

DIN EN ISO 25119-1



ICS 35.240.99; 65.060.01

Einsprüche bis 2018-12-12
Vorgesehen als Ersatz für
DIN EN 16590-1:2014-11

Entwurf

**Traktoren und Maschinen für die Land- und Forstwirtschaft –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze
(ISO/FDIS 25119-1:2018);
Deutsche und Englische Fassung FprEN 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/FDIS 25119-1:2018);
German and English version FprEN ISO 25119-1:2018

Tracteurs et matériels agricoles et forestiers –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux pour la conception et le développement
(ISO/FDIS 25119-1:2018);
Version allemande et anglaise FprEN ISO 25119-1:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-10-12 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@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 Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64, 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 68 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

Sie beinhaltet die Deutsche Fassung der vom Technischen Komitee ISO/TC 23 „Tractors and Machinery for Agriculture and Forestry“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 144 „Traktoren und land- und forstwirtschaftliche Maschinen“ im Europäischen Komitee für Normung (CEN) ausgearbeiteten FprEN ISO 25119-1:2018.

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 wurden 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 sicherheitsbezogenen Teilen von Steuerungen für Traktoren und Maschinen für die Land- und Forstwirtschaft sowie der Berufsgenossenschaften waren 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.

Die im Abschnitt 2 und den Literaturhinweisen zitierten Internationalen Normen sind, sofern diese gleichzeitig als Europäische Normen übernommen worden sind, als DIN-EN-ISO-Normen mit gleicher Zählnummer veröffentlicht.

Für die zitierten Internationalen Normen und Dokumente, sofern sie nicht als DIN-ISO-Normen mit gleicher Zählnummer veröffentlicht sind, gibt es keine nationalen Entsprechungen.

Änderungen

Gegenüber DIN EN 16590-1:2014-11 wurden folgende Änderungen vorgenommen:

- a) die ISO 25119-1 wurde überarbeitet und an EN 16590-1 angepasst, sodass keine modifizierte Übernahme unter anderer Normnummer notwendig ist.

**Traktoren und Maschinen für die Land- und Forstwirtschaft —
Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine
Gestaltungs- und Entwicklungsleitsätze (ISO/FDIS 25119-1:2018)**

*Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 1 :
Principes généraux pour la conception et le développement (ISO/FDIS 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/FDIS 25119-1:2018)*

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: parallele formelle Abstimmung vorgelegt
Dokumentsprache: D

STD Version 2.9d

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	9
3 Begriffe	9
4 Abkürzungen	16
5 Qualitätsmanagementsystem	17
6 Management während des gesamten Sicherheitslebenszyklus	17
6.1 Ziele	17
6.2 Allgemeines	17
6.2.1 Einführung in das Konzept des Sicherheitslebenszyklus	17
6.2.2 Externe funktionale Sicherheitsmaßnahmen	17
6.3 Voraussetzungen	18
6.4 Anforderungen — Aktivitäten des funktionalen Sicherheitsmanagements über alle Lebenszyklen hinweg	20
6.4.1 Kultur der funktionalen Sicherheit	20
6.4.2 Ständige Verbesserung	21
6.4.3 Schulung und Qualifizierung	21
6.4.4 Zuweisung der Verantwortlichkeiten für die Sicherheit	21
6.4.5 Zuweisung der Aufgaben	21
6.4.6 Planung aller Sicherheitsmanagementaktivitäten während der Entwicklung	22
6.5 Arbeitsprodukte	23
7 Beurteilung der funktionalen Sicherheit	24
7.1 Ziele	24
7.2 Allgemeines	24
7.3 Voraussetzungen	24
7.4 Anforderungen	24
7.4.1 Hinweise für die Bewertung der funktionalen Sicherheit	24
7.4.2 Verifizierung	25
7.5 Arbeitsprodukte	27
8 Funktionale Sicherheitsmanagementaktivitäten nach Produktionsanlauf (SOP)	27
8.1 Ziele	27
8.2 Allgemeines	27
8.3 Voraussetzungen	27
8.4 Anforderungen	27
8.4.1 Produktionsmanagement und Modifikationsprozeduren	27
8.4.2 Aufgaben zur Vorbereitung und Durchführung der Fertigung und End-of-Line- Kontrollen	27
8.4.3 Aufgaben für den sicheren Betrieb, die Instandhaltung, die Instandsetzung und die Außerbetriebnahme der Maschine	28
8.5 Arbeitsprodukte	28
9 Plan für die Herstellung und Installation sicherheitsbezogener Systeme	28

