BRITISH STANDARD

BS EN
15233:2007

Methodology for functional safety assessment of protective systems for potentially explosive atmospheres

The European Standard EN 15233:2007 has the status of a British Standard

ICS 13.230

BSI
British Standards

National foreword

This British Standard is the UK implementation of EN 15233:2007.

The UK participation in its preparation was entrusted to Technical Committee FSH/23, Fire precautions in industrial and chemical plant.

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.

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 31 October 2007

ISBN 978 0 580 55414 8

Amendments issued since publication

Amd. No.	Date	Comments

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 15233

August 2007

ICS 13.230

English Version

Methodology for functional safety assessment of protective systems for potentially explosive atmospheres

Méthodologie relative à l'évaluation de la sécurité fonctionnelle des systèmes de protection pour atmosphères explosibles

Methodik zur Bewertung der funktionalen Sicherheit von Schutzsystemen für explosionsgefährdete Bereiche

This European Standard was approved by CEN on 13 July 2007.

CEN 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 CEN Management Centre or to any CEN 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 CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

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

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN 15233:2007: E

Contents

Page

Foreword

This document (EN 15233:2007) has been prepared by Technical Committee CEN/TC 305 “Potentially explosive atmospheres - Explosion prevention and protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2008, and conflicting national standards shall be withdrawn at the latest by February 2008.

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

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive 94/9/EC.

For relationship with EU Directive 94/9/EC, see informative Annex ZA, which is an integral part of this document.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

The function of this type A standard is to describe principles for a consistent systematic procedure for functional safety assessment for the design and manufacture of protective systems.

Annex A is informative and contains methods for estimating and assessing functional safety and reliability.

Annex B is informative and contains an example for functional safety assessment of a protective system.

Performing functional safety assessment is referred to in written instructions for use and possible additional precautions are introduced in the documentation.

It is in both the manufacturer's and user's interest to establish a common methodology for achieving functional safety, reliability and effectiveness in the operation of protective systems. Thus, functional safety assessment is a tool which provides the essential link between manufacturers and users, however, only aspects which directly address manufacturers are incorporated in this standard.

Integrated explosion safety is conceived to prevent the formation of explosive atmospheres as well as sources of ignition and, should an explosion nevertheless occur, to halt it immediately and/or to limit its effects. In this connection protective systems must be designed and constructed after due analysis of possible operating faults that limit or prevent the capacity of the system to stop an explosion. Therefore it is absolutely necessary to conduct a functional safety assessment process.

1 Scope

This European Standard provides guidance on the procedure and information required to allow functional safety assessment to be carried out for the design of protective systems.

The purpose of this European Standard is to assist technical standardization committees responsible for specific families of protective systems in preparing safety standards. Such standards should be as homogenous as possible and should have the basic structure of functional safety assessment as it is stated in this standard.

If there are no specific standards for a particular protective system, the manufacturer should use this standard for functional safety assessment of this protective system.

In this procedure the following information is to be taken into account to ensure a sufficient level of functional safety:

a) intended use,

b) possible operating faults,

c) reliability of protective systems,

d) misuse which can reasonably be anticipated.

A sufficient level of functional safety is characterized by the following objectives:

1) System can stop an explosion at a very early stage or reduce the impact of an explosion to an acceptable level.

2) In the event of faults, failures and/or interference[1)] the capacity to function remains effective by use e.g. of fail safe techniques or redundancy.

This European Standard does not cover identification of possible ignition sources.

NOTE 1 The identification of possible ignition sources is covered by EN 15198.

This European Standard only deals with the functional behaviour of the protective system i.e. hazards caused by malfunctions, e.g. false activations are excluded.

This European Standard specifies neither specific methods to analyse fault conditions, nor specific requirements for a given type of protective system (see EN 1127-1). It specifies the methodology of functional safety assessment.

This European Standard provides advice for decisions to be made for all types of protective systems referred to in EU Directive 94/9/EC, but does not provide means to prove the conformity of a given type of protective systems.

NOTE 2 Equipment is dealt with in EN 15198 owing to the fact that the procedure and information required to allow ignition hazard assessment is different from the procedure above.

1) Interference is everything in normal operation that can disturb the normal operation of the system e.g. electromagnetic waves, heat, flames and pressure waves.

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 13237:2003, *Potentially explosive atmospheres – Terms and definitions for equipment and protective systems intended for use in potentially explosive atmospheres*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 13237:2003 and the following apply.

3.1
failure
event, or inoperable state, in which any system item or part of an item or any management function task or process does not, or would not, perform as previously specified

[ISO/IEC Guide 73:2002]

3.2
functional safety
part of the overall safety relating to the intended use in terms of the function and integrity of the protective system including any safety related devices that are part of the protective system performance

NOTE 1 Functional safety covers all aspects where safety depends on the correct functioning of the protective system and other technology safety-related systems.

NOTE 2 This definition deviates from the definition in EN 61508-4 to reflect differences in explosion safety terminology.

