

DIN EN 17955:2024-11 (E)

Industrial valves - Functional safety of safety-related automated valves

| 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 B10D 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 |