SLOVENSKI STANDARD
oSIST prEN 17955:2023

01-april-2023

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: **prEN 17955**

ICS:

23.060.01 Ventili na splošno Valves in general

oSIST prEN 17955:2023 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17955

February 2023

ICS 23.060.01

English Version

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

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

Industrieamaturen - Funktionale Sicherheit sicherheitsbezogener Industriearmaturen und Antriebe

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 69.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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 4

Introduction 5

2 Scope 6

3 Normative references 6

4 Terms and definitions 7

5 Relationship and conformity with EN 61508-1, –2, –4, –6 and –7 11

6 Basic requirements for development and production 12
6.1 Evaluation of systematic capability 12
6.2 Documentation management 13
6.3 Functional safety management 13
6.4 Safety lifecycle requirements for development and production of safety-related automated industrial valves 13
6.4.1 Objectives and requirements 13
6.4.2 Mechanical requirements specification 17
6.4.3 Mechanical validation planning 18
6.4.4 Mechanical design 19
6.4.5 Mechanical system integration 21
6.4.6 Mechanical system installation, commissioning, operation and maintenance procedures 22
6.4.7 Mechanical system safety validation 24
6.4.8 Production 24
6.4.9 Modification of component 25
6.5 Verification 26
6.5.1 Objective 26
6.5.2 Requirements 26
6.6 Functional safety assessment 28
6.6.1 Objective 28
6.6.2 Requirements 28

7 Classification of the component 28
7.1 Demand mode and utilization rate 28
7.2 Type of final element/component 31

8 Field failure data 31
8.1 Field failure data analysis procedure 31
8.2 Use of field failure data for pre-existing components 32

9 Qualification testing (during development) 33
9.1 General 33
9.2 Test planning/test conditions 33
9.3 Pre-conditioning of test samples 33
9.4 Number of required test samples 33
9.5 Cycle testing and B_{10D} values according to EN ISO 13849-1:2015, C.4.2 33
9.6 Environmental testing 34

10 Determination of failure rates 34
11 Operational testing, maintenance and time restrictions 34
11.1 Online diagnostic tests 34
11.2 Proof test 35
11.3 Proof test coverage (PTC) 35
11.4 Maintenance 35
11.5 Useful lifetime 35
11.6 Storage time 36
12 Safety manual in addition to an IOM (installation, operation, and maintenance manual) 36
Annex A (normative) Checklist for determination of systematic capability 38
Annex B (normative) Techniques and measures to avoid and control systematic failures 39
Annex C (normative) List of failure rates for common components 46
Annex D (normative) L FME(D)A to identify and evaluate the effects of different failure modes 49
D.1 FME(D)A 49
D.2 Input information to carry out an FME(D)A 49
D.3 FME(D)A procedure 49
D.4 FMEDA example 52
D.5 List of functional units and their failure rates with a low utilization rate (LUR) 56
D.6 List of functional units and their failure rates with a high utilization rate (HUR) 57
Annex E (informative) Safety manual 60
Annex F (informative) Examples for the evaluation of the mechanical design 63
F.1 General 63
F.2 Examples 63
F.2.1 Screw connections 63
F.2.2 Force-locked connections 64
F.2.3 Form-locked connections (structural part strength) 65
F.2.4 Springs 65
F.2.5 Bearings 66
F.2.6 Gears and force transmission linkages 66
Annex G (informative) Estimation of random failure rates with Bayesian integration between “basic” failure rates and field feedback 67
G.1 General 67
G.2 Procedure 67
G.3 Formula 68
Bibliography 70

European foreword

This document (prEN 17955:2023) has been prepared by Technical Committee CEN/TC 69 “Industrial valves”, the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

Introduction

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

In the case of mechanical components, separation between random and systematic failures is not always possible. A method for determining random failure rates is described. Failures of unknown origin might be included in a random failure rate in the sense that all causes of systematic defects are not known yet. Hence, the random failure rate has to be understood as a worst case estimation which includes failures of unknown origin. This method may 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 for manufacturers of final elements or their components to enable a consistent approach to evaluate the functional safety of their components. The components are considered individually according to the specifications of this document. The final combination is evaluated according to the principles defined in EN 61508-1, –2, –4, –6 and –7 and derived application standards such as EN 61511-1 and –2.

