# DIN EN 17955:2024-11 (D)

## Industriearmaturen - Funktionale Sicherheit sicherheitsbezogener automatisierter Industriearmaturen; Deutsche Fassung EN 17955:2024

## Inhalt

Seite


**Europäisches Vorwort** ... 9

**Einleitung** ... 10

**1 Anwendungsbereich** ... 10

**2 Normative Verweisungen** ... 11

**3 Begriffe und Abkürzungen** ... 11

**4 Zusammenhang und Übereinstimmung mit EN 61508-1, −2, −4, −6 und −7** ... 18

**5 Grundlegende Anforderungen für Entwicklung und Produktion** ... 19
**5.1 Bewertung der systematischen Eignung** ... 19
**5.2 Dokumentationsmanagement** ... 20
**5.3 Management der funktionalen Sicherheit** ... 20
**5.4 Anforderungen des Sicherheitslebenszyklus an die Entwicklung und Produktion von sicherheitsbezogenen automatisierten Industriearmaturen** ... 20
**5.4.1 Ziele und Anforderungen** ... 20
**5.4.2 Spezifikation der mechanischen Anforderungen** ... 26
**5.4.3 Planung der mechanischen Validierung** ... 27
**5.4.4 Mechanische Konstruktion und Entwicklung** ... 28
**5.4.5 Integration des mechanischen Systems** ... 31
**5.4.6 Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren des mechanischen Systems** ... 33
**5.4.7 Validierung der Sicherheit des mechanischen Systems** ... 34
**5.4.8 Produktion** ... 35
**5.4.9 Modifikation von konformen Objekten** ... 36
**5.5 Verifizierung** ... 37
**5.5.1 Ziel** ... 37
**5.5.2 Anforderungen** ... 37
**5.6 Bewertung der funktionalen Sicherheit** ... 38
**5.6.1 Ziel** ... 38
**5.6.2 Anforderungen** ... 38

**6 Klassifizierung des konformen Objekts** ... 39
**6.1 Betriebsart und Nutzungsrate** ... 39
**6.2 Typ des Stellglieds/konformen Objekts** ... 42

**7 Feldausfalldaten** ... 42
**7.1 Verfahren zur Analyse der Feldausfalldaten** ... 42
**7.2 Verwendung von Feldausfalldaten für bereits vorhandene konforme Objekte** ... 43

**8 Qualifizierungsprüfungen** ... 44
**8.1 Allgemeines** ... 44
**8.2 Prüfungsplanung/Prüfbedingungen** ... 44
**8.3 Vorkonditionierung der Prüfmuster** ... 44
**8.4 Dauerprüfung und $B_{10D}$-Werte** ... 45
**8.5 Umweltprüfungen** ... 45

**9 Bestimmung der Ausfallrate** ... 45

**10 Betriebsprüfungen, Wartung und zeitliche Beschränkungen** ... 46

10.1 Online-Diagnosetests ... 46
10.2 Wiederholungsprüfung ... 46
10.3 Deckungsgrad der Wiederholungsprüfung (PTC) ... 46
10.4 Instandhaltung ... 47
10.5 Gebrauchsdauer ... 47
10.6 Lagerzeit ... 47

11 Sicherheitshandbuch zusätzlich zu einer Installations-, Betriebs- und Wartungsanleitung ... 47

Anhang A (normativ) Verfahren und Maßnahmen zur Vermeidung und Kontrolle systematischer Ausfälle ... 50

Anhang B (normativ) Liste der Ausfallraten gängiger konformer Objekte ... 56

Anhang C (normativ) FME(D)A zur Identifizierung und Bewertung der Auswirkungen verschiedener Ausfallarten ... 60
C.1 FME(D)A ... 60
C.2 Eingabeinformationen zur Durchführung einer FME(D)A ... 60
C.3 FME(D)A-Verfahren ... 61
C.4 FMEDA-Beispiel ... 63
C.5 Liste der Funktionseinheiten und ihrer Ausfallraten bei einer niedrigen Nutzungsrate (LUR) ... 66
C.6 Liste der Funktionseinheiten und ihrer Ausfallraten bei einer hohen Nutzungsrate (HUR) ... 68

