

	DIN EN ISO 25119-3	
ICS 35.240.99; 65.060.01	Ersatz für die 2023-10 zurückgezogene Norm DIN EN 16590-3:2015-04 Traktoren und Maschinen für die Land- und Forstwirtschaft – Sicherheitsbezogene Teile von Steuerungen – Teil 3: Serienentwicklung, Hardware und Software (ISO 25119-3:2018 + Amd 1:2020); Deutsche Fassung EN ISO 25119-3:2023 + A1:2023 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part 3: Series development, hardware and software (ISO 25119-3:2018 + Amd 1:2020); German version EN ISO 25119-3:2023 + A1:2023 Tracteurs et matériels agricoles et forestiers – Parties des systèmes de commande relatives à la sécurité – Partie 3: Développement en série, matériels et logiciels (ISO 25119-3:2018 + Amd 1:2020); Version allemande EN ISO 25119-3:2023 + A1:2023	
		Gesamtumfang 83 Seiten
DIN-Normenausschuss Maschinenbau (NAM)		

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen.

Der Text von ISO 25119-3:2018 + Amd 1:2020 wurde vom Technischen Komitee ISO/TC 23 „Tractors and machinery for agriculture and forestry“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO 25119-3:2023 + A1:2023 vom Technischen Komitee CEN/TC 144 „Traktoren und Maschinen für die Land- und Forstwirtschaft“ übernommen, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Die nationalen Interessen bei der Erarbeitung wurden vom Ausschuss NA 060-16-12 AA „TA E – Elektronik – Landtechnik (SpA ISO/TC 23/SC 19)“ im Fachbereich „Landtechnik“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von Landmaschinen sowie der Berufsgenossenschaften waren an der Erarbeitung beteiligt.

Dieses Dokument enthält die Änderung 1, angenommen von CEN am 9. Januar 2023.

Der Beginn und das Ende von neuem oder geändertem Text werden durch die Markierungen   angezeigt.

Diese Norm 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.

Ab dem Zeitpunkt ihrer Bezeichnung als Harmonisierte Norm im Amtsblatt der Europäischen Union kann der Hersteller bei ihrer Anwendung davon ausgehen, dass er die von der Norm behandelten Anforderungen der Maschinenrichtlinie eingehalten hat (so genannte Vermutungswirkung).

DIN EN ISO 25119 besteht unter dem allgemeinen Titel *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen* aus den folgenden Teilen:

- Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze
- Teil 2: Konzeptphase
- Teil 3: Serienentwicklung, Hardware und Software
- Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse

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

IEC 61000-4-1*	siehe	DIN EN 61000-4-1
IEC 61496-1	siehe	DIN EN IEC 61496-1 (VDE 0113-201)
ISO 9001	siehe	DIN EN ISO 9001
ISO 12100	siehe	DIN EN ISO 12100
ISO 25119-1	siehe	DIN EN ISO 25119-1
ISO 25119-2:2019	siehe	DIN EN ISO 25119-2:2024-07
ISO 25119-4:2018, ISO 25119-4:2018/AMD 1:2020	siehe	DIN EN ISO 25119-4:2024-07

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

Änderungen

Gegenüber der 2023-10 zurückgezogenen Norm DIN EN 16590-3:2015-04 wurden folgende Änderungen vorgenommen:

- a) die Einleitung wurde geändert, um spezifische Informationen zu Sicherheitsnormen hinzuzufügen;
- b) die Voraussetzungen für die Funktionssicherheit wurden festgelegt;
- c) Abschnitt 5 wurde geändert, um:
 - die Voraussetzungen für die Funktionssicherheit festzulegen und
 - die allgemeinen Anforderungen technischer Sicherheitskonzepte zu vereinfachen;
- d) zusätzliche Anweisungen wurden im gesamten Dokument hinzugefügt, um die Konsistenz der Prüfspezifikationen und Berichte zu verifizieren;
- e) Anhang B wurde in einen normativen Anhang geändert;
- f) das Dokument wurde redaktionell überarbeitet.

