented e.g. by using a protected access procedure for the safety related software function. All parameters that can be modified by the user shall be unambiguously described.

NOTE 1   This can be done by installing an access code or by a deliberate manual, mechanical confirmation (e.g. button behind special locking device).

Wherever possible, the plausibility of any parameter inputs shall be checked automatically. Invalid inputs shall be refused.

To increase the Safety Integrity Level of a safety device a multi-channel architecture can be used. If the individual channels use the same software, failures cannot be considered to be independent. In this case the software shall comply with the required Safety Integrity Level of the final system.

NOTE 2   Different revisions of software generally are based on the same method which indicates that they don't fulfil the requirements of independence of the two channels.

EXAMPLE     A safety device of the architecture 1oo2 is equipped with 2 channels. The hardware of each channel is independent of the other and complies with SIL 1. Both channels use the same software. In order to achieve an overall SIL 2, this software shall meet the requirements of SIL 2 according to EN 61508-3.

### 5.3.4 Determination of random hardware failure rates and modes

The random hardware failure rates and modes of the safety device shall be determined. Different methods are suitable like Failure Mode and Effect Analysis (FMEA, EN 60812), Fault tree analysis (FTA, EN 61025), Application of Markov Techniques (EN 61165).

The component failure rates can be derived from several industry databases (e.g. [5], [6], [7]). Where available, data provided by the supplier may be used as well. Generally, these failure rates can be expected on average under given ambient conditions. They are determined under reference conditions, which correspond to the majority of applications for the stated components e.g. a mean ambient temperature of 40 °C. Under extreme ambient conditions, e.g. if the safety device is operated continuously at the maximum (or minimum) specified ambient temperature, the failure rates shall be modified for that average ambient temperature using the corresponding formula given in the referenced databases.

To determine the hardware failure rates in the FMEA, the impact of every fault presumption for each assembly shall be determined and assessed. If the impact of any assembly faults on the safety function of a safety device cannot be determined, this fault shall be regarded as dangerous. The failure rate should be proportioned 50 % detected and 50 % undetected (according to EN 61508 series).

Faults, for which proper fault exclusion can be presumed (e.g. the assembly meets the requirements of appropriate standards), may not be considered. The component is considered to be infallible with respect to this fault.

Fault presumptions and the reasons for fault exclusion shall follow acknowledged technical standards (e.g. EN 60079 series, EN 61241 series, EN 61496-1, EN ISO 13849-2 and EN 61010-1) and shall be documented.

Failures, which cause a loss of the safety function, are considered as dangerous, others as safe. Failures which are indicated or visible (e.g. causing a fault alarm) are considered as detected, others as undetected. Finally, the failures are classified into the failure modes safe-detected (sd), safe-undetected (su), dangerous-detected (dd) and dangerous-undetected (du). The corresponding failure rates $\lambda_{sd}$, $\lambda_{su}$, $\lambda_{dd}$, $\lambda_{du}$ of all components are summarized and used for the calculation of the basic safety parameters PFD/PFH, SFF from which the Safety Integrity Level is determined.

The method indicated in Annex B fulfils the requirements of this standard.

### 5.3.5  Simple Safety Devices

Simple safety devices shall comply either with definition of "Type A" in [EN 61508-2], or

a)  the failure modes of all constituent components are well defined, and

b)  the behaviour of the safety device under fault conditions can be completely determined and

c)  systematic failures can be excluded (verification of safety function can be completely determined by test), and

d)  where the safety device is formed by an assembly of components, the probability of random hardware failures can be determined (e.g. by FMEA)

A simple safety device does not require a complete functional safety assessment according to 5.3.1 - 5.3.4. It can be assessed according to its dangerous hardware failure rate in a FMEA (see Annex A). For simplification, the dangerous hardware failure rate may be estimated by the inverse of its total MTBF value (see Annex A). The safety device shall comply with the failure rate per hour (PFH) of the required SIL-Level and with the fault tolerance requirement of Table 1. Instead of a regular functional proof test according to 6.3 a useful lifetime may be specified.

## 6  Tests

### 6.1  Type tests

The safety function of the safety device shall be verified according to the relevant standards, e.g. EN 61508 series. Appropriate functional tests shall be done to ensure, that the safety function is performed correctly under all specified conditions.

Test conditions:

The safety function of the safety device shall be tested under the specified ambient and operational conditions separately (supply voltage limits, EMC, temperature, vibration, humidity). If not practical due to weight or dimension of the test sample the tests can be performed with the individual components separately at the resulting operational conditions of the component.

NOTE    EMC testing should be performed according to the applicable product standards.

Acceptance criteria:

The safety device shall perform its safety function correctly under all conditions according to the safety requirement specifications.

## 6.2  Routine tests

The manufacturer shall carry out the verifications or tests necessary to ensure that the electrical equipment complies with the technical documentation.

The manufacturer shall also carry out any routine tests required by any of the standards which were used for the conformity assessment.

## 6.3  Regular functional proof tests

The user shall perform functional proof tests of the safety function at regular intervals. Automated functional tests are preferred. The maximum test intervals and test procedure shall be part of the maintenance work, which is specified by the manufacturer in the instruction manual. Maintenance tests (including self testing routines at regular operation) may be allowed during normal operation unless explosion protection is not violated.

## 7  Marking

Safety devices in the scope of this standard are intended for use with equipment in a type of protection according EN 60079-0 or EN 61241-0. The requirements for marking may depend therefore on the type of protection of the equipment under control (EUC).

EXAMPLE       A pressurisation system intended for use exclusively for pressurised equipment is marked with [Ex[p].

Safety devices shall be marked according to their classification:

a)  safety devices which are incorporated into the equipment under control. The EUC is marked with the type of protection and category of the combined equipment. No marking is affixed to the safety device itself;

b)  safety devices which are not combined with equipment and provide a specific safety function in conformity with a specific type of protection. Those safety devices are marked as associated apparatus.

EXAMPLES FOR SAFETY DEVICES MARKING:

– Overload protection for an motor in type of protection flame proof enclosures "Ex d"          [Ex d]

– Temperature limiter for equipment in type of protection increased safety "Ex e"          [Ex e]

– Controlling device for equipment in type of protection pressurization "Ex py"          [Ex py]

If a safety device is installed in the explosion hazardous area it shall additionally be marked as equipment according to EN 60079-0 or EN 61241-0 (marking of type of protection).

