

DIN EN 17955



ICS 23.060.01

Einsprüche bis 2023-04-03

Entwurf

**Industriearmaturen –
Funktionale Sicherheit sicherheitsbezogener Industriearmaturen und
Antriebe;
Deutsche und Englische Fassung prEN 17955:2023**

Industrial valves –
Functional safety of safety-related valves and actuators;
German and English version prEN 17955:2023

Robinetterie industrielle –
Sécurité fonctionnelle des appareils de robinetterie et actionneurs liés à la sécurité;
Version allemande et anglaise prEN 17955:2023

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-02-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an naa@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Armaturen (NAA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 150 Seiten

DIN-Normenausschuss Armaturen (NAA)

Nationales Vorwort

Dieses Dokument (prEN 17955:2023) wurde vom Technischen Komitee CEN/TC 69 „Industriearmaturen“ erarbeitet, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 003-01-01 AA „Grundnormen“ im DIN-Normenausschuss Armaturen (NAA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 281 siehe DIN ISO 281

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO 281, *Wälzlager — Dynamische Tragzahlen und nominelle Lebensdauer*

– *Entwurf* –

E DIN EN 17955:2023-03

– Leerseite –

**Industriearmaturen – Funktionale Sicherheit sicherheitsbezogener
Industriearmaturen und Antriebe**

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

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

Inhalt

	Seite
Europäisches Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	8
4 Zusammenhang und Übereinstimmung mit EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7	12
5 Grundlegende Anforderungen für Entwicklung und Produktion	13
5.1 Bewertung der systematischen Fähigkeit	13
5.2 Dokumentenmanagement	14
5.3 Funktionssicherheitsmanagement	14
5.4 Anforderungen an den Sicherheitslebenszyklus für die Entwicklung und Produktion von sicherheitsbezogenen automatisierten Industriearmaturen	14
5.4.1 Ziele und Anforderungen	14
5.4.2 Spezifikation der mechanischen Anforderungen	19
5.4.3 Planung der mechanischen Validierung	20
5.4.4 Mechanische Auslegung	21
5.4.5 Integration des mechanischen Systems	23
5.4.6 Installations-, Inbetriebnahme-, Betriebs- und Wartungsverfahren des mechanischen Systems	25
5.4.7 Validierung der Sicherheit des mechanischen Systems	26
5.4.8 Produktion	27
5.4.9 Änderung einer Komponente	28
5.5 Verifizierung	29
5.5.1 Ziel	29
5.5.2 Anforderungen	29
5.6 Funktionssicherheitsbewertung	30
5.6.1 Ziel	30
5.6.2 Anforderungen	30
6 Klassifizierung der Komponente	30
6.1 Bedarfsmodus und Nutzungsrate	30
6.2 Art des Aktors/der Komponente	34
7 Feldausfalldaten	34
7.1 Verfahren zur Analyse der Feldausfalldaten	34
7.2 Verwendung von Feldausfalldaten für bereits vorhandene Komponenten	35
8 Qualifikationsprüfungen (während der Entwicklung)	35
8.1 Allgemeines	35
8.2 Prüfungsplanung/Prüfbedingungen	36
8.3 Vorkonditionierung der Prüfproben	36
8.4 Anzahl der erforderlichen Prüfproben	36
8.5 Zyklusprüfung und B_{10D} -Werte nach EN ISO 13849-1:2015, C.4.2	36
8.6 Umweltprüfungen	37
9 Bestimmung der Ausfallhäufigkeit	37
10 Betriebsprüfungen, Wartung und zeitliche Beschränkungen	37
10.1 Online-Diagnoseprüfungen	37
10.2 Nachweisprüfung	38
10.3 Nachweisprüfungsdeckungsgrad (PTC)	38
10.4 Wartung	38
10.5 Nutzungsdauer	38
10.6 Lagerzeit	39
11 Sicherheitshandbuch zusätzlich zu einer Installations-, Betriebs- und Wartungsanleitung	39

Anhang A (normativ) Checkliste zur Bestimmung der systematischen Fähigkeit	41
Anhang B (normativ) Verfahren und Maßnahmen zur Vermeidung und Kontrolle systematischer Ausfälle	43
Anhang C (normativ) Liste der Ausfallhäufigkeit gängiger Komponenten	50
Anhang D (normativ) L FME(D)A zur Identifizierung und Bewertung der Auswirkungen verschiedener Ausfallarten	54
D.1 FME(D)A	54
D.2 Eingabeinformationen zur Durchführung einer FME(D)A	54
D.3 FME(D)A-Verfahren	55
D.4 FMEDA-Beispiel	57
D.5 Liste der Funktionseinheiten und ihrer Ausfallhäufigkeit mit einer niedrigen Nutzungsrate (LUR)	61
D.6 Liste der Funktionseinheiten und ihrer Ausfallhäufigkeit mit einer hohen Nutzungsrate (HUR)	63
Anhang E (informativ) Sicherheitshandbuch	65
Anhang F (informativ) Beispiele für die Bewertung der mechanischen Auslegung	68
F.1 Allgemeines	68
F.2 Beispiele	68
F.2.1 Schraubverbindungen	68
F.2.2 Kraftschlüssige Verbindungen	69
F.2.3 Formschlüssige Verbindungen (strukturelle Bauteilfestigkeit)	70
F.2.4 Federn	70
F.2.5 Lager	71
F.2.6 Zahnräder und Kraftübertragungsgestänge	71
Anhang G (informativ) Schätzung von zufälligen Ausfallhäufigkeiten mit Bayes'scher Integration zwischen „grundlegenden“ Ausfallhäufigkeiten und Feldrückmeldungen	72
G.1 Allgemeines	72
G.2 Verfahrensweise	72
G.3 Gleichung	73
Literaturhinweise	75

Bilder

Bild 1 — Grenzdefinition — Armaturen (EN ISO 14224:2016, A.2.5.4, modifiziert)	9
Bild 2 — Sicherheitslebenszyklus für die Auslegung von automatisierten Industriearmaturen . .	15

Tabellen

Tabelle 1 — Zusammenhang zwischen EN 61508 und diesem Dokument	12
Tabelle 2 — Übersicht — Umsetzungsphase des Sicherheitslebenszyklus	16
Tabelle 3 — Beziehung zwischen HFT und SIL in Bezug auf bauliche Beschränkungen für den mechanischen Teil eines Aktors	21
Tabelle 4 — Beziehung zwischen Bedarfsmodus und Nutzungsrate	31
Tabelle 5 — Anzahl der Einsätze im Jahr und Nutzungsrate	32
Tabelle A.1 — Checkliste zur Bestimmung der systematischen Fähigkeit (SC)	42
Tabelle B.1 — Verfahren und Maßnahmen zur Kontrolle systematischer Ausfälle, die durch die mechanische Auslegung verursacht werden	43
Tabelle B.2 — Verfahren und Maßnahmen zur Kontrolle systematischer Ausfälle, die durch Umweltbelastungen oder -einflüsse verursacht werden	44
Tabelle B.3 — Verfahren und Maßnahmen zur Kontrolle systematischer Betriebsausfälle	44
Tabelle B.4 — Verfahren und Maßnahmen zur Vermeidung von Fehlern bei der Spezifikation von mechanischen Anforderungen	45

Tabelle B.5 — Verfahren und Maßnahmen zur Vermeidung der Einbringung von Fehlern bei der mechanischen Auslegung und Entwicklung des Systems	45
Tabelle B.6 — Verfahren und Maßnahmen zur Vermeidung von Fehlern bei der Integration des mechanischen Systems	46
Tabelle B.7 — Verfahren und Maßnahmen zur Vermeidung von Fehlern und Ausfällen während des Betriebs und der Wartung des Systems	46
Tabelle B.8 — Verfahren und Maßnahmen zur Vermeidung von Fehlern bei der Sicherheitsvalidierung des mechanischen Systems	48
Tabelle C.1 — Gefahrbringende Ausfallhäufigkeiten bei Stellantrieben	50
Tabelle C.2 — Gefahrbringende Ausfallhäufigkeiten bei Getrieben	51
Tabelle C.3 — Gefährliche Ausfallhäufigkeiten bei Armaturen	51
Tabelle C.4 — Gefahrbringende Ausfallhäufigkeiten bei Steuereinrichtungen	52
Tabelle D.1 — Bestimmung des O-Faktors (Beispiel)	56
Tabelle D.2 — Bestimmung des D-Faktors (Beispiel)	56
Tabelle D.3 — Beispiel einer FMEDA	58
Tabelle D.4 — Liste der Funktionseinheiten und ihrer Ausfallhäufigkeit mit einer niedrigen Nutzungsrate	61
Tabelle D.5 — Liste der Funktionseinheiten und ihrer Ausfallhäufigkeit mit einer hohen Nutzungsrate	63
Tabelle E.1 — Inhalt eines Sicherheitshandbuchs	65

Europäisches Vorwort

Dieses Dokument (prEN 17955:2023) wurde vom Technischen Komitee CEN/TC 69 „Industriearmaturen“ erarbeitet, dessen Sekretariat von AFNOR gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Einleitung

Mechanische Komponenten wie Armaturen oder Stellantriebe sind feste Bestandteile vieler automatisierter sicherheitstechnischer Systeme. Daher ist es erforderlich, die Eignung mechanischer Komponenten innerhalb der Sicherheitsfunktionen ebenso zu bewerten wie die der elektrischen Komponenten. Dieses Dokument definiert Aspekte für die Umsetzung von Sicherheitsfunktionen mit mechanischen Komponenten. Es beschreibt Verfahren und Methoden, mit denen alle relevanten Komponenten bewertet werden können, um sie in ein sicherheitsbezogenes System zu integrieren. Es kann außerdem auf die mechanischen Bauteile einer Komponente angewendet werden, wenn sie nur teilweise aus mechanischen Bauteilen besteht.

Bei mechanischen Komponenten ist eine Trennung zwischen zufälligen und systematischen Ausfällen nicht immer möglich. Es ist ein Verfahren zur Bestimmung der Häufigkeit von zufälligen Ausfällen beschrieben. Ausfälle unbekannten Ursprungs können in die Häufigkeit von zufälligen Ausfällen einbezogen werden, da noch nicht alle Ursachen für systematische Ausfälle bekannt sind. Daher ist die Häufigkeit zufälliger Ausfälle als ungünstiger Fall zu betrachten, bei dem auch Ausfälle unbekannten Ursprungs berücksichtigt werden. Dieses Verfahren kann in Fällen verwendet werden, in denen keine eindeutige Identifizierung von Ausfallmechanismen (z. B. Ermüdung, Verschleiß oder Alterung) möglich ist. Alle anderen identifizierten systematischen Ausfälle können durch systematische Maßnahmen nach dem Grundsatz „erst qualifizieren – dann quantifizieren“ verhindert werden. Maßnahmen zur Vermeidung von systematischen Fehlern sind zum Beispiel Funktionssicherheitsmanagement, Planungsberechnung, Fertigungsüberwachung, Prüfung oder Benutzerinformationen.

Dieses Dokument richtet sich an Hersteller von Endprodukten oder deren Komponenten, um einen einheitlichen Ansatz zur Bewertung der Funktionssicherheit ihrer Komponenten zu ermöglichen. Die Komponenten werden einzeln nach den Vorgaben dieses Dokuments betrachtet. Die endgültige Kombination wird nach den Grundsätzen der Normen EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 sowie abgeleiteten Anwendungsnormen wie EN 61511-1 und EN 61508-2 bewertet.

1 Anwendungsbereich

Dieses Dokument definiert die Verfahren und Methoden, mit denen alle relevanten mechanischen Komponenten von automatisierten industriellen Armaturenpaketen, die als endgültige Elemente in einem sicherheitstechnischen System verwendet werden, nach den Grundsätzen von EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 bewertet werden können, um sie in ein sicherheitstechnisches System (en: safety instrumented system, SIS) zu integrieren. Es bietet ein Verfahren zur Bestimmung aller relevanten Faktoren, die mit dem Produkt in Verbindung stehen und die in vollem Umfang berücksichtigt werden sollten, um so den spezifischen Bedürfnissen der Anwender des Produkts gerecht zu werden.

Die grundlegende Voraussetzung für die Anwendung dieses Dokuments ist die Kenntnis der Zweckbestimmung. Dieses Dokument beschreibt ein System zur Vermeidung von systematischen Fehlern, um das angestrebte Sicherheits-Integritätslevel zu erreichen.

Dieses Dokument gilt für automatisierte industrielle Armaturenpakete, die als letzte Elemente in einem sicherheitstechnischen System verwendet werden. Er wird auf einzelne Komponenten (z. B. Armatur, Stellantrieb oder mechanische Bauteile von Magnetschaltern) oder auf Baugruppen aus mehreren dieser Komponenten und Verbindungsteilen (z. B. Getriebe, Adapter, Halterungen usw.) angewendet. Elektrische, elektronische oder programmierbare elektronische Teile müssen nach EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 bewertet werden.

Dieses Dokument gilt nicht für:

- handbetätigte Armaturen;
- Komponenten in Sicherheitssystemen oder risikomindernde Einrichtungen, die nicht nach den Grundsätzen der Funktionssicherheit bewertet und betrieben werden (z. B. automatische Sicherheitsventile wie Druckbegrenzungsventile).

Die beschriebenen Verfahren können auch für andere mechanische Komponenten in einem letzten Element des sicherheitstechnischen Systems verwendet werden, wenn die Anwendbarkeit durch entsprechendes Expertenwissen bestätigt wird (z. B. Dämpfer, Bremsen, Kupplungen).

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 61508-1:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 1: Allgemeine Anforderungen*

EN 61508-2:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

EN 61508-4, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 4: Begriffe und Abkürzungen*

EN 61508-6, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3*

EN 61508-7:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 7: Überblick über Verfahren und Maßnahmen*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 61508-4 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Bauteil

kleinste Einrichtung, die keine Baugruppe ist

Anmerkung 1 zum Begriff: Diese Teile verfügen in der Regel über keine zugehörige Sicherheitsfunktion und können nicht mit einer eigenständigen Sicherheitsanweisung versehen werden.

Anmerkung 2 zum Begriff: Typische mechanische Teile sind z.B. eine Stange, ein Lager, eine Dichtung oder eine Schraube.

3.2

Funktionseinheit

Kombination von Teilen, die eine Funktion einer Komponente ausführt oder für diese verantwortlich ist

Anmerkung 1 zum Begriff: Typische Funktionseinheiten sind z.B. Gehäuse, Batteriesatz, Sitz/Verkleidung, Federsatz oder Getriebesystem.

3.3

Komponente

Segment eines sicherheitsbezogenen Systems, dem eine sicherheitstechnische Funktion der Komponente und eine Sicherheitsanweisung zugewiesen ist, sowie ein Produkt, das von einem Hersteller in Kombination mit einer Sicherheitsanweisung (definiert in seinem Sicherheitshandbuch) für eine komponentenbezogene Sicherheitsfunktion verkauft wird

Anmerkung 1 zum Begriff: EN 61511-1 und EN 61511-2 verwenden den Begriff Einrichtung in gleicher Weise.