1 Scope

This document defines the procedures and methods with which all relevant mechanical components of automated industrial valve packages that are used as final elements in a safety instrumented system can be evaluated according to the principles of EN 61508-1, −2, −4, −6 and −7 in order to integrate them into a safety instrumented system (SIS). It provides a method to determine all relevant factors, associated with the product, which should be fully taken into account 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 avoid systematic faults to achieve the targeted Safety Integrity Level.

This document applies to automated industrial valve packages that are used as final elements in a safety instrumented system. It is applied to single components (e.g. valve, actuator or mechanical parts of solenoid valves) or to assemblies of several of these components and interconnecting parts (e.g. gears, adaptors, brackets, etc.). Electrical, electronic or programmable electronic parts have to be assessed according to EN 61508-1, −2, −4, −6 and −7.

This document does not apply to:

— manually operated valves;

— components 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 components in a final element of the safety instrumented 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 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements*

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*

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

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*

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

EN IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 61508-4 and the following apply.

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

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

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

3.1
part
smallest device, not being an assembly

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

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

3.2
functional unit
combination of parts that performs or is responsible for a function of a component

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

3.3
component
segment of a safety-related system that is assigned a component safety instrumented function and a safety statement and also a product sold by a manufacturer in combination with a safety statement (defined in its safety manual) for a component-related safety function

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 component 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 component comprises parts. Different components can be assembled together with parts to form a final element or safety-related system.

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

3.4
final element
subsystem that is classified as consisting out of various components which are used in combination in a safety-related system