Frühere Ausgaben

DIN EN 16590-3: 2015-04, 2014-11

* IEC 61000-4-1:2006 wurde zurückgezogen und mit unverändertem Titel ersetzt durch IEC/TR 61000-4-1:2016.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 61000-4-1, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-1: Prüf- und Messverfahren — Übersicht über die Reihe IEC 61000-4*

DIN EN IEC 61496-1 (VDE 0113-201), *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 1: Allgemeine Anforderungen und Prüfungen*

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 12100, *Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung*

DIN EN ISO 25119-1, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze*

DIN EN ISO 25119-2:2024-07, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Konzeptphase (ISO 25119-2:2019); Deutsche Fassung EN ISO 25119-2:2023*

DIN EN ISO 25119-4:2024-07, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse (ISO 25119-4:2018 + Amd 1:2020); Deutsche Fassung EN ISO 25119-4:2023 + A1:2023*

Deutsche Fassung

Traktoren und Maschinen für die Land- und
Forstwirtschaft —
Sicherheitsbezogene Teile von Steuerungen —
Teil 3: Serienentwicklung, Hardware und Software
(ISO 25119-3:2018 + Amd 1:2020)

Tractors and machinery for agriculture and forestry —
Safety-related parts of control systems —
Part 3: Series development, hardware and software
(ISO 25119-3:2018 + Amd 1:2020)

Tracteurs et matériels agricoles et forestiers —
Parties des systèmes de commande relatives à la
sécurité —
Partie 3: Développement en série, matériels et logiciels
(ISO 25119-3:2018 + Amd 1:2020)

Diese Europäische Norm wurde vom CEN am 9. Januar 2023 angenommen. Die Änderung A1 modifiziert die Europäische Norm EN ISO 25119-3:2023. Sie wurde vom CEN am 09. Januar 2023 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	5
Ⓐ Europäisches Vorwort der Änderung 1 Ⓐ	6
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG	7
Vorwort	12
Ⓐ Vorwort der Änderung 1 Ⓐ	14
Einleitung	15
1 Anwendungsbereich	17
2 Normative Verweisungen	18
3 Begriffe	18
4 Abkürzungen	18
5 Systementwurf	19
5.1 Ziele	19
5.2 Allgemeines	19
5.3 Voraussetzungen	20
5.4 Anforderungen	20
5.4.1 Gliederung der Sicherheitsanforderungen	20
5.4.2 Technisches Sicherheitskonzept	21
5.5 Arbeitsprodukte	23
6 Hardware	23
6.1 Ziele	23
6.2 Allgemeines	23
6.3 Voraussetzungen	23
6.4 Anforderungen	23
6.5 Hardwarekategorien	25
6.6 Arbeitsprodukte	26
7 Software	26
7.1 Software-Entwicklungsplanung	26
7.1.1 Ziele	26
7.1.2 Allgemeines	26
7.1.3 Voraussetzungen	26
7.1.4 Anforderungen	27
7.1.5 Arbeitsprodukte	29
7.2 Festlegung der Sicherheitsanforderungen an die Software	29
7.2.1 Ziele	29
7.2.2 Allgemeines	29
7.2.3 Voraussetzungen	29
7.2.4 Anforderungen	30
7.2.5 Arbeitsprodukte	33
7.3 Gestaltung der Software-Architektur	33
7.3.1 Ziele	33
7.3.2 Allgemeines	33
7.3.3 Voraussetzungen	34
7.3.4 Anforderungen	34
7.3.5 Arbeitsprodukte	35
7.4 Gestaltung und Implementierung von Softwarekomponenten	35
7.4.1 Ziele	35
7.4.2 Allgemeines	36
7.4.3 Voraussetzungen	36
7.4.4 Anforderungen	36
7.4.5 Arbeitsprodukte	46