Anmerkung 2 zum Begriff: Eine typische mechanische Komponente kann ein Stellantrieb, ein Stellungsregler, ein Magnetschalter, ein Ventil, ein Getriebe oder ein kompletter Aktor sein, der z.B. einen Stellantrieb und eine Armatur enthält.

Anmerkung 3 zum Begriff: Eine Komponente besteht aus Bauteilen. Verschiedene Komponenten können zusammen mit Bauteilen zu einem Aktor oder sicherheitsbezogenen System zusammengesetzt werden.

Anmerkung 4 zum Begriff: Ein Verfahren zur Kombination mehrerer Komponenten ist in EN 61508-1, EN 61511-2, EN 61511-4, EN 61511-6 und EN 61511-7, EN 61511-1 und EN 61511-2 beschrieben.

3.4

Aktor

Teilsystem, das aus verschiedenen Komponenten besteht, die in einem sicherheitsbezogenen System kombiniert eingesetzt werden

Anmerkung 1 zum Begriff: Ein typischer Aktor ist in Bild 1 dargestellt.

Anmerkung 2 zum Begriff: Als Aktoren werden im Zusammenhang mit diesem Dokument in der Regel Industriearmaturen mit Stellantrieben und anderen Komponenten für den Betrieb der Armatur bezeichnet, wie z.B. Magnetschalter, Getriebe oder Stellungsregler.

Anmerkung 3 zum Begriff: Die Grenzen zwischen den verschiedenen Komponenten eines Aktors sind Teil der entsprechenden Produktnormen.

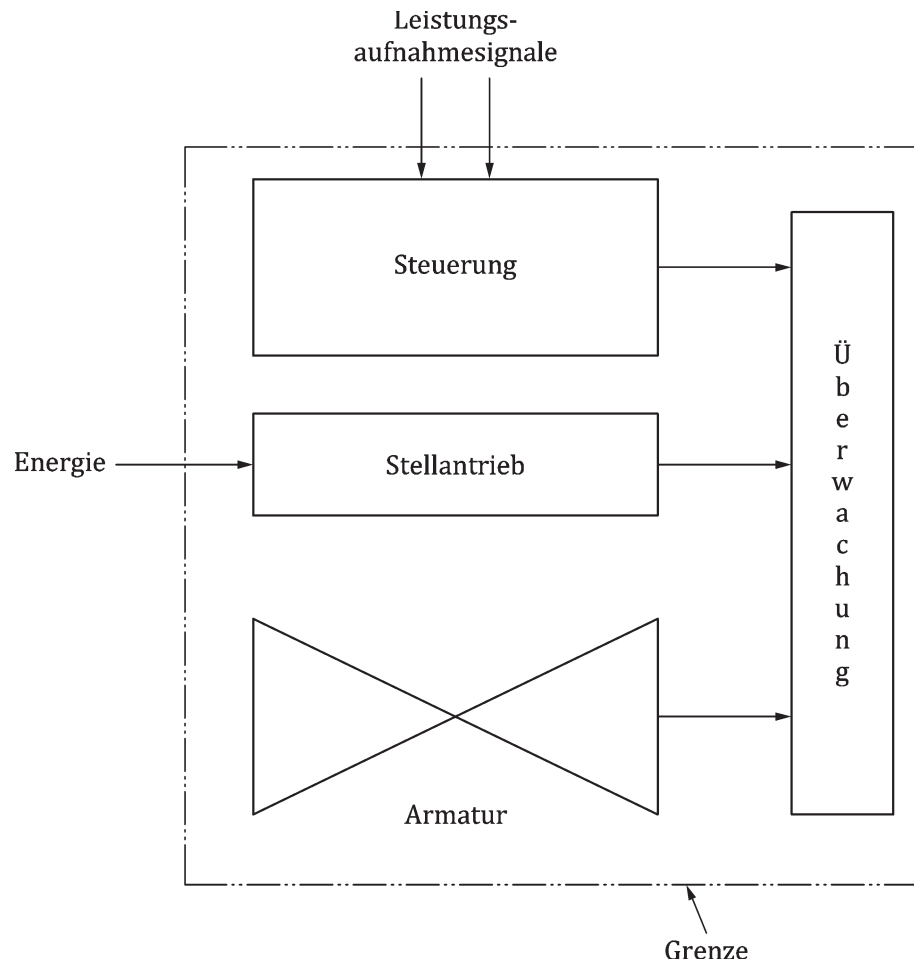


Bild 1 — Grenzdefinition — Armaturen (EN ISO 14224:2016, A.2.5.4, modifiziert)

3.5

Hersteller

jede Person oder jedes Unternehmen, die/das Komponenten oder eine Baugruppe von Komponenten gestaltet und/oder fertigt und diese Komponente oder Baugruppe unter ihrem/seinem eigenen Namen oder ihrer/seiner eigenen Marke vertreibt oder für ihren/seinen eigenen Gebrauch verwendet

Anmerkung 1 zum Begriff: Ein Hersteller kann auch ein Hersteller eines Aktors sein.

3.6

Systemintegrator

Person oder Unternehmen, die/das Komponenten zu einem kompletten sicherheitstechnischen System kombiniert, um die Funktions- und Sicherheitsanforderungen zu erfüllen

Anmerkung 1 zum Begriff: Der Systemintegrator ist verantwortlich für die (Gesamt-)Planung, für das Engineering und möglicherweise für die Installation und Inbetriebnahme kompletter sicherheitstechnischer Systeme, die nach EN 61508-1, EN 61511-2, EN 61511-4, EN 61511-6 und EN 61511-7 oder abgeleiteten Normen betrieben werden. Der Systemintegrator kann auch der Endnutzer oder ein vom Endnutzer beauftragter Dritter sein. Der Systemintegrator muss durch Verfahren und durch Dokumentation nachweisen, dass die sicherheitstechnischen Systeme die geforderten SIL-Fähigkeiten aufweisen.

3.7

Aktorintegrator

Integrator der Komponenten und Bauteile, verantwortlich für die Auslegung, den Zusammenbau und die Validierung des Teilsystems des Aktors

Anmerkung 1 zum Begriff: Der Integrator des Aktors kann auch ein Hersteller einer oder mehrerer Komponenten sein, die zum Teilsystem des Aktors gehören.

3.8

Endnutzer

Organisation, die die Gesamtverantwortung für eine verfahrenstechnische Anlage und die dort installierten sicherheitstechnischen Systeme während aller Phasen des Sicherheitslebenszyklus trägt

Anmerkung 1 zum Begriff: Dies beinhaltet, ist jedoch nicht beschränkt auf, die Verantwortung für die Planung, die Installation, die Inbetriebnahme, den Betrieb, die Wartung und die Außerbetriebsetzung des/der sicherheitstechnischen Systems/Systeme. Der Endnutzer kann bestimmte Lebenszyklusphasen oder Aktivitäten an Unterauftragnehmer auslagern.

3.9

Nutzungsrate

Gesamtzahl der Bewegungen der mechanischen Komponente je Jahr

Anmerkung 1 zum Begriff: Dazu gehören unter anderem Bewegungen aufgrund der Anforderung der Sicherheitsfunktion sowie Bewegungen aufgrund von Prüfungen (automatische Online-Diagnoseprüfungen oder manuelle Prüfungen) sowie vom Steuersystem der überwachten Einrichtung (en: equipment under control, EUC) angeforderte Betätigungen.

Anmerkung 2 zum Begriff: EN 61508-2 definiert verschiedene Betriebsarten, die lediglich die Anzahl der Anforderungen der Sicherheitsfunktion je Jahr berücksichtigen. Bei mechanischen Komponenten hängt die primäre Fehlerursache jedoch weitgehend von der Gesamtzahl der Bewegungen der Komponente ab (einschließlich Prüfungen, Anforderungen des EUC-Steuersystems usw.), und nicht nur von der Anzahl der Bewegungen aufgrund einer Anforderung an die Sicherheitsfunktion. Daher wird in diesem Dokument zusätzlich zur Betriebsart eine Nutzungsrate definiert, damit verschiedene Fehlerursachen wie Alterung, Verschleiß und Ermüdung korrekt berücksichtigt werden können.

Anmerkung 3 zum Begriff: Die Nutzungsrate verschiedener Komponenten in einer SIF oder einem Aktor kann unterschiedlich sein, z. B. wenn bestimmte, jedoch nicht alle Komponenten durch eine Vollhubprüfung geprüft werden oder wenn bestimmte Komponenten auch für die grundlegende Prozesssteuerung verwendet werden.

Anmerkung 4 zum Begriff: Ein Teilhub gilt als Bewegung und wird daher bei der Nutzungsrate berücksichtigt.

Anmerkung 5 zum Begriff: Da die Alterungseffekte eher von der Anzahl der Bewegungen als von der zurückgelegten Entfernung abhängen, ist die Anzahl der Bewegungen entscheidend und nicht der prozentuale Anteil oder die absolute Entfernung.

3.10

niedrige Nutzungsrate

LUR, en: low utilization rate

Nutzungsrate der Komponente, die so niedrig ist, dass davon ausgegangen werden kann, dass der Verschleiß keinen oder nur einen geringfügigen Einfluss auf die Ausfallhäufigkeit der Komponente hat

3.11

hohe Nutzungsrate

HUR, en: high utilization rate

Nutzungsrate der Komponente, die so hoch ist, dass davon ausgegangen werden kann, dass Verschleiß die maßgebliche Fehlerursache ist, die zum Ausfall der Komponente führt

3.12

Teilhubprüfung

PST, en: partial stroke test

Prüfverfahren, mit dem geprüft wird, ob z. B. ein Ventil über einen Teil seines gesamten Hubbereichs betrieben wird

Anmerkung 1 zum Begriff: Mit diesem kurzen Betriebshub wird bestätigt, dass bestimmte Fehlerarten der Komponente nicht vorliegen und dass die Komponente in Bezug auf diese Fehlerursachen funktionsfähig ist.

Anmerkung 2 zum Begriff: In diesem Dokument wird der Begriff „Teilhubprüfung“ verwendet, es wird jedoch anerkannt, dass für Armaturen und Stellantriebe „Teilventilhubprüfung (PVST)“ als gleichwertiger Begriff verwendet wird.

Anmerkung 3 zum Begriff: Grundsätzlich kann eine Teilhubprüfung Fehler aufgrund bestimmter Ausfallarten erkennen, ist aber nicht in der Lage, alle Ausfallarten der Komponente zu prüfen. Mit einer Teilhubprüfung eines Ventils mit Sicherheitsposition „GESCHLOSSEN“ kann beispielsweise festgestellt werden, ob ein Ventil in seiner Stellung klemmt, doch lässt sich üblicherweise nicht prüfen, ob das Ventil in der Lage ist, bis in seine Sicherheitsstellung zu verfahren oder ob es in der Schließstellung dicht abschließt. Daher wird z. B. mithilfe einer Fehlermöglichkeits- und -einflussanalyse (en: failure mode and effects analysis, FMEA) bewertet, welche Ausfallarten durch eine Teilhubprüfung in der jeweiligen Anwendung erkannt werden können bzw. nicht erkannt werden können.

Anmerkung 4 zum Begriff: Eine PST wird meist zur Prüfung von mechanischen, pneumatischen oder hydraulischen Komponenten verwendet. Die Prüfung kann auch elektrische oder elektromechanische Bauteile umfassen, z. B. ein Relais, das für den Betrieb des Stellantriebs einer geprüften Armatur verwendet wird.

Anmerkung 5 zum Begriff: Der begrenzte Hub bei der Prüfung ist so kurz vorgesehen, dass keine (oder nur minimale) Beeinträchtigungen des Betriebsablaufs der überwachten Einrichtung (EUC) auftreten. Es wird empfohlen, zu prüfen, ob der Einfluss auf den grundlegenden Prozess vertretbar ist.

Anmerkung 6 zum Begriff: Eine PST wird üblicherweise an dem kompletten Aktor durchgeführt, so dass alle relevanten Komponenten gleichzeitig geprüft werden.

3.13

Vollhubprüfung

FST, en: full stroke test

Prüfverfahren, mit dem geprüft wird, ob z. B. ein Ventil über seinen gesamten Hubbereich betrieben wird

Anmerkung 1 zum Begriff: Mit diesem Hub wird bestätigt, dass bestimmte Fehlerarten der Komponente nicht vorliegen und dass die Komponente in Bezug auf diese Fehlerursachen funktionsfähig ist.

Anmerkung 2 zum Begriff: Grundsätzlich kann eine Vollhubprüfung mehr Fehler an der Komponente aufdecken als eine Teilhubprüfung, jedoch nicht alle. Mit einer Vollhubprüfung eines Ventils mit der Sicherheitsposition „geschlossen“ kann beispielsweise bestätigt werden, dass ein Ventil nicht in seiner Stellung klemmt und in der Lage ist, bis in seine Sicherheitsstellung zu verfahren, jedoch kann ohne zusätzliche Mittel nicht geprüft werden, ob das Ventil in der Schließstellung dicht abschließt. Daher wird z. B. mithilfe einer Fehlermöglichkeits- und einflussanalyse (en: failure mode and effects analysis, FMEA) bewertet, welche Ausfallarten durch eine Vollhubprüfung in der jeweiligen Anwendung erkannt werden können bzw. nicht erkannt werden können.

Anmerkung 3 zum Begriff: Wie eine PST wird die FST am kompletten Aktor durchgeführt, so dass alle relevanten Komponenten gleichzeitig geprüft werden.

3.14

Nachweisprüfungsdeckungsgrad

PTC, en: proof test coverage

Anteil der gefahrbringenden unentdeckten Ausfälle, die bei einer Nachweisprüfung aufgedeckt werden können

Anmerkung 1 zum Begriff: Die Grundgesamtheit für die Berechnung des Nachweisprüfungsdeckungsgrads ist die Anzahl der gefahrbringenden Ausfälle, die nicht durch Online-Diagnoseprüfungen der untersuchten Komponente(n)

entdeckt wurden. Eine Analyse gibt Aufschluss über die Anzahl der gefahrbringenden, unentdeckten Ausfälle jeder Ausfallart eines jeden Bauteils oder einer Gruppe von Bauteilen, die durch eine Nachweisprüfung aufgedeckt werden können. Der Nachweisprüfungsdeckungsgrad ist der Anteil der gefahrbringenden, unentdeckten Ausfälle der Komponente (nach Online-Diagnoseprüfungen), die durch die Nachweisprüfung aufgedeckt werden können. Gefahrbringende Ausfälle, die durch Online-Diagnoseprüfungen entdeckt werden, sichere Ausfälle, Ausfälle ohne Bauteil und ohne Auswirkungen werden bei der Berechnung des Nachweisprüfungsdeckungsgrads nicht berücksichtigt.