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

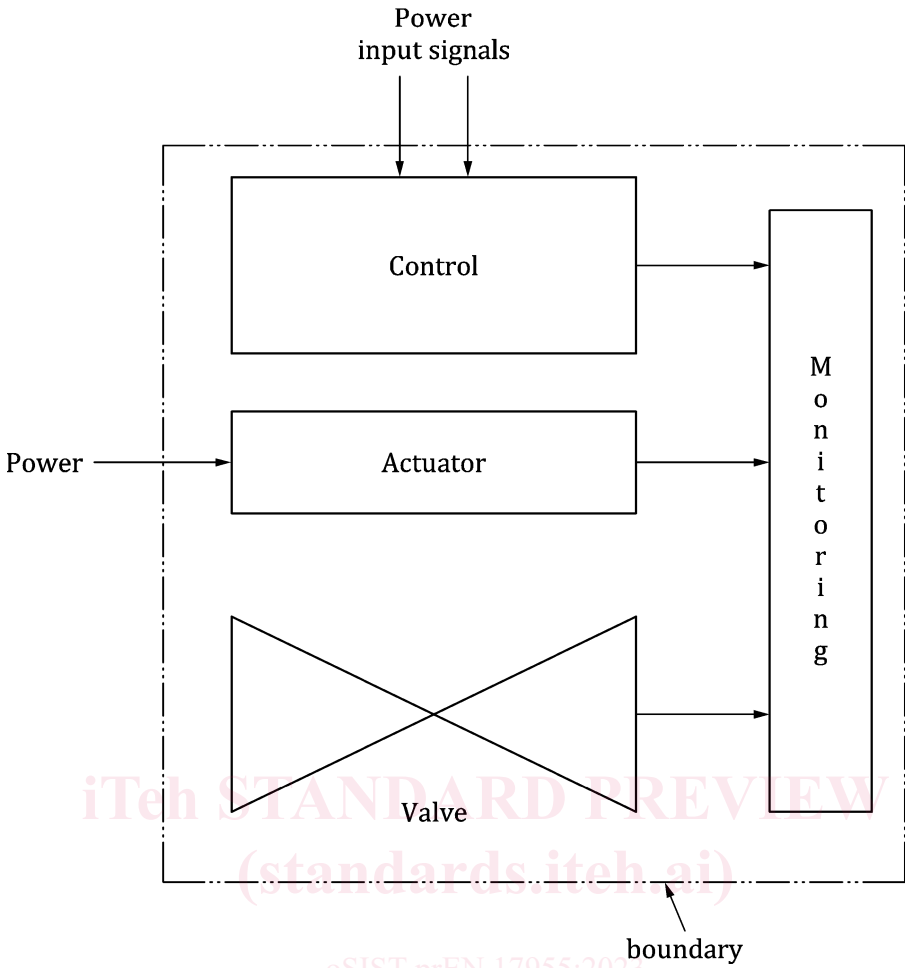

Figure 1 — Boundary definition – valves (EN ISO 14224:2016, A.2.5.4 modified)

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

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

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

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

3.6
system integrator
person or company, who combines components as a complete safety instrumented 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 instrumented 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 instrumented systems achieve the required SIL capabilities.

3.7
final element integrator
integrator of the components and parts, 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 of more components included in the final element subsystem.

3.8
end user
organisation that has overall responsibility for a process facility and its installed safety instrumented 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 instrumented system(s). The end user can outsource certain lifecycle phases or activities to sub-contractors.

3.9
utilization rate
total movements of the mechanical component 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 take into account the number of demands of the safety function per year. However, for mechanical components the primary fault mechanism largely depends on the overall number of movements of the component (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 take into account different fault mechanisms like ageing, wear and fatigue.

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

Note 4 to entry: A partial stroke is considered as a movement and is therefore taken into account 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 and not the percentage or absolute distance.

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

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

3.12
partial stroke test
PST
test method that checks if e.g. a valve is 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 component are not present and that the component 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 valves and actuators “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 component. 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 components. The test can also include electrical or electromechanical parts 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 so as 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 components are tested simultaneously.

3.13
full stroke test
FST

test method that checks if e.g. a valve is operated through its complete stroke range

Note 1 to entry: This stroke verifies that certain failure modes of the component are not present and that the component 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 component 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 performed on the complete final element, thus all relevant components are tested simultaneously.

3.14
proof test coverage
PTC
fraction of the dangerous undetected failures that can be revealed during a proof test

Note 1 to entry: The basic population for calculating the proof test coverage is the rate of dangerous failures not detected by online diagnostic tests of the component(s) under investigation. An analysis reveals the rate of dangerous undetected failures of each failure mode of each part or group of parts that can be detected by a proof test. The proof test coverage is the fraction of the dangerous undetected failures of the component (after online diagnostic tests) that can be detected by the proof test. Dangerous failures detected by online diagnostic tests, safe failures, no-part and no-effect failures are not considered in calculating the proof test coverage.

3.15
ageing
degradation process of a part or assembly of parts 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.

3.16
wear
degradation process of a part or assembly of parts that depends on the number and intensity of movements that the part 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.

3.17
fatigue
degradation process of a part that depends on the number and intensity of deformations that the part is exposed to

3.18
FIT
abbreviation for "failure in time"

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

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 1 (by cross-referencing just the main clauses). Conformity requirements for the mechanical parts of SIS final elements are indicated in the corresponding notes.