7.5	Softwarekomponentenprüfung	47
7.5.1	Ziele	47
7.5.2	Allgemeines	47
7.5.3	Voraussetzungen	47
7.5.4	Anforderungen	47
7.5.5	Arbeitsprodukte	56
7.6	Software-Integration und -Prüfung	56
7.6.1	Ziele	56
7.6.2	Allgemeines	56
7.6.3	Voraussetzungen	56
7.6.4	Anforderungen	57
7.6.5	Arbeitsprodukte	58
7.7	Software-Sicherheitsprüfung	58
7.7.1	Ziele	58
7.7.2	Allgemeines	59
7.7.3	Voraussetzungen	59
7.7.4	Anforderungen	59
7.7.5	Arbeitsprodukte	63
7.8	Softwarebasierte Parametrierung	63
7.8.1	Ziel	63
7.8.2	Allgemeines	63
7.8.3	Voraussetzungen	64
7.8.4	Anforderungen	64
7.8.5	Arbeitsprodukte	65
Anhang A (informativ) Beispiel einer Agenda für die Beurteilung der funktionalen Sicherheit bei AgPL = e		66
A.1	Funktionen des Systems	66
A.2	Hardware	66
A.3	Sicherheitskonzept	66
A.4	Sicherheitsanalyse und Sicherheitsdaten	66
A.5	Sicherheitsentwurfsprozess für die Phasen des Lebenszyklus	66
A.6	Software-Entwicklung	67
A.7	Verifizierung und Prüfung	67
A.8	Dokumentation und Sicherheitsdokumentation	67
A.9	Zusammenfassung und Beurteilung	67
Anhang B (normativ) Unabhängigkeit durch Softwarepartitionierung		68
B.1	Übersicht	68
B.2	Begriffe und Abkürzungen	68
B.2.1	Begriffe	68
B.2.2	Abkürzungen	71
B.3	Ziele	72
B.4	Allgemeines	72
B.5	Anforderungen	72
B.5.1	Allgemeine Anforderungen	72
B.5.2	Mehrere Partitionen in einem einzelnen Mikrocontroller	73
B.5.3	Mehrere Partitionen im Rahmen eines Mikrocontroller-Netzwerks	75
Literaturhinweise		79

Bilder

Bild 1 — Gliederung der Sicherheitsanforderungen	20
Bild 2 — V-Modell der Hardwareentwicklung	24
Bild 3 — Beispiel eines integrierten Systems für die Hardwarekategorie 2	25
Bild 4 — V-Modell der Software-Entwicklung	28
Bild 5 — Prüfschnittstelle einer ECU eines E/E/PES-Systems	60

Bild 6 — Prüfung innerhalb des Netzwerks der elektronischen Steuereinheit eines E/E/PES-Systems 61

Bild 7 — Hardware-in-the-Loop-Prüfung einer ECU eines E/E/PES-Systems 62

Bild 8 — Prüfung in der Maschine eines E/E/PES-Systems 62

Bild B.1 — Mehrere Partitionen in einem einzelnen Mikrocontroller 73

Bild B.2 — Mehrere Partitionen innerhalb eines Mikrocontroller-Netzwerks 76

Bild B.3 — Mehrere Partitionen innerhalb einer ECU mit mehreren Prozessoren 76

Tabellen

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG 7

Tabelle ZA.2 — Anwendbare Normen, die die Konformitätsvermutung gemäß diesem Anhang ZA begründen 11

Tabelle 1 — Festlegung der Sicherheitsanforderungen an die Software 30

Tabelle 2 — Gestaltung der Software-Architektur 34

Tabelle 3 — Software-Entwurf und -Entwicklung — Unterstützungswerkzeuge und Programmiersprache 36

Tabelle 4 — Softwarekomponentenprüfung 47

Tabelle 5 — Software-Integrationsprüfung (Komponente) 57

Tabelle 6 — Software-Sicherheitsprüfung 59

Tabelle B.1 — Verfahren und Maßnahmen innerhalb des Mikrocontrollers 74

Tabelle B.2 — Verfahren und Maßnahmen innerhalb eines Mikrocontroller-Netzwerks 77

Europäisches Vorwort

Der Text von ISO 25119-3:2018 wurde vom Technischen Komitee ISO/TC 23 „Tractors and machinery for agriculture and forestry“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/TC 144 „Traktoren und Maschinen für die Land- und Forstwirtschaft“ als EN ISO 25119-3:2023 übernommen, dessen Sekretariat von AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis März 2024, und etwaige entgegenstehende nationale Normen müssen bis März 2024 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinie(n)/-Verordnung(en).

Zum Zusammenhang mit EU-Richtlinie(n)/-Verordnung(en) siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

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

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 25119-3:2018 wurde von CEN als EN ISO 25119-3:2023 ohne irgendeine Abänderung genehmigt.