EXAMPLES:

– A pressurisation system for equipment in type of protection pressurization "px", protection of the          Ex d [px] I
safety device in type of protection flame proof enclosure "Ex d", intended for use in mines susceptible to firedamp

– Overload device intended to protect an Ex e motor, protection of the safety device in type of          Ex d [e]IIA T4
protection flame proof enclosure "Ex d"

– Temperature limiter for equipment in type of protection flame proof enclosure "Ex d", protection of          Ex ib [d]IIB T3
the safety device in type of protection intrinsic safety "Ex ib"

## 8 Safety instructions

The manufacturer of a safety device shall provide safety instructions in a separate part of the instruction manual. The safety instructions shall contain information according to EN 60079-0 and EN 61241-0 and the necessary information for the design of the safety-related system and for the equipment combination according to Table 1, e.g.

– description of the device and its safety function,

– safety relevant instructions for installation, calibration, putting into service and use,

– nominal values for the interfaces (voltage, current, power, etc.),

– the associated type of protection, if relevant,

– SIL capability [1] depending on the system architecture,

– hardware fault tolerance (HFT),

– safe state and power off condition,

– interface for the safety function,

– ambient and operational conditions according to 5.1.1,

– activation threshold according to 5.1.2 (e.g. electrical thresholds, temperatures),

– reaction time of the safety function,

– regular proof test interval [2] and a detailed description of the test procedure.

If complex safety devices are placed on the market as components, additional information for the design of the safety instrumented system is required, e.g.

– failure rates $\lambda_{du}$, $\lambda_{dd}$, $\lambda_{su}$, $\lambda_{sd}$,

– Safe Failure Fraction (SFF),

– Probability of a Failure on Demand (PFD), and/or

– Probability of dangerous Failure per Hour (PFH).

All information which is relevant for the complete lifecycle of the safety device shall be provided.

---

[1] For simple safety devices a dangerous failure rate (PFH) may be specified instead of a SIL capability.

[2] For simple safety devices a useful lifetime may be specified instead of a regular proof test.

## Annex A
(informative)

### Example of an assessment procedure for a simple safety device

1) Verify that the safety device complies with the definition of a 'simple safety device', e.g. the safety function does not depend on software and systematic failures can be excluded (see 5.3.5).

   NOTE 1   If there are any revealed or perceived systematic failure modes, treat the device as a complex safety device.

2) If the safety device shall be located in the hazardous area, verify that it is protected according to the required equipment category (e.g. Encapsulation "mb" for Category 2).

3) Verify that the safety function requirements have been satisfied under all specified conditions (refer to the safety requirements specification). This may require assessment and tests (e.g. functional, environmental, vibration, EMC, interactions between other components, etc).

4) Assess the failure rate *for loss of the specified safety function*. This is normally done using an appropriate failure modes and effects analysis. Use actual component manufacturer's failure data if available, suitably adjusted for the relevant environmental conditions to be encountered. If manufacturer's failure data is not available, the following failure data may be used (as available) in the following order of preference:

   a)   failure data from similar industrial applications to those for which the safety device is intended;

   b)   generic failure data from a recognised source.

   A FMEA for loss of the specified safety function gives $\lambda_{du}$.

   NOTE 2   Rather than performing an FMEA, 'worst case' figures can be estimated for $\lambda_{du}$ by performing an MTBF analysis (e.g., not specifically considering loss of the safety function). The estimation provides $\lambda_{du} \leq 1/MTBF$.

   The dangerous undetected failure rate $\lambda_{du}$ shall comply with the PFH range of the required SIL capability (see Table B.2).

   EXAMPLE   For SIL 1 capability the failure rate shall be $\lambda_{du} < 10^{-5} \cdot 1/h$.

5) Verify that the fault tolerance of the simple safety device complies with Table 1 for the specified combination.

## Annex B
(informative)

## Example of an assessment procedure
## for the hardware safety integrity of a safety device

### B.1 Failure Mode and Effects Analysis (FMEA)

The determination of the Safety Integrity Level is based on a <u>F</u>ailure <u>M</u>ode and <u>E</u>ffects <u>A</u>nalysis (FMEA). Hardware failures of all safety relevant components are presumed and the effects on the safety function analysed. Failures, which can be excluded e.g. by complying with appropriate harmonised standards (e.g. EN 60079-0, EN 61241-0, EN 61496-1, EN ISO 13849-2 and EN 61010-1) are not considered in the FMEA.

The FMEA is carried out theoretically. Alternatively, tests can be performed to determine the behaviour of the safety device under fault conditions experimentally.

Generally, for electrical components, the following failure types shall be presumed:

– open-circuit;

– short-circuit;

– drift;

– function.

NOTE  When analysing the fault presumption drift, it shall be considered that this comprises a change of the nominal value of a module within the limits prescribed by the standards mentioned in 5.4.4. Therefore the change of values shall be analysed towards a positive as well as a negative direction. Hence the fault presumption of drift consists of two considerations that consequently shall be assessed as two fault conditions.

If not otherwise specified the failure rate shall be allocated equally to the relevant failure types using the following formula:

$$\lambda_{\text{failure type}} = \lambda_{\text{component}} \text{ / number of relevant failure types}$$

Component failures can lead to different effects on the safety device:

– detectable faults (detected during normal operation); or

– undetectable faults (undetected during normal operation);

– safe faults (safety function maintained); or

– dangerous faults (safety function lost).

In the FMEA these failures are classified into 4 failure modes with the respective failure rates $\lambda$, which consists of the sum of the failure rates of all components leading to the same failure mode:

**Table B.1 – Failure rates assuming a series failure model**

| Failure modes | Detected faults | Undetected faults |
|---|---|---|
| Safe faults | $\lambda_{sd} = \sum_{i=1}^{n} \lambda_{sd}^{(i)}$ | $\lambda_{su} = \sum_{i=1}^{n} \lambda_{su}^{(i)}$ |
| Dangerous faults | $\lambda_{dd} = \sum_{i=1}^{n} \lambda_{dd}^{(i)}$ | $\lambda_{du} = \sum_{i=1}^{n} \lambda_{du}^{(i)}$ |
| **Key**<br>sd = safe detected<br>dd = dangerous detected<br>su = safe undetected<br>du = dangerous undetected<br>n = number of components | | |

Alternatively, the integral failure rates of the different failure modes can be determined from documented field reliability data from previous use according to EN 61511 series, e.g. by analysing repair statistics. However, it should be stressed that the modes and conditions of use associated with the historical field data must be relevant to the SIL determination in question.