Table 1 — Relationship between EN 61508 and this document

Normative requirement from EN 61508	EN 61508 parts and clauses	Clause(s) from this document	See Notes
Documentation	Part 2: 5 (Part 1: 5)	5.2	[1]
Management of functional safety	Part 2: 6 (Part 1: 6)	5.3	[1]
E/E/PE system realization lifecycle (Phase 10), incorporating:	Part 2: 7	5.4	a
10.1 Design requirements specification	Part 2: 7.2	5.4.2	a
10.2 Validation planning	Part 2: 7.3	5.4.3	a
10.3 Design and development	Part 2: 7.4	5.4.4	a
10.4 Integration	Part 2: 7.5	5.4.5	a
10.5 Installation, commissioning, operations and maintenance procedures	Part 2: 7.6	5.4.6	b
10.6 Validation	Part 2: 7.7	5.4.7, 7, 8	a
System modification	Part 2: 7.8	5.4.9	a
System verification	Part 2: 7.9	5.5	a
Functional safety assessment	Part 2: 8 (Part 1: 8)	5.6	a
Avoidance of systematic faults	Part 2: 7.4.6	0	a c
Control of systematic faults	Part 2: 7.4.7	0	a c
Diagnostic coverage	Part 2: Annex C	10.1	d
Safety manual for compliant items	Part 2: Annex D	11, Annex E	a b

[a] For this topic EN 61508-2 is generally applicable; additional comments or specific conformity requirements that apply to mechanical parts of a SIS final element are provided in this document.

[b] Manufacturers of mechanical parts of a SIS final element are required to supply relevant information (e.g. in the safety manual) to enable others to comply fully with the cluases of EN 61508-1, −2, −4, −6 and −7.

[c] There may be other references in EN 61508-1, −2, −4, −6 and −7 for this topic that are applicable to E/E/PE technologies; additional comments or specific conformity requirements that apply to mechanical parts of a SIS final element are provided in this document.

[d] For this topic EN 61508-1, −2, −4, −6 and −7 are generally applicable; no additional requirements are provided in this document.

5 Basic requirements for development and production

5.1 Evaluation of systematic capability

The systematic capability according to EN 61508-2 can be met by achieving one of the following compliance routes:

— Route 1_S: compliance with the requirements for the avoidance of systematic faults (see 5.4.4.4) and the requirements for the control of systematic faults (see 5.4.4.5); or

— Route 2_S: compliance with the requirements for evidence that the equipment is proven in use (see EN 61508-2: 2010, 7.4.10).

In the following, the procedure for Route 1_S is described. For Route 2_S see EN 61508-2.

One aim of this document is to assess the systematic capability of the component. The systematic capability property of a component is described in EN 61508-2 and has a discrete value of 1, 2, 3 or 4. The differences between SC 1, SC 2 and SC 3 are so marginal for safety-related automated industrial valves that within this document no differentiation is necessary. SC 4 is not covered by this document.

The requirements of this document, including the requirements of 5.2 to 5.6, the checklist in Annex A and the relevant techniques and measures in Annex B shall be applied to achieve a systematic capability of SC 3. However, if one of the requirements is not met, the component shall be considered as not adequate for use in safety-related systems.

If a component that fits into the scope of this document shall be used with a SC 4, the requirements of this document for SC 3 shall be fulfilled and additional requirements of EN 61508-2 for SC 4 shall be applied.

5.2 Documentation management

The requirements of EN 61508-1:2010, Clause 5 shall be observed.

5.3 Functional safety management

The requirements of EN 61508-1:2010, Clause 6 shall be observed.

5.4 Safety lifecycle requirements for development and production of safety-related automated industrial valves

5.4.1 Objectives and requirements

5.4.1.1 General

This subclause sets out the objectives and requirements of the safety lifecycle phases for the development of safety-related automated industrial valves. It shall also be applied to other components of a final element if they have a safety statement.

For all phases of the safety lifecycle, Table 2 indicates:

— the objectives to be achieved;

— the scope of the phase;

— a reference to the subclause containing the requirements;

— the required inputs to the phase;

— the outputs required to comply with the subclause.

NOTE 1 In the safety lifecycle according to EN 61508-2, the “manufacturing” and “assembly” lifecycle phases are mentioned in the realization phase but not covered deeply. These phases, however, play a very important role in achieving a reliable and safe component. For this reason, this document also sets requirements for the lifecycle phases “manufacturing” and “assembly” that specify the requirements of EN 61508.

5.4.1.2 Objectives

The first objective of the requirements of this subclause is to structure, in a systematic manner, the phases in the safety lifecycle that shall be considered to achieve the required functional safety of the safety-related automated industrial valves.