Industrial valves - Functional safety of safety-related automated valves

EVS EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 17955:2024 sisaldab Euroopa standardi EN 17955:2024 ingliskeelset teksti.	This Estonian standard EVS-EN 17955:2024 consists of the English text of the European standard EN 17955:2024.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 07.08.2024.	Date of Availability of the European standard is 07.08.2024.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 23.060.01

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

Ref. No. EN 17955:2024 E

Contents

Page

European foreword 4
Introduction 5
1 Scope 6
2 Normative references 6
3 Terms, definitions and abbreviations 7
4 Relationship and conformity with EN 61508-1, –2, –4, –6 and –7 12
5 Basic requirements for development and production 14
5.1 Evaluation of systematic capability 14
5.2 Documentation management 14
5.3 Functional safety management 14
5.4 Safety lifecycle requirements for development and production of safety-related automated industrial valves 14
5.4.1 Objectives and requirements 14
5.4.2 Mechanical requirements specification 19
5.4.3 Mechanical validation planning 20
5.4.4 Mechanical design and development 21
5.4.5 Mechanical system integration 23
5.4.6 Mechanical system installation, commissioning, operation and maintenance procedures 24
5.4.7 Mechanical system safety validation 26
5.4.8 Production 26
5.4.9 Modification of compliant items 27
5.5 Verification 28
5.5.1 Objective 28
5.5.2 Requirements 28
5.6 Functional safety assessment 30
5.6.1 Objective 30
5.6.2 Requirements 30
6 Classification of the compliant item 30
6.1 Demand mode and utilization rate 30
6.2 Type of final element/compliant item 33
7 Field failure data 33
7.1 Field failure data analysis procedure 33
7.2 Use of field failure data for pre-existing compliant items 34
8 Qualification testing 34
8.1 General 34
8.2 Test planning/test conditions 34
8.3 Pre-conditioning of test samples 35
8.4 Cycle testing and B_{10D} values 35
8.5 Environmental testing 35
9 Determination of failure rates 35
10 Operational testing, maintenance and time restrictions 36

10.1 Online diagnostic tests **36**
10.2 Proof test **36**
10.3 Proof test coverage (PTC) **36**
10.4 Maintenance **37**
10.5 Useful lifetime **37**
10.6 Storage time **37**
11 Safety manual in addition to an installation, operation, and maintenance manual **37**
Annex A (normative) **Techniques and measures to avoid and control systematic failures** **39**
Annex B (normative) **List of failure rates for common compliant items** **46**
Annex C (normative) **FME(D)A to identify and evaluate the effects of different failure modes** **49**
C.1 FME(D)A **49**
C.2 Input information to carry out an FME(D)A **49**
C.3 FME(D)A procedure **49**
C.4 FMEDA example **52**
C.5 List of functional units and their failure rates with a low utilization rate (LUR) **54**
C.6 List of functional units and their failure rates with a high utilization rate (HUR) **56**
Annex D (informative) **Safety manual** **58**
Annex E (informative) **Examples for the evaluation of the mechanical design** **60**
E.1 General **60**
E.2 Examples **60**
E.2.1 Bolting connections **60**
E.2.2 Force-locked connections **61**
E.2.3 Form-locked connections (structural component strength) **62**
E.2.4 Springs **62**
E.2.5 Bearings **62**
E.2.6 Gears and force transmission linkages **63**
Annex F (informative) **Estimation of random failure rates with Bayesian integration between "basic" failure rates and field feedback** **64**
F.1 General **64**
F.2 Procedure **64**
F.3 Formula **65**
F.3.1 General **65**
F.3.2 Estimation of the verisimilitude factor V **66**
Bibliography **68**

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*