3.3
protective system
device other than components of the equipment, which is intended to halt incipient explosions immediately and/or to limit the effective range of an explosion and which is placed separately on the market as autonomous system

[EN 13237:2003, A.5]

3.4
functional safety estimation
determination of the probability of occurrence of the failures violating the functional safety of the protective system

3.5
functional safety evaluation
procedure to determine whether the functional safety of the protective system meets the predefined acceptance criteria

4 General requirements

4.1 Basic concept

Functional safety assessment is a series of logical steps (see Figure 1) that enable designers and safety engineers to examine in a systematic way, the function of a protective system or a part of it. The objective shall be to achieve an adequate level of functionality and reliability according to the state of the art and technical and economic requirements at the time of construction.

This assessment includes the following four steps:

a) description of the protective system (5.2);

b) identification of failures (5.3);

c) functional safety estimation (5.4);

   1) functionality;

   2) reliability;

d) functional safety evaluation (5.5).

These four steps are the basis for the decision whether the intended level of functional safety necessary for the intended use is achieved. The result of the assessment shall be detailed in the technical documentation (see Clause 6).

If the required function and level of reliability is not achieved, it shall be necessary to improve the protective system or to define an appropriate intended use.

NOTE The choice of the suitable measures is not part of the standard.

If the assessment is done by the manufacturer the result of the assessment shall be detailed in the technical documentation (see Clause 6).

Decisions in functional safety assessment shall be supported by qualitative methods complemented, where appropriate, by quantitative methods.

4.2 Extent of functional safety assessment

The protective system shall be assessed on the basis of the information specified in 4.3.

The functional safety assessment shall be limited to the intended use and the misuse, which can reasonably be anticipated for a particular protective system.

NOTE Misuse which can reasonably be anticipated means an incorrect use and/or operation of the protective system by the operator due to negligence or misunderstanding. Misuse is not part of the normal operation. Intent is not included in foreseeable misuse.

4.3 Information needed

The information needed to perform the functional safety assessment shall include the following where appropriate:

a) intended use;

b) safety characteristics used for the design of protective systems;

c) requirements for maintenance;

d) actual and foreseeable surrounding area conditions;

e) relevant design drawings;

f) results of design calculations made, examinations carried out;

if available:

g) test reports;

h) accident history;

i) publications on relevant safety aspects.

If an accident history is not available for the protective system, available information for similar protective systems shall be used; it is unlikely that the protective system is so unique that similar protective systems cannot be found. The absence of an accident history, a small number of accidents or low severities of accidents shall not be taken as an automatic presumption of a low risk.

Possible additional precautions shall be documented.

The information shall be updated as the design develops and modifications are required.

For quantitative assessment, data from data bases, handbooks, laboratories and manufacturer specifications shall be used provided there is confidence in its suitability. Any uncertainty associated with the data shall be documented.

NOTE The data is used to define foreseeable operation requirements related to reliability, serviceability, durability, disposability, benign failure and failsafe characteristics and labelling, warnings, identification, traceability requirements and instructions. Data based on the consensus of expert opinion derived indirectly from experience as opposed to measured data, may be used to supplement qualitative assessment.