The total failure rate of the device is:

$$\lambda_{tot} = \lambda_{su} + \lambda_{sd} + \lambda_{du} + \lambda_{dd}$$

The Mean Time Between Failures (MTBF) if $\lambda$ is constant with time is:

$$MTBF = 1/\lambda_{tot}$$

The impact of every fault presumption for each assembly shall be determined and assessed.

Hereby the following criteria shall be applied:

a) Evaluation whether the impact of the fault presumed on the safety device is regarded as a safe or dangerous failure.

   A failure is regarded as safe if its impact

   • does not influence the safety function of safety device (e.g. breakdown of the LED connection in a failure monitoring circuit, if the safety function is not influenced by this fault), or

   • influences the safety function of the device only to an extent that the safety function is conducted at a less critical point of time than originally provided by the safety device (e.g. a drift fault at the input switch of a PTC thermistor measuring relay causes a shut down at lower temperatures than originally provided), or

   • if the safety device ensures the safe condition of the EUC immediately or at a short time lag. (e.g. breaking the emitter connection of a transistor that, when connected through, connects an output relay with ground potential whereas the deactivated relay is to be equated with the safe condition).

A failure is regarded as dangerous if its impact

- prevents the safety function of the safety device to be conducted (e.g. fused terminals of an output relay whereas the opened relay contacts are to be equated with the safe condition), or

- influences the safety function of the device to such an extent that its safety function is only conducted at a more critical point than originally provided by the device (e.g. a drift fault at the input switch of a PTC thermistor measuring relay causes a shut down at higher temperatures than originally provided).

b) An assessment shall be made whether the presumed fault is detected or undetected during normal operation.

For example, a fault may be detected by

- fault-detecting measures that are integrated into the safety device (e.g. by comparing the monitored parameters under control in a redundant safety device), or

- immediately ensuring the safe condition of the EUC (e.g. shut down of a motor driving an assembly belt where it can be assumed that the failure of the installation or of parts of the installation shall be discovered by the operating personnel or the control system immediately during normal operation).

A fault shall be regarded as undetected if e.g.

- it can be discovered by a functional test of the safety device as part of maintenance work only.

If the impact of any faults on the safety function of a safety device cannot be determined, this fault shall be regarded as dangerous and classified as 50 % detected and 50 % undetected according to EN 61508 series.

The results of the FMEA shall be documented.

## B.2 Determination of the Safety Integrity Level of the hardware

To identify the Safety Integrity Level of a device the following parameters shall be determined from its hardware architecture and its failure rates resulting from the FMEA (see Clause B.1):

a) PFD: Probability of a Failure on Demand (demand mode) or PFH: Probability of a dangerous Failure per Hour (continuous mode);

b) SFF: Safe Failure Fraction;

c) HFT: Hardware Fault Tolerance.

### B.2.1 Probability of a Failure on Demand (PFD) and the Probability of a dangerous Failure per Hour (PFH)

The determination of the PFD or PFH depends on the architecture of the safety device.

EN 61508 series / EN 61511 series provide appropriate measures to determine these parameters.

EXAMPLE    For a single channel safety device used in low demand mode the average PFD can be approximated by

$$PFD_{av} \approx 0,5 \times \lambda_{du} \times T_1$$

where

$\lambda_{du}$ = total probability of dangerous undetected failures (see Clause B.1);

$T_1$ = proof test interval of routine functional test specified by the manufacturer.

NOTE    In the example the mean time to restoration (MTTR) is considered to be negligible. The failure distribution safe/dangerous is 50 % each.

For multi-channel devices (e.g. 1oo2 architecture) appropriate calculation models can be applied [see EN 61508-6 and EN 61508-7] e.g. Markov model [EN 61508-7:2001, C.6.4].

### B.2.2 Safe Failure Fraction (SFF)

The safe failure fraction can be calculated by the summarised failure rates of the different failure modes resulting from the FMEA (see Clause B.1).

$$SFF = \frac{\lambda_{sd} + \lambda_{su} + \lambda_{dd}}{\lambda_{tot}}$$

### B.2.3 Hardware Fault Tolerance (HFT)

The Hardware Fault Tolerance is defined by the number of independent faults, which may occur in the safety device, without losing the safety function. If the HFT = n, the safety function is lost with n+1 faults.

EXAMPLE    A device with single channel architecture complies with HFT = 0: one fault may lead to the loss of the safety function.

**Multi-channel safety devices:**

Using multi-channel safety devices can increase the integrity level according to EN 61508 series [see EN 61508-2].

EXAMPLE    A safety device of the architecture 1oo2 is equipped with a channel of SIL 1 and the redundant channel conforms to SIL 2. Both channels are independent from each other and are used to perform the same safety function. As a result, the overall Safety Integrity Level of the safety device conforms to SIL 3.

As regards to this approach the requirements of EN 61508 series shall be considered. (Guidelines for the application of EN 61508-2 and EN 61508-3 can be found in EN 61508-6).

### B.2.4 Safety Integrity Level (SIL)

To achieve a required Safety Integrity Level, the overall safety lifecycle of the device shall be considered (EN 61508-1). The required PFD or PFH are reflected in Table B.2.

**Table B.2 – Safety Integrity Levels: Target failure measures for a safety function**

| Safety Integrity Level | Low demand mode of operation PFD (Average probability of dangerous failure to perform its design function on demand) | High demand or continuous mode of operation PFH (Probability of dangerous failure per hour) |
|---|---|---|
| SIL 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | $\geq 10^{-9}$ to $< 10^{-8}$ |
| SIL 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | $\geq 10^{-8}$ to $< 10^{-7}$ |
| SIL 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | $\geq 10^{-7}$ to $< 10^{-6}$ |
| SIL 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | $\geq 10^{-6}$ to $< 10^{-5}$ |

The hardware architecture shall comply with EN 61508-2. The required SFF and HFT can be derived from Table B.3.

