SLOVENSKI STANDARD
SIST EN 17955:2024

01-oktober-2024

Industrijski ventili - Funkcionalna varnost varnostnih ventilov in pogonov

Industrial valves - Functional safety of safety-related valves and actuators

Industrieamaturen - Funktionale Sicherheit sicherheitsbezogener Industriearmaturen und Antriebe

Robinetterie industrielle - Sécurité fonctionnelle des appareils de robinetterie et actionneurs liés à la sécurité

Ta slovenski standard je istoveten z: **EN 17955:2024**

ICS:

23.060.01 Ventili na splošno Valves in general

SIST EN 17955:2024 **en,fr,de**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 17955

August 2024

ICS 23.060.01

English Version

Industrial valves - Functional safety of safety-related automated valves

Robinetterie industrielle - Sécurité fonctionnelle des appareils de robinetterie automatisés assurant une fonction de sécurité

Industriearmaturen - Funktionale Sicherheit sicherheitsbezogener automatisierter Industriearmaturen

This European Standard was approved by CEN on 7 July 2024.

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-CENELEC 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-CENELEC Management Centre has the same status as the official versions.

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

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (EN 17955:2024) has been prepared by Technical Committee CEN/TC 69 “Industrial valves”, the secretariat of which is held by AFNOR.

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 2024, and conflicting national standards shall be withdrawn at the latest by February 2024.

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

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

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

Introduction

Mechanical compliant items such as valves or actuators are integral parts of many automated safety-related systems. It is therefore necessary to assess the suitability of mechanical compliant items within the safety functions as well as those of electrical compliant items. This document defines aspects for implementing safety-related functions with mechanical compliant items. It describes procedures and methods with which all relevant compliant items can be evaluated in order to integrate them into a safety-related system. It can also be applied to the mechanical portion of a compliant item if it consists only partially of mechanical components.

In the case of mechanical compliant items, separation between random and systematic failures is not always possible. A method for determining random failure rates is described. Failures of unknown origin are to be included in a random failure rate if no systematic cause of the failure could be identified and resolved. Hence, the random failure rate is understood as a worst-case estimation which includes failures of unknown origin. This method can be used in cases where no clear identification of failure mechanisms (e.g. fatigue, wear or ageing) is possible. Any other identified systematic failures can be prevented by systematic measures according to the principle “first qualify – then quantify”. Systematic fault avoidance measures are for example functional safety management, design calculation, fabrication surveillance, testing or user instructions.

This document is intended for manufacturers of final elements or their compliant items to enable a consistent approach to evaluate the functional safety of their compliant items. The compliant items are considered individually according to the specifications of this document. The final combination is evaluated according to the principles defined in EN 61508 and derived application standards such as EN 61511.

NOTE “Safety-related system” is used as equivalent to “safety instrumented system (SIS)” in this document.

1 Scope

This document defines the requirements for how mechanical compliant items in a final element can be evaluated according to the principles of EN 61508 to integrate them into a safety-related system. It provides a method to determine all relevant factors, associated with the product, and thereby meet the specific needs of users of the product.

The basic prerequisite for the application of this document is that the intended use is known. This document describes a system to minimize systematic faults to achieve the targeted Safety Integrity Level (SIL).

This document is applied to single compliant items (e.g. valve, actuator or mechanical portions of solenoid valves) or to assemblies of several of these compliant items and interconnecting compliant items and components (e.g. gears, adaptors, brackets, etc.). Electrical, electronic or programmable electronic components are assessed according to EN 61508.

This document does not apply to:

— manually operated valves;

— items in safety systems or risk-reducing devices that are not assessed and operated according to the principles of functional safety (e.g. automatic safety valves like pressure relief valves).