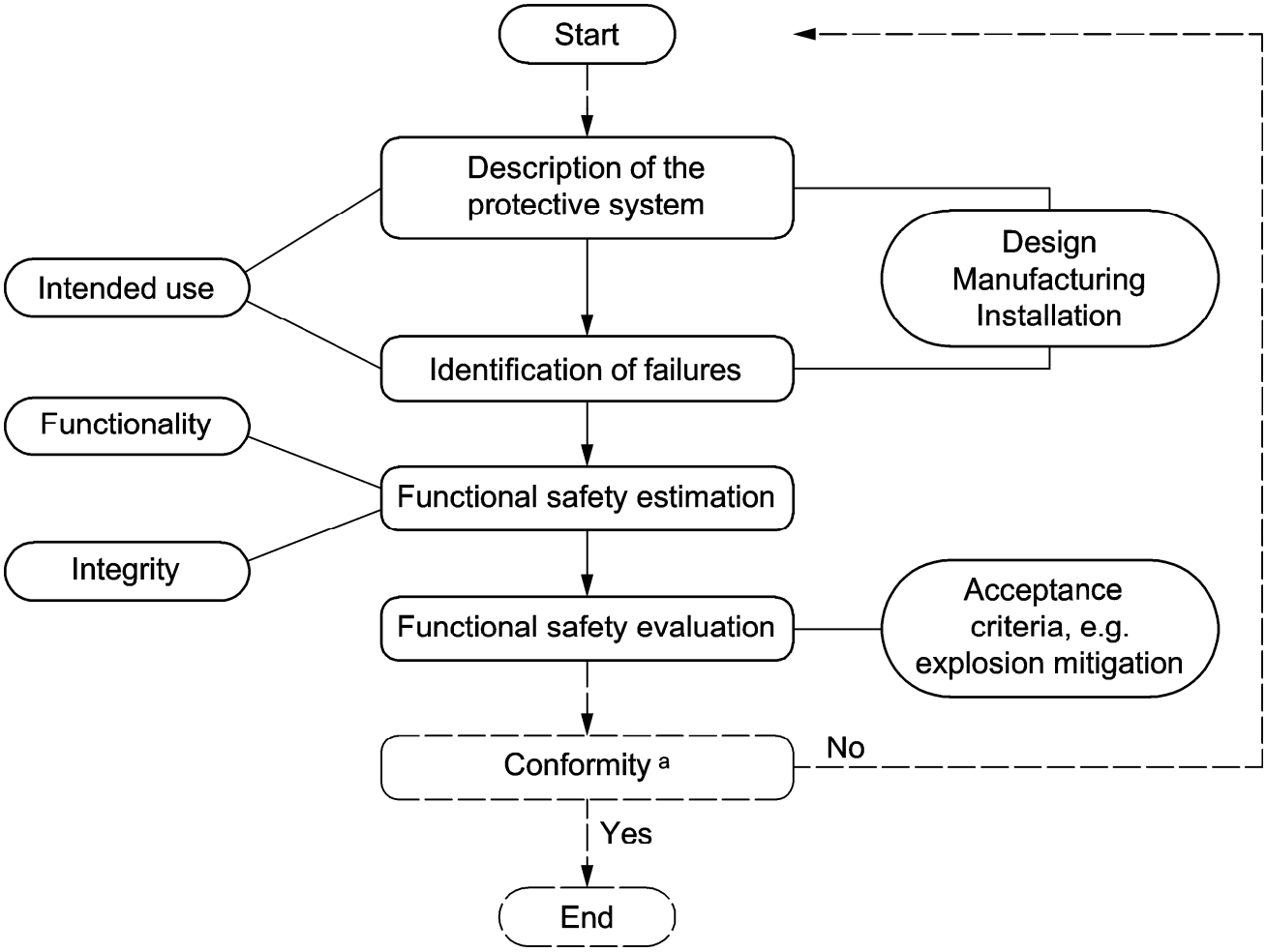
5 Functional safety assessment procedure

5.1 Principle

The principal steps for the functional safety assessment procedure are shown in Figure 1. It is comprised of four steps taking into consideration the information in the oval blocks.

Maintenance requirements shall also be considered in the assessment.

The manufacturer shall consider all necessary maintenance requirements in the instruction manual and shall also consider lack of maintenance relevant for the intended use.



Key

[a] Conformity is not part of functional safety assessment.

NOTE Dotted lines are not part of this standard.

Figure 1 — Functional safety assessment for design of protective systems

5.2 Description of the protective system

The step-approach (by following flow-chart in Figure 1) shall be carried out with an understanding of the function of the protective system and of the types of explosions.

Intended use shall consider, for example, the following items:

a) life cycles of the protective system;

b) limits in terms of use, time, space;

c) accurate definition of the function;

d) selection of materials for construction;

e) performance, lifetime and configuration;

f) description of the type of explosions;

g) limits of process conditions;

h) maintenance requirements.

5.3 Identification of failures

5.3.1 General

Generally, a protective system shall be assessed by potential sources of failure of the protective system. A functional and state analysis for the intended use shall be undertaken for this purpose.

Protective systems are distinguished in the following way:

a) passive systems (e.g. flame arrester, venting system),

b) active systems (e.g. suppression system).

An illustrative example of such an approach is given in Annex A.

The possible failures shall be assessed through a functional and systematic analysis and shall be considered separately with regard to whole lifecycle:

NOTE The listed possible failures are examples. Additional failures may occur.

5.3.2 Assessment

5.3.2.1 Design and manufacturing

In the phase of planning and design the following shall be considered:

a) that the compliance of the intended use shall be achieved. Examples are:

   1) sufficient heat conduction of flame arresters,

   2) effective pressure release of venting devices,

   3) sufficient suppression efficacy of suppression systems.

b) mechanical dimensioning of the protective system is adequate. Failures can occur due to e.g.:

   1) insufficient pressure resistance,

   2) insufficient temperature resistance,

   3) insufficient resistance against vibration and shock,

   4) insufficient resistance against ageing or corrosion.

c) incorrect installation location, an incorrect installation position or an installation method with regard to the nature of the explosion shall be avoided.

d) correct mode with regard to the process, the ambient temperature, the ambient pressure shall be taken into account as well as the correct operating threshold or sensitivity.

e) use of non appropriate software and controlling equipment (hardware).

f) resistance of the hardware against electromagnetic disturbance.

g) additional fail-safe means.

h) in the case of a power failure the intended use of the system shall be maintained as required.

5.3.2.2 Installation

To be able to provide proper information on the installation the manufacturer shall consider the following possible failures:

a) lacking or deficient consideration of effects due to the intended function (e.g. vacuum breakers, danger areas in front of pressure-relief devices, recoil forces, risk of injuries);

b) insufficient sealing or possible circumvention;

c) insufficient electric conditions (e.g. short circuit, open circuit, overload and earth faults);

d) insufficient energy supply and/or back-up power supply for controlling and indicating equipment (CIE).