**Table B.3 – Hardware safety integrity: Architectural constrains
on Type A or B safety-related subsystems**

| Safe Failure Fraction (SFF) | Type A Subsystem | | | Type B Subsystem | | |
|---|---|---|---|---|---|---|
| | Hardware fault tolerance | | | Hardware fault tolerance | | |
| | 0 | 1 | 2 | 0 | 1 | 2 |
| < 60 % | SIL 1 | SIL 2 | SIL 3 | Not permitted | SIL 1 | SIL 2 |
| 60 % - < 90 % | SIL 2 | SIL 3 | SIL 4 | SIL 1 | SIL 2 | SIL 3 |
| 90 % - < 99 % | SIL 3 | SIL 4 | SIL 4 | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99 % | SIL 3 | SIL 4 | SIL 4 | SIL 3 | SIL 4 | SIL 4 |

NOTE 1   Type A subsystem. Any system based on analogue technology (i.e. based on neither programmable electronics nor software) (cross reference EN 61511-1:2004, 3.2.47).

NOTE 2   Type B subsystem. Any system based on one or more programmable modules.

EXAMPLES:

– sensors equipped with microprocessors ("smart sensors");

– programmable systems of electronic logics such as

  • programmable control units,

  • PLC, programmable logic controller;

  • control units (cross reference EN 61511-1:2004, 3.2.55).

NOTE 3   Provided the conditions of EN 61511-1:2004, 11.4.4 (e.g. prior use reliability data, restricted and protected parameter adjustment, SIL < 4) are met, the SFF specified in Table B.3 may be reduced by one level (line).

**Annex C**
(informative)

## Example of determining the hardware safety integrity level

### C.1  Component failure rate distribution

Using the example of an IC with four terminal pins, the determination of the following factors should illustrated in a simplified manner:

$\lambda_s$    component hardware failure rate for safe failures;

$\lambda_d$    component hardware failure rate for dangerous failures;

$\lambda_{sd}$    component hardware failure rate for detected safe failures;

$\lambda_{su}$    component hardware failure rate for undetected safe failures;

$\lambda_{dd}$    component hardware failure rate for detected dangerous failures;

$\lambda_{du}$    component hardware failure rate for undetected dangerous failures.

Component considered:

Integrated circuit with four pins and a total component hardware failure rate of

$$\lambda_{ic} = 50 \times 10^{-9} \, \frac{1}{h} \, .$$

Failure rates:

For reasons of simplification only short circuits and open circuits were considered in this example. Hence the number of failure types is 2.

FMEA results:

The FMEA provided the following results:

– open circuits:
    – pin 1  safe, detected,
    – pin 2  safe, undetected,
    – pin 3  safe, undetected,
    – pin 4  dangerous, undetected;

– short circuits:
    – pin 1 / pin 2  dangerous, undetected,
    – pin 1 / pin 3  dangerous, undetected,
    – pin 1 / pin 4  safe, undetected,
    – pin 2 / pin 3  non definable $\Rightarrow$ dangerous, detected by 50 %,
    – pin 2 / pin 4  safe, detected,
    – pin 3 / pin 4  non definable $\Rightarrow$ dangerous, detected by 50 %.

Distribution of the component hardware failure rate to the individual failure types:

$$\lambda_{\text{failure type}} = \frac{\lambda_{\text{component}}}{\text{number of failure types}} = \frac{\lambda_{\text{IC}}}{2}$$

$$\lambda_{\text{failure type}} = \lambda_{\text{short circuit}} = \lambda_{\text{open circuit}} = 25 \times 10^{-9} \frac{1}{\text{h}}$$

## C.2 Component hardware failure rates

### C.2.1 Component hardware failure rate for safe failures, related to one failure type

Failure type "open circuit":

| | |
|---|---|
| the sum of all possible failures of the failure type "open circuit": | 4 |
| the sum of all safe failures of the failure type "open circuit": | 3 |
| Qualitative proportion of the safe failures to the failure type "open circuit": | 0,75 |

Component hardware failure rate for safe failures:

$$\lambda_{\text{S open circuit}} = \lambda_{\text{open circuit}} \times 0,75$$

$$\lambda_{\text{S open circuit}} = 18,75 \times 10^{-9} \frac{1}{\text{h}}$$

Failure type "short circuit":

| | |
|---|---|
| the sum of all possible failures of the failure type "short circuit": | 6 |
| the sum of all safe failures of the failure type "short circuit": | 2 |
| Qualitative proportion of the safe failures to the failure type "short circuit": | 0,333 |

Component hardware failure rate for safe failures:

$$\lambda_{\text{S short circuit}} = \lambda_{\text{short circuit}} \times 0,333$$

$$\lambda_{\text{S short circuit}} = 8,33 \times 10^{-9} \frac{1}{\text{h}}$$

### C.2.2    Component hardware failure rate for dangerous failures, related to one component

Failure type "open circuit":

the sum of all possible failures of the failure type "open circuit":                                      4

the sum of all dangerous failures of the failure type "open circuit":                                     1

Qualitative proportion of dangerous failures to the failure type "open circuit":                          0,25

Component hardware failure rate for dangerous failures:

$$\lambda_{D\,opencircuit} = \lambda_{opencircuit} \times 0{,}25$$

$$\lambda_{D\,opencircuit} = 6{,}25 \times 10^{-9}\,\frac{1}{h}$$

Failure type short circuit:

the sum of all possible failures of the failure type "short circuit":                                     6

the sum of all dangerous failures of the failure type "short circuit":                                    4

Qualitative proportion of dangerous failures to the failure type "short circuit":                         0,667