Ⓐ Europäisches Vorwort der Änderung 1 Ⓐ

Ⓐ Der Text von ISO 25119-3:2018/Amd 1:2020 wurde vom Technischen Komitee ISO/TC 23 „Tractors and machinery for agriculture and forestry“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/TC 144 „Traktoren und Maschinen für die Land- und Forstwirtschaft“ als EN ISO 25119-3:2023/A1:2023 übernommen, dessen Sekretariat von AFNOR gehalten wird.

Diese Änderung zur Europäischen Norm EN ISO 25119-3:2023 muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis März 2024, und etwaige entgegenstehende nationale Normen müssen bis März 2024 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde unter einem Normungsauftrag erarbeitet, das CEN von der Europäischen Kommission und der Europäischen Freihandelszone erteilt wurde, und unterstützt grundlegende Anforderungen der EU-Richtlinie(n)/Verordnung(en).

Zum Zusammenhang mit EU-Richtlinie(n)/Verordnung(en) siehe informativen Anhang ZA, der Bestandteil von EN ISO 25119-3:2023 ist.

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

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 25119-3:2018/Amd 1:2020 wurde von CEN als EN ISO 25119-3:2023/A1:2023 ohne irgendeine Abänderung 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/EG 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 dieser 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 EU-Maschinenrichtlinie 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)	Abschnitt 5, Abschnitt 6, Abschnitt 7, Abschnitt B.5	
1.1.2 (c)	Abschnitt 5, Abschnitt 6, Abschnitt 7, Abschnitt B.5	
1.1.2 (d)		NICHT ABGEDECKT
1.1.2 (e)		NICHT ABGEDECKT
1.1.3. Materialien und Produkte		NICHT ABGEDECKT
1.1.4. Beleuchtung		NICHT ABGEDECKT
1.1.5. Konstruktion der Maschine im Hinblick auf die Handhabung		NICHT ABGEDECKT
1.1.6. Ergonomie		NICHT ABGEDECKT
1.1.7. Bedienungsplätze		NICHT ABGEDECKT
1.1.8. Sitze		NICHT ABGEDECKT
1.2. STEUERUNGEN UND BEFEHLSEINRICHTUNGEN	—	
1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen	Abschnitt 5, Abschnitt 6, Abschnitt 7, Abschnitt B.5	
1.2.2. Stellteile		NICHT ABGEDECKT
1.2.3. Ingangsetzen		NICHT ABGEDECKT
1.2.4. Stillsetzen	—	
1.2.4.1. Normales Stillsetzen		NICHT ABGEDECKT
1.2.4.2. Betriebsbedingtes Stillsetzen		NICHT ABGEDECKT

Tabelle ZA.1 (fortgesetzt)

Grundlegende Anforderungen der EU-Maschinenrichtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser Europäischen Norm	Erläuterungen/Anmerkungen
1.2.4.3. Stillsetzen im Notfall		NICHT ABGEDECKT
1.2.4.4. Gesamtheit von Maschinen		NICHT ABGEDECKT
1.2.5. Wahl der Steuerungs- oder Betriebsarten		NICHT ABGEDECKT
1.2.6. Störung der Energieversorgung	Abschnitt 5, Abschnitt 6, Abschnitt 7, Abschnitt B.5	
1.3. SCHUTZMASSNAHMEN GEGEN MECHANISCHE GEFÄHRDUNGEN	—	
1.3.1. Risiko des Verlusts der Standsicherheit		NICHT ABGEDECKT
1.3.2. Bruchrisiko beim Betrieb		NICHT ABGEDECKT
1.3.3. Risiken durch herabfallende oder herausgeschleuderte Gegenstände		NICHT ABGEDECKT
1.3.4. Risiken durch Oberflächen, Kanten und Ecken		NICHT ABGEDECKT
1.3.5. Risiken durch mehrfach kombinierte Maschinen		NICHT ABGEDECKT
1.3.6. Risiken durch Änderung der Verwendungsbedingungen		NICHT ABGEDECKT
1.3.7. Risiken durch bewegliche Teile		NICHT ABGEDECKT
1.3.8. Wahl der Schutzeinrichtungen gegen Risiken durch bewegliche Teile		NICHT ABGEDECKT
1.3.9. Risiko unkontrollierter Bewegungen		NICHT ABGEDECKT
1.4. ANFORDERUNGEN AN SCHUTZEINRICHTUNGEN	—	
1.4.1. Allgemeine Anforderungen		NICHT ABGEDECKT
1.4.2. Besondere Anforderungen an trennende Schutzeinrichtungen		NICHT ABGEDECKT
1.4.3. Besondere Anforderungen an nichttrennende Schutzeinrichtungen		NICHT ABGEDECKT
1.5. RISIKEN DURCH SONSTIGE GEFÄHRDUNGEN	—	
1.5.1. Elektrische Energieversorgung		NICHT ABGEDECKT
1.5.2. Statische Elektrizität		NICHT ABGEDECKT
1.5.3. Nichtelektrische Energieversorgung		NICHT ABGEDECKT
1.5.4. Montagefehler		NICHT ABGEDECKT
1.5.5. Extreme Temperaturen		NICHT ABGEDECKT
1.5.6. Brand		NICHT ABGEDECKT
1.5.7. Explosion		NICHT ABGEDECKT
1.5.8. Lärm		NICHT ABGEDECKT
1.5.9. Vibrationen		NICHT ABGEDECKT
1.5.10. Strahlung		NICHT ABGEDECKT
1.5.11. Strahlung von außen		NICHT ABGEDECKT