5.3.2.3 Operational and maintenance requirements

The possible failures that can occur during the use and maintenance of the protective system, shall be considered. The manufacturer shall advise the user how to prevent them. Possible failures, which may arise during the use and maintenance, are:

a) Contamination;

b) incorrect or insufficient intervention by persons (faulty operation, faulty mounting, incorrect maintenance, unintended interventions);

c) indication of fault messages and lack of emergency stop procedures.

Such lacking or deficient situations and the possible failures that may occur shall be described clearly in the instructions for use.

5.3.2.4 Modification

Any safety related modification of a protective system shall be considered a new system which shall require a reassessment.

5.4 Functional safety estimation

5.4.1 General

After the failure identification the functional safety of the protective system has to be estimated by determining the probability of failure occurrence.

The functional safety estimation can be done qualitatively, semi-quantitative or quantitative depending on the criticality of the protective system in reducing the probability of failure and/or the complexity of the system and the safety related devices.

The required performance of the protective system shall be considered in terms of its:

a) function, i.e. the ability to perform the functions required by the intended use of the system (e.g. halt an incipient explosion, reduce explosion pressure), and

b) integrity, i.e. the reliability in performing those functions (on demand or in time).

The ability to perform the required function can be partly quantified by reliability data and/or expression of the fault tolerance of the system structure.

The reliability shall be estimated and evaluated for each of the identified parameters that can lead to a failure of the protective function of the system i.e. for the function and integrity requirements.

5.4.2 Functionality

This part of the functional safety estimation shall include both technical and operating faults in terms of occurrence frequency for failures (e.g. predicting the behaviour from hardware faults, use and misuse which can reasonably be anticipated during the different modes of operation and maintenance activities as well as during the event itself).

The functional safety estimation shall generally be founded on worst case situations, i.e. without the safety function of the protective system, for the defined explosion characteristics. In cases where this is not appropriate, the functional safety shall be estimated for situations that only partly affects the performance of the protective system, e.g. where it partly can reduce the hazard from an explosion, i.e. partly reduce the explosion overpressure.

Each type of failures identified (see 5.3) shall be subject to an evaluation of to what degree they will reduce the performance and the related probability. In this, the criticality of the various parameters that affects the system behaviour must be considered and rated e.g.:

a) condition and operating modes (e.g. installation and operating requirements, maintenance requirements, testing, resetting, interlocks, bypasses);

b) required response and reaction time (response time sensor to actuator and reaction time of the preventive action);

c) fault functions and states;

d) fail-safe functions, safe states;

e) monitoring and detectability of dangerous faults and related actions;

f) sensitivities of the protective system taking into account the safety characteristics;

g) design and control parameters;

h) system structure, redundancy, fault tolerance;

i) interface and influence of system components and safety related control elements and safety devices;

j) inspection/test methods;

k) dependence / independence of other systems for the proper function;

l) systematic- / test independent failures (see 5.4.3, NOTE).

5.4.3 Integrity estimation

The safety integrity requirements in terms of reliability of the function shall be defined and estimated for the safety related devices that are part of the protective system performance.

Simple prevention systems not relying on safety systems and devices that have shown to comply with the required functions through proven experience or evaluations can be estimated on that basis (i.e. proven in use).

If prior use cannot be documented or for novel or more complex systems including safety related control systems and devices a more comprehensive approach using appropriate methods for reliability calculations has to be used (e.g. in accordance with series EN 61508, EN ISO 13849-1 and EN 62061).

For each safety function the frequency of the circumstances that can result in that the safety function can not be realized, (failure rate or probability of failure on demand) shall be estimated considering:

a) mode of operation (demand mode/ continuous mode);

b) assumed demand rates;

c) architecture/ architectural constraints;

d) systematic failures (see 5.4.3, NOTE);

e) common cause failures;

f) mean time to repair (MTTR);

g) inspection/test intervals;

h) diagnostic coverage and safe failure fraction.

The outcome from the integrity estimation should be in the form of reliability figures in the form of probability of failure on demand (PFD) or probability of a dangerous failure per hour (i.e. failure rate) as appropriate, both individually for the different functions and for the protective system function as a whole.

These results will be required for the functional safety evaluation and for the user to verify how the protective system will contribute in an integrated explosion risk evaluation and the prerequisites for performing in reducing the total explosion risk.

Such results therefore shall be a part of the documentation.

NOTE Included in this are failures that may not be revealed by testing or monitoring devices, design failures, software errors, discrimination of signals, installation discrepancies.

5.5 Functional safety evaluation

The acceptability of the functional safety estimation shall be evaluated. Therefore, acceptance criteria shall be defined on beforehand based on the intended use. The acceptance criteria can be qualitatively, semi-quantitatively or quantitatively.

As for the probability estimate the acceptability criteria can be qualitatively, semi-quantitatively or quantitatively.

Comparison of the determined probability that the protective system will fail on demand with the defined acceptability criteria will show whether risk reduction measures are necessary.