The methods described can also be used for other mechanical compliant items in a final element of the safety-related system if the applicability is confirmed by appropriate expert knowledge (e.g. dampers, brakes, clutches).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

EN 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements (IEC 61508-1:2010)*

EN 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2010)*

EN 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations (IEC 61508-4:2010)*

EN 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

EN 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in EN 61508-4, below and the abbreviations given in Table 1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

Table 1 — Abbreviations

Abbreviation	Full expression	Reference
BPCS	Basic process control system	
CAE	Computer aided engineering	
CFD	Computational fluid dynamics	
DC	Diagnostic coverage	EN 61508-4:2010, 3.8.6
E/E/PE	Electrical/electronic/programmable electronic	
EUC	Equipment under control	EN 61508-4:2010, 3.2.1
FAT	Factory acceptance test	
FEA	Finite element analysis	
FIT	Failure in time	
FME(D)A	Failure mode and effect (and diagnostic) analysis	
FSM	Functional safety management	
FST	Full stroke test	
FTA	Fault tree analysis	
HFT	Hardware fault tolerance	EN 61508-2:2010, 7.4.4
HUR	High utilization rate	
IOM	Installation, operating and maintenance manual	
LUR	Low utilization rate	
MRT	Mean repair time	EN 61508-4:2010, 3.6.22
PFD_{avg}	Average probability of dangerous failure on Demand	EN 61508-4:2010, 3.6.17
PFH	Average frequency of dangerous failure [h^{-1}]	EN 61508-4:2010, 3.6.19
PST	Partial stroke test	
PTC	Proof test coverage	
PVST	Partial valve stroke test	

Abbreviation	Full expression	Reference
RPN	Risk priority number	Annex C
S	Safety factor	
SC	Systematic capability	EN 61511-1:2017, 3.2.80
SFF	Safe failure fraction	EN 61508-4:2010, 3.6.15
SIF	Safety instrumented function	EN 61511-1:2017, 3.2.66 "Safety-related function" is used as equivalent to "safety instrumented function" in this document.
SIL	Safety integrity level	EN 61508-4:2010, 3.5.8
SIS	Safety instrumented system	EN 61511-1:2017, 3.2.67 "Safety-related system" is used as equivalent to "safety instrumented system" in this document.
SOD	Severity occurrence detection	Annex C

3.1
component
smallest piece of a compliant item

Note 1 to entry: These components typically do not have a related safety function and cannot be assigned a standalone safety statement.

Note 2 to entry: Typical mechanical components are e.g. a rod, a bearing, a seal, or a screw.

3.2
functional unit
combination of components that performs or is responsible for a function of a compliant item

Note 1 to entry: Typical functional units are e.g. pressurized body, non-pressurized housing, packing, seat/trim, spring set or gearing system.

3.3
compliant item
item for which a compliance claim is being made with respect to hardware safety integrity, systematic capability, and supported with functional safety assessment

Note 1 to entry: EN 61511-1 and −2 is using the term device in an equivalent way.

Note 2 to entry: A typical mechanical compliant item can be an actuator, a positioner, a solenoid valve, a valve, a gearbox or a complete final element containing e.g. an actuator and a valve.

Note 3 to entry: A compliant item comprises components. Different compliant items can be assembled together with components to form a final element or safety-related system.

Note 4 to entry: A method for combining several compliant items is described in EN 61508-1, −2, −4, −6 and −7, EN 61511-1 and −2.

3.4
final element
(final) subsystem in a SIS that contains the compliant items which physically perform the safety function

Note 1 to entry: A typical final element is shown in Figure 1.