9.1	Ziele	28
9.2	Allgemeines	29
9.3	Voraussetzungen	29
9.4	Anforderungen	29
9.4.1	Produktionsplan	29
9.4.2	Prüfplan	29
9.4.3	Produktion und Prüfung	29
9.4.4	Prozessfähigkeit	29
9.4.5	Dokumentation	30
9.4.6	Nichterfüllung	30
9.4.7	Rückverfolgbarkeit	30
9.4.8	Lager- und Transportbedingungen	30
9.4.9	Änderung	30
9.5	Arbeitsprodukte	30
	Anhang A (informativ) Beispiel für die Gliederung eines projektspezifischen Sicherheitsplans	31
A.1	Allgemeines	31
A.2	Änderungsprotokoll	31
A.3	Ziel des Gesamtprojekts	31
A.4	Terminplan	31
A.5	Projektorganisation	31
A.5.1	Projektteamorganisation	31
A.5.2	Projektteammitglieder	32
A.5.3	Sicherheitsmanagement	32
	Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG	34
	Literaturhinweise	35

Europäisches Vorwort

Dieses Dokument (FprEN ISO 25119-1:2018) wurde vom Technischen Komitee ISO/TC 23 „Tractors and Machinery for Agriculture and Forestry“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 144 „Traktoren und land- und forstwirtschaftliche Maschinen“ erarbeitet, dessen Sekretariat von AFNOR gehalten wird.

Dieses Dokument ist derzeit zur parallelen formellen Abstimmung vorgelegt.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelszone CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinien.

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

Anerkennungsnotiz

Der Text von ISO/FDIS 25119-1:2018 wurde von CEN als FprEN ISO 25119-1:2018 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von ISO Technischen Komitees 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*, Subcommittee SC 19, *Agricultural electronics* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 25119-1:2010), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Die Einleitung wurde geändert, um spezifische Informationen zu Sicherheitsnormen hinzuzufügen;
- Die Tabellen 1 bis 3 wurden gelöscht und die nachfolgenden Tabellen neu nummeriert;
- Abschnitt 5 (Managementsystem) wurde eingefügt und die nachfolgenden Abschnitte wurden neu nummeriert;
- In 8.5 wurden die Arbeitsprodukte der Sicherheitsmanagementaktivitäten nach SOP festgelegt;
- Bild 2 wurde geändert;
- das Dokument wurde redaktionell überarbeitet.

Eine Liste aller Teile der Normenreihe ISO 25119 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an die nationale Normungsorganisation des Anwenders gerichtet werden. Ein vollständiges Verzeichnis dieser Organisationen kann unter www.iso.org/members.html abgerufen werden.

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 sicherheitsbezogenes Teil 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 darf 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 wie etwa 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, die zu potenziellen gefahrbringenden Situationen führen, hervorrufen können, 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 stellt allgemeine Grundlagen und Leitsätze heraus für die Gestaltung und 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:

- 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 gestaltetes 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.

Dieses Dokument 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 25119-2:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

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 processes*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

— ISO Online Browsing Platform: unter <https://www.iso.org/obp>

— IEC Electropedia: unter <http://www.electropedia.org/>

3.1

landwirtschaftlicher Performance Level (en: agricultural performance level)

AgPL

Level, der die Fähigkeit von sicherheitsbezogenen Teilen des Steuerungssystems spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

Anmerkung 1 zum Begriff: In ISO 25119 (alle Teile) ist die Performance für jede Funktion in die fünf Stufen a, b, c, d und e unterteilt, wobei die vom SRP/CS beigesteuerte funktionale Sicherheit in „a“ niedrig und in „e“ hoch ist.

3.2

geforderter landwirtschaftlicher Performance Level (en: required agricultural performance level)

AgPL_r

zu erreichende(r) Performance Level (AgPL) für jede Sicherheitsfunktion

Anmerkung 1 zum Begriff: Je nach potenziellem Verhalten einer fehlerhaften UoO kann eine Sicherheitsfunktion mehr als einen AgPL_r haben. So können beispielsweise ein teilweiser Verlust einer Funktion, der plötzliche vollständige Verlust einer Funktion und die Unfähigkeit, eine Funktion zu ermöglichen, drei unterschiedliche AgPL_r haben.

3.3

Kategorie

Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstands gegen gefahrbringende Ausfälle unter Berücksichtigung des nachfolgenden Verhaltens im Fehlerzustand, das durch die bauliche Anordnung (Architektur) der Teile erreicht wird

3.4

Kanal

Kombination aus Eingabe-, Logik- und Ausgabeelementen, die erforderlich ist, um eine oder mehrere Funktion(en) auszuführen

3.5

Ausfall infolge gemeinsamer Ursache (en: common-cause failure)

CCF

mehrere Ausfälle innerhalb einer UoO aufgrund eines einzelnen Ereignisses, wenn diese Ausfälle nicht auf einer gegenseitigen Ursache beruhen

Anmerkung 1 zum Begriff: Ausfälle infolge gemeinsamer Ursache sollten nicht mit gleichartigen Ausfällen verwechselt werden, da gleichartige Ausfälle unterschiedliche Ursachen haben können.

3.6

Beherrschbarkeit

Möglichkeit der betroffenen Person, Schaden in der sie gefährdenden Situation zu vermeiden

3.7

erkannte gefahrbringende Ausfallrate

λ_{DD}

erkannte Ausfallrate innerhalb der UoO, die zu keiner oder einer minimalen Erhöhung des Risikos führt, jedoch bei Nichterkennung zu einer unmittelbaren Erhöhung des Risikos führen würde

3.8

gefahrbringender Ausfall

ein Ausfall (und mehrere Ausfälle mit gemeinsamer Ursache), bei dem ein SRP/CS nicht mehr in der Lage ist, die vorgesehene Funktion aufrechtzuerhalten und das resultierende Maschinenverhalten zu einer Gefährdungssituation führen könnte

3.9

gefährliche Ausfallrate

λ_D

Anteil aller Komponenten mit einem *gefahrbringenden Ausfall* (3.8) pro Zeiteinheit

Anmerkung 1 zum Begriff: λ_D ist der Kehrwert des $MTTF_D$.

3.10

Diagnosedeckungsgrad

DC

Anteil der Wahrscheinlichkeit erkannter gefahrbringender Ausfälle λ_{DD} und der Wahrscheinlichkeit der gesamten *gefahrbringenden Ausfälle* λ_D (3.9)

3.11

Diagnoseprüfintervall

Intervall zwischen Online-Tests zur Erkennung von Fehlern in einem sicherheitsbezogenen System, die einen vorgegebenen *Diagnosedeckungsgrad* (3.10) aufweisen

3.12

E/E/PES-Architektur

Zuweisung von Sicherheitsfunktionen an elektronische Steuereinheiten (ECU) und Klassifizierung in Hardware und Software, einschließlich Kommunikation

3.13

Umgebungsbedingung

physische Bedingungen, unter denen ein System verwendet wird

3.14

Aufenthaltsdauer

Zeitdauer und Häufigkeit, mit der sich eine Person in einer Situation befindet, in welcher die potenzielle Gefahr besteht

3.15

Ausfall

Beendigung der Fähigkeit eines Elements innerhalb der UoO, wie vorgesehen zu funktionieren

Anmerkung 1 zum Begriff: Nach einem Ausfall weist die UoO einen Fehler auf.

Anmerkung 2 zum Begriff: „Ausfall“ ist ein Ereignis, im Unterschied zu einem „Fehler“ (3.16), bei dem es sich um einen Zustand handelt.

Anmerkung 3 zum Begriff: Der so definierte Begriff gilt nicht für eine UoO, die nur aus Software besteht.

3.16

Fehler

Zustand einer UoO, charakterisiert durch die Unfähigkeit, eine geforderte Funktion auszuführen, ausgenommen der Unfähigkeit während vorbeugender Instandhaltung oder sonstiger planmäßiger Arbeiten oder aufgrund eines Mangels an externen Mitteln

Anmerkung 1 zum Begriff: Ein Fehler ist häufig das Ergebnis eines *Ausfalls* (3.15), kann aber auch ohne vorherigen Ausfall auftreten.

Anmerkung 2 zum Begriff: In ISO 25119 (alle Teile) bedeutet der Begriff „Fehler“ *zufälliger Fehler*.

3.17

Funktion

definiertes Verhalten einer oder mehrerer elektronischer Steuereinheiten (ECU)

3.18

funktionale Anforderung

Anforderung an eine vorgesehene Funktion des E/E/PES-Systems

3.19

funktionale Sicherheit

System, das auf eine Weise funktioniert, welche kein unangemessen hohes Verletzungsrisiko eines Bedieners oder Umstehenden darstellt

3.20

funktionales Sicherheitskonzept

die gesamte Sammlung der Anforderungen an die *funktionale Sicherheit* (3.19) einschließlich ihrer Wechselwirkungen zur Erreichung der funktionalen Sicherheit

Anmerkung 1 zum Begriff: Dies wird während der Konzeptphase des Sicherheitslebenszyklus entwickelt.

3.21

funktionale Sicherheitsanforderung

Anforderung an eine Sicherheitsfunktion des E/E/PES-Systems

3.22

Hardware-Sicherheitsanforderung

Anforderung, die sich auf sicherheitsbezogene Hardware bezieht und als Element einer technischen Sicherheitsanforderung darin enthalten ist

3.23

Schaden

physische Verletzung oder Gesundheitsschäden von Personen

3.24

Gefährdung

potenzielle Quelle eines *Schadens* (3.23)

3.25

Gefahrenanalyse und Risikobeurteilung

HARA

Verfahren zur Identifizierung und Einstufung von Gefährdungssituationen der UoO und zur Festlegung von Sicherheitszielen, AgPL_r, in Verbindung mit der Vermeidung oder Minderung der damit verbundenen Gefahren, um ein unangemessenes Risiko zu vermeiden

3.26

Gefährdungssituation

Sachlage, bei der eine Person einer Gefährdung oder mehreren *Gefährdungen* (3.24) ausgesetzt ist, deren *Exposition* (3.14) unmittelbar oder über längere Zeit zu Schäden führen kann/können

3.27

bestimmungsgemäßer Gebrauch

<einer Maschine> in Übereinstimmung mit den in der Benutzerinformation bereitgestellten Informationen

3.28

Inspektion

systematische, formale Überprüfungsmethode zur Bewertung der Produktqualität

Anmerkung 1 zum Begriff: Während einer Inspektion wird das Arbeitsprodukt von einem oder mehreren Begutachtern auf Einhalten der Anforderungen geprüft. Die Inspektion wird von einem Inspektionsleiter organisiert und moderiert. Der Ersteller des Arbeitsprodukts nimmt zwar an der Inspektion teil, darf aber den Prozess nicht selbst leiten.

3.29

Lebensdauer der Maschine

Lebenszyklus

Dauer zwischen Herstellung und Außerbetriebnahme

3.30

manuelle Rückstellung

Funktion innerhalb der SRP/CS zur manuellen Wiederherstellung einer oder mehrerer Sicherheitsfunktionen vor dem Neustart einer Maschine

3.31

Maschinenhersteller

Hersteller von Traktoren für die Land- und Forstwirtschaft, selbstfahrenden Aufsitzmaschinen sowie Anbau-, Aufsattel- und Anhängemaschinen für die Landwirtschaft, sowie von mobilen kommunalen Geräten

Anmerkung 1 zum Begriff: Siehe auch Lieferant (3.50).

3.32

mittlere Zeit bis zum gefahrbringenden Ausfall (en: mean time to dangerous failure)

MTTF_D

erwartete mittlere Zeit bis zu einem *gefahrbringenden* Ausfall (3.8)

Anmerkung 1 zum Begriff: MTTF_D ist der Kehrwert zu λ_D .

3.33

Überwachung

automatische Überwachung

eine automatische Funktion, die sicherstellt, dass eine *Schutzmaßnahme* (3.36) eingeleitet wird, wenn die Fähigkeit SRP/CS, eine Funktion auszuführen, vermindert ist oder die Betriebsbedingungen so verändert werden, dass Gefahren entstehen

3.34

Muting

vorübergehende automatische Unterdrückung einer Sicherheitsfunktion durch sicherheitsbezogene Teile der Steuerung

3.35

programmierbares elektronisches System

PES

System zur Steuerung, zum Schutz oder zur Überwachung, dessen Betrieb von einem oder mehreren programmierbaren elektronischen Geräten abhängt

Anmerkung 1 zum Begriff: Es bezieht alle Elemente des Systems wie Stromversorgung, Sensoren und andere Eingabegeräte, Datenautobahnen und andere Kommunikationswege sowie Aktoren und andere Ausgabegeräte ein.

3.36

Schutzmaßnahme

Maßnahme, mit der die funktionale Sicherheit erreicht werden soll, umgesetzt vom Konstrukteur (eigensichere Konstruktion, Sicherungs- und ergänzende Maßnahmen, Benutzerinformation) und vom Benutzer (Organisation, sichere Arbeitsabläufe, Beaufsichtigung, Arbeitsgenehmigung, Systeme, zusätzliche Sicherungen, persönliche Schutzausrüstung, Schulung)

3.37

vernünftigerweise vorhersehbare Fehlanwendung

Verwendung einer Maschine auf eine vom Konstrukteur nicht beabsichtigte Weise, die sich jedoch aus dem leicht vorhersagbaren menschlichen Verhalten ergeben kann

3.38

Reaktionszeit

maximal verstrichene Zeit zwischen dem Auftreten eines Fehlers und dem Erlangen eines *sicheren Zustands* (3.43)

3.39

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines *Schadens* (3.23) und seiner *Schwere* (3.47)

3.40

Risikoanalyse

Kombination aus der Festlegung der Grenzen der Maschine, der Gefährdungsidentifikation und der Risikoeinschätzung

3.41

Risikobeurteilung

Gesamtheit eines Verfahrens, bestehend aus *Risikoanalyse* (3.40) und *Risikobewertung* (3.42)

3.42

Risikobewertung

Beurteilung anhand der Risikoanalyse bzw. ob ein akzeptables Risiko erreicht ist

3.43

sicherer Zustand

Betriebszustand eines Systems, verbunden mit einem tragbaren Risiko

BEISPIEL vorgesehener Betriebsmodus, Back-up-Betriebsmodus oder abgeschaltete Betriebsmodi.

3.44

Sicherheitsziel

Beschreibung, wie eine bestimmte Gefährdung vermeidbar ist

BEISPIEL Vermeiden einer Bewegung im Leerlauf.

Anmerkung 1 zum Begriff: Dies ist das oberste Ziel als Ergebnis der Gefahrenanalyse und Risikobeurteilung und wenn Sicherheitsfunktionen abgeleitet werden.

Anmerkung 2 zum Begriff: Ein Sicherheitsziel kann mit mehreren Gefahren und mehrere Sicherheitsziele können mit einer einzelnen Gefahr verbunden sein.

3.45

Sicherheitsfunktion

Funktion einer Maschine, deren Ausfall zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

3.46

Sicherheitsbezogenes Teil eines Steuerungssystems

SRP/CS

Teil oder Unterteil(e) einer Steuerung, welches auf Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt

Anmerkung 1 zum Begriff: Die Kombination sicherheitsbezogener Teile einer Steuerung beginnt an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden (z. B. des Schaltnockens und der Rolle des Positionsschalters), und endet am Ausgang der Leistungssteuerungselemente (z. B. der Hauptkontakte des Schützes). Hierzu gehören auch Überwachungssysteme.

3.47

Schwere

die Schwere des wahrscheinlichsten Schadens, den eine gefährdete Person erleiden kann, wenn ein Schaden auftritt

3.48

Software-Anforderungs-Level (en: software requirement level)

SRL

Fähigkeit sicherheitsbezogener Teile, eine *sicherheitsbezogene Funktion* (3.45) einer Software unter vorhersehbaren Bedingungen auszuführen

Anmerkung 1 zum Begriff: Der SRL ist in vier Gruppen klassifiziert: SRL = B, 1, 2 und 3.

3.49

Software-Sicherheitsanforderung

Anforderung, die sich auf sicherheitsbezogene Software bezieht und als Element einer *technischen Sicherheitsanforderung* (3.54) enthalten ist

3.50

Anbieter

Hersteller und Händler von Neuteilen und Ersatzteilen für Traktoren für die Land- und Forstwirtschaft, selbstfahrende Aufsitzmaschinen sowie Anbau-, Aufsattel- und Anhängemaschinen für die Landwirtschaft sowie für kommunale Geräte

3.51

symmetrischer Kanal

numerische Kombination eines Einzelkanal-MTTF_{DC} für ein Doppel- oder redundantes Kanalsystem

3.52

systematischer Ausfall

Ausfall mit deterministischem Bezug zu einer bestimmten Ursache, der nur durch Änderung der Gestaltung oder des Herstellungsprozesses, des Betriebsverfahrens, der Dokumentation oder anderer relevanter Faktoren beseitigt werden kann

BEISPIEL menschliches Versagen bei der Spezifikation der Sicherheitsanforderungen, der Gestaltung, Herstellung, Installation, dem Betrieb der Hardware, oder der Gestaltung und Realisierung der Software.

Anmerkung 1 zum Begriff: Durch Instandsetzung ohne Änderung kann die Ausfallursache in der Regel nicht beseitigt werden.

Anmerkung 2 zum Begriff: Ein systematischer Ausfall kann durch Simulation der Ausfallursache hervorgerufen werden.

3.53

technisches Sicherheitskonzept

vollständige Sammlung *technischer Sicherheitsanforderungen* (3.54) zur Implementierung des *funktionalen Sicherheitskonzepts* (3.20) und zur Aufgliederung entsprechend der Systemarchitektur

Anmerkung 1 zum Begriff: Teil der Systemspezifikation, die während des Systemdesigns spezifiziert wird.

3.54

technische Sicherheitsanforderung

Anforderung an das SRP/CS entsprechend eines bestimmten *technischen Sicherheitskonzepts* (3.53)

3.55

Betrachtungseinheit

Betrachtungseinheiten

UoO

elektrisches, elektronisches, elektrisch programmierbares System oder Funktion und dessen Anwendungsbereich, Kontext und Zweck

Anmerkung 1 zum Begriff: Die UoO kann eine oder mehrere Sicherheitsfunktionen umfassen, welche über mehrere Systeme verteilt sein können.

3.56

Walkthrough

systematische, informelle Überprüfungsmethode zur Bewertung der Produktqualität

Anmerkung 1 zum Begriff: Während einer Begutachtung liefert der Verfasser eines Arbeitsprodukts an einen oder mehrere Begutachter einen detaillierten Report über alle einzelnen Schritte. Ziel ist es, ein gemeinsames Verständnis des Arbeitsprodukts zu schaffen und alle Fehler, Störstellen, Unstimmigkeiten oder Probleme im Arbeitsprodukt zu erkennen. Ein Walkthrough ist weniger stringent als eine Inspektion.

3.57

Arbeitsprodukt

Ergebnis einer Konstruktion oder einer Entwicklungsaktivität

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

AgPL	landwirtschaftlicher Performance Level (en: agricultural performance level)
AgPL _r	geforderter landwirtschaftlicher Performance Level (en: required agricultural performance level)
CAD	computergestützte Konstruktion
Cat	Hardwarekategorie
CCF	Ausfall infolge gemeinsamer Ursache (en: common-cause failure)
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
FSM	Funktionssicherheitsmanagement (en: functional safety management)
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 (en: unit of observation)

5 Qualitätsmanagementsystem

Ein Qualitätsmanagementsystem ist ein wichtiger Teil der Funktionssicherheit. Nutzer dieses Dokument müssen die Konformität mit den Abschnitten 6 bis 9 nachweisen durch

- Anwendung der Qualitätsmanagementgrundsätze wie etwa in ISO 9001 unter Nutzung der Abschnitte 6 bis 9 als Anleitung oder
- Anwendung der spezifischen Abschnitte in den Abschnitten 6 bis 9 wie in diesem Dokument formuliert.

ANMERKUNG Diese Optionen beziehen sich nur auf dieses Dokument.

6 Management während des gesamten Sicherheitslebenszyklus

6.1 Ziele

Dieser Abschnitt hat zum Ziel, die Verantwortlichkeiten der Personen, Abteilungen und Organisationen festzulegen, welche für jede Phase während des gesamten Sicherheitslebenszyklus oder für Aktivitäten innerhalb der diversen Phasen verantwortlich sind. Dies bezieht sich sowohl auf die Aktivitäten, die notwendig sind, um das geforderte Maß an funktionaler Sicherheit für die UoO sicherzustellen, als auch auf die Bestätigungsmaßnahmen, die dieses Maß an funktionaler Sicherheit bescheinigen. Ein weiteres Ziel ist die Festlegung der Managementaktivitäten während des gesamten Sicherheitslebenszyklus.

Das E/E/PES-System muss in einer Form entwickelt und konstruiert sein, mit der die Grundlagen von Risikoanalyse, Risikobewertung und ein iterativer Prozess für die Entwicklung sicherheitsbezogener Teile von Steuerungen vollständig beachtet werden (siehe Bild 1).

ANMERKUNG ISO 25119 (alle Teile) behandelt lediglich die Auswertung der Sicherheitsaspekte des E/E/PES.

6.2 Allgemeines

6.2.1 Einführung in das Konzept des Sicherheitslebenszyklus

Der Sicherheitslebenszyklus (siehe Bild 2) fasst die wichtigsten sicherheitsbezogenen Aktivitäten in der Konzeptphase, während der Serienentwicklung und bei Produktionsanlauf (SOP) zusammen. Diese Aktivitäten sind in ISO 25119-2 und ISO 25119-3 ausführlich beschrieben. Die Planung, Koordinierung und Verifizierung dieser Aktivitäten über alle Phasen des Lebenszyklus hinweg ist eine Hauptaufgabe des Managements.

ANMERKUNG Die Aktivitäten während der Konzeptphase, der Serienentwicklung und nach dem SOP sind in ISO 25119-2, ISO 25119-3 und ISO 25119-4 ausführlich beschrieben.

6.2.2 Externe funktionale Sicherheitsmaßnahmen

Dies sind Maßnahmen, die nicht durch die UoO beeinflusst werden können, aber bei der Konstruktion der UoO zu berücksichtigen sind. Die externe funktionale Sicherheit umfasst die Merkmale der beteiligten Personen (z. B. körperlich, Sprache) oder die Umgebungseigenschaften (z. B. EMV, Temperatur, Feuchte und andere Eigenschaften). Bei der Risikoanalyse muss die externe funktionale Sicherheit berücksichtigt werden.

ANMERKUNG 1 Der Nachweis der Wirksamkeit der äußeren Funktionssicherheit fällt nicht unter den Anwendungsbereich von ISO 25119 (alle Teile).

ANMERKUNG 2 Ausfälle anderer Technologien wie etwa Mechanik und Hydraulik werden von ISO 25119 (alle Teile) nicht berücksichtigt. Die Verifizierung der funktionalen Sicherheit dieser Technologien liegt außerhalb des Anwendungsbereichs von ISO 25119 (alle Teile).

6.3 Voraussetzungen

Die Durchführung einer geeigneten Risikobeurteilung und Risikoreduzierung (z. B. ISO 12100) für die gesamte Maschine ist eine Voraussetzung für die Anwendung der Norm ISO 25119 (alle Teile).

Die notwendigen Voraussetzungen für den Gestaltungs-, Herstellungs-, Instandhaltungs- und Außerbetriebnahmeprozess sind ein bewährter Qualitätssicherungsplan (z. B. IATF 16949 oder gleichwertig) und ein Gesamtprojektplan.

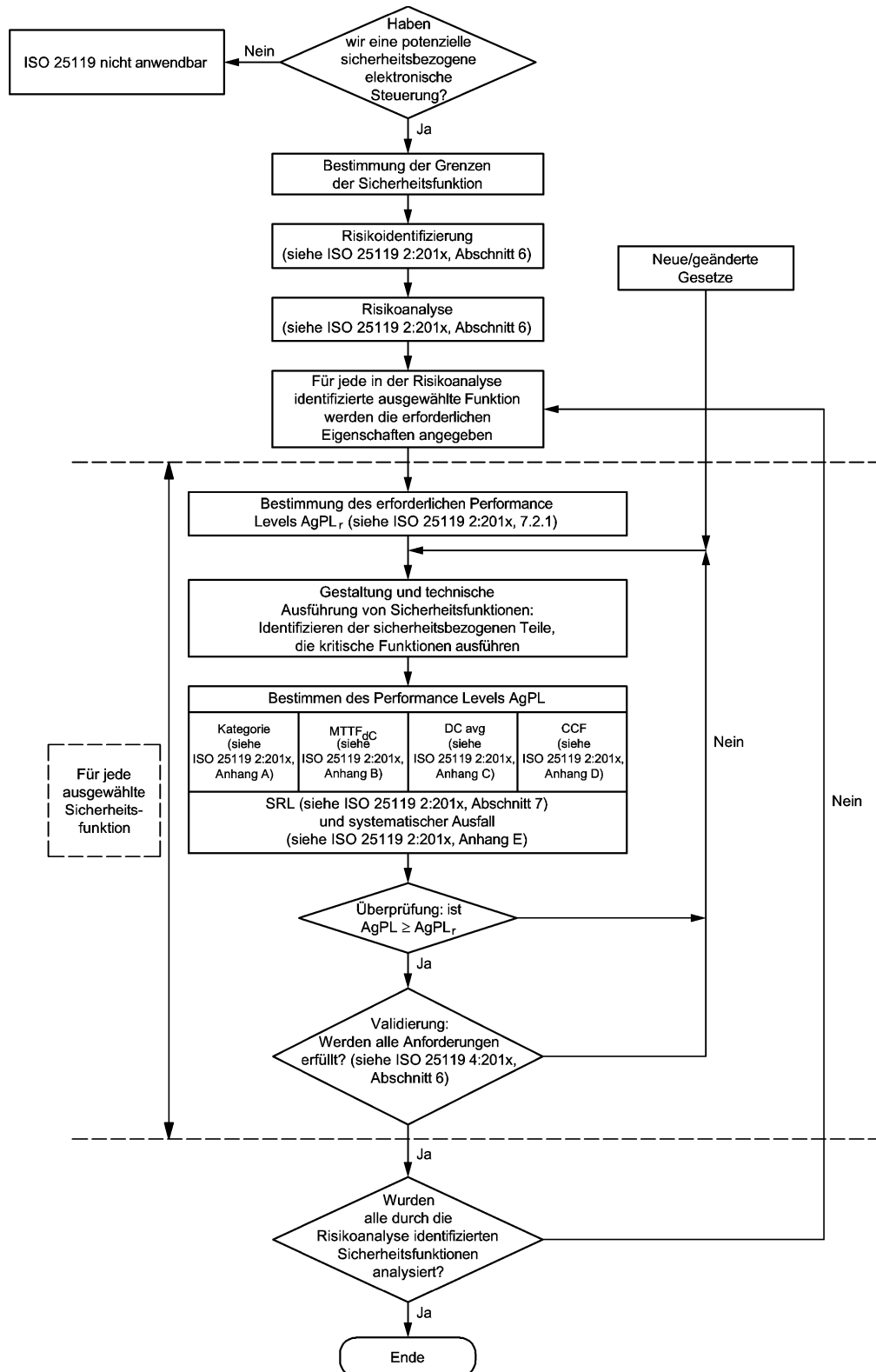


Bild 1 — Iterativer Prozess für die Gestaltung des SRP/CS