To identify risk reduction measures, those components or properties of a protective system which are determinant for the overall risk shall be considered first. Each of the identified risk reduction measures shall be analysed reviewing the safety benefit and practicability associated with each of them.

6 Documentation

6.1 Documentation for the manufacturer

The following documentation shall be part of the documentation of the protective system.

Documentation of functional safety assessment shall demonstrate the procedure that has been followed and the results which have been achieved. This documentation includes when relevant:

a) protective system for which the assessment has been made (e.g. specifications, limits, intended use, operational description) (see 4.2 and 5.2);

b) any relevant assumptions which have been made (e.g. loads, strengths, safety factors);

c) instructions for use according to 4.3, a), b), c), d);

d) further information on which functional safety assessment was based (see 4.3);

e) data used and the source references (e.g. data bases, accident histories, experiences gained from functional safety increasing applied to similar machinery) (the uncertainty associated with the data used and its impact on the functional safety assessment has to be taken into account);

f) failures identified (see 5.3);

g) result of the final functional safety estimation (see 5.4);

h) safety measures implemented to eliminate identified failures or to increase functional safety (e.g. from standards or others specifications);

i) result of the final functional safety evaluation (see 5.5).

6.2 Information to be provided to the user

The following information from 6.1 shall be provided to the user when relevant:

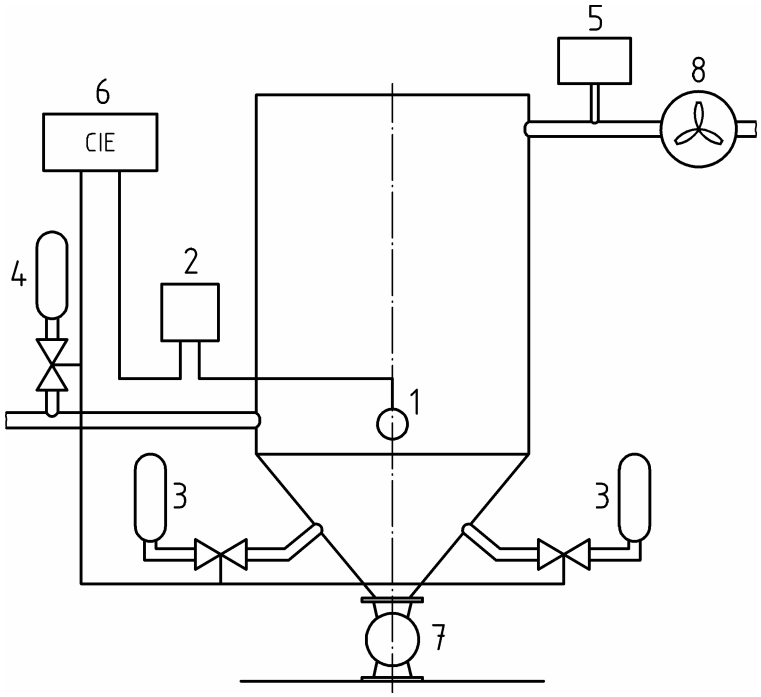
— 6.1, items a), d), h) and i).

Annex A
(informative)

Example of a functional safety assessment

A.1 Introduction

The following is one example of a possible form how an outcome of a functional safety assessment based on the use of an FMECA (failure mode, effects and criticality analysis) can look like.



Key

1 Pressure transducer coupled to an analysing unit
2 Analysing unit for pressure transducer
3 HRD-extinguishers to suppress explosion in filter unit
4 HRD-extinguisher to isolate the filter unit from upstream process units
5 Dust concentration monitoring equipment
6 Controlling and indicating equipment (CIE)
7 Rotary lock-valve
8 Fan

NOTE The example is fictitious and not complete. As such it must therefore only be read as an illustration.

Figure A.1 — Explosion suppression and isolation system of a filter unit

Figure A.1 shows the most important components of an explosion suppression and isolation system mounted to a filter unit. The system operation is as follows:

a) In case of an explosion in the filter unit pressure will start to increase. This pressure increase is registered by the pressure transducer. The pressure-time history registered by the transducer is continuously

analysed by the analysing unit. Upon reaching the alarm level (a certain explosion pressure generated within a certain time) the analysing unit will send a signal to the control unit.

b) Control unit activates the two HRD-extinguishers mounted onto the filter unit to suppress the explosion there.

c) Simultaneously the HRD-extinguisher mounted onto the duct leading to the filter unit, to stop explosions from running back into equipment coupled to the filter unit, is activated.

It is also possible to de-activate the explosion proof rotary valve at the outlet of the filter unit in case of an explosion in the filter unit but this has not been considered in this example.

Thus, the function starts inside the filter upon detection of a too high rate of pressure rise, indicating the occurrence of an explosion, and ends within the process with the triggering of the HRD-extinguishers.

In case of power failure the batteries of the explosion protection system will take over. There will be power for another 4 h. The loss of the safety function after these 4 h is not considered. In case of short circuit, open circuit etc. the system will force the process to go to a safe state. In the analysis the residual risk of an explosion in the de-activated process is not taken into account.