3.15

Alterung

Degradierungsprozess eines Bauteils oder einer Baugruppe von Bauteilen, der abhängig von der vergangenen Zeit ist

Anmerkung 1 zum Begriff: Dies steht im Gegensatz zu Degradierungsprozessen, die von der Anzahl der ausgeführten Bewegungen abhängen („Verschleiß“). Bei Fehlern, die auf Ermüdung zurückzuführen sind, muss geprüft werden, ob die Ursache Alterung oder Verschleiß ist, wie in diesem Dokument definiert.

3.16

Verschleiß

Degradierungsprozess eines Bauteils oder einer Baugruppe von Bauteilen, der von der Anzahl und Intensität der Bewegungen abhängt, denen das Bauteil ausgesetzt ist

Anmerkung 1 zum Begriff: Dies steht im Gegensatz zu Degradierungsprozessen, die von der vergangenen Zeit abhängen („Alterung“). Bei Fehlern, die auf Ermüdung zurückzuführen sind, muss geprüft werden, ob die Ursache Alterung oder Verschleiß ist, wie in diesem Dokument definiert.

3.17

Ermüdung

Degradierungsprozess eines Bauteils, der von der Anzahl und Intensität der Verformungen abhängt, denen das Bauteil ausgesetzt ist

3.18

FIT

Abkürzung für „failure in time“ (Ausfälle je Zeiteinheit)

Anmerkung 1 zum Begriff: 1 FIT = 10^{-9} /h.

4 Zusammenhang und Übereinstimmung mit EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7

Der Zweck dieses Dokuments besteht nicht darin, geltende Anforderungen der Normenreihe EN 61508 zu ersetzen. Der Zusammenhang zwischen diesem Dokument und EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 ist in Tabelle 1 dargestellt (durch Querverweise nur auf die Hauptabschnitte). Die Konformitätsanforderungen für die mechanischen Bauteile der SIS-Aktoren sind in den entsprechenden Anmerkungen angegeben.

Tabelle 1 — Zusammenhang zwischen EN 61508 und diesem Dokument

Normative Anforderung aus EN 61508	Teile und Abschnitte von EN 61508	Abschnitt(e) aus diesem Dokument	Siehe Anmerkungen
Dokumentation	Teil 2: 5 (Teil 1: 5)	5.2	[1]
Management der funktionalen Sicherheit	Teil 2: 6 (Teil 1: 6)	5.3	[1]
Realisierungslebenszyklus des E/E/PE-Systems (Phase 10), einschließlich:	Teil 2: 7	5.4	a
10.1 Spezifikation der Auslegungsanforderungen	Teil 2: 7.2	5.4.2	a

Tabelle 1 (fortgesetzt)

Normative Anforderung aus EN 61508	Teile und Abschnitte von EN 61508	Abschnitt(e) aus diesem Dokument	Siehe Anmerkungen
10.2 Validierungsplanung	Teil 2: 7.3	5.4.3	a
10.3 Auslegung und Entwicklung	Teil 2: 7.4	5.4.4	a
10.4 Integration	Teil 2: 7.5	5.4.5	a
10.5 Installations-, Inbetriebnahme-, Betriebs- und Wartungsverfahren	Teil 2: 7.6	5.4.6	b
10.6 Validierung	Teil 2: 7.7	5.4.7, 7, 8	a
Systemänderung	Teil 2: 7.8	5.4.9	a
Systemverifizierung	Teil 2: 7.9	5.5	a
Funktionssicherheitsbewertung	Teil 2: 8 (Teil 1: 8)	5.6	a
Vermeidung systematischer Fehler	Teil 2: 7.4.6	0	a,c
Kontrolle systematischer Fehler	Teil 2: 7.4.7	0	a,c
Diagnosedeckungsgrad	Teil 2: Anhang C	10.1	d
Sicherheitshandbuch für konforme Objekte	Teil 2: Anhang D	11, Anhang E	a,b
^a Für dieses Thema ist EN 61508-2 allgemein anwendbar; zusätzliche Bemerkungen oder spezifische Konformitätsanforderungen, die für mechanische Bauteile eines SIS-Aktors gelten, sind in diesem Dokument enthalten. ^b Hersteller von mechanischen Bauteilen eines SIS-Aktors müssen relevante Informationen (z. B. im Sicherheitshandbuch) bereitstellen, damit andere Personen die Abschnitte von EN 61508-1, -2, -4, -6 und -7 vollständig einhalten können. ^c Es kann weitere Verweisungen in EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 zu diesem Thema geben, die auf E/E/PE-Technologien anwendbar sind; zusätzliche Bemerkungen oder spezifische Konformitätsanforderungen, die für mechanische Bauteile eines SIS-Aktors gelten, sind in diesem Dokument enthalten. ^d Für dieses Thema sind EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 allgemein anwendbar; in diesem Dokument werden keine zusätzlichen Anforderungen gestellt.			

5 Grundlegende Anforderungen für Entwicklung und Produktion

5.1 Bewertung der systematischen Fähigkeit

Die systematische Fähigkeit (en: systematic capability, SC) nach EN 61508-2 kann durch eine der folgenden Vorgehensweisen zur Erfüllung der Konformitätsanforderungen erreicht werden:

- Vorgehensweise 1_S: Einhaltung der Anforderungen zur Vermeidung systematischer Fehler (siehe 5.4.4.4) und der Anforderungen zur Kontrolle von systematischen Fehlern (siehe 5.4.4.5); oder
- Vorgehensweise 2_S: Einhaltung der Anforderungen für den Nachweis, dass sich die Einrichtung im Betrieb bewährt hat (siehe EN 61508-2: 2010, 7.4.10).

Im Folgenden wird das Verfahren für Vorgehensweise 1_S beschrieben. Für Vorgehensweise 2_S siehe EN 61508-2.

Ein Ziel dieses Dokuments ist die Bewertung der systematischen Fähigkeit der Komponente. Die Eigenschaft der systematischen Fähigkeit einer Komponente ist in EN 61508-2 beschrieben und hat einen diskreten Wert von 1, 2, 3 oder 4. Die Unterschiede zwischen SC 1, SC 2 und SC 3 sind bei sicherheitsbezogenen automatisierten Industriearmaturen so gering, dass im Rahmen dieses Dokuments keine Differenzierung erforderlich ist. SC 4 ist nicht Gegenstand dieses Dokuments.

Die Anforderungen dieses Dokuments, einschließlich der Anforderungen von 5.2 bis 5.6, die Checkliste in Anhang A und die relevanten Verfahren und Maßnahmen in Anhang B müssen angewendet werden, um eine systematische Fähigkeit von SC 3 zu erreichen. Wenn jedoch eine der Anforderungen nicht erfüllt ist, muss die Komponente als nicht geeignet für die Verwendung in sicherheitsbezogenen Systemen gelten.

Wenn eine Komponente, die in den Anwendungsbereich dieses Dokuments passt, mit SC 4 verwendet werden soll, müssen die Anforderungen dieses Dokuments für SC 3 erfüllt werden und es müssen zusätzliche Anforderungen nach EN 61508-2 für SC 4 angewendet werden.

5.2 Dokumentenmanagement

Es müssen die Anforderungen nach EN 61508-1:2010, Abschnitt 5 beachtet werden.

5.3 Funktionssicherheitsmanagement

Es müssen die Anforderungen nach EN 61508-1:2010, Abschnitt 6 beachtet werden.

5.4 Anforderungen an den Sicherheitslebenszyklus für die Entwicklung und Produktion von sicherheitsbezogenen automatisierten Industriearmaturen

5.4.1 Ziele und Anforderungen

5.4.1.1 Allgemeines

In diesem Unterabschnitt sind die Ziele und Anforderungen der Phasen des Sicherheitslebenszyklus für die Entwicklung von sicherheitsbezogenen automatisierten Industriearmaturen festgelegt. Sie muss auch auf andere Komponenten von Aktoren angewendet werden, wenn für diese eine Sicherheitsanweisung gilt.

Tabelle 2 gibt für alle Phasen des Sicherheitslebenszyklus Folgendes an:

- die zu erreichenden Ziele;
- den Umfang der Phase;
- eine Verweisung auf den Unterabschnitt, der die Anforderungen enthält;
- die erforderlichen Eingaben für die Phase;
- die Ausgaben, die erforderlich sind, um die Anforderungen des Unterabschnitts zu erfüllen.

ANMERKUNG Im Sicherheitslebenszyklus nach EN 61508-2 werden die Lebenszyklusphasen „Herstellung“ und „Zusammenbau“ zwar in der Umsetzungsphase erwähnt, aber nicht ausführlich beschrieben. Diese Phasen spielen jedoch eine entscheidende Rolle bei der Herstellung eines zuverlässigen und sicheren Bauteils. Aus diesem Grund legt dieses Dokument auch Anforderungen für die Lebenszyklusphasen „Herstellung“ und „Zusammenbau“ fest, die die Anforderungen von EN 61508 präzisieren.

5.4.1.2 Ziele

Das erste Ziel der Anforderungen dieses Unterabschnitts ist die systematische Strukturierung der Phasen im Sicherheitslebenszyklus, die berücksichtigt werden müssen, um die erforderliche Funktionssicherheit der sicherheitsbezogenen automatisierten Industriearmaturen zu erreichen.

Das zweite Ziel der Anforderungen dieses Unterabschnitts ist die Dokumentation aller Informationen, die für die Sicherstellung der Funktionssicherheit der sicherheitsbezogenen automatisierten Industriearmaturen während des gesamten Sicherheitslebenszyklus relevant sind.

Der Lebenszyklus entspricht der Phase 10 des gesamten Sicherheitslebenszyklus aus EN 61508-1:2010, Bild 2 und basiert auf dem Lebenszyklus der Systemsicherheit in EN 61508-2:2010, Bild 2.

5.4.1.3 Anforderungen

Der Sicherheitslebenszyklus der automatisierten Industriearmaturen, der bei der Erklärung der Konformität mit diesem Dokument verwendet werden muss, ist in Bild 2 festgelegt.

Wenn ein anderer Sicherheitslebenszyklus für die Entwicklung der automatisierten Industriearmaturen verwendet wird, muss dieser als Teil der Aktivitäten zum Management der Funktionssicherheit festgelegt werden und alle Ziele und Anforderungen jedes Unterabschnitts in diesem Dokument müssen erfüllt werden.

Die Verfahren für das Management der Funktionssicherheit nach EN 61508-1:2010, Abschnitt 6 müssen parallel zu den Phasen des Sicherheitslebenszyklus ablaufen.

Jede Phase des Sicherheitslebenszyklus muss in einzelne Aktivitäten unterteilt werden, wobei Anwendungsbereich, Eingaben und Ausgaben für jede Phase festgelegt werden (siehe Tabelle 2).

Die Ausgaben jeder Phase des Sicherheitslebenszyklus müssen dokumentiert werden.

Die Ausgaben jeder Phase des Sicherheitslebenszyklus müssen die für jede Phase festgelegten Ziele und Anforderungen erfüllen (siehe Tabelle 2).

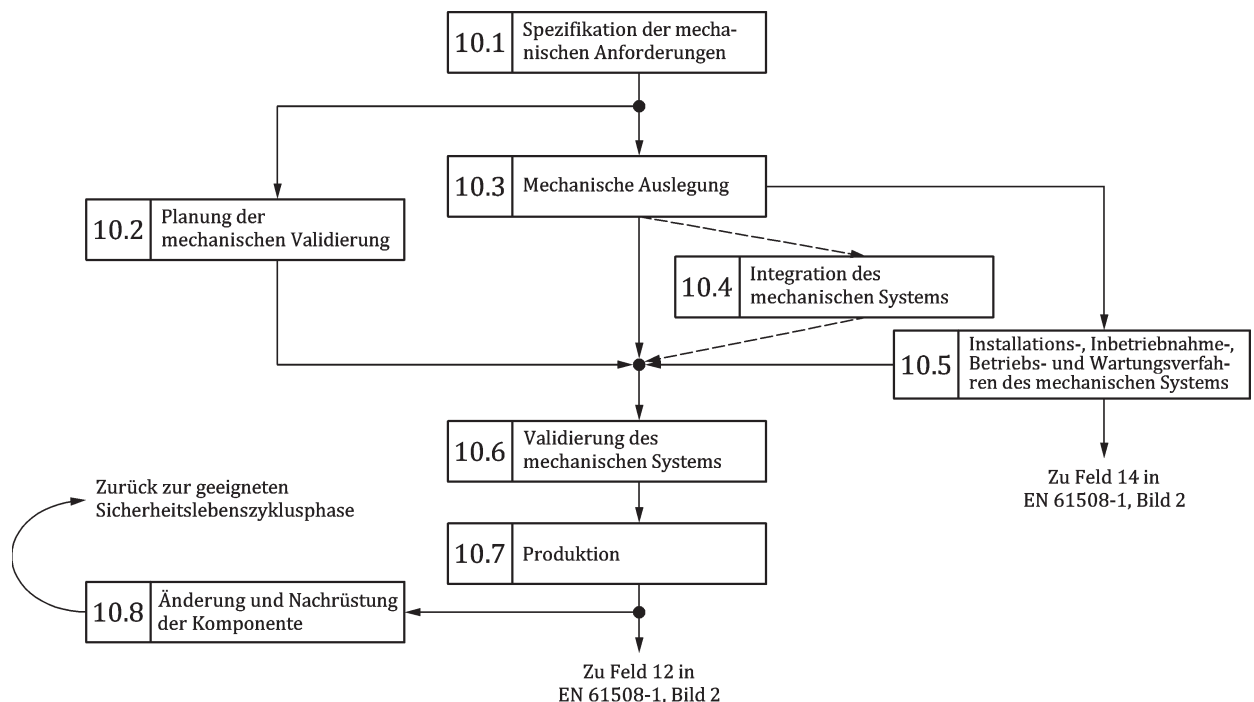


Bild 2 — Sicherheitslebenszyklus für die Auslegung von automatisierten Industriearmaturen

- Entwurf -

Tabelle 2 — Übersicht — Umsetzungsphase des Sicherheitslebenszyklus

Phase oder Aktivität des Sicherheitslebenszyklus		Ziele	Anforderungen	Eingaben	Ausgaben
Feld-nummer Bild 2	Titel		Unterabschnitt		
1	Spezifikation der mechanischen Anforderungen	Festlegen der Anforderungen an automatisierte Industriearmaturen im Hinblick auf die erforderlichen Sicherheitsfunktionen und die erforderliche Sicherheitsintegrität, um die erforderliche Funktionssicherheit zu erreichen.	5.4.2	Beispielsweise Marktspezifikation	Spezifikation der Sicherheitsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen
2	Planung der mechanischen Validierung	Planung der Validierung der Sicherheit der sicherheitsbezogenen automatisierten Industriearmaturen	5.4.3	Sicherheitsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen	Plan für die Sicherheitsvalidierung der sicherheitsbezogenen automatisierten Industriearmaturen.
3	Mechanische Auslegung	Planung der sicherheitsbezogenen automatisierten Industriearmaturen zur Erfüllung der Anforderungen an die Sicherheitsfunktionen und die Sicherheitsintegrität	5.4.4	Sicherheitsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen	Auslegung der sicherheitsbezogenen automatisierten Industriearmaturen in Übereinstimmung mit den Auslegungsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen; Plan für die Prüfung der sicherheitsbezogenen Integration von automatisierten Industriearmaturen.

- Entwurf -

Tabelle 2 (fortgesetzt)

Phase oder Aktivität des Sicherheitslebenszyklus		Ziele	Anforderungen	Eingaben	Ausgaben
Feld-nummer Bild 2	Titel		Unterabschnitt		
4	Integration des mechanischen Systems	Integration und Prüfung der sicherheitsbezogenen automatisierten Industriearmaturen	5.4.5	Auslegung sicherheitsbezogener automatisierter Industriearmaturen Integrationsprüfplan für sicherheitsbezogene automatisierte Industriearmaturen	Vollständig funktionierende sicherheitsbezogene automatisierte Industriearmaturen in Übereinstimmung mit der Auslegung Ergebnisse der Integrationsprüfungen
5	Installations-, Inbetriebnahme-, Betriebs- und Wartungsverfahren des mechanischen Systems	Entwicklung von Verfahren, mit denen sichergestellt wird, dass die Funktionssicherheit der sicherheitsbezogenen automatisierten Industriearmaturen während der Installation, der Inbetriebnahme, des Betriebs und der Wartung aufrechterhalten wird	5.4.6	Sicherheitsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen Auslegung sicherheitsbezogener automatisierter Industriearmaturen	Betriebs- und Wartungsverfahren für sicherheitsbezogene automatisierte Industriearmaturen
6	Validierung der Sicherheit des mechanischen Systems	Validierung, dass die sicherheitsbezogenen automatisierten Industriearmaturen in jeder Hinsicht die Anforderungen an die Sicherheit in Bezug auf die erforderlichen Sicherheitsfunktionen und die erforderliche Sicherheitsintegrität erfüllen	5.4.7	Sicherheitsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen Plan für die Sicherheitsvalidierung der sicherheitsbezogenen automatisierten Industriearmaturen	Vollständig sicherheitsvalidierte sicherheitsbezogene automatisierte Industriearmaturen Ergebnisse der Validierung der sicherheitsbezogenen automatisierten Industriearmaturen

- Entwurf -

Tabelle 2 (fortgesetzt)

Phase oder Aktivität des Sicherheitslebenszyklus		Ziele	Anforderungen	Eingaben	Ausgaben
Feld-nummer Bild 2	Titel		Unterabschnitt		
7	Produktion	Entwicklung und Aufrechterhaltung eines Produktionsprozesses für sicherheitsbezogene automatisierte Industriearmaturen	5.4.8	Spezifizierung der Anforderungen in Bezug auf die Produktion	Implementierung eines Produktionsverfahrens für sicherheitsbezogene automatisierte Industriearmaturen
8	Änderung einer Komponente	Sicherstellung der erforderlichen Sicherheitsintegrität nach Korrekturen, Ergänzungen oder Anpassungen an den sicherheitsbezogenen automatisierten Industriearmaturen	5.4.9	Sicherheitsanforderungen für sicherheitsbezogene automatisierte Industriearmaturen	Ergebnisse der sicherheitsbezogenen Änderung automatisierter Industriearmaturen

5.4.2 Spezifikation der mechanischen Anforderungen

5.4.2.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Festlegung der Anforderungen an die sicherheitsbezogenen automatisierten Industriearmaturen im Hinblick auf die erforderliche Funktion und die erforderliche Sicherheitsintegrität, um die erforderliche Funktionssicherheit zu erreichen.

ANMERKUNG Die Spezifikation der mechanischen Anforderungen kann auf der Grundlage eines bestehenden Spezifikationsblattes, einer Spezifikation der funktionalen Anforderungen und der Beschreibung der Zweckbestimmung und der Sicherheitsfunktion(en) erstellt werden.

5.4.2.2 Allgemeine Anforderungen

Die Sicherheitsanforderungen für die sicherheitsbezogenen automatisierten Industriearmaturen müssen so formuliert und strukturiert werden, dass sie:

- klar, präzise, eindeutig, unmissverständlich, verifizierbar, prüfbar, wartbar und durchführbar sind; und
- für Personen, die die Informationen in jeder Phase des Sicherheitslebenszyklus wahrscheinlich nutzen werden, verständlich sind.

Die Spezifikation der Anforderungen an die sicherheitsbezogenen automatisierten Industriearmaturen muss die Anforderungen an die Sicherheitsfunktion und die Anforderungen an die Sicherheitsintegrität umfassen.

5.4.2.3 Anforderungen

Die Spezifikation der mechanischen Anforderungen muss Folgendes enthalten:

- eine Beschreibung der Sicherheitsfunktionen und ihrer Eignung für die Sicherheits-Integritätslevels, die erforderlich sind, um die geforderte Funktionssicherheit zu erreichen, die:
 - umfassende detaillierte Anforderungen enthalten muss, die für die Auslegung und Entwicklung der sicherheitsbezogenen automatisierten Industriearmaturen ausreichend sind,
 - die Beschreibung des sicheren Zustands der sicherheitsbezogenen automatisierten Industriearmaturen umfassen muss,
 - festlegen muss, ob die sicherheitsbezogenen automatisierten Industriearmaturen in Betriebsarten mit geringer Belastung oder mit hoher Belastung bzw. dauerhaft und mit niedriger oder hoher Nutzungsrate betrieben werden können;
- Ansprechzeit;
- Bedienerchnittstellen, die zum Erreichen der erforderlichen Funktionssicherheit erforderlich sind;
- alle Schnittstellen zwischen den sicherheitsbezogenen automatisierten Industriearmaturen und jedem anderen System;
- Vorbereitung für den Gebrauch, einschließlich Einstellung und Anpassung;
- Inbetriebnahme, automatischer, manueller, halbautomatischer, stationärer Betrieb;
- stationärer Betrieb bei Nichtbetätigung, Neueinstellung, Abschaltung, Wartung;
- vernünftigerweise vorhersehbare anormale Bedingungen;

- Analyse des ungünstigsten Falls für die sicherheitsbezogenen automatisierten Industriearmaturen (z. B. zeitliche Beschränkungen, Umgebungsbedingungen);
- alle spezifischen Anforderungen im Zusammenhang mit den Verfahren für die Inbetriebnahme und Wiederinbetriebnahme der sicherheitsbezogenen automatisierten Industriearmaturen;
- die extremen Umgebungsbedingungen, die bei Herstellung, Lagerung, Transport, Prüfung, Installation, Inbetriebnahme, Betrieb und Wartung auftreten können;
- die Anforderungen, Einschränkungen, Funktionen und Prüfeinrichtungen, um die Nachweisprüfung der automatisierten Industriearmaturen zu ermöglichen.

Um Fehler bei der Spezifikation der mechanischen Anforderungen zu vermeiden, müssen die Verfahren und Maßnahmen nach Tabelle B.4 und Tabelle B.5 angewendet werden.

5.4.3 Planung der mechanischen Validierung

5.4.3.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Planung der Validierung der sicherheitsbezogenen automatisierten Industriearmaturen.

ANMERKUNG Die Planung der mechanischen Validierung kann auf der Grundlage des Spezifikationsblattes und der Prüfspezifikation erstellt werden.

5.4.3.2 Anforderungen

Es muss eine Planung durchgeführt werden, um die Schritte (sowohl verfahrenstechnisch als auch technisch) festzulegen, mit denen nachgewiesen werden muss, dass die sicherheitsbezogenen automatisierten Industriearmaturen die Spezifikation der mechanischen Anforderungen einhalten (siehe 5.4.2).

Bei der Planung der Validierung der sicherheitsbezogenen automatisierten Industriearmaturen muss Folgendes berücksichtigt werden:

- Spezifikation der relevanten Betriebsarten der sicherheitsbezogenen automatisierten Industriearmaturen, einschließlich:
 - Vorbereitung für den Gebrauch, einschließlich Einstellung und Anpassung,
 - Inbetriebnahme, automatischer, manueller, halbautomatischer, stationärer Betrieb,
 - stationärer Betrieb bei Nichtbetätigung, Neueinstellung, Abschaltung, Wartung;
- vernünftigerweise vorhersehbare anormale Bedingungen;
- Verweis (Rückverfolgbarkeit) auf die Spezifikation der mechanischen Anforderungen;
- die Verfahren, die zur Validierung der korrekten Umsetzung der Sicherheitsfunktion des sicherheitsbezogenen automatisierten Industriearmatur angewendet werden müssen, sowie die Kriterien für das Bestehen/Nichtbestehen der Prüfungen;
- die Verfahren, die angewendet werden müssen, um zu validieren, dass die Sicherheitsfunktion der sicherheitsbezogenen automatisierten Industriearmaturen über die erforderliche Sicherheitsintegrität verfügt, sowie die Kriterien für das Bestehen/Nichtbestehen der Prüfungen;
- die erforderliche Umgebung, in der die Prüfung durchgeführt werden soll, einschließlich aller erforderlichen kalibrierten Werkzeuge und Einrichtungen;

- Prüfevaluationsverfahren (mit Begründungen);
- Richtlinien für die Behebung von Validierungsfehlern.

Um zu validieren, dass die mechanischen Anforderungen erfüllt sind, müssen Qualifikationsprüfungen entsprechend Abschnitt 8 durchgeführt werden.

5.4.4 Mechanische Auslegung

5.4.4.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Auslegung und Implementierung der sicherheitsrelevanten automatisierten Industriearmaturen, um die mechanischen Anforderungen zu erfüllen (siehe 5.4.2).

ANMERKUNG Die mechanische Auslegung kann auf der Grundlage der Anforderungsspezifikation, der technischen Zeichnungen, Berechnungen, Simulationen und Analysen erfolgen.

5.4.4.2 Allgemeine Anforderungen

Es muss eine Auslegung in Übereinstimmung mit der Spezifikation der mechanischen Anforderungen erstellt werden, die alle Anforderungen von 5.4.2 berücksichtigt.

Die Auslegung der sicherheitsrelevanten automatisierten Industrieventile muss alle folgenden Anforderungen erfüllen:

- die Anforderungen an die systematische Sicherheitsintegrität (systematische Fähigkeit);
- die Anforderungen zur Quantifizierung der Auswirkungen zufälliger Ausfälle (siehe Abschnitt 9).

Um die Auslegung korrekt zu analysieren, muss eine FMEA der Auslegung durchgeführt werden.

Die Anforderungen für die Verwendung von Felldrückmeldungen sind in Abschnitt 7 aufgeführt.

Die geforderte minimale Toleranz gegenüber Hardwareausfall (en: hardware failure tolerance, HFT) für den mechanischen Teil des Aktors muss Tabelle 3 entsprechen.

Tabelle 3 — Beziehung zwischen HFT und SIL in Bezug auf bauliche Beschränkungen für den mechanischen Teil eines Aktors

SIL	Minimale HFT des mechanischen Teils eines Aktors	
	Betriebsart mit geringer Belastung	Betriebsart mit hoher Belastung
1	0	0
2	0	1
3	1	1
ANMERKUNG 1 Diese Anforderung entspricht EN 61508-2:2010, 7.4.4.3 und EN 61511-1:2017, 11.4.5.		
ANMERKUNG 2 Für die Definition der Betriebsarten mit niedriger und hoher Belastung siehe EN 61508.		

Die Auslegung muss auf einer Unterteilung in Komponenten beruhen, wobei für jede Komponente eine bestimmte Auslegung und eine Reihe von Integrationsprüfungen festgelegt wird (siehe 5.4.5.2).

Wenn die erste Auslegung der sicherheitsbezogenen automatisierten Industriearmaturen abgeschlossen ist, muss eine Analyse durchgeführt werden, um festzustellen, ob ein nach vernünftigem Ermessen vorhersehbares Versagen des sicherheitsbezogenen Systems eine gefährliche Situation verursachen oder eine andere

Risikobeherrschung erforderlich machen könnte. Wenn ein vernünftigerweise vorhersehbares Versagen eine dieser Auswirkungen haben könnte, dann muss die erste Priorität darin bestehen, die Auslegung des sicherheitsbezogenen Systems zu ändern, um solche Ausfallarten zu vermeiden. Falls dies nicht möglich ist, müssen Maßnahmen ergriffen werden, um die Wahrscheinlichkeit solcher Ausfallarten zu verringern.

Für die sicherheitsbezogenen automatisierten Industriearmaturen muss ein Sicherheitshandbuch zur Verfügung gestellt werden (siehe Abschnitt 11).

5.4.4.3 Anforderungen für Nachweisprüfungen und Diagnoseprüfungen

In Übereinstimmung mit anerkannten Normen zur grundlegenden Methodik der Funktionssicherheit, wie z. B. EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7, werden Nachweisprüfungen als regelmäßige Prüfungen definiert, die durchgeführt werden, um gefahrbringende versteckte Fehler in einem SIS zu erkennen, so dass, sofern erforderlich, eine Reparatur das System in einen „neuwertigen“ Zustand oder so weit wie möglich in diesen Zustand zurückversetzen kann. Für mechanische Komponenten müssen ebenfalls regelmäßige Nachweisprüfungen nach einem schriftlichen Verfahren durchgeführt werden, um nicht erkannte Fehler aufzudecken, die verhindern, dass das SIS-Element in Übereinstimmung mit der Spezifikation der Sicherheitsanforderungen arbeitet. Typische Nachweisprüfungen für mechanische Komponenten können oft nicht alle verborgenen Fehler erkennen, so dass diese Komponenten wieder in einen „neuwertigen“ Zustand versetzt werden können. Es ist daher wichtig, den Nachweisprüfungsdeckungsgrad für die Komponenten zu bewerten (für weitere Einzelheiten siehe 10.3).

Im Hinblick auf Online-Diagnoseprüfungen dürfen häufige automatische Prüfungen (siehe 6.1 und 10.1) zur Erkennung von Fehlern bei mechanischen Komponenten aufgrund fehlender interner Diagnosemittel extern durchgeführt werden.

Empfehlungen zu Nachweisprüfungen und Online-Diagnoseprüfungen, die von Endnutzern implementiert werden sollen, müssen von den Anbietern auf der Grundlage von und in engem Zusammenhang mit den in einer FMEA ermittelten und im Sicherheitshandbuch dargestellten Informationen gegeben werden, z. B. Verschleiß-/Alterungsteile, typische Ausfallarten, wie sie für die Zweckbestimmung der Produkte vorgesehen sind. Dazu gehören Empfehlungen für die Gestaltung der Prüfungen sowie die Häufigkeit der Prüfungen und des daraus resultierenden Prüfungsdeckungsgrads (DC und PTC).

Zusätzliche Anforderungen für Nachweisprüfungen und Diagnoseprüfungen sind in 10.1, 10.2 und 10.3 definiert.

5.4.4.4 Anforderungen zur Vermeidung von systematischen Fehlern

Es muss eine geeignete Reihe von Verfahren und Maßnahmen angewendet werden, die darauf ausgelegt sind, die Einführung von Fehlern während der mechanischen Auslegung und Entwicklung der sicherheitsbezogenen automatisierten Industriearmaturen zu verhindern (siehe Tabelle B.6).

Zu diesem Zweck muss das gewählte Auslegungsverfahren über Eigenschaften verfügen, die Folgendes erleichtern:

- qualifiziertes Personal für die verschiedenen Auslegungsstufen;
- wiederholbare und rückverfolgbare Berechnungen;
- eine klare und präzise Beschreibung der Funktionalität und der Schnittstellen der Teilsysteme;
- eine klare und präzise Dokumentation für den Benutzer;
- angemessene Qualitätssicherungsprozesse.

Für die Berechnung der Teile von Druckgeräten müssen gültige Normen verwendet werden.

Andere Komponenten, die für die Übertragung von Schubkraft/Drehmoment benötigt werden, müssen nach den Regeln der guten Ingenieurspraxis konstruiert und gefertigt werden, um einen sicheren Gebrauch und angemessene Sicherheitsfaktoren sicherzustellen.

Darüber hinaus können zusätzliche Ausfälle vermieden werden, wenn bewährte Konstruktionen oder bereits verwendete Komponenten und Bauteile verwendet werden. Die Wartungsanforderungen müssen bereits in der Auslegungsphase formalisiert werden.

5.4.4.5 Anforderungen zur Kontrolle von systematischen Fehlern

Zur Kontrolle von systematischen Fehlern muss die mechanische Auslegung über Konstruktionsmerkmale verfügen, die die sicherheitsbezogenen automatisierten Industriearmaturen widerstandsfähig machen gegenüber:

- etwaige verbleibende konstruktionsbedingte Fehler in der Mechanik, es sei denn, die Möglichkeit von mechanischen Konstruktionsfehlern kann ausgeschlossen werden (siehe Tabelle B.1);
- Umweltbelastungen (siehe Tabelle B.2);
- Fehler des Bedieners (siehe Tabelle B.3).

Wartbarkeit und Prüfbarkeit müssen während der Auslegungs- und Entwicklungsaktivitäten berücksichtigt werden, um die Implementierung dieser Eigenschaften im endgültigen sicherheitsbezogenen automatisierten Industriearmaturensystem zu erleichtern.

Die Auslegung der sicherheitsbezogenen automatisierten Industriearmaturen muss die menschlichen Fähigkeiten und Einschränkungen berücksichtigen und für die den Bedienern und dem Wartungspersonal zugewiesenen Tätigkeiten geeignet sein. Die Auslegung aller Schnittstellen muss sich an den bewährten Verfahren für menschliche Faktoren orientieren und dem wahrscheinlichen Ausbildungs- oder Kenntnisstand der Bediener entsprechen.

5.4.4.6 Anforderungen für die Implementierung des Systems

Die Auslegung des Aktors muss auf einer Unterteilung in Komponenten beruhen, wobei für jede Komponente eine bestimmte Auslegung und eine Reihe von Integrationsprüfungen festgelegt wird.

Die Implementierung der sicherheitsbezogenen automatisierten Industriearmaturen muss entsprechend der Auslegung der sicherheitsbezogenen automatisierten Industriearmaturen erfolgen.

Es muss für alle Komponenten angegeben werden, ob sie sicherheitsbezogen sind oder nicht, und falls dies der Fall ist, dann zusätzlich:

- ob sie neu, bestehend oder proprietär sind; und
- ob sie vorab förmlich bewertet worden sind.

Wenn für die sicherheitsbezogenen automatisierten Industriearmaturen ein zuvor entwickeltes System oder eine Komponente – bei der es sich auch um eine genormte Komponente handeln darf – verwendet werden soll, dann muss diese eindeutig identifiziert und dokumentiert werden.

5.4.5 Integration des mechanischen Systems

5.4.5.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist es, die Kombination der mechanischen Komponenten der sicherheitsbezogenen automatisierten Industriearmaturen zu integrieren und zu prüfen.

ANMERKUNG 1 Wenn nur eine Komponente (z. B. Ventil oder Stellantrieb) hergestellt wird, kann diese Phase ausgelassen werden. Wenn zwei Komponenten (z. B. Ventil und Stellantrieb) hergestellt werden, oder eine Komponente hergestellt und eine von einem anderen Hersteller erworben wird und beide Komponenten integriert werden, kann diese Phase nicht ausgelassen werden.

ANMERKUNG 2 Das Verfahren zur Integration des mechanischen Systems kann anhand der Dokumentation der Integrationsprüfungen dokumentiert werden.

5.4.5.2 Anforderungen

Die Komponenten (z. B. Ventil, Stellantrieb) des Aktors müssen entsprechend der festgelegten mechanischen Konstruktion integriert und entsprechend den festgelegten Integrationsprüfungen geprüft werden.

Im Rahmen der Integration von Komponenten in einen Aktor muss der Aktor wie festgelegt geprüft werden. Mit diesen Prüfungen muss nachgewiesen werden, dass alle Komponenten korrekt zusammenwirken, um ihre vorgesehene Funktion zu erfüllen, und so ausgelegt sind, dass sie keine unerwünschten Funktionen ausführen.

Es muss eine angemessene Dokumentation der Integrationsprüfung des Aktors erstellt werden, in der die Prüfergebnisse und die Erfüllung der in der Auslegungs- und Entwicklungsphase festgelegten Ziele und Kriterien festgehalten werden. Im Falle eines Ausfalls müssen die Gründe für den Ausfall dokumentiert werden.

Während der Integration und Prüfung müssen alle Modifikationen oder Änderungen am Aktor einer Auswirkungsanalyse unterzogen werden, in der alle betroffenen Komponenten und die erforderlichen Aktivitäten zur erneuten Verifizierung ermittelt werden müssen.

Bei der Prüfung der Integration des mechanischen Systems müssen die folgenden Informationen dokumentiert werden:

- die Version der verwendeten Prüfspezifikation;
- die Kriterien für die Abnahme der Integrationsprüfungen;
- die Version der geprüften sicherheitsbezogenen automatisierten Industriearmaturen;
- die verwendeten Werkzeuge und Einrichtungen zusammen mit den Kalibrierungsdaten;
- die Ergebnisse der einzelnen Prüfungen;
- jegliche Abweichung zwischen erwarteten und tatsächlichen Ergebnissen;
- die durchgeführte Analyse und die Entscheidungen darüber, ob die Prüfung fortgesetzt oder eine Änderungsanforderung gestellt werden soll, falls Abweichungen auftreten.

Zur Vermeidung von Fehlern bei der Integration des mechanischen Systems müssen die Verfahren und Maßnahmen nach Tabelle B.6 angewendet werden.

Die Integrationsprüfungen müssen mindestens die folgenden Aspekte umfassen und berücksichtigen.

- Verifizierung des Zusammenbaus:
 - visuelle Verifizierung, dass die Komponenten in Übereinstimmung mit der mechanischen Auslegung zusammengebaut wurden (einschließlich Verifizierung der mechanischen Anschlüsse des Ventils/Stellantriebs);
 - Verifizierung, dass die Komponenten unter Verwendung der Auslegungswerte für das Anzugsmoment mechanisch verbunden wurden.

- Funktionsprüfungen:
 - Verifizierung der Sicherheitsfunktion, bei der das Ventil dem erforderlichen Betriebsdruck ausgesetzt ist, einschließlich:
 - Verifizierung der korrekten Bewegung einschließlich einer sichtbaren und/oder hörbaren Prüfung auf teilweises Verklemmen;
 - Verifizierung der Ansprechzeit;
 - Verifizierung der Dichtigkeit der Leitungen;
 - Verifizierung von externen Diagnoseprüfungen, z. B. Teilhubprüfung, sofern zutreffend.

Während der Funktionsprüfungen muss die Armaturenbaugruppe entsprechend der endgültigen SIS-Konfiguration ausgerichtet sein, d. h. es kann erforderlich sein, die Armatur mit einem horizontalen Schaft zu prüfen.

Vor Beginn einer Integrationsprüfung sollten die Komponenten einer vollständigen Werksabnahmeprüfung in Übereinstimmung mit den einschlägigen Produktnormen und Spezifikationen unterzogen werden.

5.4.6 Installations-, Inbetriebnahme-, Betriebs- und Wartungsverfahren des mechanischen Systems

5.4.6.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Entwicklung von Verfahren, mit denen sichergestellt wird, dass die erforderliche Funktionssicherheit der sicherheitsbezogenen automatisierten Industriearmaturen während der Installation, der Inbetriebnahme, des Betriebs und der Wartung aufrechterhalten wird.

ANMERKUNG Die Verfahren für die Installation, die Inbetriebnahme, den Betrieb und die Wartung des mechanischen Systems können auf der Grundlage der Installations-, Betriebs- und Wartungsanleitung und des Sicherheitshandbuchs dokumentiert werden.

5.4.6.2 Anforderungen

Die folgenden Anforderungen gelten direkt für Hersteller von Aktoren oder Systemintegratoren. Die Hersteller von Komponenten sollten alle relevanten Informationen in ihren Sicherheitshandbüchern bereitstellen, damit andere Personen die unten beschriebenen Verfahren vorbereiten können.

Es müssen Verfahren zur Installation, zum Betrieb und zur Wartung von sicherheitsbezogenen automatisierten Industriearmaturen erstellt werden, in denen Folgendes festgelegt ist:

- die Routinemaßnahmen, die durchgeführt werden müssen, um die Funktionssicherheit des Systems „wie ausgelegt“ zu installieren und aufrechtzuerhalten;
- die Maßnahmen und Einschränkungen, die erforderlich sind (z. B. während der Installation, der Inbetriebnahme, des Normalbetriebs, der routinemäßigen Prüfung, vorhersehbarer Störungen, Fehler oder Ausfälle und der Abschaltung), um einen unsicheren Zustand zu verhindern und/oder die Folgen eines gefährlichen Ereignisses zu mindern;
- die Dokumentation, die über Systemausfälle und Leistungsdaten von sicherheitsrelevanten automatisierten Industrieventilen geführt werden muss;
- die Dokumentation, die über die Ergebnisse von Audits und Prüfungen des sicherheitsbezogenen automatisierten Industrieventils geführt werden muss;
- die Wartungsverfahren, die beim Auftreten von Fehlern oder Ausfällen in den sicherheitsbezogenen automatisierten Industriearmaturen beachtet werden müssen, einschließlich:

- Verfahren zur Fehlerdiagnose und Reparatur;
- Verfahren zur erneuten Validierung;
- Anforderungen an die Berichterstattung bezüglich der Wartung;
- es müssen die Verfahren zur Meldung der Durchführung der Wartung festgelegt werden. Im Besonderen:
 - Verfahren zur Meldung von Ausfällen;
 - Verfahren zur Analyse von systematischen Ausfällen;
- die für die Wartung und die erneute Validierung erforderlichen Werkzeuge und die Verfahren zur Wartung der Werkzeuge und Einrichtungen.

Die Verfahren für die Installation, den Betrieb und die Wartung von sicherheitsbezogenen automatisierten Industriearmaturen müssen kontinuierlich aktualisiert werden, z. B. durch Eingaben wie:

- die Ergebnisse von Audits der Funktionssicherheit; und
- Prüfungen an den sicherheitsbezogenen automatisierten Industriearmaturen.

Zur Vermeidung von Fehlern oder Ausfällen bei der Installation, dem Betrieb und der Wartung des mechanischen Systems müssen die Verfahren und Maßnahmen nach Tabelle B.7 angewendet werden.

Der Hersteller muss die erforderlichen Informationen bereitstellen, damit der Systemintegrator und/oder der Endnutzer die Eignung der Komponente für die vorgesehene Verwendung verifizieren kann. Diese Informationen müssen Teil des Sicherheitshandbuchs sein (siehe Abschnitt 11).

5.4.7 Validierung der Sicherheit des mechanischen Systems

5.4.7.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Validierung, dass die sicherheitsbezogenen automatisierten Industriearmaturen in jeder Hinsicht die Anforderungen an die Sicherheit in Bezug auf die erforderliche Sicherheitsfunktion und die Sicherheitsintegrität erfüllen (siehe 5.4.2).

ANMERKUNG Das Verfahren zur Validierung des mechanischen Systems kann auf der Grundlage einer bestehenden Dokumentation von Prototyp-Prüfungen und der Freigabe für die Produktion dokumentiert werden.

5.4.7.2 Anforderungen

Die Validierung der sicherheitsbezogenen automatisierten Industriearmaturen muss in Übereinstimmung mit einem vorbereiteten Plan erfolgen.

Alle für die Validierung verwendeten Prüf- und Messvorrichtungen müssen nach einer Norm kalibriert werden, die auf eine nationale Norm rückführbar ist, sofern vorhanden, oder nach einem anerkannten Verfahren. Alle Prüfeinrichtungen müssen auf ihren ordnungsgemäßen Betrieb überprüft werden.

Alle in der Spezifikation der mechanischen Anforderungen (siehe 5.4.2) festgelegten Anforderungen sowie alle Verfahren für den Betrieb und die Wartung müssen durch Prüfungen und/oder Analysen validiert werden.

Es muss eine angemessene Dokumentation der Validierungsprüfung der sicherheitsbezogenen automatisierten Industriearmaturen erstellt werden, in der für die Sicherheitsfunktion(en) Folgendes angegeben:

- die Version des verwendeten Validierungsplans;
- die zu prüfende (oder zu analysierende) Sicherheitsfunktion;

- die verwendeten Werkzeuge und Einrichtungen zusammen mit den Kalibrierungsdaten;
- die Ergebnisse der einzelnen Prüfungen;
- Abweichung zwischen erwarteten und tatsächlichen Ergebnissen.

Wenn Abweichungen auftreten (d. h. die tatsächlichen Ergebnisse weichen von den erwarteten Ergebnissen um mehr als die angegebenen Toleranzen ab), müssen die Ergebnisse der Validierungsprüfung des mechanischen Systems dokumentiert werden, einschließlich:

- die durchgeführte Analyse; und
- die Entscheidung, ob die Prüfung fortgesetzt werden soll oder ob eine Änderungsanforderung gestellt werden kann und zu einem vorherigen Bauteil der Validierungsprüfung zurückgekehrt wird.

Zur Vermeidung von Fehlern bei der Validierung des mechanischen Systems müssen die Verfahren und Maßnahmen nach Tabelle B.8 angewendet werden.

5.4.8 Produktion

5.4.8.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Entwicklung und Aufrechterhaltung eines Produktionsprozesses für sicherheitsbezogene automatisierte Industriearmaturen.

ANMERKUNG Das Produktionsverfahren kann auf der Grundlage bestehender Produktionsanweisungen und abschließender Prüfverfahren dokumentiert werden.

5.4.8.2 Anforderungen

Der Produktionsprozess ist untrennbar mit einem Qualitätssystem verbunden. Der Hersteller muss ein zugelassenes Qualitätssicherungssystem für den gesamten Lebenszyklus betreiben, insbesondere für die Herstellung der betreffenden Komponenten. Alle Qualitätsmaßnahmen während des gesamten Lebenszyklus müssen einer Überwachung unterliegen.

Sämtliche vom Hersteller angewendeten Bestandteile, Anforderungen und Bestimmungen müssen in systematischer und ordentlicher Weise in Form schriftlich festgelegter Vorgehensweisen, Verfahrensabläufe und Anweisungen dokumentiert werden. Diese Qualitätssystemdokumentation muss eine einheitliche Auslegung der Qualitätsprogramme, -pläne, -handbücher und -berichte ermöglichen.

Sie muss insbesondere eine angemessene Beschreibung enthalten von

- den Qualitätszielen und der Organisationsstruktur sowie den Verantwortlichkeiten und Befugnissen des Managements in Bezug auf die Qualität der Komponente,
- den entsprechenden Herstellungs-, Qualitätskontroll- und Qualitätssicherungsverfahren, Prozessen und systematischen Handlungen, die verwendet werden können, insbesondere Verfahren, die zur permanenten Verbindung von Bauteilen verwendet werden,
- den Untersuchungen und Prüfungen, die vor, während und nach der Fertigung durchgeführt werden können, sowie der Häufigkeit, mit der sie durchgeführt werden,
- den Qualitätsaufzeichnungen, wie Inspektionsberichte und Prüfdaten, Kalibrierungsdaten, Berichte über die Qualifikation oder Zulassung des betreffenden Personals, insbesondere des Personals, das die dauerhafte Verbindung der Bauteile und die zerstörungsfreien Prüfungen vornimmt,
- den Mitteln zur Überwachung der Erreichung der geforderten Qualität und des wirksamen Betriebs des Qualitätssicherungssystems,

- der Beschaffung von Materialien und Bauteilen,
- der Prozessführung für die Herstellungs- und Montageprozesse,
- der Genehmigung von kritischen Prozessschritten,
- der Kontrolle von nicht konformen Produkten, und
- der Kommunikation zwischen allen beteiligten Abteilungen und Parteien.

ANMERKUNG Ein Qualitätssicherungssystem in Übereinstimmung mit der Richtlinie 2014/68/EU, Anhang III, 5 (Modul D) kann als ausreichend für die Erfüllung der Anforderungen angesehen werden.

5.4.9 Änderung einer Komponente

5.4.9.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Sicherstellung der geforderten Sicherheitsintegrität nach Korrekturen, Erweiterungen oder Anpassungen an den sicherheitsbezogenen automatisierten Industriearmaturen durch den Originalhersteller.

ANMERKUNG 1 Das Änderungsverfahren kann auf der Grundlage bestehender Änderungsverfahren aus dem Qualitätsmanagementsystem dokumentiert werden.

ANMERKUNG 2 Wenn die Änderung durch den Endnutzer in Phase 15 von EN 61508-1 vorgenommen wird, wird Bild 2 herangezogen.

5.4.9.2 Anforderungen

Für jede Änderungsaktivität muss eine angemessene Dokumentation erstellt und gepflegt werden. Die Dokumentation muss Folgendes enthalten:

- die detaillierte Spezifikation der Modifikation oder Änderung;
- eine Analyse der Auswirkungen der Änderungsaktivität auf das Gesamtsystem, einschließlich der menschlichen Interaktion, der Umwelt und möglicher Wechselwirkungen;
- alle Genehmigungen für Änderungen;
- Fortschritt der Änderungen;
- Prüffälle einschließlich Daten der erneuten Validierung;
- Verlauf des Konfigurationsmanagements;
- Abweichung vom Normalbetrieb und den Normalbedingungen;
- erforderliche Änderungen an den Systemverfahren; und
- erforderliche Änderungen an der Dokumentation.

Die Hersteller müssen ein System betreiben, mit dem sie (sicherheitsrelevante) Änderungen einleiten und, insbesondere bei serienmäßig hergestellten Systemen und/oder Einrichtungen, die Benutzer darüber informieren können, ob die Komponente von einem sicherheitsrelevanten Rückruf betroffen ist.

Die Änderung muss mit dem gleichen Maß an Fachwissen, automatisierten Werkzeugen, Planung und Management durchgeführt werden wie die ursprüngliche Entwicklung der sicherheitsbezogenen Systeme.

Nach der Änderung müssen die sicherheitsbezogenen automatisierten Industriearmaturen verifiziert und erneut validiert werden.

5.5 Verifizierung

5.5.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Prüfung und Bewertung der Ergebnisse einer bestimmten Phase, um die Korrektheit und Einheitlichkeit in Bezug auf die Produkte und Normen sicherzustellen, die als Eingabe für diese Phase bereitgestellt wurden.

5.5.2 Anforderungen

Die Verifizierung der sicherheitsbezogenen automatisierten Industriearmaturen muss zeitgleich mit der Entwicklung (siehe 5.4.4) für jede Phase des Sicherheitslebenszyklus geplant und dokumentiert werden.

Die Verifizierungsplanung bezieht sich auf alle Kriterien, Verfahren und Werkzeuge, die bei der Verifizierung in jeder Phase verwendet werden sollen.

Bei der Verifizierungsplanung müssen die durchzuführenden Aktivitäten festgelegt werden, um die Korrektheit und Einheitlichkeit in Bezug auf die Produkte und Normen sicherzustellen, die als Eingabe für diese Phase bereitgestellt werden.

Bei der Verifizierungsplanung muss Folgendes berücksichtigt werden:

- die Auswahl von Strategien und Verfahren zur Verifizierung;
- die Auswahl und Nutzung der Prüfeinrichtungen;
- die Auswahl und Dokumentation der Verifizierungsaktivitäten;
- die Auswertung von Verifizierungsergebnissen, die direkt von Verifizierungseinrichtungen und aus Prüfungen stammen.

In jeder Auslegungs- und Entwicklungsphase muss nachgewiesen werden, dass die Funktions- und Sicherheitsanforderungen erfüllt werden.

Das Ergebnis jeder Verifizierung muss dokumentiert werden, wobei entweder angegeben wird, dass die sicherheitsbezogenen automatisierten Industriearmaturen die Verifizierung bestanden haben, oder die Gründe für die Ausfälle angegeben werden. Folgendes ist zu berücksichtigen:

- Komponenten, die einer oder mehreren relevanten Anforderungen des Sicherheitslebenszyklus nicht entsprechen (siehe 5.4.2);
- Komponenten, die nicht mit einer oder mehreren relevanten Gestaltungsnormen übereinstimmen (siehe 5.4.4);
- Komponenten, die eine oder mehrere relevante Anforderungen an das Sicherheitsmanagement nicht erfüllen (siehe 5.3).

Bei der Verifizierung der mechanischen Anforderungen muss nach der Festlegung der mechanischen Anforderungen (siehe 5.4.2) und vor Beginn der nächsten Phase (Auslegung und Entwicklung) die Verifizierung:

- feststellen, ob die mechanischen Anforderungen ausreichen, um die bei der Sicherheitsplanung festgelegten Anforderungen an Sicherheit, Funktionalität und andere Anforderungen zu erfüllen;

- feststellen, ob die Prüfungen (siehe 5.4.4) alle mechanischen Anforderungen (siehe 5.4.2) angemessen berücksichtigen; und
- auf Inkompatibilitäten prüfen zwischen
 - den mechanischen Anforderungen (siehe 5.4.2), und
 - der mechanischen Auslegung (siehe 5.4.4).

Für die Verifizierung der mechanischen Auslegung und Entwicklung muss nach Abschluss der mechanischen Auslegung und Entwicklung (siehe 5.4.4) und vor Beginn der nächsten Phase (Integration) die Verifizierung:

- feststellen, ob die Prüfungen für die mechanische Auslegung und Entwicklung angemessen sind (siehe 5.4.4);
- die Konsistenz und Vollständigkeit der mechanischen Auslegung und Entwicklung (siehe 5.4.4) in Bezug auf die mechanischen Anforderungen (siehe 5.4.2) feststellen; und
- auf Inkompatibilitäten prüfen zwischen
 - den mechanischen Anforderungen (5.4.2),
 - der mechanischen Auslegung und Entwicklung (5.4.4), und
 - den Prüfungen.

Bei der Verifizierung der mechanischen Integration muss die Integration der sicherheitsbezogenen automatisierten Industriearmaturen verifiziert werden, um zu bestätigen, dass die Anforderungen von 5.4.5 erfüllt sind.

Es müssen die in Abschnitt 8 festgelegten Qualifikationsprüfungen durchgeführt werden.

Die Prüffälle und ihre Ergebnisse müssen dokumentiert werden.

ANMERKUNG Die Anforderungen aus Anhang B für Sicherheitsvalidierung, Fehleranalyse und Prüfverfahren gelten auch für die Verifizierung.

5.6 Funktionssicherheitsbewertung

5.6.1 Ziel

Das Ziel der Anforderungen dieses Unterabschnitts ist die Untersuchung und Beurteilung der Funktionssicherheit, die durch sicherheitsbezogene automatisierte Industriearmaturen erreicht wird.

5.6.2 Anforderungen

Es müssen die Anforderungen nach EN 61508-1:2010, Abschnitt 8 beachtet werden.

6 Klassifizierung der Komponente

6.1 Bedarfsmodus und Nutzungsrate

EN 61508-2 definiert für die Sicherheitsfunktion eine Betriebsart mit niedrigem Bedarf, eine mit hohem Bedarf und eine dauerhafte Betriebsart. Diese Definitionen für die Betriebsart der Sicherheitsfunktion werden auch in diesem Dokument verwendet.

Neben dem Betrieb aufgrund einer Anforderung an die Sicherheitsfunktion können zusätzliche Bewegungen von Komponenten eines SIS auftreten. Diese können auf Online-Diagnoseprüfungen wie eine PST, Nachweisprüfungen oder Befehle des EUC-Steuersystems zurückzuführen sein. Daher kann die Gesamtzahl der Bewegungen einer Komponente eines SIS jährlich erheblich von der Anzahl der Anforderungen abweichen, die das SIS anfordern kann.

Die häufigsten Fehlerursachen bei mechanischen Komponenten sind entweder Alterung, Verschleiß oder Ermüdung. Bei diesen Fehlerursachen ist die Gesamtzahl der jährlichen Bewegungen der entscheidende Faktor und nicht die Anzahl der Anforderungen durch das Sicherheitssystem.

Daher wird in diesem Dokument zusätzlich zwischen einer hohen und einer niedrigen Nutzungsrate unterschieden.

Die Nutzungsrate ist immer eine Eigenschaft einer einzelnen Komponente eines SIS und kann für verschiedene Komponenten innerhalb desselben SIS abweichen, während der Bedarfsmodus eine Eigenschaft des SIF als Ganzes ist und somit für alle im SIF verwendeten Komponenten identisch ist. In Tabelle 4 sind die wichtigsten Fälle und Unterschiede aufgeführt.

Tabelle 4 — Beziehung zwischen Bedarfsmodus und Nutzungsrate

Bedarfsmodus	Hoch	Hoch	Niedrig	Niedrig
Nutzungsrate	Hoch	Niedrig	Hoch	Niedrig
Anforderungen an die Sicherheitsfunktion/Jahr	> 1	> 1	≤ 1	≤ 1
Gesamtzahl der Bewegungen je Jahr	viele ^a	wenige ^a	viele ^a	wenige ^a
Hauptfehlerursache für mechanische Komponenten	Verschleiß	Alterung	Verschleiß	Alterung
Anwendungsbeispiel	Fabrikautomatisierung, bei der die Sicherheitsfunktion mehrmals je Schicht eingesetzt wird	Komponente, die ausschließlich im SIS mit SIF-Bedarf verwendet wird, z. B. 2 bis 10 Mal jährlich (z. B. Fluttor)	Komponente, die gleichzeitig im SIS und vom EUC-Steuersystem verwendet wird (z. B. Ventil), mit weniger als 1 Bedarf des SIF jährlich	Komponente, die ausschließlich im SIS verwendet wird, mit geringem SIF-Bedarf (z. B. Sicherheitsfunktion in der chemischen Industrie)
Anforderungen von EN 61508-2 für ... Bedarfsmodus für die mechanischen Komponenten	Hoch	Niedrig ^b	Niedrig	Niedrig

^a Für eine genauere Erklärung von „viele“ und „wenige“ siehe Haupttext.

^b In diesem speziellen Fall, in dem die Bedarfsrate an der Sicherheitsfunktion hoch, die Nutzungsrate jedoch niedrig ist, wird die Nutzungsdauer der mechanischen Komponenten eher durch Alterung als durch Verschleiß eingeschränkt. EN 61508-2 berücksichtigt diesen besonderen Fall nicht. Da die Anforderungen für den hohen Bedarfsmodus für Komponenten vorgesehen sind, die nicht durch Alterung eingeschränkt sind, ist es sinnvoller, in diesem Fall die Anforderungen für den niedrigen Bedarfsmodus zu verwenden. Noch wichtiger ist, dass die Anforderung von EN 61508-2:2010, 7.4.4.1.4 und 7.4.5.3, eine Prüfung mit einer Ausfallhäufigkeit von mindestens dem 100-fachen der Bedarfshäufigkeit vorzusehen, dazu führt, dass Verschleiß als zusätzliche signifikante Ausfallart hinzukommt, wodurch die Sicherheit eher verringert als erhöht wird.

Bei mechanischen Komponenten mit einer Nutzungsrate von 1 im Jahr oder weniger muss davon ausgegangen werden, dass sie mit einer geringen Nutzungsrate betrieben werden, es sei denn, eine Analyse zeigt, dass Verschleiß die vorherrschende Fehlerursache ist.

Bei mechanischen Komponenten mit einer Nutzungsrate von 500 im Jahr oder mehr muss davon ausgegangen werden, dass sie mit einer hohen Nutzungsrate betrieben werden, es sei denn, eine Analyse zeigt, dass Alterung die vorherrschende Fehlerursache ist.

Bei mechanischen Komponenten mit einer Nutzungsrate zwischen 1 und 500 im Jahr muss ausgewertet werden, ob Alterung oder Verschleiß die vorherrschende Fehlerursache für die Ausfallhäufigkeit der Komponente ist. Das Ergebnis der Auswertung muss dokumentiert werden.

Tabelle 5 zeigt, wie sich die Nutzungsrate aus der Gesamtzahl der Einsätze im Jahr ableiten lässt:

Tabelle 5 — Anzahl der Einsätze im Jahr und Nutzungsrate

Gesamtzahl der Bewegungen je Jahr	< 1	1 ... 500	> 500
Auswertung erforderlich?	Nein (wahlweise möglich)	vorgeschrieben	Nein (wahlweise möglich)
Nutzungsrate	Niedrig oder wahlweise Auswertung zeigt, dass „hoch“ angemessener ist	Niedrig oder hoch, je nach Auswertungsergebnis	Hoch oder wahlweise Auswertung zeigt, dass „niedrig“ angemessener ist

Der Hersteller darf die Zweckbestimmung (und Ausfallhäufigkeit) angeben für

- niedrige und hohe Nutzungsrate, oder
- nur für niedrige Nutzungsrate, oder
- nur für hohe Nutzungsrate.

In jedem Fall muss der Hersteller die Gesamtzahl der Einsätze im Jahr angeben, bis zu denen die Auswertung gültig ist. Diese Grenzwerte müssen im Sicherheitshandbuch und in jeder Dokumentation, die eine Angabe zu den Ausfallhäufigkeiten enthält, angegeben werden. Der Hersteller muss auch eine Angabe über die angenommene Betriebsgeschwindigkeit machen.

Wenn der Hersteller die Komponente sowohl für eine hohe als auch für eine niedrige Nutzungsrate bewertet, muss er eine Nutzungsrate bewerten und angeben, bis zu der die Komponente als mit einer niedrigen Nutzungsrate betrieben gilt. Dies darf unabhängig von einer bestimmten Anwendung geschehen, wenn die in diesem Dokument genannten Kriterien angewendet und alle möglichen Bedingungen der Zweckbestimmung berücksichtigt werden. In diesem Fall muss der Hersteller die Ausfallhäufigkeit für eine niedrige Nutzungsrate bis zu dem festgestellten Schwellenwert und die für eine hohe Nutzungsrate berechnete Ausfallhäufigkeit für Nutzungswerte oberhalb des Schwellenwerts angeben. Dieser Schwellenwert muss im Sicherheitshandbuch und in jeder Dokumentation, die eine Angabe zu den Ausfallhäufigkeiten enthält, angegeben werden.

Unabhängig von der Nutzungsrate und den zugrunde gelegten Ausfallhäufigkeiten müssen die Zweckbestimmung und insbesondere etwaige Einschränkungen der möglichen Bewegungen innerhalb der Lebensdauer vom Endnutzer immer beachtet werden.

Mechanische Komponenten, die in einem hohen Bedarfsmodus und mit hoher Nutzungsrate verwendet werden, müssen

- die Anforderungen der geltenden Normen für einen hohen Bedarfsmodus erfüllen, und
- die Anforderungen an eine hohe Nutzungsrate nach diesem Dokument erfüllen.

Mechanische Komponenten, die in einem hohen Bedarfsmodus und mit niedriger Nutzungsrate verwendet werden, müssen

- die Anforderungen der geltenden Norm für den Bedarfsmodus erfüllen [hinsichtlich der (Online-) Prüfung und der Prozesssicherheitszeit müssen sie nicht die Anforderungen von EN 61508-2 oder der geltenden Normen erfüllen, die nur für den Bedarfsmodus gelten; für eine Begründung siehe Tabelle 4, Fußnote b)],
- die Anforderungen an eine niedrige Nutzungsrate nach diesem Dokument erfüllen.

Mechanische Komponenten, die in einem niedrigen Bedarfsmodus und mit hoher Nutzungsrate verwendet werden, müssen

- die Anforderungen der geltenden Normen für einen niedrigen Bedarfsmodus erfüllen, und
- die Anforderungen an eine hohe Nutzungsrate nach diesem Dokument erfüllen.

Mechanische Komponenten, die in einem niedrigen Bedarfsmodus und mit niedriger Nutzungsrate verwendet werden, müssen

- die Anforderungen der geltenden Normen für einen niedrigen Bedarfsmodus erfüllen, und
- die Anforderungen an eine niedrige Nutzungsrate nach diesem Dokument erfüllen.

Siehe auch Tabelle 4 für einen Überblick über die vier möglichen Fälle und die daraus resultierenden Konsequenzen.

Wenn Online-Diagnoseprüfungen im Bedarfsmodus oder bei geringer Nutzungsrate berücksichtigt werden, muss die Prüfungsrate deutlich über der Bedarfsrate liegen.

ANMERKUNG 1 Eine Komponente, die ursprünglich für eine niedrige Nutzungsrate vorgesehen war, kann später für eine hohe Nutzungsrate verwendet werden (oder umgekehrt), wenn sie sowohl für eine hohe als auch für eine niedrige Nutzungsrate bewertet wurde und alle daraus resultierenden Änderungen in der Sicherheitsbewertung vorgenommen wurden. Wenn die Nutzungsrate nicht auf hohe und niedrige Werte geprüft wurde, ist eine Änderung der Nutzungsrate ein gefahrbringender systematischer Fehler.

ANMERKUNG 2 Ein Faktor von etwa 5 bis 10 höher gilt in den meisten Fällen als „signifikant höher“.

ANMERKUNG 3 Wenn eine Komponente weniger als einmal im Jahr betätigt wird, ist die Alterung wahrscheinlich die vorherrschende Fehlerursache für diese Komponente.

ANMERKUNG 4 Wenn eine Komponente mehr als etwa alle 18 h betätigt wird (etwa 500 Betätigungen im Jahr), spielt die Alterung wahrscheinlich eine untergeordnete Rolle bei den Fehlerursachen der Komponente.

ANMERKUNG 5 Mögliche Bedingungen der vorgesehenen Verwendung sind z. B. alle Umgebungsbedingungen, die nach den Vorgaben des Herstellers zulässig sind.

ANMERKUNG 6 Die Anzahl der Bewegungen kann für verschiedene Bauteile desselben SIS stark voneinander abweichen, z. B. wenn ein Bauteil auch für die grundlegende Prozesssteuerung verwendet wird, andere Bauteile des SIS jedoch vom EUC-Steuersystem getrennt sind. So kann es zu einer Situation kommen, in der z. B. das SIF als Ganzes im Bedarfsmodus betrieben wird, der Aktor mit einer hohen Nutzungsrate betrieben wird und andere Komponenten des SIS mit einer niedrigen Nutzungsrate betrieben werden.

6.2 Art des Aktors/der Komponente

Die Bewertung muss in Übereinstimmung mit EN 61508-2:2010, 7.4.4.1.2 und 7.4.4.1.3 erfolgen.

Rein mechanische Komponenten dürfen nach EN 61508-2 als Typ A klassifiziert werden, da:

- das Ausfallverhalten aller Bauteile der verwendeten Komponente klar definiert werden kann;
- das Verhalten der Komponente unter Fehlerbedingungen vollständig bestimmt werden kann;
- es ausreichende Zuverlässigkeitsdaten für die in der Komponente verwendeten Bauteile gibt, um nachzuweisen, dass die Ausfallhäufigkeiten für erkannte und nicht erkannte gefahrbringende Ausfälle erreicht werden.

Wenn für mechanische Komponenten und technische Lösungen langjährige Erfahrungen vorliegen, dann kann der letzte Punkt üblicherweise als erfüllt angesehen werden. In diesem Fall können diese Ausfälle für eine Bewertung nach Vorgehensweise 2_H verwendet werden.

ANMERKUNG Das Ausfallverhalten ist bekannt, wenn z. B. entsprechende Prüfungen durchgeführt wurden, um die Eignung gegenüber den Grenzwerten (z. B. Temperatur, Bewegungsgeschwindigkeit, Medien) zu ermitteln.

7 Feldausfalldaten

7.1 Verfahren zur Analyse der Feldausfalldaten

Die Hersteller müssen Anstrengungen unternehmen, um Feldausfalldaten von Endnutzern zu erfassen und diese zu analysieren, um zu prüfen, ob die quantitativen und qualitativen Maßnahmen im Laufe der Zeit ihr Ziel erreichen. Das entsprechende Verfahren sollte die Feldausfalldaten entweder in zufällige Hardware-Ausfälle oder systematische Ausfallarten einteilen, um die folgenden Analysen zu erleichtern.

- Zufällige Hardware-Ausfalldaten sollten unter Verwendung geeigneter statistischer Verfahren und unter Berücksichtigung aller relevanten Faktoren (wie z. B. des wahrscheinlichen Anteils aller ausgefallenen Einheiten, die tatsächlich gemeldet wurden) analysiert werden, um sie mit der Ausfallhäufigkeit zu vergleichen, die durch die Verfahren in diesem Dokument vorausgesagt wurde, um zu bestätigen, dass die Feldausfalldaten nicht ungünstiger sind als die theoretische Vorhersage.
- Systematische Ausfälle sollten analysiert und mit den qualitativen Verfahren und Maßnahmen des Herstellers (einschließlich der Informationen im Sicherheitshandbuch) verglichen werden, die zur Behebung solcher Ausfälle vorgesehen sind.
- Sofern vernünftigerweise möglich:
 - muss eine Untersuchung durchgeführt werden, um die Ursache des systematischen Ausfalls zu ermitteln; und
 - muss die Ursache beseitigt werden.
- Wenn eine Untersuchung durchgeführt wurde, aber eine Ursache nicht mit angemessenem Aufwand ermittelt und beseitigt werden konnte, müssen die beobachteten Ausfälle in die Rate der zufälligen Hardware-Ausfälle eingerechnet werden.

Wenn die Ergebnisse einer der beiden oben genannten Analysen darauf hindeuten, dass die festgelegten Ziele für die Sicherheitsintegrität nicht erreicht werden, sollte der Hersteller die erforderlichen Korrekturmaßnahmen ergreifen, entweder im Rahmen der Auslegung, der Herstellung, des Sicherheitshandbuchs oder der direkten Anleitungen für Endnutzer. Dies sollte im Rahmen des FSM-Systems des Herstellers erfolgen, einschließlich aller erforderlichen Neubewertungen.

Wenn Feldrückmeldungen in ausreichender Menge und Qualität vorliegen, könnten diese zur Anpassung der Ausfallraten verwendet werden (Anhang G).

EN 61508-2:2010, 7.4.4.3.3, Anmerkung 1 gibt an, dass Endnutzer eine geeignete Norm für die Erfassung von Zuverlässigkeitsdaten verwenden sollten. Die Hersteller sind möglicherweise auch in der Lage, die Endnutzer zu ermutigen, dies als Teil ihrer Verantwortung für den Sicherheitslebenszyklus zu betrachten und Fehlerdaten an die Hersteller zurückzumelden.

ANMERKUNG 1 Die Einstufung der Ausfallarten als zufällig oder systematisch kann bei der Ermittlung der geeigneten Abhilfemaßnahmen hilfreich sein. Beispielsweise kann das Auftreten bestimmter systematischer Ausfälle darauf hinweisen, dass die in den einzelnen Phasen des Lebenszyklus eingesetzten Maßnahmen keine ausreichende Wirkung haben. Diese Mängel betreffen in der Regel alle Einheiten in ähnlicher Weise und unter den gleichen Bedingungen, wie z. B. ungeeignete Materialien, Auslegungsfehler, Fertigungsfehler, Transportschäden, Installations- oder Betriebsfehler, Unklarheiten in der Spezifikation, unzureichende Betriebsanleitungen usw.

ANMERKUNG 2 Siehe EN 61508-2:2010, Abschnitt C.1 bezüglich der Verwendung von Felddaten der Komponenten zur Unterstützung der FMEA.

ANMERKUNG 3 Siehe EN 61508-7:2010, B.5.4 für das Verfahren / die Maßnahme „Felderfahrung“, auf die in Tabelle B.3, Tabelle B.5 und Tabelle B.6 von EN 61508-2:2010 verwiesen wird.

7.2 Verwendung von Feldausfalldaten für bereits vorhandene Komponenten

In einigen Fällen sind möglicherweise Feldausfalldaten für bereits existierende Komponenten vorhanden, die seit Jahren im bewährten Betrieb eingesetzt werden. In diesem Fall ersetzen die aus der Analyse der Feldrückmeldungen abgeleiteten Fehlerdaten nicht die Notwendigkeit, die in diesem Dokument festgelegten Lebenszyklusphasen einzuhalten, jedoch können sie als Nachweis verwendet werden, um die Anforderungen für Prüfungen und Qualifizierungsprüfungen zu reduzieren (siehe Abschnitt 8). Bei der Verwendung von Feldrückmeldungsdaten muss Folgendes berücksichtigt werden:

- 1) Einsatz in ähnlichen Anwendungen, Konfigurationen und Umgebungen (z. B. Nutzungsrate, Temperatur, Einsatz, Medien usw.); und
- 2) die Daten werden in Übereinstimmung mit den relevanten internationalen Normen (z. B. EN ISO 14224) erfasst; und
- 3) die Daten werden nach der Anzahl der Feldrückmeldungen und nach dem Urteil von Sachverständigen bewertet.

Dies sollte bei der Schätzung der durchschnittlichen Ausfallhäufigkeit, des Unsicherheitsniveaus oder der Wahrscheinlichkeitsverteilung berücksichtigt werden. Zum Nachweis der Integrität muss bei der Auswertung der Daten ein Konfidenzniveau von 90 % oder höher zugrunde gelegt werden. Bei der Verwendung von Feldrückmeldedaten müssen die Funktionen, Konfigurationen und Anwendungen auf jene beschränkt werden, für die der Nachweis der Integrität erbracht wird. Dies sollte entsprechend dokumentiert werden.

ANMERKUNG 1 Siehe EN 61508-2:2010, 7.4.4.3.3 einschließlich Anmerkung 1 und Anmerkung 2.

ANMERKUNG 2 Die Analyse der Feldrückmeldungen kann vom Hersteller durchgeführt werden.

ANMERKUNG 3 Für weitere Anforderungen und Informationen siehe Anhang G.

8 Qualifikationsprüfungen (während der Entwicklung)

8.1 Allgemeines

Der entscheidende Aspekt bei der Qualifikationsprüfung ist die Ermittlung der Anwendungsgrenzen einer Komponente in jeder Hinsicht. Festgelegte Parameter wie z. B. die mechanische Lebensdauer (unter Berück-

sichtigung von Verschleiß, Ermüdung, Alterung, ...), Sicherheitsfunktionen und Leistungsparameter sowie Medienverträglichkeit und Umgebungseinflüsse müssen so weit wie möglich durch Prüfungen verifiziert werden.

Die Anforderungen bestehender und anwendbarer Produktnormen müssen erfüllt werden. In vielen Fällen decken diese Anforderungen nicht alle Aspekte der Funktionssicherheit ab. Aus diesem Grund müssen die folgenden Aspekte bei der Planung und Durchführung von Qualifikationsprüfungen zusätzlich berücksichtigt werden.

8.2 Prüfungsplanung/Prüfbedingungen

Alle Prüfungen müssen unter „möglichst realen“ Betriebsbedingungen durchgeführt werden. Einige Parameterkombinationen sind nur schwer auf einen Laboraufbau übertragbar (z. B. Zyklusprüfungen unter extremen Temperaturen und angewandtem Volumenstrom). Deshalb ist es unerlässlich, die relevanten Ausfallursachen innerhalb einer Komponente zu identifizieren (Konstruktions-FMEA, siehe 5.4.4). Im zweiten Schritt muss die Qualifikationsprüfspezifikation entsprechend erstellt werden.

Parameterkombinationen, die nicht mit vertretbarem Aufwand in einer Prüfung untersucht werden können, dürfen durch eine theoretische Einflussanalyse zur Ergänzung der Eignungsprüfung abgedeckt werden.

Alle Prüfungen müssen unter reproduzierbaren Bedingungen durchgeführt werden. Die Messungen müssen mit geeigneten Sensoren und Datenloggern durchgeführt werden.