Anhang D (informativ) Sicherheitshandbuch ... 70

Anhang E (informativ) Beispiele für die Bewertung der mechanischen Konstruktion ... 72
E.1 Allgemeines ... 72
E.2 Beispiele ... 72
E.2.1 Schraubverbindungen ... 72
E.2.2 Kraftschlüssige Verbindungen ... 73
E.2.3 Formschlüssige Verbindungen (strukturelle Bauteilfestigkeit) ... 74
E.2.4 Federn ... 74
E.2.5 Lager ... 75
E.2.6 Zahnräder und Kraftübertragungsgestänge ... 75

Anhang F (informativ) Schätzung von zufälligen Ausfallraten mit Bayes‘scher Integration zwischen „grundlegenden“ Ausfallraten und Rückmeldungen aus dem Feld ... 76
F.1 Allgemeines ... 76
F.2 Verfahrensweise ... 76
F.3 Gleichung ... 77
F.3.1 Allgemeines ... 77
F.3.2 Schätzung des Plausibilitätsfaktors V ... 78

Literaturhinweise ... 80

**Bilder**

Bild 1 — Grenzdefinition — Armaturen (EN ISO 14224:2016, A.2.5.4, modifiziert) ... 15

Bild 2 — Sicherheitslebenszyklus für die Entwicklung von automatisierten Industriearmaturen ... 22

Bild F.1 — Verhältnis der Ausfallraten zwischen Federkartusche, kinematischem Mechanismus und Zylinder ... 79

**Tabellen**

**Tabelle 1 — Abkürzungen** ... **11**

**Tabelle 2 — Zusammenhang zwischen EN 61508 und diesem Dokument** ... **18**

**Tabelle 3 — Übersicht — Umsetzungsphase des Sicherheitslebenszyklus** ... **23**

**Tabelle 4 — Beziehung zwischen HFT und SIL in Bezug auf Einschränkungen hinsichtlich der Architektur für den mechanischen Teil eines Stellglieds** ... **28**

**Tabelle 5 — Beziehung zwischen Betriebsart und Nutzungsrate** ... **39**

**Tabelle 6 — Anzahl der Bestätigungen je Jahr und Nutzungsrate** ... **40**

**Tabelle A.1 — Verfahren und Maßnahmen zur Kontrolle systematischer Ausfälle, die durch die mechanische Entwicklung verursacht werden** ... **50**

**Tabelle A.2 — Verfahren und Maßnahmen zur Kontrolle systematischer Ausfälle, die durch Umweltbelastungen oder -einflüsse verursacht werden** ... **50**

**Tabelle A.3 — Verfahren und Maßnahmen zur Kontrolle systematischer Ausfälle im Betrieb** ... **51**

**Tabelle A.4 — Verfahren und Maßnahmen zur Vermeidung von Fehlern bei der Spezifikation von mechanischen Anforderungen** ... **51**

**Tabelle A.5 — Verfahren und Maßnahmen zur Vermeidung der Einbringung von Fehlern bei der mechanischen Konstruktion und Entwicklung des Systems** ... **52**

**Tabelle A.6 — Verfahren und Maßnahmen zur Vermeidung von Fehlern bei der Integration des mechanischen Systems** ... **53**

**Tabelle A.7 — Verfahren und Maßnahmen zur Vermeidung von Fehlern und Ausfällen während des Betriebs und der Wartung des Systems** ... **53**

**Tabelle A.8 — Verfahren und Maßnahmen zur Vermeidung von Fehlern bei der Sicherheitsvalidierung des mechanischen Systems** ... **54**

**Tabelle B.1 — Rate gefahrbringender Ausfälle bei Stellantrieben** ... **56**

**Tabelle B.2 — Rate gefahrbringender Ausfälle bei Getrieben** ... **57**

**Tabelle B.3 — Rate gefährlicher Ausfälle bei Armaturen** ... **57**

**Tabelle B.4 — Rate gefahrbringender Ausfälle bei Steuergeräten** ... **58**

**Tabelle C.1 — Bestimmung des O-Faktors (Beispiel)** ... **62**

**Tabelle C.2 — Bestimmung des D-Faktors (Beispiel)** ... **63**

**Tabelle C.3 — Beispiel einer FMEDA** ... **64**

**Tabelle C.4 — Liste der Funktionseinheiten und ihrer Ausfallraten bei einer niedrigen Nutzungsrate** ... **66**

**Tabelle C.5 — Liste der Funktionseinheiten und ihrer Ausfallraten bei einer hohen Nutzungsrate** ... **68**

**Tabelle D.1 — Inhalt eines typischen Sicherheitshandbuchs** ... **70**