A.2 Quantification of safety functions

The Reliability Block Diagram for this function is given below (Figure A.2). The PFD quantification is presented in Table A.1

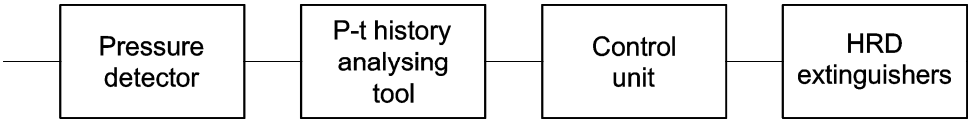


Figure A.2 — Block diagram for system function

A.3 System Requirements

The function is to open each extinguisher flap valve when a signal from the sensor/analyser is given.

The critical parts in the explosion suppression and isolation system are the sensor, the control unit and the HRD extinguisher. Hence, only these parts of the system will be investigated in this example. It is assumed that the safety function of the system fails when one of the HRD-extinguishers does not open (the suppression ability of the system may still be given for weaker explosions; the isolation may very well not be necessary if the ignition in the filter unit is effected far from the connection of the duct to the filter unit. The flame would be extinguished by the suppression system in the filter unit).

It is assumed that the demand frequency will be once per year for the system. The dust explosion will be caused by either an electrostatic discharge or burning particles reaching the filter.

A.4 HRD-extinguishers

A.4.1 General

A very important part of the suppression and isolation system are the HRD-extinguishers themselves. The extinguishers used in this example use electromechanically activated flap valves. The discharge of a condenser activates a torque motor releasing the locking mechanism of the flap valve. The container connected to the valve containing the suppressant has been pressurised up to 60 bar using nitrogen. The

nitrogen pushes the flap valve away releasing the suppressant into the structure to be protected via a nozzle. Both the torque motor and the release electronics have been installed twice in the suppressor for redundancy reasons. Both sets of torque motor and release electronics are fully operational.

An FMECA was performed for the HRD-extinguisher. In total 77 different parts were used. The following mentioned failure rates are fictitious data.

A.4.2 Failure rates of the parts of an HRD-extinguisher

The failure rates of the each part was estimated (examples are given below). The failure rates are given as number of failures per one million hours of operation:

Table A.1 — Examples of failure rates of parts of an HRD-extinguisher

ID No.	Part description	Number of parts	Failure rate per part	Total failure rate
1	Inline filter	1	0,300	0,300
5	Housing	1	0,040	0,040
6	Flap valve	1	0,040	0,040
7	Arbour	1	0,100	0,100
9	Lock pin	1	0,150	0,150
15	Flat gasket	1	0,140	0,140
41	Cylinder head screw	8	0,008	0,064
43	Joint washer	2	0,140	0,280
51	Manometric switch	1	1,100	1,100

A.4.3 Consequences and criticality of fault

For each fault the potential consequences of this fault was estimated. Often the criticality of a fault is estimated using the following classification:

Criticality 1: Very severe fault: Failure of complete system;

Criticality 2: Severe fault: No direct failure of system;

Criticality 3: Less severe fault: Only minor influences on functioning of system;

Criticality 4: Minor fault: No influence on functioning of system.

In the documentation of the FMECA both a description of the consequences and the criticality according to the classification described above need to be given (see Table A.2).

Table A.2 — Consequences and criticality of parts of HRD-extinguisher

ID No.	Item	Functional Identification	Type of Failure	Failure Rate ($\times 10^{-6}$) [per h]	Failure Effect(s)	Critic-ality	Remarks
2	Inline filter	Filters nitrogen during filling	Clogging	0,300	No filling possible	4	Is monitored
5	Housing	Contains all functional parts	Crack, fracture	0,040	Pressure loss	2	Is monitored
6	Flap valve	Closes off pressurised container	Crack, fracture	0,040	Pressure loss	2	Is monitored
7	Arbour	Axis of rotation for flap valve	Fracture	0,090	Pressure loss	2	Is monitored
			Seizing up	0,010	No opening of valve possible upon demand	1	Sleeping failure; is prevented by choice of material combinations and surface treatment
9	Lock pin	Manual locking of opening mechanism	Seizing up		Flap valve cannot be locked or unlocked	3	Is noticed when locking or unlocking
			Fracture	0,090	Flap valve cannot be locked or unlocked	3	Is noticed when locking or unlocking
			Forget-ting to unlock	0,010	No opening of valve possible upon demand	2	Is monitored electrically
15	Flat gasket	Gasket between housings of valve and actuation mechanism	Leakage	0,140	none	4	
41	Cylinder head screw	Fixes housing of electronics	Getting loose, fracture	0,064	None	4	
43	Joint washer	Sealing of bolt	Leakage	0,280	None	4	
51	Manometric switch	Monitors system pressure	Does not open	0,500	Pressure loss is not recognised	2	Sleeping failure; is first recognised during first inspection
			Does not close	0,500	Alarm	3	Is monitored
			Leakage	0,100	Pressure loss	2	Is monitored

NOTE Only a part of all components and functions considered as part of the FMECA are presented in this table).