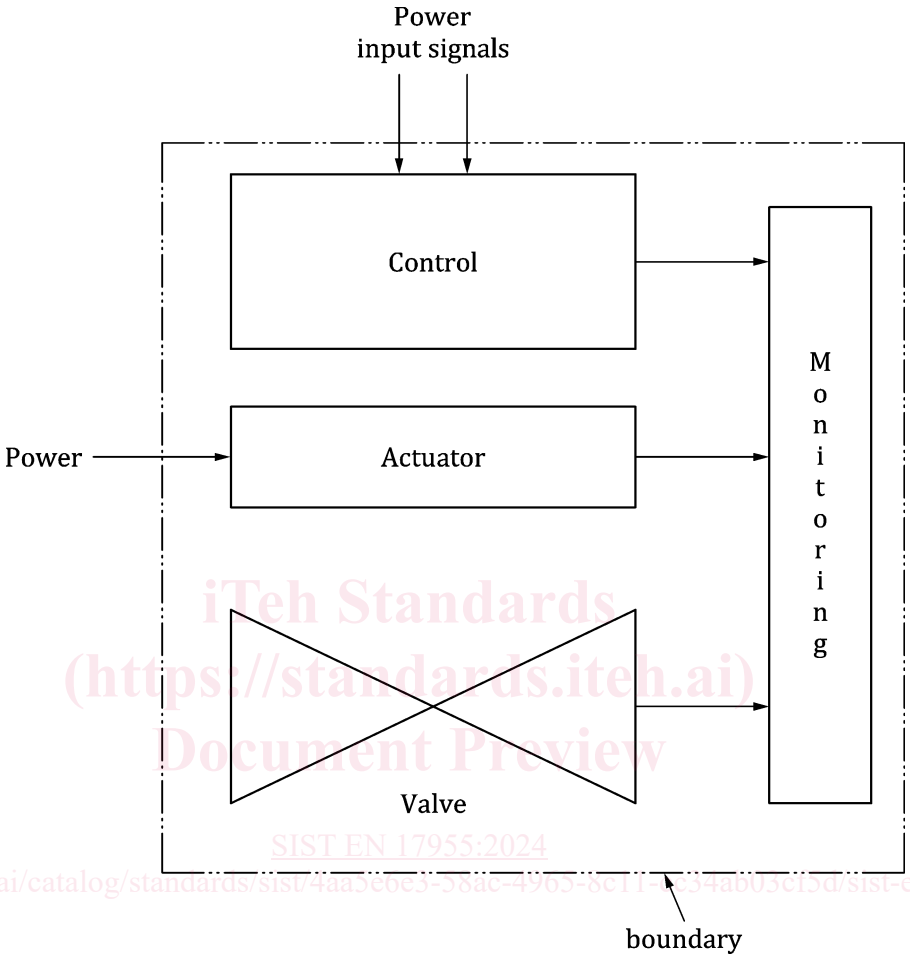

Figure 1 — Boundary definition – valves (EN ISO 14224:2016, A.2.5.4 modified)

Note 2 to entry: Final elements, in the context of this document, generally consist of industrial valves with actuators and other compliant items for operating the valve, such as solenoid valves, gearboxes or positioners.

Note 3 to entry: The boundary between the different compliant items of a final element is part of the corresponding product standards.

3.5
manufacturer
person or company who designs and/or manufactures compliant items or an assembly of compliant items and markets that compliant item or assembly under his own name or trademark or uses it for his own use

Note 1 to entry: A manufacturer of a compliant item can also be a manufacturer of a final element.

3.6
system integrator
person or company, who combines compliant items as a complete safety-related system to achieve the function and safety requirements

Note 1 to entry: The system integrator is responsible for (overall) planning, for engineering and possibly for installation and commissioning of complete safety-related systems, working in accordance with EN 61508-1, –2, –4, –6 and –7 or derived standards. The system integrator can also be the end user or a third party contracted by the end user. The system integrator has to demonstrate by procedures and by documentation that the safety-related systems achieve the required SIL capabilities.

3.7
final element integrator
integrator of the compliant items and components, responsible for the design, assembly and validation of the final element subsystem

Note 1 to entry: The final element integrator can also be a manufacturer of one or more compliant items included in the final element subsystem.

3.8
end user
organization that has overall responsibility for a process facility and its installed safety-related system(s) during all safety lifecycle phases

Note 1 to entry: This includes – but is not limited to – the responsibility for the planning, installation, commissioning, operation, maintenance, and de-commissioning of the safety-related system(s). The end user can outsource certain lifecycle phases or activities to sub-contractors.

3.9
utilization rate
total movements of the mechanical compliant item per year

Note 1 to entry: This includes but is not limited to movements due to demand of the safety function plus movements due to testing (automatic online diagnostic tests or manual tests) plus operations requested by the EUC control system.

Note 2 to entry: EN 61508-2 defines different modes of operation, which only consider the number of demands of the safety function per year. However, for mechanical compliant items the primary fault mechanism largely depends on the overall number of movements of the compliant item (including testing, demands by the EUC control system, etc.), rather than depending on the number of movements due to a demand on the safety function only. Therefore, this document defines a utilization rate in addition to the mode of operation to correctly consider different fault mechanisms like ageing, wear and fatigue.