Component hardware failure rate for dangerous failures:

$$\lambda_{D\,shortcircuit} = \lambda_{shortcircuit} \times 0{,}667$$

$$\lambda_{D\,shortcircuit} = 16{,}68 \times 10^{-9}\,\frac{1}{h}$$

### C.2.3    $\lambda_S$ and $\lambda_D$ of a component

Component hardware failure rate for safe failures:

$$\lambda_{SIC} = \lambda_{S\,opencircuit} + \lambda_{S\,shortcircuit} = 18{,}75 \times 10^{-9}\,\frac{1}{h} + 8{,}33 \times 10^{-9}\,\frac{1}{h}$$

$$\lambda_{SIC} = 27{,}08 \times 10^{-9}\,\frac{1}{h}$$

Component hardware failure rate for dangerous failures:

$$\lambda_{DIC} = \lambda_{D\,opencircuit} + \lambda_{D\,shortcircuit} = 6{,}25 \times 10^{-9}\,\frac{1}{h} + 16{,}68 \times 10^{-9}\,\frac{1}{h}$$

$$\lambda_{DIC} = 22{,}93 \times 10^{-9}\,\frac{1}{h}$$

### C.2.4 Component hardware failure rates for detected and undetected safe failures ($\lambda_{sd}$ and $\lambda_{su}$)

| | |
|---|---|
| Number of safe failures of the failure type "open circuit": | 3 |

| | |
|---|---|
| Number of the detected safe failures of the failure type "open circuit": | 1 |

| | |
|---|---|
| Failure detection rate for the failure type "open circuit" for safe failures: | 0,333 |

$$\lambda_{SD\,open\,circuit} = \lambda_{S\,open\,circuit} \times 0,333$$

$$\lambda_{SD\,open\,circuit} = 6,24 \times 10^{-9}\,\frac{1}{h}$$

| | |
|---|---|
| Number of safe failures of the failure type "short circuit": | 2 |

| | |
|---|---|
| Number of the detected safe failures of the failure type "short circuit": | 1 |

| | |
|---|---|
| Failure detection rate for the failure type "short circuit" for safe failures: | 0,5 |

$$\lambda_{SD\,short\,circuit} = \lambda_{S\,short\,circuit} \times 0,5$$

$$\lambda_{SD\,short\,circuit} = 4,17 \times 10^{-9}\,\frac{1}{h}$$

The hardware failure rate of a component for detected safe failures results to:

$$\lambda_{SDIC} = \lambda_{SD\,open\,circuit} + \lambda_{SD\,short\,circuit} = 6,24 \times 10^{-9}\,\frac{1}{h} + 4,17 \times 10^{-9}\,\frac{1}{h}$$

$$\lambda_{SDIC} = 10,41 \times 10^{-9}\,\frac{1}{h}$$

| | |
|---|---|
| Number of safe failures of the failure type "open circuit": | 3 |

| | |
|---|---|
| Number of the undetected safe failures of the failure type "open circuit": | 2 |

| | |
|---|---|
| Percentage of undetected safe failures to all safe failures for the failure type "open circuit": | 0,667 |

$$\lambda_{SU\,open\,circuit} = \lambda_{S\,open\,circuit} \times 0,667$$

$$\lambda_{SU\,open\,circuit} = 12,51 \times 10^{-9}\,\frac{1}{h}$$

| | |
|---|---|
| Number of safe failures of the failure type "short circuit": | 2 |

| | |
|---|---|
| Number of the undetected safe failures of the failure type "short circuit": | 1 |

Percentage of undetected safe failures to all safe failures
for the failure type "short circuit":                                                    0,5

$$\lambda_{SU\,short\,circuit} = \lambda_{S\,short\,circuit} \times 0,5$$

$$\lambda_{SU\,short\,circuit} = 4,17 \times 10^{-9}\,\frac{1}{h}$$

The hardware failure rate of a component for undetected safe failures results to:

$$\lambda_{SUIC} = \lambda_{SU\,open\,circuit} + \lambda_{SU\,short\,circuit} = 12,51 \times 10^{-9}\,\frac{1}{h} + 4,17 \times 10^{-9}\,\frac{1}{h} = \lambda_{SIC} - \lambda_{SDIC}$$

$$\lambda_{SUIC} = 16,68 \times 10^{-9}\,\frac{1}{h}$$

### C.2.5 Component hardware failure rates for detected and undetected dangerous failures ($\lambda_{dd}$ and $\lambda_{du}$)

Number of dangerous failures of the failure type "open circuit":                         1

Number of the detected dangerous failures of the failure type "open circuit":            0

Failure detection rate for the failure type "open circuit" for dangerous failures:       0

$$\lambda_{DD\,open\,circuit} = \lambda_{D\,open\,circuit} \times 0$$

$$\lambda_{DD\,open\,circuit} = 0$$

Number of dangerous failures of the failure type "short circuit":                        4

Number of the detected dangerous failures of the failure type "short circuit":           1

Failure detection rate for the failure type "open circuit" for dangerous failures:       0,25

$$\lambda_{DD\,short\,circuit} = \lambda_{D\,short\,circuit} \times 0,25$$

$$\lambda_{DD\,short\,circuit} = 4,17 \times 10^{-9}\,\frac{1}{h}$$

The hardware failure rate of a component for detected dangerous failures results to:

$$\lambda_{DDIC} = \lambda_{DD\,open\,circuit} + \lambda_{DD\,short\,circuit} = 0 + 4,17 \times 10^{-9}\,\frac{1}{h}$$

$$\lambda_{DDIC} = 4,17 \times 10^{-9}\,\frac{1}{h}$$

Number of dangerous failures of the failure type "open circuit":                         1

Number of the undetected dangerous failures of the failure type "open circuit":          1

Percentage of undetected dangerous failures to all dangerous failures
for the failure type "open circuit":    1

$$\lambda_{DU\,open\,circuit} = \lambda_{D\,open\,circuit} \times 1$$

$$\lambda_{DU\,open\,circuit} = 6{,}25 \times 10^{-9}\, \frac{1}{h}$$

Number of dangerous failures of the failure type "short circuit":    4

Number of the undetected dangerous failures of the failure type "short circuit":    3

Percentage of undetected dangerous failures to all dangerous failures
for the failure type "short circuit":    0,75

$$\lambda_{DU\,short\,circuit} = \lambda_{D\,short\,circuit} \times 0{,}75$$

$$\lambda_{DU\,short\,circuit} = 12{,}51 \times 10^{-9}\, \frac{1}{h}$$

The hardware failure rate of a component for undetected dangerous failures results to:

$$\lambda_{DUIC} = \lambda_{DU\,open\,circuit} + \lambda_{DU\,short\,circuit} = 6{,}25 \times 10^{-9}\, \frac{1}{h} + 12{,}51 \times 10^{-9}\, \frac{1}{h} = \lambda_{DIC} - \lambda_{DDIC}$$

$$\lambda_{DUIC} = 18{,}76 \times 10^{-9}\, \frac{1}{h}$$

## C.2.6   Result

The distribution of the hardware failure rates of the integrated circuit results in:

$$\lambda_{SIC} = 27{,}08 \times 10^{-9}\, \frac{1}{h} \qquad\qquad \lambda_{DIC} = 22{,}93 \times 10^{-9}\, \frac{1}{h}$$

$$\lambda_{SDIC} = 10{,}41 \times 10^{-9}\, \frac{1}{h} \qquad\qquad \lambda_{DDIC} = 4{,}17 \times 10^{-9}\, \frac{1}{h}$$

$$\lambda_{SUIC} = 16{,}68 \times 10^{-9}\, \frac{1}{h} \qquad\qquad \lambda_{DUIC} = 18{,}76 \times 10^{-9}\, \frac{1}{h}$$