Considering criticalities of fault 1 only, the FMECA for the HRD-extinguisher, a total probability of failure upon demand can be estimated.

Similar exercises have been performed for the control unit and the sensor.

A.4.4 Calculation Results

Based on the FMECA's and/or FMEA's prepared for the HRD-extinguishers, control unit and the pressure sensor-in combination with the analysing unit the following probability for failure of the explosion suppression and isolation system is estimated.

Table A.3 — Probability for failure on demand (PFD) for the explosion suppression function

Component	No. of components	Total PFD
Sensor in combination with analysing unit	1	$8{,}8 \times 10^{-4}$
Control unit	1	$1{,}7 \times 10^{-3}$
HRD valve	3	$6{,}6 \times 10^{-3}$
Total Function	-	$9{,}1 \times 10^{-3}$

As seen from Table A.3 the function fulfils a SIL 2 requirement as per series EN 61508.

Annex B
(informative)

Methods for failure identification and functional safety assessment

B.1 General

There are many methods for identification of failures, estimating the probabilities and assessing the effects of such failures. Each method has been developed for particular applications and therefore, it may be necessary to modify some details for any application of a functional safety assessment.

Some methods that may be used are briefly described and referenced, e.g., in EN 1050:1996, Annex B and EN ISO 17776:2002, Annex B. Below descriptions are presented of two such methods giving guidance of how they can be used in functional safety assessments .

B.2 Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA)

FMEA (Failure Modes and Effects Analysis) and FMECA (Failure Modes, Effects and Criticality Analysis) are used in order to identify and describe breakdown of system, redundancy and common cause failures, functions, failure modes, causes, effects, detection methods, Mean Time To Repair (MTTR) and test interval for components critical to the safety function in the safety-related system.

To start to analyse the system must be broken down into components. It is important to find an appropriate level for this system breakdown. The level should depend on the objective of the FMEA/FMECA and the available technical documentation. In many cases the FMEA (or FMECA) is conducted as a pre-activity to a fault tree analysis or as the basis for a functional safety estimation.

The FMEA or FMECA should be carried out with a team representing the engineering disciplines as well as personnel with extensive product experience of the system. A standard form is used to document information for each component in the system (an example of FMEA/FMECA Tables is given in Annex A):

a) Name and type of component;

b) Function;

c) Failure modes;

d) Failure causes;

e) Local fault effects;

f) Global fault effects;

g) Detection of fault;

h) Compensation/safeguarding (redundancy);

i) Comments, recommendations and follow-up.

In the FMEA/FMECA a column is also used for part-quantitative assumption of the probability for the failure mode to occur and the consequence when it occurs. Both the probability and the consequence are sorted and

can be classified (low, medium, high/risk matrix, etc.). The meaning and importance of each class must be defined in the text, consequences should be classified in respect to humans, economic and environment. In the functional safety assessment a quantitative or semi-quantitative measure for the probability is often required and must be given by manufacturer or qualified from a generic data source.

B.3 Fault Tree Analysis (FTA)

A fault tree is a method by which a particular undesired system failure mode can be expressed in terms of component failure modes and operator actions. The fault tree would set out the logic for all the ways in which this could occur. This is recorded on a fault tree diagram.

A fault tree diagram contains two basic elements: "gates" and "events". Gates allow the passage of fault logic up the tree and show the relationships between events that are needed to cause the occurrence of a higher event. The two main types of gate are AND and OR. An AND gate indicates that all the events entering the gate are required to occur at the same time in order to cause the higher event. An OR gate indicates that only one of the events entering the gate is required to cause the higher event. There are also a number of other types of gates which are required less frequently to represent logic. Once the logic has been written down in a fault tree, the frequency of the top event can be calculated, given data on the frequencies/probabilities of events at the lowest level on the tree. Such frequencies/probabilities will usually apply to failure rates of electronic, electrical or mechanical components, and such data may be available from databases. The probability of failure of human operators to act as desired can also be predicted. Fault tree arithmetic, which has a basis in Boolean algebra can then be used to calculate the frequency of the top event. At any OR gate frequencies can be added together. At any AND gate, one frequency and any number of probabilities can be multiplied together (as a first order approximation). In evaluating a fault tree it is important to be clear about which data are frequencies (units of events per unit time) and which are probabilities (dimensionless). There are also specialist techniques for evaluating large and complex fault trees, such as the technique of minimum cut sets.

Fault tree analysis is usually best done by specialists as there are potential pitfalls. If the logic represented by the fault tree is incorrect then the calculated frequency will also be incorrect. It is also quite easy to get the algebra wrong specially if the occurrence of a Common Mode Failure is not taken into account.

The FTA is especially applicable to: discrete items, complete machinery, and assessing the reliability of protective systems.

FTA would be over complex and prohibitively time-consuming for more complex machinery except when used, without quantification, to give a high level overview of the interaction between different components, functions.