Note 3 to entry: The utilization rate of different compliant items in a safety-related function or a final element can differ, e.g. if some but not all compliant items are tested by a full stroke test or if some of the compliant items are used for basic process control as well.

Note 4 to entry: A partial stroke is considered as a movement and is therefore considered in the utilization rate.

Note 5 to entry: Since ageing effects depend more on the number of movements than on the distance of travel, the number of movements is decisive rather than the percentage of the stroke travelled or the absolute length of the stroke.

3.10
low utilization rate
LUR
utilization rate of the compliant item that is low enough to assume that wear has no or only a minor influence on the failure rate of the compliant item

3.11
high utilization rate
HUR
utilization rate of the compliant item that is high enough to assume that wear is the dominant fault mechanism leading to compliant item failure

3.12
partial stroke test
PST
test method that checks if e.g. a valve can be operated through a portion of its total stroke range

Note 1 to entry: This short stroke of operation verifies that certain failure modes of the compliant item are not present and that the compliant item is functional with respect to these fault mechanisms.

Note 2 to entry: In this document the term “partial stroke test” is used but it is recognized that for automated valves “partial valve stroke test (PVST)” is used as an equivalent term.

Note 3 to entry: As a general rule a partial stroke test can detect faults due to certain failure modes but is not capable to test all failure modes of the compliant item. For example, a partial stroke test of a valve with safety position CLOSE can be capable of determining if a valve is seized in position but it usually cannot test if the valve is able to travel all the way to its safety position or if it can tightly seal in the closed position. Therefore, it is assessed e.g. by means of an FMEA which failure modes can, respectively cannot, be detected by a partial stroke test in the particular application.

Note 4 to entry: A PST is most often used to test mechanical, pneumatic, or hydraulic compliant items. The test can also include electrical or electromechanical components e.g. a relay that is used to operate the actuator of a tested valve.

Note 5 to entry: The limited stroke of the test is intended to be short enough to introduce no (or a minimum of) interference with the operating flow of the equipment under control (EUC). An assessment if the influence on the basic process is acceptable is advised.

Note 6 to entry: A PST is usually performed on the complete final element, thus all relevant compliant items are tested simultaneously.

3.13
full stroke test
FST
test method that checks if e.g. a valve can be operated through its complete stroke range

Note 1 to entry: This stroke verifies that certain failure modes of the compliant item are not present and that the compliant item is functional with respect to these fault mechanisms.

Note 2 to entry: As a general rule a full stroke test can detect more faults of the compliant item than a partial stroke test but not all. For example, a full stroke test of a valve with safety position “close” can test that a valve is not seized in position and that it can travel all the way to its safety position but – without additional measures – cannot test if the valve tightly seals in the closed position. Therefore, it is assessed, e.g. by means of an FMEA, which failure modes can, respectively cannot, be detected by a full stroke test in the particular application.

Note 3 to entry: Like a PST, the FST is usually performed on the complete final element, thus all relevant compliant items are tested simultaneously.

3.14
ageing
degradation process of a component or assembly of components that depends on the elapsed time

Note 1 to entry: This contrasts with degradation processes that depend on the number of movements performed ("wear"). For faults due to fatigue, it has to be assessed if the root cause is due to ageing or wear as defined in this document.

3.15
wear
degradation process of a component or assembly of components that depends on the number and intensity of movements that the component is exposed to

Note 1 to entry: This contrasts with degradation processes that depend on the elapsed time ("ageing"). For faults due to fatigue, it has to be assessed if the root cause is due to ageing or wear as defined in this document.

3.16
fatigue
degradation process of a component that depends on the number and intensity of deformations that the component is exposed to

3.17
FIT
abbreviation for "failure in time"

Note 1 to entry: 1 FIT = 10^{-9}/h.

3.18
well-tried component
component for a safety-related application which has been either

a) widely used in the past with successful results in similar applications, or

b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications

4 Relationship and conformity with EN 61508-1, –2, –4, –6 and –7

The intention of this document is not to replace any applicable requirements of the EN 61508 series. The relationship between this document and EN 61508-1, –2, –4, –6 and –7 is shown in Table 2 (by cross-referencing just the main clauses). Conformity requirements for the mechanical portion of SIS final elements are indicated in the corresponding notes.