

DIN EN ISO 25119-2



ICS 35.240.99; 65.060.01

Entwurf

Einsprüche bis 2022-03-07
Vorgesehen als Ersatz für
DIN EN 16590-2:2014-11;
Ersatz für
E DIN EN ISO 25119-2:2018-11

**Traktoren und Maschinen für die Land- und Forstwirtschaft –
Sicherheitsbezogene Teile von Steuerungen –
Teil 2: Konzeptphase (ISO 25119-2:2019);
Deutsche und Englische Fassung prEN ISO 25119-2:2021**

Tractors and machinery for agriculture and forestry –
Safety-related parts of control systems –
Part 2: Concept phase (ISO 25119-2:2019);
German and English version prEN ISO 25119-2:2021

Tracteurs et matériels agricoles et forestiers –
Parties des systèmes de commande relatives à la sécurité –
Partie 2: Phase de projet (ISO 25119-2:2019);
Version allemande et anglaise prEN ISO 25119-2:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-01-07 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 nam@vdma.org 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 Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64 oder Lyoner Str. 18, 60528 Frankfurt am Main.

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 119 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

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.

Die nationalen Interessen bei der Erarbeitung werden vom Ausschuss NA 060-16-12 AA „TA E - Elektronik - Landtechnik“ im Fachbereich „Landtechnik“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von Landmaschinen sowie der Berufsgenossenschaften sind an der Erarbeitung beteiligt.

Dieser Norm-Entwurf konkretisiert einschlägige Anforderungen von Anhang I der EU-Maschinenrichtlinie 2006/42/EG an erstmals im Europäischen Wirtschaftsraum (EWR) in Verkehr gebrachte Maschinen, um den Nachweis der Übereinstimmung mit diesen Anforderungen zu erleichtern.

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

Änderungen

Gegenüber DIN EN 16590-2:2014-11 wurden folgende Änderungen vorgenommen:

- a) Anhang H wurde geringfügig überarbeitet, um die Klarheit und das Verständnis der vom Endanwender zu befolgenden Anforderungen an Teilsysteme, Elemente oder Bauteile, die nach ISO 26262 entworfen wurden, zu verbessern;
- b) das Dokument wurde redaktionell überarbeitet.

Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Konzeptphase (ISO 25119-2:2019)

*Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 2 :
Phase de projet (ISO 25119-2:2019)*

*Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept
phase (ISO 25119-2:2019)*

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm

Dokument-Untertyp:

Dokumentstufe: Entwurf

Dokumentsprache: D

STD Version 2.10b

Inhalt

	Seite
Europäisches Vorwort	5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe	11
4 Abkürzungen	11
5 Konzept — UoO	12
5.1 Ziele	12
5.2 Voraussetzungen	12
5.3 Anforderungen	12
5.3.1 Grundlegende Anforderungen und Umgebungsbedingungen	12
5.3.2 Grenzen der UoO und ihrer Schnittstellen zu anderen UoO	13
5.3.3 Abbildung und Zuordnung relevanter Funktionen zu beteiligten UoO, Gefährdungsquellen	13
5.3.4 Weitere Festlegungen	13
5.4 Arbeitsprodukte	14
6 HARA — Bestimmung des AgPL _r	14
6.1 Ziele	14
6.2 Voraussetzungen	14
6.3 Anforderungen	14
6.3.1 Verfahren zur Erstellung einer HARA	14
6.3.2 Aufgaben im Rahmen der HARA	14
6.3.3 Teilnehmer der HARA	15
6.3.4 Klassifizierung eines potenziellen Schadens	15
6.3.5 Beurteilung der Aufenthaltshäufigkeiten oder -dauer in der beobachteten Situation	15
6.3.6 Klassifizierung einer möglichen Schadensvermeidung	16
6.3.7 Auswahl des AgPL _r	17
6.4 Arbeitsprodukte	19
7 Funktionales Sicherheitskonzept	19
7.1 Ziele	19
7.2 Voraussetzungen	19
7.3 Anforderungen	19
7.3.1 Sicherheitsziele	19
7.3.2 Funktionale Sicherheitsanforderungen	19
7.3.3 Wert von MTTF _D	20
7.3.4 Wert für DC	20
7.3.5 Auswahl von Kategorien, MTTF _{DC} , DC und SRL	21
7.3.6 Erreichen des AgPL _r	22
7.3.7 Kompatibilität mit anderen funktionalen Sicherheitsnormen	22

7.3.8	Verbindung von E/E/PES.....	22
7.3.9	Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL	22
7.4	Arbeitsprodukte	23
Anhang A (normativ) Vorgesehene Architekturen für SRP/CS.....		24
A.1	Allgemeines	24
A.2	Kategorie B (elementar)	25
A.2.1	Allgemeines	25
A.2.2	Eigenschaften.....	25
A.3	Kategorie 1.....	25
A.3.1	Allgemeines	25
A.3.2	Eigenschaften.....	25
A.4	Kategorie 2.....	26
A.4.1	Allgemeines	26
A.4.2	Eigenschaften.....	27
A.5	Kategorie 3.....	28
A.5.1	Allgemeines	28
A.5.2	Eigenschaften.....	28
A.6	Kategorie 4.....	30
A.6.1	Allgemeines	30
A.6.2	Eigenschaften.....	30
Anhang B (informativ) Vereinfachtes Verfahren zur Abschätzung der Kanal-MTTF_{DC}.....		32
B.1	Allgemeines	32
B.2	MTTF _D -Werte von Bauteilen	32
B.2.1	Bestimmung der MTTF _D -Werte von Bauteilen aus Normen/Datenbanken.....	32
B.2.2	Bestimmung der MTTF _D -Werte von Bauteilen anhand von im Einsatz bewährten Bauteilen.....	33
B.2.3	MTTF _D für Bauteile aus B ₁₀	34
B.3	„Parts Count“-Verfahren	35
B.4	Berechnung der symmetrischen MTTF _{DC} für Zweikanal-Architekturen	36
Anhang C (informativ) Bestimmung des Diagnosedeckungsgrads (DC).....		37
C.1	Allgemeines	37
C.2	Schätzung des geforderten DC	37
C.3	Schätzung des Kanal-DC.....	42
C.4	Berechnung des Kanal-DC	42
C.5	Beispielberechnung des Kanal-DC	43
Anhang D (informativ) Schätzung von Ausfällen infolge gemeinsamer Ursache (CCF)		44
Anhang E (informativ) Systematischer Ausfall.....		46
E.1	Allgemeines	46
E.2	Anforderungen an die Beherrschung systematischer Ausfälle	46
E.3	Anforderungen an das Vermeiden systematischer Ausfälle	47
Anhang F (informativ) Merkmale von Sicherheitsfunktionen, die oftmals grundlegend für die Risikoreduzierung sind.....		49
F.1	Allgemeines	49
F.2	Anlaufsperrung	49
F.3	Stoppfunktion.....	49
F.4	Manuelle Rückstellung.....	49
F.5	Anlauf und Wiederanlauf	50
F.6	Schließzeit.....	50
F.7	Sicherheitsbezogene Parameter	50
F.8	Externe Steuerfunktion.....	51
F.9	Muting (Aussetzung von Sicherheitsfunktionen von Hand).....	51

F.10	Warnung der Bedienperson	51
Anhang G (informativ) Beispiel einer Risikoanalyse		52
G.1	Arbeitsablauf.....	52
G.2	Beispiel einer Risikoanalyse eines Elektro-Hydraulikgetriebes für eine selbstfahrende Arbeitsmaschine (Feldhäcksler) — Auszug aus einer vollständigen Risikoanalyse	52
G.2.1	Systembeschreibung	52
G.2.2	Umgebungsbedingungen	53
G.2.3	Systemzustände und Übergänge	53
G.2.4	Systemfehler.....	54
G.3	Beurteilung	55
G.3.1	Systemfehler — Unbeabsichtigtes Anhalten	55
G.3.2	Systemfehler — Trotz Anweisung keine Bewegung	56
G.4	Ergebnisse	56
Anhang H (normativ) Kompatibilität mit anderen funktionalen Sicherheitsnormen.....		57
H.1	Übersicht.....	57
H.2	Allgemeines	57
H.3	Mit IEC 61508 (alle Teile) konforme Systeme oder SRP/CS	57
H.4	Mit ISO 13849 (alle Teile) konforme Systeme oder SRP/CS	58
H.5	Mit ISO 26262 (alle Teile) konforme Systeme oder SRP/CS	59
Anhang I (informativ) Alternatives Konformitätsverfahren für verbundene Systeme.....		60
Anhang J (normativ) Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL		61
J.1	SRP/CS in Reihe	61
J.1.1	Allgemeines	61
J.1.2	Reihenabschätzung.....	61
J.1.3	Datenkommunikationen.....	62
J.2	Komplexe Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL.....	62
Literaturhinweise.....		63

Europäisches Vorwort

Der Text von ISO 25119-2:2019 wurde vom Technischen Komitee ISO/TC 23 "Traktoren und Maschinen für die Land- und Forstwirtschaft" der Internationalen Organisation für Normung (ISO) erarbeitet und wurde als prEN ISO 25119-2:2021 vom Technischen Komitee CEN/TC 144 "Traktoren und Maschinen für die Land- und Forstwirtschaft" übernommen, dessen Sekretariat von AFNOR gehalten wird.

Dieses Dokument wird derzeit der CEN-Umfrage vorgelegt.

Dieses Dokument wurde unter einem Mandat erarbeitet, das dem CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, und unterstützt grundlegende Anforderungen der EU-Richtlinie.

Zum Zusammenhang mit der EU-Richtlinie siehe informativen Anhang ZA, der integraler Bestandteil dieses Dokuments ist.

Anerkennungsnotiz

Der Text der ISO 25119-2:2019 wurde von CEN als prEN ISO 25119-2:2021 ohne Änderungen genehmigt.

Anhang ZA (informativ)

Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG

Diese Europäische Norm wurde im Rahmen eines von der Europäischen Kommission erteilten Normungsauftrages „M/396 Auftrag an CEN und CENELEC betreffend die Normung im Bereich Maschinen“ erarbeitet, um ein freiwilliges Mittel zur Erfüllung der grundlegenden Anforderungen der Richtlinie 2006/42/EU des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung) bereitzustellen.

Sobald diese Norm im Amtsblatt der Europäischen Union im Sinne dieser Richtlinie in Bezug genommen worden ist, berechtigt die Übereinstimmung mit den in Tabelle ZA.1 aufgeführten normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereichs dieser Norm zur Vermutung der Konformität mit den entsprechenden grundlegenden Anforderungen der Richtlinie und der zugehörigen EFTA-Vorschriften.

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG

Grundlegende Anforderungen der Richtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser Europäischen Norm	Erläuterungen/Anmerkungen
1.1.2. Grundsätze für die Integration der Sicherheit		
1.1.2 (a)	5.3, 6.3, 7.3, A.1, A.2, A.3, A.4, A.5, A.6, H.2, H.3, H.4, H.5	
1.1.2 (c)	5.3, 6.3, 7.3, A.1, A.2, A.3, A.4, A.5, A.6, H.2, H.3, H.4, H.5	
1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen	5.3, 6.3.2, 7.3.2, 7.3.5, A.1, A.2, A.3, A.4, A.5, A.6	
1.2.3. Ingangsetzen	6.3.2, 7.3, A.5, A.6	
1.2.4.1. Normales Stillsetzen	6.3.2, 7.3	
1.2.4.2. Betriebsbedingtes Stillsetzen	6.3.2, 7.3	
1.2.4.3. Stillsetzen im Notfall	6.3.2, 7.3	
1.2.5. Wahl der Steuerungs- oder Betriebsarten	5.3.3, 6.3.2, 7.3	
1.2.6. Störung der Energieversorgung	6.3.2, 7.3	
1.6.3. Trennung von den Energiequellen	6.3.2, 7.3	

WARNHINWEIS 1 — Die Konformitätsvermutung bleibt nur bestehen, so lange die Fundstelle dieser Europäischen Norm in der im Amtsblatt der Europäischen Union veröffentlichten Liste erhalten bleibt. Anwender dieser Norm sollten regelmäßig die im Amtsblatt der Europäischen Union zuletzt veröffentlichte Liste einsehen.

WARNHINWEIS 2 — Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Rechtsvorschriften der EU anwendbar sein.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Eine Erläuterung zum freiwilligen Charakter von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen, sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, enthält der folgende Link www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Unterkomitee SC 19, *Agricultural electronics* erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO 25119-1:2018), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Anhang H wurde geringfügig überarbeitet, um die Klarheit und das Verständnis der vom Endanwender zu befolgenden Anforderungen an Teilsysteme, Elemente oder Bauteile, die nach ISO 26262 entworfen wurden, zu verbessern.

Eine Auflistung aller Teile der Normenreihe ISO 25119 ist auf der ISO-Internetseite abrufbar.

Rückmeldungen oder Fragen zu diesem Dokument sollten an die nationale Normungsorganisation des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

ISO 25119 (alle Teile) beschreibt den Ansatz der Bewertung, Gestaltung und Verifizierung für alle Aktivitäten bezüglich des Sicherheitslebenszyklus für sicherheitsbezogene Teile, die elektrische und/oder elektronische und/oder programmierbare elektronische Systeme (E/E/PES) enthalten, welche für land- und forstwirtschaftliche Traktoren, selbstfahrende Aufsitzmaschinen sowie Anbau-, Aufsattel- und Anhängemaschinen für landwirtschaftliche Geräte verwendet werden. Sie ist auch auf mobile kommunale Geräte anwendbar.

Die Durchführung einer geeigneten Gefährdungserkennung und Risikoanalyse (z. B. ISO 12100) für die gesamte Maschine ist eine Voraussetzung für die Anwendung der Norm ISO 25119 (alle Teile). Aus diesem Grund wird häufig ein E/E/PES zugewiesen, um Sicherheitsfunktionen zu bieten, die sicherheitsbezogene Teile einer Steuerung (SRP/CS) bilden. Diese Teile können aus Hardware und Software bestehen, können separat von der oder in die Steuerung integriert sein und entweder allein Sicherheitsfunktionen ausführen oder Teil einer Betriebsfunktion sein.

Im Allgemeinen fasst der Konstrukteur (und bis zu einem gewissen Grad der Nutzer) den Entwurf und die Validierung dieser sicherheitsbezogenen Teile als Teil der Risikobeurteilung zusammen. Dadurch soll das mit einer bestimmten Gefahr (oder Gefahrensituation) verbundene Risiko unter allen Nutzungsbedingungen der Maschine gemindert werden. Dies kann durch Anwendung verschiedener Maßnahmen (sowohl SRP/CS als auch Nicht-SRP/CS) erreicht werden, wobei das Endergebnis das Erzielen eines sicheren Zustands ist.

ISO 25119 (alle Teile) unterteilt die Fähigkeit sicherheitsbezogener Teile, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, in fünf Stufen, sogenannte Performance Levels. Der Performance Level eines gesteuerten Kanals hängt von mehreren Faktoren ab: vom Systemaufbau (Kategorie), vom Umfang des Fehlererkennungsmechanismus (Diagnosedeckungsgrad), von der Zuverlässigkeit der Komponenten (mittlere Zeit bis zum gefahrbringenden Ausfall, Ausfälle gemeinsamer Ursache), von den Entwurfsverfahren, von der Beanspruchung im Betrieb, von Umweltbedingungen und von Arbeitsabläufen. Drei Arten von Ausfällen, die E/E/PES-Funktionsstörungen hervorrufen können, die zu potenziellen gefahrbringenden Situationen führen, werden berücksichtigt: systematische Ausfälle, Ausfälle gemeinsamer Ursache und Zufallsausfälle.

Darüber hinaus legt ISO 25119 (alle Teile) einen Ansatz auf Basis einer Klassifikation der Strukturen mit verschiedenen Konstruktionsmerkmalen und einem bestimmten Verhalten im Fehlerfall fest, um den Konstrukteur während der Gestaltung und Verifizierung anzuleiten und die Beurteilung des erreichten Performance Levels zu erleichtern.

Die Performance Level und Kategorien lassen sich anwenden auf Steuerungen aller Arten fahrbarer Maschinen: von einfachen Systemen (z. B. Anlassventilen) bis hin zu komplexen Systemen (z. B. Steer-by-Wire) sowie auf Steuerungen von Schutzeinrichtungen (z. B. Verriegelungsvorrichtungen, druckempfindliche Einrichtungen).

ISO 25119 (alle Teile) übernimmt für die Ermittlung der Risiken einen auf dem Risiko basierenden Ansatz zur Angabe des Soll-Performance-Levels für die von den E/E/PES-sicherheitsrelevanten Kanälen auszuführenden Sicherheitsfunktionen. Sie liefert die mit den Performance Levels verbundenen Anforderungen für den gesamten E/E/PES-Lebenszyklus (Entwicklung, Fertigung, Betrieb, Wartung, Außerbetriebnahme), die zur Erzielung der erforderlichen Funktionssicherheit für E/E/PES und der zugehörigen Performance Levels notwendig sind.

Sicherheitsnormen im Bereich Maschinenbau gliedern sich in folgende Bereiche:

- a) Typ-A-Normen (Grundnormen) enthalten Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die für alle Maschinen angewendet werden können.
- b) Typ-B-Normen (Fachgrundnormen) behandeln einen oder mehrere Sicherheitsaspekte oder eine oder mehrere Arten von Schutzeinrichtungen, die bei einer Reihe von Maschinen angewendet werden können:
 - Typ-B1-Normen behandeln bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Geräusch);
 - Typ-B2-Normen behandeln Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungen, Kontaktmatten, trennende Schutzeinrichtungen).
- c) Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen für eine bestimmte Maschine oder Gruppe von Maschinen.

Dieses Dokument ist eine Typ-B1-Norm wie in EN ISO 12100 angegeben.

Dieses Dokument ist insbesondere für die folgenden Akteurgruppen als Marktteilnehmer in Bezug auf die Maschinensicherheit relevant:

- Maschinenhersteller (kleine, mittelständische und große Unternehmen);
- Gesundheits- und Sicherheitsinstitutionen (Regulierungsbehörden, Unfallverhütungs-Organisationen, Marktaufsicht usw.).

Andere Gruppen, die von dem mit den Mitteln des Dokuments von den oben genannten Akteurgruppen erreichten Grad an Maschinensicherheit betroffen sein können:

- Maschinenbetreiber/Arbeitgeber (kleine, mittlere und große Unternehmen);
- Maschinenbetreiber/Angestellte (z. B. Gewerkschaften, Organisationen für Menschen mit besonderen Bedürfnissen);
- Dienstleister, für Instandhaltung (kleine, mittlere und große Unternehmen);
- Endkunde (im Fall von Maschinen, die für die Verwendung durch den Endkunden vorgesehen sind).

Den vorgenannten Interessengruppen wurde die Möglichkeit gegeben, an dem Entwurfsprozess zu diesem Dokument teilzunehmen.

Des Weiteren ist dieses Dokument für Normungsinstitute gedacht, die Typ-C-Normen erarbeiten.

Die Anforderungen in diesem Dokument können durch eine Typ-C-Norm ergänzt oder modifiziert werden.

Für Maschinen, die vom Anwendungsbereich einer Typ-C-Norm behandelt werden und entsprechend den Anforderungen dieser Norm gestaltet und erstellt wurden, haben die Anforderungen dieser Typ-C-Norm Vorrang.

1 Anwendungsbereich

Dieses Dokument beschreibt die Konzeptphase der Entwicklung sicherheitsbezogener Teile von Steuerungen (SRP/CS) in land- und forstwirtschaftlichen Traktoren, selbstfahrenden Aufsitzmaschinen sowie Anbau-, Aufsattel- und Anhängemaschinen für landwirtschaftliche Geräte. Sie kann auch auf fahrbare kommunale Geräte (z. B. Straßenkehrmaschinen) angewendet werden.

Dieses Dokument gilt nicht für:

- Flugzeuge und Luftkissenfahrzeuge für den landwirtschaftlichen Einsatz;
- Rasen- und Gartengeräte.

Dieses Dokument legt die Merkmale und Kategorien von SRP/CS-Systemen fest, die zur Ausführung von Sicherheitsfunktionen erforderlich sind. Es enthält keine Performance Level für bestimmte Anwendungen.

ANMERKUNG 1 Maschinenspezifische Typ-C-Normen können Performance Level (AgPL) für Sicherheitsfunktionen von Maschinen in ihrem Anwendungsbereich festlegen. Andernfalls ist der Hersteller für die Festlegung des AgPL verantwortlich.

Dieses Dokument gilt für sicherheitsbezogene Teile elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES) als Teil mechatronischer Systeme. Es behandelt die möglichen Gefahren durch Fehlfunktionen von sicherheitsbezogenen E/E/PES einschließlich der Wechselwirkungen dieser Systeme. Das Dokument behandelt nicht Gefahren in Verbindung mit Stromschlag, Feuer, Rauch, Hitze, Strahlung, Toxizität, Entflammbarkeit, Reaktivität, Korrosion, Freisetzung von Energie usw., soweit diese nicht direkt durch eine Fehlfunktion der sicherheitsbezogenen Systeme von E/E/PES verursacht werden. Darüber hinaus behandelt das Dokument die Fehlfunktionen sicherheitsbezogener Systeme von E/E/PES, die an Schutzmaßnahmen, Schutzeinrichtungen oder Sicherheitsfunktionen als Reaktion auf nicht durch E/E/PES verursachte Gefahren beteiligt sind.

Im Anwendungsbereich dieses Dokuments enthaltene Beispiele sind:

- sicherheitsbezogene Teile einer Steuerung (SRP/CS), die den Stromfluss in elektrischen Hybridsystemen begrenzen, um Isolierungsausfälle und Gefahren durch elektrischen Schlag zu verhindern;
- elektromagnetische Störungen mit dem SRP/CS;
- für Brandschutzzwecke gestaltete SRP/CS.

Im Anwendungsbereich dieses Dokuments nicht enthaltene Beispiele sind:

- Isolierungsausfälle durch Reibung, die zu der Gefahr eines elektrischen Schlags führen;
- elektromagnetische Nennstrahlung, die nahegelegene Maschinensteuerungssysteme beeinflusst;
- Korrosion, die zu einer Überhitzung von Stromkabeln führt.

Sie ist nicht anzuwenden auf Nicht-E/E/PES-Systeme (z. B. hydraulische, mechanische und pneumatische).

ANMERKUNG 2 Siehe auch EN ISO 12100 zu Gestaltungsleitsätzen für die Sicherheit von Maschinen.

Dieses Dokument gilt nicht für sicherheitsbezogene Teile von Steuerungen, die vor dem Veröffentlichungsdatum dieses Dokuments hergestellt wurden.

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).

ISO 25119-1:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

ISO 25119-3:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software*

ISO 25119-4:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: production, operation, modification and supporting*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 25119-1.

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

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

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

ADC	Analog/Digital-Wandler (en: analog to digital converter)
AgPL	landwirtschaftlicher Performance Level (en: agricultural performance level)
AgPL _r	geforderter landwirtschaftlicher Performance Level (en: required agricultural performance level)
Cat	Hardwarekategorie
CCF	Ausfall infolge gemeinsamer Ursache (en: common-cause failure)
CRC	zyklische Redundanzprüfung (en: cyclic redundancy check)
DC	Diagnosedeckungsgrad
DC _{avg}	durchschnittlicher Diagnosedeckungsgrad (en: average diagnostic coverage)
ECU	elektronische Steuereinheit
ETA	Ereignisbaumanalyse (en: event tree analysis)
E/E/PES	elektrische/elektronische/programmierbare elektronische Systeme
EMV	elektromagnetische Verträglichkeit
FMEA	Fehlermöglichkeits- und Einflussanalyse
EPROM	löscharer, programmierbarer schreibgeschützter Speicher (en: erasable programmable read-only memory)
FTA	Fehlerbaumanalyse

HARA	Gefahrenanalyse und Risikobeurteilung
HIL	Hardware in the Loop
MTTF	mittlere Zeit bis zum Ausfall (en: mean time to failure)
MTTF _D	mittlere Zeit bis zum gefahrbringenden Ausfall (en: mean time to dangerous failure)
MTTF _{DC}	mittlere Zeit bis zum gefahrbringenden Ausfall für jeden Kanal (en: mean time to dangerous failure for each channel)
PES	programmierbares elektronisches System
QM	Qualitätssicherungsmaßnahmen (en: quality measures)
RAM	Arbeitsspeicher (en: random-access memory)
SOP	Produktionsanlauf (en: start of production)
SRL	Software-Anforderungs-Level (en: software requirement level)
SRP/CS	sicherheitsbezogene Teile von Steuerungen
UoO	Betrachtungseinheit

5 Konzept — UoO

5.1 Ziele

Das Ziel dieser Phase ist die Entwicklung eines ausreichenden Verständnisses für die UoO, um alle im Sicherheitslebenszyklus festgelegten Aufgaben zufriedenstellend erfüllen zu können (siehe ISO 25119-1:2018, Bild 2). Für jede UoO muss ein geeignetes Verfahren zur Bestimmung des erforderlichen Performance Levels verwendet werden. Zu den geeigneten Verfahren zählen die Risikoanalyse (im Folgenden beschrieben), andere Normen, gesetzliche Vorschriften und Fachkenntnisse von Prüfinstitutionen oder eine Kombination der Verfahren.

5.2 Voraussetzungen

Die notwendigen Voraussetzungen sind eine Beschreibung der von der UoO zu liefernden sicherheitsbezogenen Funktion, ihrer Schnittstellen, der bereits bekannten Anforderungen an die Sicherheit und Zuverlässigkeit sowie des Anwendungsbereichs der Einheit.

5.3 Anforderungen

5.3.1 Grundlegende Anforderungen und Umgebungsbedingungen

Die folgenden Informationen müssen für die sicherheitsbezogene Funktion der UoO zur Verfügung stehen:

- a) Umfang, Kontext, Zweck und bekannte Elemente;
- b) Funktionsanforderungen;
- c) sonstige Anforderungen und Umgebungsbedingungen, die zu berücksichtigen sind, einschließlich;
 - technischer oder physikalischer Anforderungen, z. B. Betriebs-, Umwelt- und Umgebungsbedingungen und Beschränkungen;
 - gesetzliche Anforderungen, insbesondere sicherheitsbezogene Gesetze, Vorschriften und Normen (national und international);

- d) historische Anforderungen an Sicherheit und Zuverlässigkeit und Grad der erreichten Sicherheit und Zuverlässigkeit für ähnliche oder verwandte UoO.

5.3.2 Grenzen der UoO und ihrer Schnittstellen zu anderen UoO

Um ein Verständnis der Funktionsweise der UoO in ihrem Umfeld zu erlangen, müssen folgende Informationen in Erwägung gezogen werden:

- die Grenzen der UoO;
- ihre Schnittstellen und Wechselwirkungen mit anderen UoO und Bauteilen;
- Anforderungen an sicherheitsbezogene Funktionen in Verbindung mit anderen UoO.

5.3.3 Abbildung und Zuordnung relevanter Funktionen zu beteiligten UoO, Gefährdungsquellen

Die Gefährdungsquellen, die die Sicherheit und Zuverlässigkeit der UoO beeinträchtigen könnten, müssen bestimmt werden. Hierzu zählen:

- die Wechselwirkung verschiedener UoO;
- Beanspruchungen physikalischer oder chemischer Art (Energiegehalt, Toxizität, Explosivität, Korrosion, Reaktivität, Brennbarkeit usw.);
- andere externe Vorgänge [Temperatur, Stoß, elektromagnetische Verträglichkeit (EMV) usw.];
- vernünftigerweise vorhersehbare menschliche Bedienungsfehler;
- Beanspruchungen, die von der UoO ausgehen, und Vorkommnisse, die zu einem Ausfall führen (z. B. während der Montage oder Instandhaltung).

5.3.4 Weitere Festlegungen

Neben den in 5.3.2 beschriebenen Aktivitäten müssen folgende Festlegungen oder Maßnahmen getroffen werden:

- Entscheidung, ob die zu entwickelnde UoO eine Modifizierung oder Anpassung oder Ableitung einer bestehenden UoO ist oder ob es sich um eine Neuentwicklung handelt. Im Fall einer Modifizierung muss zur entsprechenden Anpassung des Lebenszyklus eine Auswirkungsanalyse durchgeführt werden;
- Erstellen eines Plans und einer Spezifikation zur Verifizierung und Validierung der Anforderungen bezüglich der UoO, die in 5.3.1 beschrieben sind;
- Festlegung des Projektmanagements für die entsprechenden Phasen im Lebenszyklus;
- ausreichende Eingangsdaten für die Zuverlässigkeitsprüfung;
- ausreichende Verfahren und Anwendung der Werkzeuge und Technologien;
- ausreichend qualifiziertes Personal zur Ausführung der Aufgaben.

5.4 Arbeitsprodukte

Die eventuellen Arbeitsprodukte der UoO müssen sein:

- a) in der UoO enthaltene Elemente;
- b) die Festlegung der grundlegenden Anforderungen und Umgebungsbedingungen;
- c) Grenzen der UoO und ihre Schnittstellen zu anderen UoO;
- d) Gefährdungsquellen;
- e) weitere Festlegungen.

6 HARA — Bestimmung des AgPL_r

6.1 Ziele

Die Hauptziele bestehen darin, Risiken in Verbindung mit einer fehlerhaften UoO (die die sicherheitsbezogenen Funktionen nicht wie vorgesehen ausführt, beispielsweise indem sie nicht ordnungsgemäß anhält, das Fahrzeug sich im Leerlauf fortbewegt, in die falsche Richtung steuert) zu analysieren und anschließend einen geeigneten AgPL_r zuzuweisen. Risiko wird festgelegt als Kombination aus der Wahrscheinlichkeit, mit der ein Schaden eintritt, und der Schwere dieses Schadens (ISO 25119-1:2018, 3.39). Bei der Betrachtung der Wahrscheinlichkeit des Auftretens eines Schadens kann die Wahrscheinlichkeit, einer gefahrbringenden Situation durch eine fehlerhafte UoO ausgesetzt zu werden, berücksichtigt werden.

Die in 6.2 bis 6.4 beschriebene Vorgehensweise liefert eine Anleitung zur Bestimmung des AgPL_r auf der Grundlage der HARA.

6.2 Voraussetzungen

Die UoO-Festlegung in Verbindung mit jeder sicherheitsbezogenen Funktion.

6.3 Anforderungen

6.3.1 Verfahren zur Erstellung einer HARA

Die HARA muss die gesamte sicherheitsbezogene Funktion berücksichtigen, sodass eine angemessene Spezifikation für das SRP/CS erstellt werden kann. Werden in späteren Phasen des Sicherheitslebenszyklus Entscheidungen getroffen, welche die Festlegung des Anwendungsbereichs verändern, so muss die HARA entsprechend angepasst werden. Um die Änderungen und ihre Auswirkung auf die Arbeitsprodukte zu identifizieren, muss eine Auswirkungsanalyse nach ISO 25119-4 durchgeführt werden.

6.3.2 Aufgaben im Rahmen der HARA

Die Betriebsbedingungen, unter denen die Fehlfunktion der UoO bei korrekter Anwendung und vorhersehbarer falscher Anwendung zu einer Gefährdungssituation führt, müssen in Betracht gezogen werden.

6.3.3 Teilnehmer der HARA

Für die Durchführung der HARA muss ausreichendes Personal eingesetzt werden, um sicherzustellen, dass alle relevanten Gutachten zur Verfügung stehen.

ANMERKUNG Die Einbindung einzelner Personen aus verschiedenen Disziplinen liefert oftmals wertvolle Eingaben für die HARA.

6.3.4 Klassifizierung eines potenziellen Schadens

Die potenzielle Schwere eines Schadens muss bestimmt und dokumentiert werden.

Potenziell schädliche Auswirkungen müssen durch die Betrachtung aller Gefährdungssituationen infolge von Fehlfunktionen der Sicherheitsfunktion unter relevanten Betriebsbedingungen, Betriebsarten und Betriebssituationen bestimmt werden.

Bei der Beschreibung der Schäden muss eine Kategorisierung angewendet werden. Aus diesem Grund wird eine Klassifizierung der Schwere des Schadens in vier Kategorien: S0, S1, S2 und S3 (siehe Tabelle 1) präsentiert.

Die Handlungen der Bedienperson der betroffenen Maschine und von Umstehenden (z. B. Personen, die Unterstützung leisten, andere Bedienpersonen von Maschinen, andere Verkehrsteilnehmer usw.) müssen unter Berücksichtigung ihrer Schadensexposition dokumentiert werden.

Das Ziel der Beurteilung und Klassifizierung eines potenziellen Schadens muss sich auf den Schaden für Personen konzentrieren und darauf beschränkt sein. Wenn die Analyse der Fehlfunktion der sicherheitsbezogenen Funktion eindeutig auf Sachschäden und nicht auf Personenschäden begrenzt ist, müssen diese Fehlfunktionen nicht als sicherheitsbezogen klassifiziert werden.

Für die der Schadensklasse S0 zugewiesenen Funktionen braucht keine weitere Risikobeurteilung durchgeführt zu werden.

Tabelle 1 — Klassifizierung von Verletzungen

S0	S1	S2	S3
Keine Verletzungen, Schaden auf Sachschäden beschränkt	Leichte und mäßige Verletzungen, medizinische Versorgung erforderlich, vollständige Genesung	Schwere und lebensbedrohliche Verletzungen (Überleben wahrscheinlich), dauerhafte Einschränkung der Arbeitsfähigkeit	Lebensbedrohliche Verletzungen (Überleben ungewiss), schwere Behinderung

6.3.5 Beurteilung der Aufenthaltshäufigkeiten oder -dauer in der beobachteten Situation

Eine HARA muss die Auswirkungen des Auftretens möglicher Fehlfunktionen von Sicherheitsfunktionen unter allen spezifischen regionalen Arbeits- und Betriebsbedingungen berücksichtigen. Diese Situationen reichen von täglichen Routinearbeiten bis zu extrem seltenen Situationen. Die Variable „E“ muss zur Kategorisierung der verschiedenen Aufenthaltshäufigkeiten oder -dauer verwendet werden. Fünf Kategorien, als E0, E1, E2, E3 und E4 bezeichnet (siehe Tabelle 2), werden für Variable E verwendet. Hier ist die Variable E eine Schätzung, wie oft oder wie lange eine Bedienperson oder ein Umstehender einer Gefahr ausgesetzt ist, wenn ein Ausfall zu einem Schaden der Bedienperson oder eines Umstehenden führen könnte. Das am besten geeignete Verfahren für jede Gefährdungssituation, die Häufigkeit oder die Dauer muss zur Bestimmung des AgPLr verwendet werden. Wenn mehr als eine Kategorie als für eine bestimmte Gefährdungssituation geeignet befunden wird, muss das Verfahren, das die höchste Kategorie ergibt, verwendet werden.

ANMERKUNG Eine Gefährdung, die Schaden verursachen kann, kann sich aus einer Kombination von Maschinenbedingungen (z. B. umgebungsbedingt und/oder betriebsbedingt) ergeben.

Tabelle 2 — Klassifizierung der Exposition gegenüber dem gefährlichen Vorfall

Beschreibung	E0	E1	E2	E3	E4
Definition der Häufigkeit	Unwahrscheinlich (aber theoretisch möglich; einmal während der Lebensdauer)	Seltene Vorfälle (weniger als einmal je Jahr)	Manchmal (mehr als einmal je Jahr)	Oft (mehr als einmal je Monat)	Häufig (bei beinahe jedem Einsatz)
Definition der Dauer $\frac{t_{\text{exp}}}{t_{\text{av op}}}$	unter 0,01 %	0,01 % bis weniger als 0,1 %	0,1 % bis weniger als 1 %	1 % bis weniger als 10 %	10 % oder mehr
t_{exp} Expositionsdauer. $t_{\text{av op}}$ durchschnittliche Betriebszeit.					

6.3.6 Klassifizierung einer möglichen Schadensvermeidung

Zur Beurteilung einer möglichen Schadensvermeidung muss eingeschätzt werden, ob eine übliche geschulte Bedienperson eine entstehende gefährliche Situation beherrscht und sie vermeiden kann, oder ob die Situation völlig unbeherrschbar ist. Gleichmaßen kann ein Umstehender ein gewisses Maß an Kontrolle haben, um eine gefährliche Situation zu vermeiden. Die Variable C ist anzuwenden, um die Fähigkeit der Schadensvermeidung zu klassifizieren. Der Wert von C für eine mögliche Schadensvermeidung darf nur die Fähigkeit von Personen, den Schaden nach einer Fehlfunktion der Sicherheitsfunktion und nicht die Zuverlässigkeit der in den SRP/CS angegebenen Maßnahmen, die das Risiko im Fall einer Fehlfunktion mindern, berücksichtigen. Die verwendeten Kategorien C0, C1, C2 und C3 stehen für eine Klassifizierung in „leicht beherrschbar“, „beherrschbar“, „im Allgemeinen beherrschbar“ und „nicht beherrschbar“ (siehe Tabelle 3).

Tabelle 3 — Klassifizierung der Schadensvermeidung

C0	C1	C2	C3
leicht beherrschbar Die Bedienperson oder der Umstehende beherrscht die Situation, Schaden wird vermieden.	beherrschbar Mehr als 99 % der Personen beherrschen die Situation. In mehr als 99 % aller Fälle führt die Situation nicht zu einem Schaden.	im Allgemeinen beherrschbar Mehr als 90 % der Personen beherrschen die Situation. In mehr als 90 % aller Fälle führt die Situation nicht zu einem Schaden.	Keine Die übliche geschulte Bedienperson oder der Umstehende kann den Schaden im Allgemeinen nicht vermeiden.

6.3.7 Auswahl des AgPL_r

Bild 2 enthält eine Anleitung zur Bestimmung des AgPL_r durch Kombination der Schwere (S), der Exposition (E) und der Beherrschbarkeit (C) für jede identifizierte Gefährdungssituation.

ANMERKUNG Die Bestimmung des AgPL_r anhand von Bild 1 erfordert Erfahrung in der sicheren Anwendung derselben oder einer ähnlichen Maschine und allgemeine Kompetenz im Schutz von Maschinen.

AgPL_r werden von AgPL_r = a bis AgPL_r = e angegeben. AgPL_r = a hat die am wenigsten strengen Systemanforderungen und AgPL_r = e die strengsten Systemanforderungen. Zusätzlich zu diesen Levels besteht eine Qualitätsgradbezeichnung QM, die indirekt eine Systementwicklung in Übereinstimmung mit einer anerkannten Qualitätsmanagementnorm (z. B. ISO 9001) fordert. Eine QM gilt nur für Funktionen mit ausreichend geringem Risiko, um als für die Zwecke von ISO 25119 (alle Teile) als nicht sicherheitsbezogen klassifiziert werden zu können.

Die identifizierten Gefährdungen, die den AgPL_r in Verbindung mit der Sicherheitsfunktion der UoO (siehe 7.3.2) festlegen, und der damit verbundene AgPL_r sind in einem HARA-Bericht zu beschreiben und zu dokumentieren.

Ein Beispiel für eine HARA und den daraus resultierenden AgPL_r ist in Anhang G enthalten.

		C0	C1	C2	C3
S0					
		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	QM	b	c	d
S3	E0	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	QM	b	c	d
	E4	QM	c	d	e

Legende

S Schwere

E Exposition gegenüber der Gefährdungssituation

C Beherrschbarkeit

QM Qualitätssicherungsmaßnahmen (en: quality measures)

a, b, c, d, e geforderter landwirtschaftlicher Performance Level (AgPL_r)

ANMERKUNG siehe 6.3.7 für eine Beschreibung der QM.

Bild 1 — Bestimmung des AgPL_r

6.4 Arbeitsprodukte

Folgendes muss bestimmt und dokumentiert werden:

- a) HARA-Bericht.

ANMERKUNG Dokumentenaufbewahrung nach ISO 25119-4.

7 Funktionales Sicherheitskonzept

7.1 Ziele

Abgeleitet aus den Ergebnissen der vorhergehenden Phasen zielen die Anforderungen dieses Absatzes darauf ab, allgemeine Gestaltungskonzepte und Anforderungen auf Systemebene festzulegen.

7.2 Voraussetzungen

- Ergebnisse der HARA
- AgPL_r für die Sicherheitsfunktionen

7.3 Anforderungen

7.3.1 Sicherheitsziele

Jede Gefährdungssituation, deren AgPL_r höher ist als der QM, muss mit einem Sicherheitsziel verbunden sein. Ein Sicherheitsziel kann mehrere Gefährdungssituationen behandeln. Wenn ähnliche Sicherheitsziele bestimmt werden, können sie in einem Sicherheitsziel kombiniert werden.

ANMERKUNG Sicherheitsziele sind oberste Sicherheitsziele für die UoO. Sie führen zu funktionalen Sicherheitsanforderungen, die erforderlich sind, um ein unangemessenes Risiko für jede Gefährdungssituation zu vermeiden.

7.3.2 Funktionale Sicherheitsanforderungen

Funktionale Sicherheitsanforderungen realisieren die Sicherheitsziele auf spezifischere Weise, indem sie die Funktionssicherheit der betreffenden UoO sicherstellen. Aus den Sicherheitszielen müssen angemessene funktionale Sicherheitsanforderungen abgeleitet werden. Die funktionalen Sicherheitsanforderungen übernehmen den AgPL_r der Gefährdungssituation und der damit verbundenen Sicherheitsziele.

Wenn eine funktionale Sicherheitsanforderung ähnliche Gefährdungssituationen mit unterschiedlichen AgPL_r behandelt, muss die funktionale Sicherheitsanforderung den höchsten AgPL_r implementieren.

Gegebenenfalls müssen sichere Zustände für jede aus dem relevanten Sicherheitsziel abgeleitete funktionale Sicherheitsanforderung bewertet werden. Der Übergang in und die Aufrechterhaltung von sicheren Zuständen muss in den technischen Sicherheitsanforderungen festgelegt werden.

Folgendes ist bei der Festlegung funktionaler Sicherheitsanforderungen zu berücksichtigen:

- systematischer Ausfall (siehe Anhang E);
- die Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen auszuführen (z. B. wie in ISO 15003 beschrieben);
- andere typische Funktionen (siehe Anhang F).

7.3.3 Wert von $MTTF_D$

Für die Zwecke von ISO 25119 (alle Teile) muss die $MTTF_D$:

- als gering, mittel oder hoch klassifiziert werden;
- individuell für jeden sicherheitsbezogenen Kanal eines SRP/CS berücksichtigt werden ($MTTF_{DC}$).

Der Wert darf direkt nach Tabelle 4 berechnet oder durch die in Anhang B enthaltenen Verfahren bestimmt werden.

ANMERKUNG Der $MTTF_D$ ist ein reziproker Wert von λ_D .

Tabelle 4 — Mittlere Zeit bis zum gefahrbringenden Ausfall

Bezeichnung	$MTTF_D$ -Anforderung
Niedrig	3 Jahre bis weniger als 10 Jahre
Mittel	10 Jahre bis weniger als 30 Jahre
Hoch	30 Jahre und mehr

7.3.4 Wert für DC

Der Wert für DC muss als gering, mittel oder hoch für die Zwecke von ISO 25119 (alle Teile) klassifiziert werden. Der Wert darf direkt nach Tabelle 5 berechnet oder durch die in Anhang C enthaltenen Verfahren bestimmt werden.

ANMERKUNG 1 Der Diagnosedeckungsgrad kann für ein gesamtes funktionales System mit hohem Risiko oder für Teile gelten wie beispielsweise für Sensoren und/oder Logik-Systeme und/oder Aktoren.

ANMERKUNG 2 Für SRP/CS, die aus mehreren Teilen bestehen, wird ein Durchschnittswert DC_{avg} für DC verwendet (siehe Anhang C).

Tabelle 5 — Diagnosedeckungsgrad (DC)

DC	$\Sigma\lambda_{DD}/\Sigma\lambda_D \times 100 \%$
Niedrig	0 % bis weniger als 60 %
Mittel	60 % bis weniger als 90 %
Hoch	90 % und mehr

7.3.5 Auswahl von Kategorien, $MTTF_{DC}$, DC und SRL

Der AgPL ist eine Funktion der folgenden vier Aspekte:

- Kategorie (siehe Anhang A);
- $MTTF_{DC}$ (siehe Anhang B);
- DC (siehe Anhang C);
- SRL nach ISO 25119-3:2018, Abschnitt 7.

Darüber hinaus müssen während des Systementwurfs folgende Punkte betrachtet werden:

- CCF für Architekturen der Kategorie 3 und 4 (siehe Anhang D);
- Änderungen des SRP/CS mit einem AgPL von mindestens "a" oder höher sollten nur durch verantwortliche Personen (oder Dienstleister) vorgenommen werden, die von dem Hersteller des Systems autorisiert wurden. Ein praktikabler Schutz gegen nicht autorisierte Änderungen nach ISO 25119-4:2018, Abschnitt 11 muss in Betracht gezogen werden.

Wie in Bild 2 angegeben, kann es möglich sein, mehr als eine Kombination aus Zuverlässigkeit (DC, SRL) und Architektur (Cat) zu verwenden, um den $AgPL_r$ zu erreichen. So ist es beispielsweise möglich, dass eine Einkanalarchitektur hoher Zuverlässigkeit den gleichen Performance Level erreicht wie durch eine Zweikanalarchitektur geringerer Zuverlässigkeit (siehe Bild 2).

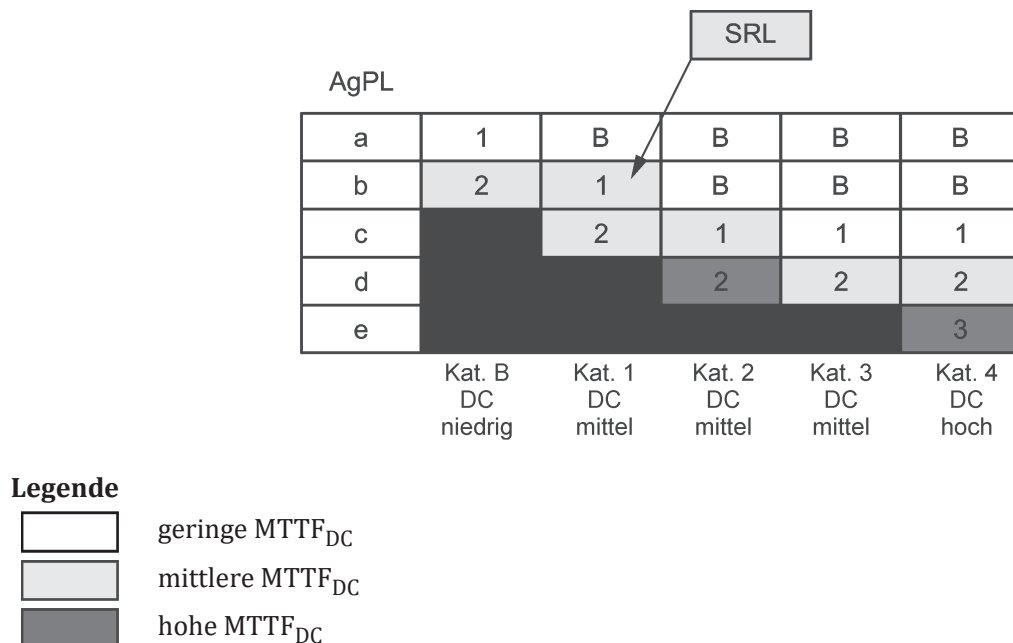


Bild 2 — Beziehung zwischen AgPL, Kategorien, $MTTF_{DC}$, DC und SRL

Auf der vertikalen Achse von Bild 2 ist der AgPL dargestellt. Die Hardware-Kategorien werden auf der horizontalen Achse aufgelistet. Jeder Kategorie sind ein Diagnosedeckungsgrad (DC), eine mittlere Zeit bis zu einem gefahrbringenden Ausfall ($MTTF_{DC}$) und ein Anforderungsniveau an die Software (SRL) zu einem gegebenen AgPL zugeordnet.

Für den AgPL muss der Konstrukteur eine Hardware-Kategorie auswählen.

ANMERKUNG Wird eine höhere Kategorie für einen gegebenen AgPL gewählt, so ist ein niedrigerer Wert für $MTTF_{DC}$ und/oder SRL möglich.

7.3.6 Erreichen des $AgPL_r$

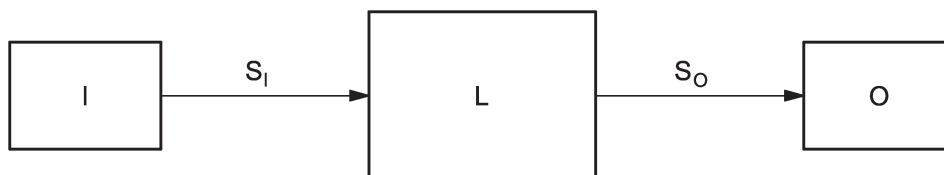
Eine sicherheitsrelevante Funktion darf durch ein oder mehrere SRP/CS implementiert werden. Der Konstrukteur darf alle verfügbaren Technologien einzeln oder in Kombination anwenden. Jedes Element darf aus einer anderen Technologie oder mehreren Technologien auf der Grundlage von E/E/PES bestehen. SRP/CS dürfen mit Sicherheitsmaßnahmen aus anderen Technologien wie etwa mechanische Sicherheitsfunktionen (z. B. mechanisch verknüpfte Kontakte) kombiniert werden.

ANMERKUNG Ausfälle von Nicht-E/E/PES liegen nicht im Anwendungsbereich dieses Dokuments.

Das funktionale Sicherheitskonzept muss durch Festlegung der Eigenschaften für ein SRP/CS oder Kombinationen von SRP/CS, die die funktionalen Sicherheitsanforderungen erfüllen, festgelegt werden. Die Auswahl von Hardware-Kategorien, $MTTF_{DC}$, DC und SRL muss so erfolgen, dass der resultierende AgPL des einzelnen oder der Kombination von SRP/CS alle $AgPL_r$ der zugeordneten funktionalen Sicherheitsanforderungen erfüllt oder übertrifft.

Bild 3 zeigt einen typischen Steuerkanal mit den zugeordneten Elementen mit der Aufgabe der Erfüllung einer sicherheitsbezogenen Funktion mit Eingabegerät (I), E/E/PES (L), Ausgabegerät/Leistungssteuerungselement (O) und Verbindungsmittel (z. B. elektrisch, optisch). Alle Verbindungsmittel sind in den SRP/CS enthalten.

BEISPIEL Eingang bestehend aus einem mit einem licht-aktivierten Signalwandler verbundenen Geschwindigkeits-Signalgeber.



Legende

- I Eingabegerät (z. B. Sensor)
- L Logik
- O Ausgabegerät (z. B. Aktor)
- S_I verbindender Signaleingang
- S_O verbindender Signalausgang

Bild 3 — Schema einer Kombination sicherheitsbezogener Teile

7.3.7 Kompatibilität mit anderen funktionalen Sicherheitsnormen

Die Verwendung aus der Anwendung anderer funktionaler Sicherheitsnormen abgeleiteter SRP/CS ist nur in Übereinstimmung mit Anhang H erlaubt.

7.3.8 Verbindung von E/E/PES

Eine Anleitung zur Kombination eines E/E/PES (z. B. Traktor und Arbeitsgerät) ist in Anhang I enthalten.

7.3.9 Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL

Die in Anhang J angegebenen alternativen Verfahren sind zur Bestimmung des gesamten AgPL anzuwenden, wenn es praktikabel ist, mehrere SRP/CS mit bestehenden separaten AgPL zu verbinden.

7.4 Arbeitsprodukte

Das funktionale Sicherheitskonzept muss folgende Arbeitsprodukte haben:

- a) Sicherheitsziele;
- b) funktionale Sicherheitsanforderungen und zugeordneter AgPLr;
- c) ausgewählte Kategorien, $MTTF_{DC}$, DC und SRL;
- d) gegebenenfalls CCF.

Anhang A (normativ)

Vorgesehene Architekturen für SRP/CS

A.1 Allgemeines

Bild 3 und Bild A.1 bis Bild A.3 legen die erforderliche Architektur für jede respektive Hardware-Kategorie fest.

Alle Architekturen müssen bewährte Sicherheitsgrundsätze anwenden wie etwa:

- Vermeidung bestimmter Fehler, z. B. Vermeidung von Kurzschlüssen durch Trennung;
- Verringerung der Wahrscheinlichkeit von Fehlern, z. B. Überdimensionierung oder Leistungsherabsetzung von Bauteilen;
- Kontrolle des Fehlermodus, z. B. durch Sicherstellung eines offenen Stromkreises, wenn es wichtig ist, den Strom im Fall eines Fehlers abzuschalten (üblicherweise offener Kontakt);
- Erkennung von Fehlern vor dem Auftreten der Gefährdung, falls praktikabel.

Die Verwendung bewährter Bauteile wird für die Kategorie B empfohlen und ist für die Kategorien 1 bis 4 vorgeschrieben. Ein bewährtes Bauteil für eine sicherheitsbezogene Anwendung muss ein Bauteil sein, das

- a) in der Vergangenheit weithin erfolgreich in vergleichbaren Anwendungen eingesetzt wurde oder
- b) unter Verwendung von Prinzipien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen nachweisen.

Neu entwickelte Bauteile können als gleichwertig zu bewährten Bauteilen betrachtet werden, wenn sie die vorstehend genannte Bedingung b) erfüllen.

Die Bilder sind keine Beispiele, sondern allgemeine Architekturen. Eine Abweichung von diesen Architekturen ist jederzeit möglich. Jede Abweichung von diesen Kategorien erfordert eine Begründung mittels angemessener Analysewerkzeuge, dass die Architektur die geforderte Kategorie erfüllt.

ANMERKUNG 1 Redundanz wie etwa redundante Messfühler kann angewendet werden, um den Diagnosedeckungsgrad zu verbessern.

ANMERKUNG 2 Andere Hardware-Architekturen sind beispielsweise in IEC 61508-6:2010, Anhang B zu finden.

A.2 Kategorie B (elementar)

A.2.1 Allgemeines

Siehe Bild 3 für die vorgesehene Architektur.

A.2.2 Eigenschaften

- DC = niedrig.
- $MTTF_{DC}$ für Kanal = niedrig bis mittel.
- Die Berücksichtigung von Ausfällen mit gemeinsamer Ursache ist nicht relevant.
- Das Auftreten eines einzelnen Fehlers kann zum Verlust der Sicherheitsfunktion führen.
- Ungeeignet für Ein-Fehler-tolerante Systeme.

A.3 Kategorie 1

A.3.1 Allgemeines

Siehe Bild 3 für die vorgesehene Architektur.

A.3.2 Eigenschaften

- DC = mittel.
- $MTTF_{DC}$ für Kanal = niedrig bis mittel.
- Die Berücksichtigung von Ausfällen mit gemeinsamer Ursache ist nicht relevant.
- Redundante Eingänge sind unter Umständen für den Diagnosedeckungsgrad erforderlich.
- Ungeeignet für Ein-Fehler-tolerante Systeme.
- Verwendung bewährter Komponenten.

Das Auftreten eines einzelnen Fehlers kann zum Verlust der Sicherheitsfunktion führen. In einigen Fällen ist jedoch ein sicherer Zustand erreichbar (beispielsweise bei erkannten Fehlern an den Eingängen).

Der Einzelfehler wird bei oder vor der nächsten Anforderung an die Sicherheitsfunktionen erkannt, indem gegebenenfalls eine Prüfung bei Einschalten der Sicherheitsfunktion und/oder eine regelmäßige Prüfung durchgeführt wird/werden.

Diese Prüfung kann automatisch oder von Hand eingeleitet werden. Die Prüfung selbst darf nicht zu einer gefährlichen Situation führen. Jede Prüfung der Sicherheitsfunktion(en) muss entweder

- a) den Betrieb gestatten, wenn keine Fehler erkannt wurden, oder
- b) ein Ausgangssignal erzeugen, das einen entsprechenden Steuervorgang einleitet, wenn ein Fehler erkannt wird.

Geeignete Kontrollmaßnahmen können unter anderem Folgendes umfassen:

- sicherer Zustand;
- Warnung der Bedienperson;
- Deaktivierung der Funktion beim Start.

Wenn nach der Erkennung eines Fehlers ein sicherer Zustand durch das SRP/CS initiiert wird, muss der sichere Zustand aufrechterhalten werden, bis der Fehler beseitigt wurde.

ANMERKUNG 1 Dem/den Bauteil(en), das/die Kontrollmaßnahmen nach der Erkennung eines Fehlers ausführt/ausführen, wird kein SRL, $MTTF_D$, DC zugeordnet.

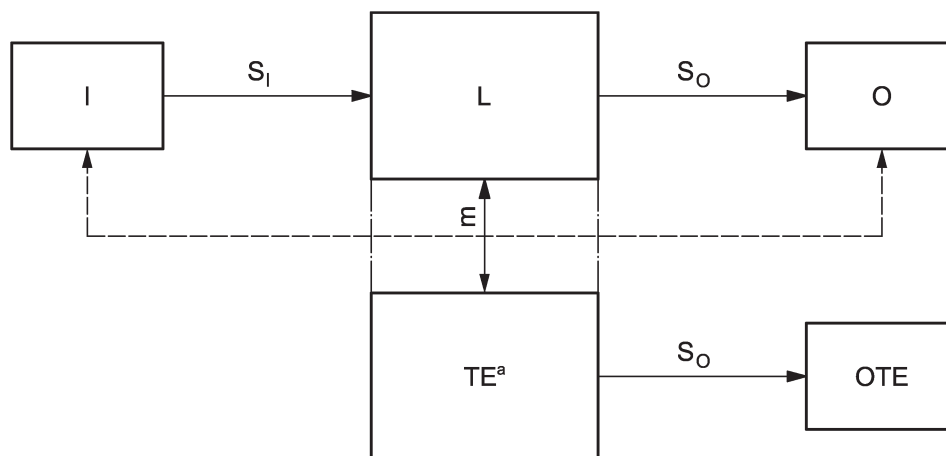
ANMERKUNG 2 Dem/den Bauteil(en), das/die die Warnung an die Bedienperson ausgibt/ausgeben, wird kein SRL, $MTTF_D$, DC zugeordnet.

Das Auftreten eines einzelnen Fehlers kann zu einem Verlust der Sicherheitsfunktion führen, doch die Wahrscheinlichkeit des Auftretens ist geringer als bei Kategorie B.

A.4 Kategorie 2

A.4.1 Allgemeines

Siehe Bild A.1 für die bezeichnete Architektur.



Legende

- I Eingabegerät (z. B. Sensor)
- L Logik
- O Ausgabegerät (z. B. Aktor)
- TE Prüfgerät (zusätzlich zur Logik)
- OTE Ausgang des Prüfgeräts
- S_1 verbindender Signaleingang
- S_0 verbindender Signalausgang
- m Überwachung
- a notwendig zum Erreichen des Diagnosedeckungsgrads, jedoch nicht zwingend ein separater Kanal.

Bild A.1 — Vorgesehene Architektur für 2

A.4.2 Eigenschaften

- Eingangssensor- und Ausgangsaktorfehler werden in der Prüfeinrichtung erkannt.
- DC = mittel.
- $MTTF_{DC}$ für Kanal = niedrig, mittel, hoch.
- Die Berücksichtigung von Ausfällen mit gemeinsamer Ursache ist nicht relevant.
- Redundante Eingänge sind unter Umständen für den Diagnosedeckungsgrad erforderlich.
- Ausgänge „O“ und „OTE“ können je nach sicherem Zustand in Reihe oder parallel geschaltet werden.
- Ungeeignet für Ein-Fehler-tolerante Systeme.
- Warnung der Bedienungsperson ist erforderlich.
- Verwendung bewährter Komponenten.
- Die MTTF des OTE wird berücksichtigt.
- Das Auftreten eines einzigen Fehlers kann zum Verlust der Sicherheitsfunktion führen, jedoch wird ein sicherer Zustand erreicht, wenn der Fehler erkannt wird, sofern praktikabel.

Der Einzelfehler wird bei oder vor der nächsten Anforderung an die Sicherheitsfunktionen erkannt, indem gegebenenfalls eine Prüfung bei Einschalten der Sicherheitsfunktion und/oder eine regelmäßige Prüfung durchgeführt wird/werden.

Die Einleitung dieser Prüfung muss nach Möglichkeit automatisch erfolgen oder manuell, wenn dies nicht möglich ist. Die Prüfung selbst darf nicht zu einer gefährlichen Situation führen. Die Prüfausrüstung kann in den (die) sicherheitsbezogene(n) Teil(e), der/die die Sicherheitsfunktion bereitstellt/bereitstellen, integriert oder davon getrennt sein. Jede Prüfung der Sicherheitsfunktion(en) muss entweder

- a) den Betrieb gestatten, wenn keine Fehler erkannt wurden, oder
- b) ein Ausgangssignal erzeugen, das einen entsprechenden Steuervorgang einleitet, wenn ein Fehler erkannt wird.

Dieses Ausgangssignal muss nach Möglichkeit und unter Berücksichtigung der $MTTF_D$ und DC einen sicheren Zustand einleiten. Ist die Einleitung eines sicheren Zustands nicht möglich (z. B. Verschmoren des Kontakts im Schaltgerät), so muss das Ausgangssignal die Bedienungsperson vor der Gefahr warnen. Wenn nach der Erkennung eines Fehlers ein sicherer Zustand durch das SRP/CS initiiert wird, muss der sichere Zustand aufrechterhalten werden, bis der Fehler beseitigt wurde.

ANMERKUNG 1 In manchen Fällen ist Kategorie 2 nicht anwendbar, weil die Prüfung der Sicherheitsfunktion nicht auf alle Bauteile anwendbar und darum der DC nicht erreichbar ist, wie etwa für Druckschalter oder Temperaturfühler.

ANMERKUNG 2 Im Allgemeinen kann Kategorie 2 mit elektrischen Mitteln realisiert werden (z. B. in Schutzeinrichtungen und in speziellen Steuerungen).

ANMERKUNG 3 Es gibt Bauteile mit hoher Zuverlässigkeit, die nur von Zeit zu Zeit überprüft werden müssen. Geschwindigkeitssensoren können nur im Betrieb (Sensor zählt) überprüft werden, jedoch können Funktionalität und Leitungsunterbrechungen während des Startprogramms geprüft werden. Maschinen werden in der Regel mehrmals täglich gestartet, d. h. es werden mehrere Prüfprogramme je Tag ausgeführt.

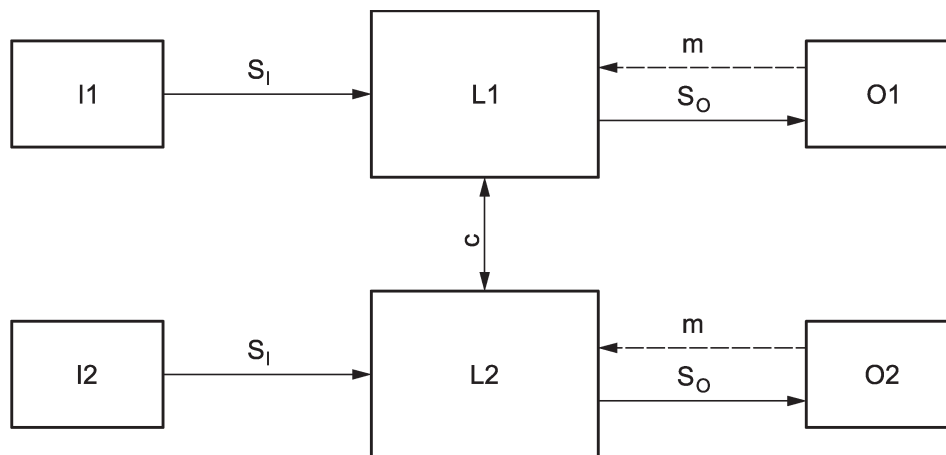
ANMERKUNG 4 In manchen Fällen führt die Bedienperson zur Überprüfung sicherheitsbezogener Teile wie etwa Sitzschalter eine regelmäßige manuelle Prüfung durch.

ANMERKUNG 5 Dem/den Bauteil(en), das/die die Warnung an die Bedienperson ausgibt/ausgeben, wird kein SRL, $MTTF_D$, DC zugeordnet.

A.5 Kategorie 3

A.5.1 Allgemeines

Siehe Bild A.2 für die bezeichnete Architektur.



Legende

- I1, I2 Eingabegerät (z. B. Sensor)
- L1, L2 Logik
- O1, O2 Ausgabegerät, z. B. Aktor
- S_I verbindender Signaleingang
- S_O verbindender Signalausgang
- m Überwachung
- c Querüberwachung

Bild A.2 — Vorgesehene Architektur für 3

A.5.2 Eigenschaften

- Eingangssensor-, Logik- und Ausgangsaktorfehler werden in der Steuerlogik erkannt.
- DC = mittel.
- $MTTF_{DC}$ für Kanal = niedrig, mittel.
- Die Betrachtung von Ausfällen mit gemeinsamer Ursache ist erforderlich (siehe Anhang D).
- Redundante Eingänge sind unter Umständen für den Diagnosedeckungsgrad erforderlich.
- Zusätzliche redundante Ausgänge sind unter Umständen für einen sicheren Zustand erforderlich.
- Ausgänge O1 und O2 können je nach sicherem Zustand in Reihe oder parallel geschaltet werden.
- Geeignet für Ein-Fehler-tolerante Systeme mit redundanter Stromversorgung.

- Warnung der Bedienungsperson ist erforderlich.
- Verwendung bewährter Komponenten.
- Wenn ein erkannter Einzelfehler auftritt, wird die Sicherheitsfunktion stets ausgeführt oder das System fällt in einen sicheren Zustand aus, jedoch kann eine Anhäufung unerkannter Fehler zum Verlust der Sicherheitsfunktion führen.

Wann immer dies sinnvoll durchführbar ist, wird der Einzelfehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt, indem gegebenenfalls eine Prüfung beim Einschalten der Sicherheitsfunktion und/oder eine regelmäßige Prüfung, falls erforderlich, durchgeführt wird/werden.

Die Einleitung dieser Prüfung muss nach Möglichkeit automatisch erfolgen oder manuell, wenn dies nicht möglich ist. Die Prüfung selbst darf nicht zu einer gefährlichen Situation führen. Die Prüfausrüstung kann in den (die) sicherheitsbezogene(n) Teil(e), der/die die Sicherheitsfunktion bereitstellt/bereitstellen, integriert oder davon getrennt sein. Jede Prüfung der Sicherheitsfunktion(en) muss entweder

- a) den Betrieb gestatten, wenn keine Fehler erkannt wurden, oder
- b) ein Ausgangssignal erzeugen, das einen entsprechenden Steuervorgang einleitet, wenn ein Fehler erkannt wird.

Dieses Ausgangssignal muss nach Möglichkeit und unter Berücksichtigung der $MTTF_D$, DC und CCF einen sicheren Zustand einleiten. Das System muss die Bedienungsperson warnen, sobald ein Fehlerzustand erkannt wird. Wenn nach der Erkennung eines Fehlers ein sicherer Zustand durch das SRP/CS initiiert wird, muss der sichere Zustand aufrechterhalten werden, bis der Fehler beseitigt wurde.

ANMERKUNG 1 Es gibt Bauteile mit hoher Zuverlässigkeit, die nur von Zeit zu Zeit überprüft werden müssen. Geschwindigkeitssensoren können nur im Betrieb (Sensor zählt) überprüft werden, jedoch können Funktionalität und Leitungsunterbrechungen während des Startprogramms geprüft werden. Maschinen werden in der Regel mehrmals täglich gestartet, d. h. es werden mehrere Prüfprogramme je Tag ausgeführt.

ANMERKUNG 2 In manchen Fällen führt die Bedienungsperson zur Überprüfung sicherheitsbezogener Teile wie etwa Sitzschalter eine regelmäßige manuelle Prüfung durch.

ANMERKUNG 3 Diese Anforderung an die Einzelfehlererkennung heißt nicht, dass alle Fehler erkannt werden. Daher kann eine Anhäufung unerkannter Fehler zu einem unbeabsichtigten Ausgangssignal und zu einer gefährlichen Situation an der Maschine führen. Typische Beispiele für durchführbare Maßnahmen zur Fehlererkennung sind die gekoppelte Bewegung von Relaiskontakten und die Überwachung redundanter elektrischer Ausgangssignale.

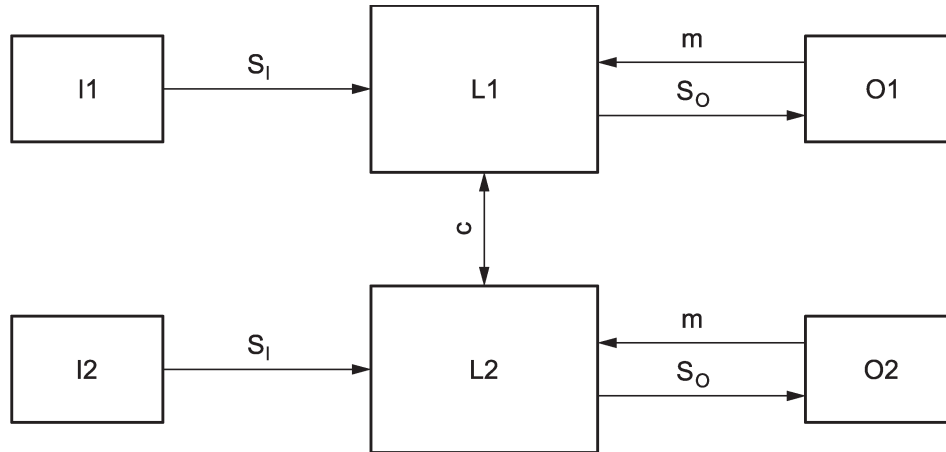
ANMERKUNG 4 Es wird empfohlen, den/die Fehlerzustand(e) zur späteren Bewertung zu speichern.

ANMERKUNG 5 Dem/den Bauteil(en), das/die die Warnung an die Bedienungsperson ausgibt/ausgeben, wird kein SRL, $MTTF_D$, DC zugeordnet.

A.6 Kategorie 4

A.6.1 Allgemeines

Siehe Bild A.3 für die bezeichnete Architektur.



Legende

- I1, I2 Eingabegerät (z. B. Sensor)
- L1, L2 Logik
- O1, O2 Ausgabegerät, z. B. Aktor
- S_I verbindender Signaleingang
- S_O verbindender Signalausgang
- m Überwachung
- c Querüberwachung

ANMERKUNG Feste Überwachungsleitungen stellen einen Diagnosedeckungsgrad dar, der höher als in der vorgesehenen Architektur für Kategorie 3 ist.

Bild A.3 — Vorgesehene Architektur für 4

A.6.2 Eigenschaften

- Eingangssensor-, Logik- und Ausgangsaktorfehler werden in der Steuerlogik erkannt.
- DC = hoch.
- MTTF_{DC} für Kanal = niedrig, mittel, hoch_{DD}.
- Die Betrachtung von Ausfällen mit gemeinsamer Ursache ist erforderlich (siehe Anhang D).
- Redundante Eingänge sind unter Umständen für den Diagnosedeckungsgrad erforderlich.
- Zusätzliche redundante Ausgänge sind unter Umständen für einen sicheren Zustand erforderlich.
- Ausgänge 1 und 2 können je nach sicherem Zustand in Reihe oder parallel geschaltet werden.
- Geeignet für Ein-Fehler-tolerante Systeme mit redundanter Stromversorgung.
- Warnung der Bedienungsperson ist erforderlich.
- Verwendung bewährter Komponenten.

- Beim Auftreten eines erkannten Einzelfehlers wird die Sicherheitsfunktion stets ausgeführt oder das System fällt in einen sicheren Zustand aus. Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen, jedoch ist die Eintrittswahrscheinlichkeit geringer als bei Kategorie 3.

Der Einzelfehler wird bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt, indem gegebenenfalls eine Prüfung beim Einschalten der Sicherheitsfunktion und/oder eine regelmäßige Prüfung durchgeführt wird/werden.

Die Einleitung dieser Prüfung muss nach Möglichkeit automatisch erfolgen oder manuell, wenn dies nicht möglich ist. Die Prüfung selbst darf nicht zu einer gefährlichen Situation führen. Die Prüfausrüstung kann in den (die) sicherheitsbezogene(n) Teil(e), der/die die Sicherheitsfunktion bereitstellt/bereitstellen, integriert oder davon getrennt sein. Jede Prüfung der Sicherheitsfunktion(en) muss entweder

- a) den Betrieb gestatten, wenn keine Fehler erkannt wurden, oder
- b) ein Ausgangssignal erzeugen, das einen entsprechenden Steuervorgang einleitet, wenn ein Fehler erkannt wird.

Dieses Ausgangssignal muss nach Möglichkeit und unter Berücksichtigung der $MTTF_D$, DC und CCF einen sicheren Zustand einleiten. Das System muss die Bedienperson warnen, sobald ein gefahrbringender Fehlerzustand erkannt wird. Wenn nach der Erkennung eines Fehlers ein sicherer Zustand durch das SRP/CS initiiert wird, muss der sichere Zustand aufrechterhalten werden, bis der Fehler beseitigt wurde.

ANMERKUNG 1 Es gibt Bauteile mit hoher Zuverlässigkeit, die nur von Zeit zu Zeit überprüft werden müssen. Geschwindigkeitssensoren können nur im Betrieb (Sensor zählt) überprüft werden, jedoch können Funktionalität und Leitungsunterbrechungen während des Startprogramms geprüft werden. Maschinen werden in der Regel mehrmals täglich gestartet, d. h. es werden mehrere Prüfprogramme je Tag ausgeführt.

ANMERKUNG 2 In manchen Fällen führt die Bedienperson zur Überprüfung sicherheitsbezogener Teile wie etwa Sitzschalter eine regelmäßige manuelle Prüfung durch.

ANMERKUNG 3 Diese Anforderung an die Einzelfehlererkennung heißt nicht, dass alle Fehler erkannt werden. Daher kann eine Anhäufung unerkannter Fehler zu einem unbeabsichtigten Ausgangssignal und zu einer gefährlichen Situation an der Maschine führen. Typische Beispiele für durchführbare Maßnahmen zur Fehlererkennung sind die gekoppelte Bewegung von Relaiskontakten und die Überwachung redundanter elektrischer Ausgangssignale.

ANMERKUNG 4 Es wird empfohlen, den/die Fehlerzustand(e) zur späteren Bewertung zu speichern.

ANMERKUNG 5 Dem/den Bauteil(en), das/die die Warnung an die Bedienperson ausgibt/ausgeben, wird kein SRL, $MTTF_D$, DC zugeordnet.

Anhang B (informativ)

Vereinfachtes Verfahren zur Abschätzung der Kanal-MTTF_{DC}

B.1 Allgemeines

Dieser Anhang beschreibt die zum Berechnen der Kanal-MTTF_{DC} angewendeten Verfahren.

Für Zweikanalarchitekturen (Kategorien 3 und 4) wird eine Gleichung für die Berechnung der symmetrischen Kanal-MTTF_{DC} angegeben.

Für diese Berechnungen wird das Ground-Mobile-Modell aus den Datenbanken für die Bauteil-Ausfallrate angewendet. Entwurf, Software und Probleme bei der Herstellung werden hierbei nicht berücksichtigt.

Beim Betrachten der Ausfallursachen einiger Bauteile können möglicherweise bestimmte Fehler ausgeschlossen werden. In diesem Fall sollten Analysen oder Daten als Nachweis vorgelegt werden (z. B. überdimensionierter Leiter).

ANMERKUNG 1 ISO 13849-1:2015 Abschnitt 7 und ISO 13849-2:2012, Anhang D enthalten nützliche Informationen zur Fehleranalyse und zu Fehlerausschlüssen.

B.2 MTTF_D-Werte von Bauteilen

B.2.1 Bestimmung der MTTF_D-Werte von Bauteilen aus Normen/Datenbanken

Folgende Normen/Datenbanken und andere liefern MTTF-Werte für Einzelbauteile:

- MIL-HDBK-217F^[9];
- SN 29500^[10];
- RDF 2000^[11];
- IEC/TR 62380^[12];
- FIDES Guide 2004^[13].

Für den Zugriff auf diese Datenbanken stehen Software-Werkzeuge zur Verfügung. Beim Abrufen von Daten aus diesen Datenbanken sollte der Konstrukteur die Lastspiele und das Beanspruchungsniveau der Bauteile (Wärme, Leistung usw.) angeben. Bei Steckern, Schützen, Sicherungen usw. sollte bei der Angabe der Lastspiele besonders vorsichtig vorgegangen werden, weil diese Bauteile häufig mit der Anzahl der Lastspiele (B_{10D}) bemessen werden. Leiter sind nicht enthalten.

Wenn der Konstrukteur des E/E/PES über zuverlässige spezifische Daten der eingesetzten Bauteile verfügt, wird besonders empfohlen, diese spezifischen Daten anstelle der vorstehend gelisteten Verweisungen zu verwenden.

Bei der Umrechnung der MTTF in die $MTTF_D$ wird empfohlen, entweder:

- den Ausfallmodus jeder Komponente unter Anwendung einer Gefahrenanalyse in Verbindung mit einer Fehlerbaumanalyse oder einem vergleichbaren Analyseverfahren zu bewerten, um den tatsächlichen Prozentsatz gefahrbringender Ausfälle zu ermitteln, oder
- die konservative Annahme, dass 50 % aller Ausfälle gefahrbringend sind, anzuwenden.

Ein Ausfall, der korrigiert wird, bevor er zu einer gefahrbringenden Situation in einem E/E/PES-System führt, kann vernachlässigt werden. Im Speicher des Controllers ist der Fehlerkorrekturcode (ECC) ein Beispiel für einen Mechanismus, der einen Fehler korrigiert, bevor er Schaden verursachen kann. Die Überwachung des ECC während des Betriebs und der Prüfung des Korrekturmechanismus während der Boot-Phase des Controller-Speichers wird dringend empfohlen.

$MTTF_D = MTTF / \text{Prozentsatz an gefahrbringenden Ausfällen}$ (siehe Tabelle B.1).

Die Bauteile sollten nicht in Systemen eingesetzt werden, die über die vom Bauteil-Hersteller angegebenen Grenzwerte hinaus betrieben werden.

Alternativ kann die MTTF mithilfe einer der folgenden Methoden oder von Kombinationen derselben bestimmt werden:

- c) bewährt im Einsatz unter gegebenen Anforderungen an Umgebung und Betrieb;
- d) Prüfung;
- e) Analysen.

Bei der Prüfung wird das elektronische Bauteil den Umgebungs- und Betriebsbedingungen ausgesetzt, für die es entworfen wurde, und die Erfüllung der Anforderungen wird überprüft.

B.2.2 Bestimmung der $MTTF_D$ -Werte von Bauteilen anhand von im Einsatz bewährten Bauteilen

Bestehende Hardware kann im Einsatz bewährte Daten im folgenden Verfahren anwenden, um die $MTTF_D$ für den Kanal oder das System zu bestimmen.

Verwendung von Daten (z. B. Zwischenfallberichte und -analysen) aus einem kontrollierten Prozess zur Berechnung der historischen erreichten $MTTF_D$ durch:

- a) Bestimmung einer statisch signifikanten Probe der Population:
 - 1) Bestimmung der Gesamtbetriebszeit der Probe der Population (T);
 - 2) Bestimmung der Gesamtzahl gefahrbringender Ausfälle der Probe der Population (r);
- b) Die Gleichung für die Konfidenz um $MTTF_D$ stellt sich wie folgt dar:

1) $MTTF_D = \frac{2T}{\chi^2_{(\alpha, 2R+2)}}$;

2) $\chi^2_{(\alpha, 2r+2)}$ = Chi-Quadrat-Verteilung:

- i) χ^2 ist das Symbol der Chi-Quadrat-Verteilung;

- ii) $(\alpha, 2r + 2)$ legt die Parameter für die Berechnung von Chi-Quadrat fest;
- iii) $\alpha = 1 - \text{Konfidenzniveau}$;
- 3) Das Konfidenzniveau muss mindestens 70 % betragen;
- c) Die Wirkungsanalyse sollte angewendet werden, um historische Daten anzupassen, wenn die erwartete Betriebsumgebung mehr oder weniger belastend ist.
 - 1) Dies kann durch ein Beschleunigungsmodell wie Arrhenius oder Inverse Power Law erfolgen.

B.2.3 MTTF_D für Bauteile aus B₁₀

Für elektromechanische Bauteile (z. B. Relais, Schütze, Schalter usw.) ist es unter Umständen schwierig, die mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF_D) zu berechnen. Die Hersteller dieser Art von Bauteilen geben oftmals nur die mittlere Anzahl der Zyklen an, bis 10 % der Bauteile ausfallen (B₁₀) oder gefahrbringend ausfallen (B_{10D}). In diesem Abschnitt wird ein Verfahren zur Berechnung einer MTTF_D für Bauteile unter Verwendung von B₁₀ entsprechend Herstellerangaben beschrieben.

Gibt der Hersteller B_{10D} nicht an, ist es üblich, B₁₀ in B_{10D} umzurechnen durch die Annahme, dass 50 % der Ausfälle gefahrbringend sind:

$$B_{10D} = 2 B_{10}$$

MTTF_D kann anhand der Gleichung (B.1) geschätzt werden:

$$MTTF_D = \frac{B_{10D}}{0,1 \times n_{op}} \quad (B.1)$$

Um die Anzahl der Betätigungen, n_{op} , zu berechnen, müssen einige Annahmen zu der Anwendung des Bauteils getroffen werden. Siehe Gleichung (B.2):

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600}{t_{cycle}} \quad (B.2)$$

Dabei ist

h_{op} die mittlere Betriebsdauer, in Stunden je Tag;

d_{op} die mittlere Betriebsdauer, in Tagen je Jahr;

t_{cycle} die mittlere Zeit zwischen dem Beginn von zwei aufeinander folgenden Lastspielen des Bauteils (z. B. Schalten eines Ventils), in Sekunden.