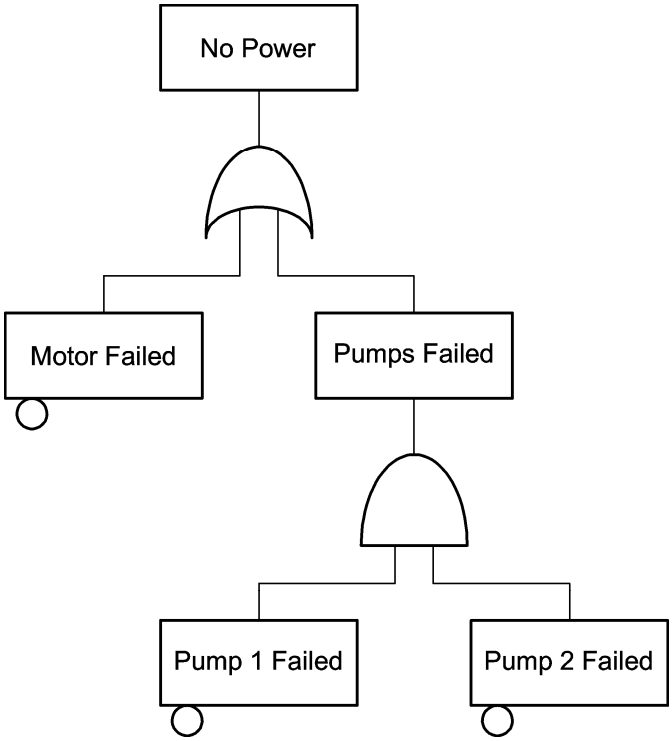


Figure B.1 — Fault Tree Showing Failure of Power Supply

Annex ZA
(informative)

Relationship between this European Standard and the Essential Requirements of EU Directive 94/9/EC

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association to provide a means of conforming to Essential Requirements of the New Approach 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.

Once this standard is cited in the Official Journal of the European Communities under that Directive and has been implemented as a national standard in at least one Member State, compliance with the clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding Essential Requirements of that Directive and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 94/9/EC

Clause(s)/sub-clause(s) of this EN	Essential Requirements (ERs) of Directive 94/9/EC	Qualifying remarks/Notes
	1 Common requirements for equipment and protective systems	
	1.0 General requirements	
Clause 4, Clause 5	1.0.1 Principles of integrated explosion safety	
Clause 4, Clause 5	1.0.2 Analysis of possible operating faults	
6.2	1.0.6 Instructions	
	3 Supplementary requirements in respect of protective systems	
	3.0 General requirements	
5.3.2.1	3.0.3 Power failure	
Clause 4, Clause 5	3.1 Planing and design	

WARNING — Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this standard.

Bibliography

EN ISO 13849-1:2006, *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)*

EN 1050:1996, *Safety of machinery – Principles for risk assessment*

EN 1127-1, *Explosive atmospheres – Explosion prevention and protection – Part 1: Basic concepts and methodology*

EN 12874, *Flame arresters – Performance requirements, test methods and limits for use*

EN 14373, *Explosion suppression systems*

EN 14460, *Explosion resistant equipment*

EN 14491, *Dust explosion venting protective systems*

EN 14797, *Explosion venting devices*

EN 14994, *Gas explosion venting protective systems*

prEN 15089, *Explosion isolation systems*

EN 15198, *Methodology for the risk assessment of non-electrical equipment and components for intended use in potentially explosive atmospheres*

EN 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMES)*

EN 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (IEC 61508-1:1998 + Corrigendum 1999)*

EN 61508-2, *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 61508-3:1998 + Corrigendum 1999)*

EN 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations (IEC 61508-4:1998 + Corrigendum 1999)*

EN 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5:1998 + Corrigendum 1999)*

EN 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6:2000)*

EN 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures (IEC 61508- 7:2000)*

EN 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (IEC 62061:2005)*

EN ISO 12100-1, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology (ISO 12100-1:2003)*

EN ISO 12100-2, *Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles (ISO 12100-2:2003)*

EN ISO/IEC 17000, *Conformity assessment – Vocabulary and general principles (ISO/IEC 17000:2004)*

EN ISO 17776:2002, *Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment (ISO 17776:2000)*

CEN/TR 15281, *Guidance on Inerting for the Prevention of Explosions*

CEN Guide 414, *Safety of machinery – Rules for the drafting and presentation of safety standards*

EN 61025, *Fault tree analysis (FTA) (IEC 61025:2006)*

ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*

ISO/IEC Guide 51 *Safety aspects – Guidelines for their inclusion in standards*

BS 5760-5, *Reliability of systems, equipment and components – Guide to failure modes, effects and criticality analysis (FMEA and FMECA)*

94/9/EC, *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*

Lees, Frank P., *Loss Prevention in the Process Industries*, 2nd Ed. 1996, Chapter 8.15

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. 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 9000. Fax: +44 (0)20 8996 7400.

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

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.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 Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI 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@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL