SLOVENSKI STANDARD
SIST EN 15233:2007

01-oktober-2007

Metodologija za varnostno oceno delovanja zaġļ itnih sistemov za potencialno eksplozivne atmosfere

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

Methodik zur Bewertung der funktionalen Sicherheit von Schutzsystemen für explosionsgefährdete Bereiche

Méthodologie relative a l'évaluation de la sécurité fonctionnelle des systemes de protection pour atmospheres explosibles

Ta slovenski standard je istoveten z: **EN 15233:2007**

ICS:

13.230	Varstvo pred eksplozijo	Explosion protection

SIST EN 15233:2007 **en,fr,de**

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.

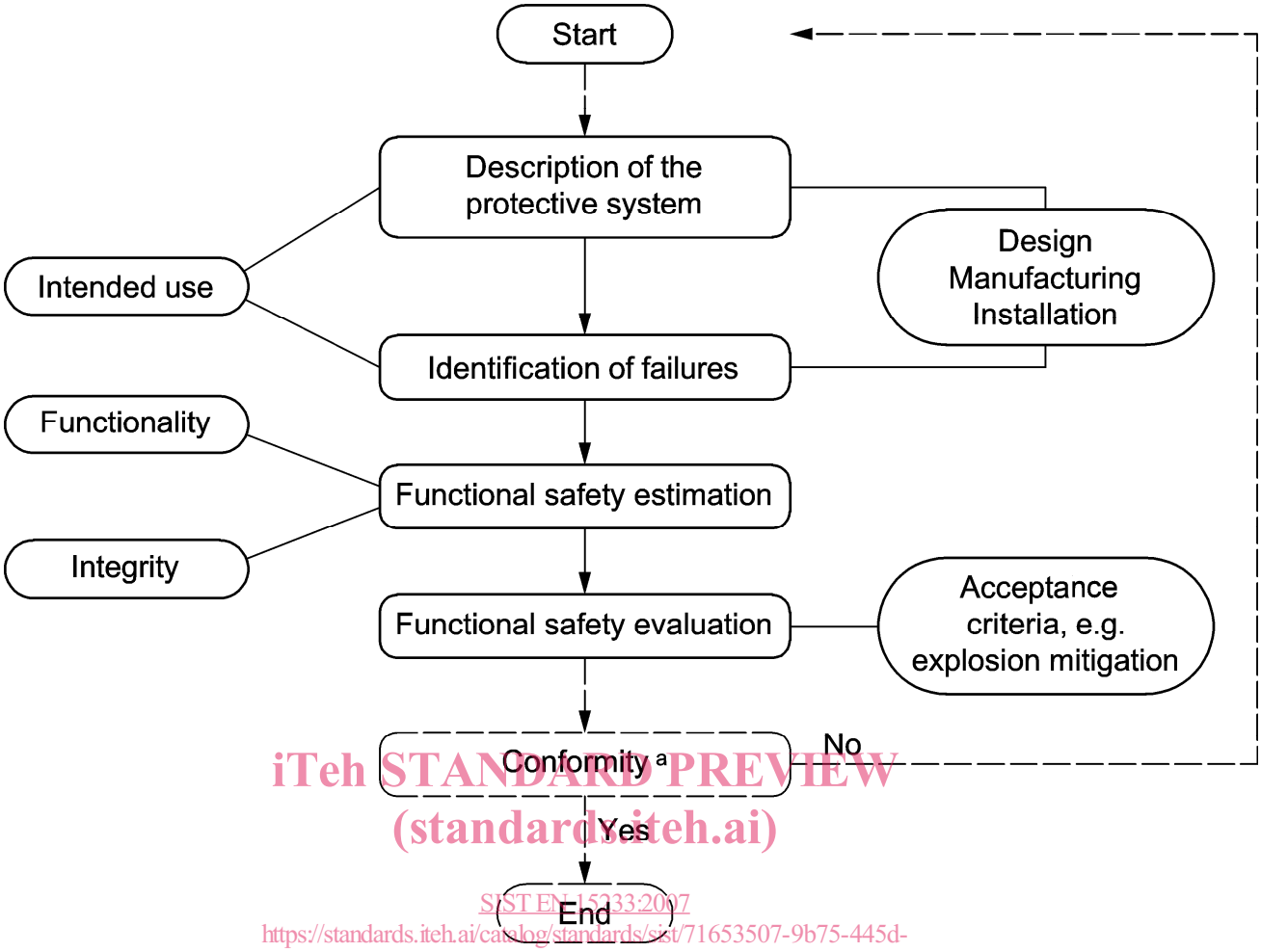
5 Functional safety assessment procedure

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;