## C.3  Determination of the parameters SFF and PFD of a notional circuit

For further consideration it is assumed, that the IC is part of a notional electrical circuit. This circuit is the safety related part of a safety component and is of Type A according to EN 61508 series. The architecture of the circuit is 1oo1. The MTTR amounts 8 h and the proof test interval, $T_1$, is one year (8 760 hours). Additionally to the IC, which was considered in Clause A.1, the following components are part of the safety related circuit.

| | | | | |
|---|---|---|---|---|
| Capacitor | C1 | $\lambda_{C1}$ | = | $6{,}80 \times 10^{-9}\ \dfrac{1}{h}$ |
| Capacitor | C2 | $\lambda_{C2}$ | = | $16{,}20 \times 10^{-9}\ \dfrac{1}{h}$ |
| Diode | D1 | $\lambda_{D1}$ | = | $1{,}00 \times 10^{-9}\ \dfrac{1}{h}$ |
| Zener-Diode | D2 | $\lambda_{D2}$ | = | $25{,}00 \times 10^{-9}\ \dfrac{1}{h}$ |
| Fuse | F1 | $\lambda_{F1}$ | = | $25{,}00 \times 10^{-9}\ \dfrac{1}{h}$ |
| Operational Amplifier | O1 | $\lambda_{O1}$ | = | $9{,}00 \times 10^{-9}\ \dfrac{1}{h}$ |
| Resistor | R1 | $\lambda_{R1}$ | = | $0{,}20 \times 10^{-9}\ \dfrac{1}{h}$ |
| Transistor | T1 | $\lambda_{T1}$ | = | $5{,}40 \times 10^{-9}\ \dfrac{1}{h}$ |

A Failure Mode and Effects Analysis (FMEA) of the notional electrical circuit provided the following partitioning of the different component failure rates (procedure according to Clause B.1):

**Table C.1 – Total hardware failure rates**

| Component | $\lambda$Component in Fit | Failure type | Percentage of failure type | Effect of failure | | Diagnostic coverage of dangerous failure | Partitioning of the component failure rate in safe in dangerous failures (Values in Fit) | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Safe | Dangerous | | $\lambda_S$ | $\lambda_D$ | $\lambda_{du}$ | $\lambda_{dd}$ |
| C1 | 6,80 | Open circuit | 0,333 | 1 | 0 | ----- | 2,27 | 0 | 0 | 0 |
| | | Short circuit | 0,333 | 0 | 1 | 0 | 0 | 2,27 | 2,27 | 0 |
| | | Drift | 0,333 | 0,5 | 0,5 | 0 | 1,13 | 1,13 | 1,13 | 0 |
| C2 | 16,20 | Open circuit | 0,333 | 1 | 0 | ----- | 5,4 | 0 | 0 | 0 |
| | | Short circuit | 0,333 | 0 | 1 | 0,5 | 0 | 5,4 | 2,7 | 2,7 |
| | | Drift | 0,333 | 1 | 0 | ----- | 5,4 | 0 | 0 | 0 |
| D1 | 1,00 | Open circuit | 0,333 | 0 | 1 | 0 | 0 | 0,33 | 0,33 | 0 |
| | | Short circuit | 0,333 | 0 | 1 | 0 | 0 | 0,33 | 0,33 | 0 |
| | | Drift | 0,333 | 1 | 0 | ----- | 0,33 | 0 | 0 | 0 |
| D2 | 25,00 | Open circuit | 0,333 | 0 | 1 | 0 | 0 | 8,33 | 8,33 | 0 |
| | | Short circuit | 0,333 | 1 | 0 | ----- | 8,33 | 0 | 0 | 0 |
| | | Drift | 0,333 | 0,5 | 0,5 | 0 | 4,17 | 4,17 | 4,17 | 0 |
| F1 | 25,00 | Open circuit | 0,5 | 1 | 0 | ----- | 12,5 | 0 | 0 | 0 |
| | | Short circuit | 0,5 | 1 | 0 | ----- | 12,5 | 0 | 0 | 0 |
| IC | 50,00 | Open circuit | 0,5 | 0,75 | 0,25 | 0 | 18,75 | 6,25 | 6,25 | 0 |
| | | Short circuit | 0,5 | 0,333 | 0,667 | 0,25 | 8,33 | 16,68 | 12,51 | 4,17 |
| O1 | 9,00 | Open circuit | 0,333 | 0,625 | 0,375 | 0,333 | 1,88 | 1,12 | 0,75 | 0,37 |
| | | Short circuit | 0,333 | 0,286 | 0,714 | 0,25 | 0,86 | 2,14 | 1,6 | 0,54 |
| | | Drift | 0,333 | 1 | 0 | ----- | 3,0 | 0 | 0 | 0 |
| R1 | 0,20 | Open circuit | 0,333 | 1 | 0 | ----- | 0,07 | 0 | 0 | 0 |
| | | Short circuit | 0,333 | 0 | 1 | 0 | 0 | 0,07 | 0,07 | 0 |
| | | Drift | 0,333 | 1 | 0 | ----- | 0,07 | 0 | 0 | 0 |
| T1 | 5,40 | Open circuit | 0,333 | 1 | 0 | ------ | 1,8 | 0 | 0 | 0 |
| | | Short circuit | 0,333 | 0,25 | 0,75 | 0 | 0,45 | 1,35 | 1,35 | 0 |
| | | Drift | 0,333 | 1 | 0 | ----- | 1,8 | 0 | 0 | 0 |
| | | | | | | Sums: | 89,04 | 49,57 | 41,79 | 7,78 |

1 Fit = $1 \times 10^{-9} \dfrac{1}{h}$

NOTE   In this application, it was not required to consider the fault type "function".

Table C.1 supplies the following results:

1.      the total hardware failure rate of the notional electrical circuit for safe failures ($\lambda_S$)

$$\lambda_{S\,circuit} = 89{,}04 \times 10^{-9}\,\frac{1}{h}$$

2.      the total hardware failure rate of the notional electrical circuit for dangerous failures ($\lambda_D$)

$$\lambda_{D\,circuit} = 49{,}57 \times 10^{-9}\,\frac{1}{h}$$

3.      the total hardware failure rate of the notional electrical circuit for detected dangerous failures ($\lambda_{dd}$)

$$\lambda_{DD\,circuit} = 7{,}78 \times 10^{-9}\,\frac{1}{h}$$

4.      the total hardware failure rate of the notional electrical circuit for undetected dangerous failures ($\lambda_{du}$)

$$\lambda_{DU\,circuit} = 41{,}79 \times 10^{-9}\,\frac{1}{h}$$

5.      the total hardware failure rate of the notional electrical circuit

$$\lambda_{tot\,circuit} = \lambda_{S\,circuit} + \lambda_{D\,circuit} = 89{,}04 \times 10^{-9}\,\frac{1}{h} + 49{,}57 \times 10^{-9}\,\frac{1}{h}$$

$$\lambda_{tot\,circuit} = 138{,}6 \times 10^{-9}\,\frac{1}{h}$$

Hence the Safe Failure Fraction results to

$$SFF_{circuit} = \frac{\lambda_{S\,circuit} + \lambda_{DD\,circuit}}{\lambda_{tot\,circuit}}$$

$$SFF_{circuit} = 69{,}85\ \% \approx 70\ \%$$

$$t_{CE\,circuit} = \frac{\lambda_{DU\,circuit}}{\lambda_{D\,circuit}} \cdot \left( \frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD\,circuit}}{\lambda_{D\,circuit}} \cdot MTTR = 3\ 700{,}6\ h$$

The Probability of Failure on Demand results to

$$PFD_{circuit} = \lambda_{D\,circuit} \cdot t_{CE\,circuit} = 49{,}57 \times 10^{-9}\,\frac{1}{h} \cdot 3\ 700{,}6\ h$$

$$PFD_{circuit} = 1{,}83 \cdot 10^{-4}$$

Result:

a $PFD_{circuit}$ of $1{,}83 \times 10^{-4}$ fulfils the requirements of a SIL capability of 3;

a SFF of about 70 % limits (at a hardware fault tolerance of 0) the SIL capability to 2.

Hence the SIL capability of the notional electrical circuit is 2.

## Annex D
### (informative)

## Examples for safety devices

### D.1 Heating device

A heating device incorporating an element, thermostat and regulator (the "EUC") is designed to be safe in normal operation and under regular service expected occurrences and so complies with Category 3 (see Table 1). Adding an independent, non-redundant, safety device to the system to protect against a fault in the EUC that might cause the occurrence of hot surfaces increases the overall fault tolerance to 1 and therefore makes the system appropriate for Category 2 (see Table 1), if the hot surfaces are the only ignition risk. If however, the safety device had a fault tolerance of 1, the overall fault tolerance would then be increased to 2. To upgrade this equipment according to Table 1, additional requirements of other standards (e.g. EN 60079-26) for the use of the EUC in a higher category have to be met. All ignition risks have to be considered.

### D.2 Ex 'd' motor

The EC-Type Examination Certificate of a Category 2 Ex 'd' motor requires the use of a direct temperature control (e.g. a PTC thermistor triggering device). The motor has a fault tolerance of 0, i.e. the motor is not a source of ignition in a fault-free operational mode. According to Table 1, the motor requires a safety device with a SIL 1 and a hardware fault tolerance of 0. With this, the motor can be used as Category 2 equipment.

NOTE   The general requirements for Ex d temperature controls are given in EN 60079-1 and EN 60079-14.

### D.3 Overload protective devices for electric motors of type of protection Ex e

According to EN 60079-7 the temperature rise for machines with cage rotors shall be limited. This can be done by using a current-dependent safety device.

In this case the fault tolerance according to the temperature rise of the motor is 0. According to Table 1 a safety device with SIL 1 and a hardware fault tolerance of 0 is necessary to fulfil the requirements of Category 2 equipment. This has additionally to be considered, when designing a complex overload protective device for an Ex e motor according to EN 60079-7.

NOTE   The general requirements for Ex e overload protection devices are given in EN 60079-7 and EN 60079-14

### D.4 Level detectors for the control of submersible pumps

Generally submersible pumps in Zone 1 are protected by standardised or special protection for category 2. If specified for Zone 0, as a second independent means of protection the pump is additionally equipped with a level sensor to ensure a continuous submersion during operation According to Table 1 an independent safety device with a SIL 2 and a hardware fault tolerance of 1 (redundant safety device) is necessary to fulfil the requirements of Category 1 equipment. All ignition risks have to be considered.

### D.5 Electrical resistance trace heating system

Electrical resistance trace heating systems construction principle "Controlled design" according to EN 60079-30-1 are suitable to Zone 1 or 2 applications. If the heating system is mounted outside a vessel or a pipe with a classification Zone 0 inside and the failure of the heating system causes a hot spot in this zone inside, the temperature must be limited with requirements according Zone 0. The sensor of the safety devices must be placed at the hottest point in case of a failure. In addition the requirements for separation of Zone 0 and Zone 2 must be fulfilled in a suitable manner.

NOTE   Installation according to EN 60079-30-2 Electrical resistance trace heating – Application guide for design, installation and maintenance is normally required for installations

## Annex E
### (informative)

## Basic concept for safety devices

This European Standard is based on the results of the SAFEC project, which are summarised in the Final Report [2]. The general concept is based both

−   on the failure tolerance requirement for the equipment categories, and

−   on the probabilistic classification of the hazardous areas into Zones according e.g. EN 60079-10.

a)  According to [1] equipment of Category 1 is required to remain functional, even in the event of rare incidents relating to equipment, with an explosive atmosphere present, and is characterized by means of protection such that:

-   either, in the event of failure of one means of protection, at least an independent second means provides the requisite level of protection, or
-   the requisite level of protection is assured in the event of two faults occurring independently of each other.

Equipment of Category 2 must be so designed and constructed as to prevent ignition sources arising, even in the event of frequently occurring disturbances or equipment operating faults, which normally have to be taken into account

Equipment of Category 3 must be safe under normal operation.

If a potential ignition source, which would become active after one fault, is controlled by a normal safety device (HFT = 0), the controlled ignition source is safe with one fault. Hence, if equipment complying with Category 3 is controlled by a normal safety device, the controlled equipment is safe with one fault and complies with the fault tolerance requirement of Category 2. Consequently, if Category 3 equipment is controlled by a redundant safety device (HFT = 1) the controlled equipment is safe with 2 faults and complies with the fault tolerance requirement of Category 1. The complete concept is shown in Table E.1:

**Table E.1 – Increase of the failure tolerance of equipment by the control of a safety device**

| EUC | Safety device | |
|---|---|---|
| | HFT 0 | HFT 1 |
| Equipment Category 2 | Safe with 2 faults | Safe with 3 faults |
| Equipment Category 3 | Safe with 1 fault | Safe with 2 faults |

b)  The classification of hazardous areas is derived from a generally acknowledged tolerable risk in the working area with respect to an explosion. The probability of an explosion results from the simultaneous occurrence of an explosive atmosphere and an ignition source. (The probability of the occurrence of an explosive atmosphere increases with decreasing Zone number. Hence, to keep the probability of an explosion constant, with decreasing Zone number the probability of the occurrence of an ignition source must be reduced accordingly, e.g. by controlling the ignition source with a safety device. The risk reduction results from the probability of the safety device to perform its function on demand.

Hence, the required safety level of a safety device can directly be linked to the different Zones or the related equipment categories.

In the SAFEC project the probabilities of the occurrence of explosive atmospheres were derived from estimations of the British Petroleum Industry [3]: In Zone 0 the occurrence of an explosive atmosphere is roughly 10 times more frequent than in Zone 1. To avoid a higher explosion probability in Zone 0, the occurrence of an ignition source must be 10 times less than in Zone 1. This can be achieved by controlling a potential ignition source, which could become active under rare incidents in Equipment of Category 2, with a safety device causing a risk reduction of factor 10. According to EN 61508 series this is equivalent to a Safety Integrity Level of 1 (SIL 1). The same consideration can be applied for the control of a potential ignition source in equipment complying to Category 3 for use in Zone 0 or 1 (see Table E.2).

**Table E.2 – Classified area, in which the ignition probability
of controlled equipment would lead to a tolerable risk**

| EUC | Safety Device | | |
|---|---|---|---|
| | No safety device | SIL 1 | SIL 2 |
| Equipment Category 2 | Zone 1 | Zone 0 | Zone 0 |
| Equipment Category 3 | Zone 2 | Zone 1 | Zone 0 |

If controlled equipment is safe with at least two faults according to Table E.1 and leads to a tolerable risk in Zone 0 according to Table E.2, it is equivalent to equipment Category 1. If controlled equipment is safe with at least one fault and leads to a tolerable risk in Zone 1 according to Table E.2, it is equivalent to equipment Category 2. The complete concept is shown in Table E.3:

**Table E.3 – Required SIL and HFT of a safety device for the control of equipment**

| Equipment under control (EUC) | Combined equipment | |
|---|---|---|
| | Equipment Category 1 | Equipment Category 2 |
| Equipment Category 2 | SIL 1, HFT 0 | n.r. |
| Equipment Category 3 | SIL 2, HFT 1 | SIL 1, HFT 0 |

If equipment contains more than one potential ignition source, appropriate measures have to be considered for each of them. The combined equipment shall comply with the relevant standards EN 60079-0 and/or EN 61241-0 for the achieved category.

## Annex ZZ
(informative)

## Coverage of Essential Requirements of EC Directives

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and within its scope the standard covers only the following essential requirements out of those given in Annex II of the EC Directive 94/9/EC:

–   Essential Requirement 1.0.1 to Essential Requirement 1.0.6;

–   Essential Requirement 1.2.1 and Essential Requirement 1.2.2;

–   Essential Requirement 1.4.1 and Essential Requirement 1.4.2;

–   Essential Requirement 1.5.1 to Essential Requirement 1.5.8;

–   Essential Requirement 1.6.3;

–   Essential Requirement 1.6.4.

Compliance with this standard provides one means of conformity with the specified essential requirements of the Directive concerned.

WARNING Other requirements and other EC Directives may be applicable to the products falling within the scope of this standard.

# Bibliography

[1]  *Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres*, OJ L 100, 19.4.1994, p. 1–29

[2]  Final Report - V1.1 (10.07.2000) *SAFEC project, the Standardisation, Measurement and Testing (SMT) Programme of the EU-Commission*, contract SMT4-CT98-2255.

[3]  *Area Classification Code for Petroleum Installations* (Part 15 of the Institute of Petroleum Model Code of Safety Practice in the Petroleum Industry), Institute of Petroleum, John Wiley, 1990.

[4]  IEEE 352, *Guide for general principles of reliability analysis of nuclear power generating station safety system*

[5]  *Ausfallraten Bauelemente, Erwartungswerte, Allgemeines*, Siemens Norm SN 29500-1, Siemens AG, 1996

[6]  *Handbook of Reliability Data 4.0*, British Telecom, 1987

[7]  EN 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion* (IEC 61709)

*This page deliberately left blank*

*This page deliberately left blank*

# British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

## Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

**Tel: +44 (0)20 8996 9001  Fax: +44 (0)20 8996 7001**

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

**Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001**
**Email: plus@bsigroup.com**

## Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.**
In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

**Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001**
**Email: orders@bsigroup.com**

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

## Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

**Tel: +44 (0)20 8996 7004  Fax: +44 (0)20 8996 7005**
**Email: knowledgecentre@bsigroup.com**

Various BSI electronic information services are also available which give details on all its products and services.

**Tel: +44 (0)20 8996 7111  Fax: +44 (0)20 8996 7048**
**Email: info@bsigroup.com**

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

**Tel: +44 (0)20 8996 7002  Fax: +44 (0)20 8996 7001**
**Email: membership@bsigroup.com**

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

## Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Manager.

**Tel: +44 (0)20 8996 7070**
**Email: copyright@bsigroup.com**

**BSI Group Headquarters**

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

*raising standards worldwide*™

**BSI**