8.3 Vorkonditionierung der Prüfproben

In vielen Fällen hängt die Wirksamkeit der Qualifikationsprüfung von der richtigen Vorkonditionierung der Prüfproben ab. Dies kann zum Beispiel für Schraubverbindungen relevant sein, bei denen anfängliche Setzungseffekte beseitigt werden müssen. Typische Verfahren zur Vorkonditionierung sind die Aussetzung gegenüber Schwingungs- und Temperaturzyklen vor Beginn der entsprechenden Prüfung.

Weitere Prüfungen, z. B. auf Wellenschlupf, müssen anschließend durchgeführt werden.

Die Grenzbedingungen für die Absetzprüfungen müssen so weit wie möglich an die Spezifikationen des Herstellers angepasst werden. Es müssen konservative Annahmen getroffen werden.

8.4 Anzahl der erforderlichen Prüfproben

Die erforderliche Anzahl von Prüfproben ergibt sich aus der Anforderung, dass eine Prüfung so geplant und durchgeführt werden muss, dass die Ergebnisse reproduzierbar und aussagekräftig sind.

8.5 Zyklusprüfung und B_{10D} -Werte nach EN ISO 13849-1:2015, C.4.2

Die Ergebnisse von Zyklusprüfungen können als Nachweis für eine Überbemessung bzw. für die Ableitung eines B_{10D} -Wertes herangezogen werden, wenn die Komponente mit einer hohen Nutzungsrate verwendet wird. Wenn Ausfallhäufigkeiten von B_{10D} -Werten abgeleitet werden, müssen die Komponenten ausgetauscht oder rekonditioniert werden, bevor diese Werte im Betrieb erreicht werden. In diesem Fall müssen die Austauschintervalle für den Benutzer auf dieser Grundlage festgelegt werden.

Die Ergebnisse dieser Schätzungen sind nur gültig, wenn die Komponenten nicht länger als bis zum Ende ihrer geprüften und/oder festgelegten mechanischen Lebensdauer verwendet werden.

B_{10} -/ B_{10D} -Werte und beschleunigte Prüfungen dürfen nicht zur Bestimmung einer Ausfallhäufigkeit für Komponenten mit geringer Nutzungsrate verwendet werden.

8.6 Umweltprüfungen

Die Grenzbedingungen müssen vom Hersteller festgelegt werden. Alle Bereiche in Bezug auf Temperatur, Druck usw. müssen durch geeignete Prüfungen verifiziert werden.

Gegebenenfalls muss die Widerstandsfähigkeit gegenüber verschiedenen Medien vorzugsweise durch Prüfung nachgewiesen werden. Wenn es nicht möglich ist, diese Prüfungen durchzuführen, ist eine theoretische Analyse erforderlich.

9 Bestimmung der Ausfallhäufigkeit

In diesem Abschnitt ist ein Verfahren zur Bestimmung von zufälligen Ausfallhäufigkeiten beschrieben. Bei mechanischen Komponenten ist eine Trennung zwischen zufälligen und systematischen Ausfällen nicht immer möglich. Ausfälle unbekannten Ursprungs können in die Häufigkeit von zufälligen Ausfällen einbezogen werden, da die verborgenen systematischen Aspekte noch nicht bekannt sind. Daher ist die zufällige Ausfallhäufigkeit als ungünstige Schätzung zu verstehen.

Das hier vorgestellte Verfahren geht von der Annahme aus, dass mechanische Einrichtungen mit ähnlicher Auslegung ähnliche Ausfallhäufigkeiten aufweisen müssen.

Anhang C enthält Tabellen für verschiedene Geräte mit Werten für grundlegende (gefahrbringende) zufällige Ausfallhäufigkeiten, die für typische Sicherheitsfunktionen, die von dem jeweiligen Gerät ausgeführt werden, angegeben werden können.

Die grundlegenden zufälligen Ausfallhäufigkeiten nach Anhang C müssen von einem Hersteller der Komponente als „Standardwert“ für zufällige Ausfallhäufigkeiten angegeben werden, wenn:

- die Komponente in Tabelle C.1, Tabelle C.2, Tabelle C.3 und Tabelle C.4 aufgeführt ist;
- die Komponente entsprechend diesem Dokument ausgelegt, gefertigt und validiert ist;
- die Mindestanforderungen an die systematische Fähigkeit erfüllt sind (Anhang A).

Ein niedrigerer Wert kann nur angegeben werden, wenn:

- eine detaillierte FME(D)A nach Anhang D durchgeführt wird (siehe unten); oder
- eine Integration mit der Feldrückmeldung nach Anhang G durchgeführt wird.

Eine detaillierte FME(D)A nach Anhang D muss auch dann durchgeführt werden, wenn die Komponente nicht in der Liste in Anhang C enthalten ist.

ANMERKUNG Die Ausfallhäufigkeit umfasst nur zufällige Ausfälle. Daher ist keine Anpassung an unterschiedliche Betriebsbedingungen erforderlich.

10 Betriebsprüfungen, Wartung und zeitliche Beschränkungen

10.1 Online-Diagnoseprüfungen

Mit Online-Diagnoseprüfungen wird das sicherheitstechnische System auf Fehler geprüft, die sich negativ auf die Verfügbarkeit der Sicherheitsfunktion(en) auswirken. Sie sind erforderlich, um einen DC > 0 % zu erhalten. Ihre Anwendung wird daher dringend empfohlen. Die Anforderungen sind in der Normenreihe EN 61508 beschrieben.

ANMERKUNG 1 Eine redundante und/oder diverse Bauweise bietet mehr Möglichkeiten, einen hohen DC zu erreichen.

ANMERKUNG 2 Auch Hubprüfungen könnten die Anforderungen an die Online-Diagnose erfüllen, wenn die Prüfungsrate, der Beginn der Prüfung, der Deckungsgrad und die Erkennungsmaßnahmen die Anforderungen erfüllen.

10.2 Nachweisprüfung

Eine regelmäßige Nachweisprüfung wird in der Regel für komplette Aktoren im Betrieb durchgeführt, um versteckte Fehler im mechanischen Teil des SIS aufzudecken, die durch Online-Diagnoseprüfungen nicht erkannt werden. Ein geeignetes Verfahren und die zu berücksichtigenden Aspekte sollten vom Hersteller im Sicherheitshandbuch vorgeschlagen werden.

10.3 Nachweisprüfungsdeckungsgrad (PTC)

Die wiederkehrende Nachweisprüfung für mechanische Komponenten muss üblicherweise für den vollständigen Aktor unter der Verantwortung des Endnutzers durchgeführt werden. Entsprechende Verfahren und die zugehörigen Faktoren für die Nachweisprüfung sind daher Bestandteil der Dokumentation für Endnutzer, zum Beispiel des NAMUR-Arbeitspapiers NA 106.

Daher muss ein Nachweisprüfungsdeckungsgrad (PTC) nicht für jede Komponente von den Herstellern im Detail berechnet werden, sondern es wird Folgendes berücksichtigt:

- Vorschlag für ein geeignetes Verfahren, und
- spezifische zu berücksichtigende Aspekte, wie z. B.
 - Bauteile, die besonders der Alterung, dem Verschleiß oder der Ermüdung ausgesetzt sind, und
 - kritische Bauteile, die einen großen Einfluss auf gefahrbringende Ausfälle haben (wie in der FMEDA beschrieben).

ANMERKUNG Da mechanische Komponenten Verschleiß unterliegen, bedeutet die Wiederherstellung des mechanischen Teils des Sicherheitssystems in einen „neuwertigen“ Zustand, dass alle Bauteile, die Verschleiß unterliegen, ausgetauscht werden müssen.

10.4 Wartung

Alle Anforderungen von EN 61508-1, EN 61508-2, EN 61508-4, EN 61508-6 und EN 61508-7 bezüglich der Wartung müssen auch für mechanische Komponenten erfüllt werden.

Darüber hinaus muss der Hersteller detaillierte Angaben zu allen Verschleißteilen und den Austauschintervallen dieser Bauteile bereitstellen, die zur Aufrechterhaltung der Ausfallhäufigkeit und SIL-Fähigkeit der Komponente erforderlich sind. Die Angaben zu den Austauschintervallen müssen – sofern für die jeweilige Komponente oder das Bauteil zutreffend – sowohl das Intervall in Bezug auf die verstrichene Zeit als auch das Intervall in Bezug auf die Bewegungen berücksichtigen. Wenn die Austauschintervalle bei bestimmten Betriebsbedingungen (z. B. Temperatur) im Bereich der vorgesehenen Verwendung erheblich variieren, müssen Informationen darüber bereitgestellt werden, wie die Intervalle entsprechend angepasst werden können.

10.5 Nutzungsdauer

Für jede sicherheitsbezogene Komponente müssen nach EN 61508-2:2010, 7.4.9.4, f) Informationen über eine etwaige Begrenzung der Nutzungsdauer der Komponente vorliegen, die nicht überschritten werden sollte, um die systematische Fähigkeit der Komponente und die Gültigkeit der geschätzten Ausfallhäufigkeiten aufrechtzuerhalten.

Die Nutzungsdauer mechanischer Komponenten beginnt, sobald sie installiert sind. Üblicherweise wird sie durch Alterung (geringe Nutzungsrate) oder Verschleißeffekte (hohe Nutzungsrate) eingeschränkt.

Der Hersteller muss im Sicherheitshandbuch Angaben darüber machen, welche Art der vorbeugenden Wartung (einschließlich des Austauschs von Bauteilen) erforderlich ist, um die angegebene Nutzungsdauer zu erreichen.

10.6 Lagerzeit

Liegt zwischen der Herstellung und dem Beginn der Nutzung der Komponente eine erhebliche Zeitspanne, so muss geprüft werden, wie sich dies auf die Zuverlässigkeit der Komponente auswirkt.

Der Systemintegrator oder Endnutzer muss vom Hersteller darüber informiert werden, was bei der Lagerung bis zur tatsächlichen Nutzung mit Steuerfunktion zu beachten ist und welche Maßnahmen erforderlich sind, um einen „möglichst neuwertigen Zustand“ der Komponenten/des Aktors sicherzustellen (z. B. Temperaturregelung, keine UV-Strahlung, kein Kontakt mit Schmutz usw.). Darüber hinaus muss der Hersteller angeben, ob die Lagerzeit in die Nutzungsdauer einbezogen werden muss oder nicht. Die Lagerbedingungen sollten im Sicherheitshandbuch beschrieben werden.

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

Die betrachtete(n) Komponente(n) müssen eindeutig beschrieben und getrennt von den für die Funktionssicherheit nicht erforderlichen Komponenten dargestellt (unterschieden) werden. Die Schnittstellen zu und Trennungen von anderen Komponenten müssen eindeutig beschrieben werden.

Es müssen die folgenden Aspekte berücksichtigt werden.

- Druck, Temperatur und die physikalischen/chemischen Eigenschaften des Medienstroms am Einlass der Industriearmatur und der äußeren Umgebung liegen in der Verantwortung des Endnutzers und/oder Bedieners (Medienanschluss).
- Alle Einflüsse des Medienflusses innerhalb der Industriearmatur und des Stellantriebs müssen der „Zweckbestimmung“ der Komponente entsprechen.
- Es liegt in der Verantwortung des Endnutzers, nicht von der vom Hersteller angegebenen Zweckbestimmung abzuweichen.
- Wenn die Funktion der Komponente das Medium negativ beeinflussen könnte (z. B. Kavitation), muss dies vom Hersteller angegeben werden.

Derartige Risiken können entweder auf die Auslegung oder auf eine Fehlfunktion der Komponenten zurückzuführen sein.

Der Zweck eines Sicherheitshandbuchs für konforme Komponenten eines sicherheitstechnischen Systems ist die Dokumentation aller Informationen, die für die Integration der Komponente in ein System in Übereinstimmung mit den Anforderungen von EN 61508 relevant sind. Weitere normative Anforderungen sind in EN 61508-2:2010, Anhang D enthalten.

Daher muss der Hersteller dem Systemintegrator und/oder dem Endnutzer geeignete Informationen für die sichere Integration, die Inbetriebnahme, den Betrieb, die Instandhaltung und Wartung sowie die Außerbetriebnahme der bereitgestellten Komponente zur Verfügung stellen.

Der Integrator des Aktors muss dem Endnutzer die nachstehend aufgeführte Dokumentation zur Auslegung und Validierung zur Verfügung stellen.

a) Auslegungsdokumente:

- 1) Auslegungsdokument (z. B. pneumatische/hydraulische Betriebsdiagramme);
- 2) Zusammenbauzeichnungen;

- 3) Komponentenliste;
 - 4) Sicherheitshandbücher und Installations-, Betriebs- und Wartungsanleitungen für jede relevante Komponente (Dokumente der Originalgerätehersteller).
- b) Validierungsdokumente:
- 1) Funktionsbericht (z. B. FAT-Bericht für die betreffende Komponente und für die gesamte Baugruppe);
 - 2) SIL-Bewertungsbericht mit Ausfallhäufigkeit, bauliche Einschränkungen und systematischer Fähigkeit (PFD_{avg} /PFH kann auf der Grundlage gegebener Annahmen aufgeführt werden).

In Übereinstimmung mit diesem Dokument muss der Hersteller die Ausfallarten der Komponenten und damit ihre Auswirkungen auf eine allgemeine Sicherheitsfunktion bewerten. Bei der Bestimmung von Ausfallarten, Ausfallhäufigkeit und damit verbundenen Einflussfaktoren ist es wahrscheinlich erforderlich, Maßnahmen zu definieren, die während oder nach der Installation der Komponente in das sicherheitstechnische System, das später vom Endnutzer betrieben und aufrechterhalten wird, durchgeführt werden müssen.

Der Hersteller muss daher die entsprechenden Maßnahmen im Sicherheitshandbuch beschreiben, damit die Sicherheitsintegrität der Komponente während ihres Lebenszyklus erhalten bleibt. Dies gilt sowohl für den quantitativen Teil der Sicherheitsintegrität als auch für die allgemeine Vermeidung von systematischen Ausfällen.

Ein Vorschlag für den Aufbau des Sicherheitshandbuchs ist in Anhang E enthalten.

ANMERKUNG Wenn PFD_{avg} zu Informationszwecken berechnet wird, kann die Berechnung auf den folgenden Annahmen beruhen: 1oo1-Architektur, $T_1 = 1$ Jahr, PTC = 90 %, MRT = 8 h, DC = 0 %.

Anhang A (normativ)

Checkliste zur Bestimmung der systematischen Fähigkeit

Die Maßnahmen zur Erfüllung der Mindestanforderungen an die Systemfähigkeit (5.1) müssen nach Tabelle A.1 dokumentiert werden. Wenn ein einziger Punkt nicht erfüllt ist, gilt die gesamte Bewertung als nicht bestanden.

Wenn ein Verfahren oder eine Maßnahme nicht bewertet werden kann, sollten die Gründe dafür in der Dokumentation des Entwicklers ausführlich dargelegt werden.