Tabelle ZA.1 (fortgesetzt)

Grundlegende Anforderungen der EU-Maschinenrichtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser Europäischen Norm	Erläuterungen/Anmerkungen
1.5.12. Laserstrahlung		NICHT ABGEDECKT
1.5.13. Emission gefährlicher Werkstoffe und Substanzen		NICHT ABGEDECKT
1.5.14. Risiko, in einer Maschine eingeschlossen zu werden		NICHT ABGEDECKT
1.5.15. Ausrutsch-, Stolper- und Sturzrisiko		NICHT ABGEDECKT
1.5.16. Blitzschlag		NICHT ABGEDECKT
1.6. INSTANDHALTUNG	—	
1.6.1. Wartung der Maschine		NICHT ABGEDECKT
1.6.2. Zugang zu den Bedienungsständen und den Eingriffspunkten für die Instandhaltung		NICHT ABGEDECKT
1.6.3. Trennung von den Energiequellen		NICHT ABGEDECKT
1.6.4. Eingriffe des Bedienungspersonals		NICHT ABGEDECKT
1.6.5. Reinigung innen liegender Maschinenteile		NICHT ABGEDECKT
1.7. INFORMATIONEN	—	
1.7.1. Informationen und Warnhinweise an der Maschine		NICHT ABGEDECKT
1.7.1.1. Informationen und Informationseinrichtungen		NICHT ABGEDECKT
1.7.1.2. Warneinrichtungen		NICHT ABGEDECKT
1.7.2. Warnung vor Restrisiken		NICHT ABGEDECKT
1.7.3. Kennzeichnung der Maschinen		NICHT ABGEDECKT
1.7.4. Betriebsanleitung		NICHT ABGEDECKT
2.4 MASCHINEN ZUR AUSBRINGUNG VON PESTIZIDEN	—	
2.4.2. Allgemeines		NICHT ABGEDECKT
2.4.3. Bedienung und Überwachung		NICHT ABGEDECKT
2.4.4. Füllung und Entleerung		NICHT ABGEDECKT
2.4.5. Ausbringung von Pestiziden	—	
2.4.5.1. Ausbringungsrate		NICHT ABGEDECKT
2.4.5.2. Verteilung, Anlagerung und Abdrift von Pestiziden		NICHT ABGEDECKT
2.4.5.3. Prüfungen		NICHT ABGEDECKT
2.4.5.4. Unbeabsichtigte Freisetzen während und nach der Abschaltung		NICHT ABGEDECKT
2.4.6. Wartung	—	
2.4.6.1. Reinigung		NICHT ABGEDECKT
2.4.6.2. Instandhaltung		NICHT ABGEDECKT
2.4.7. Kontrollen		NICHT ABGEDECKT

Tabelle ZA.1 (fortgesetzt)

Grundlegende Anforderungen der EU-Maschinenrichtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser Europäischen Norm	Erläuterungen/Anmerkungen
2.4.8. Kennzeichnung von Düsen, Sieben und Filtern		NICHT ABGEDECKT
2.4.9. Angabe des verwendeten Pestizids		NICHT ABGEDECKT
2.4.10. Betriebsanleitung		NICHT ABGEDECKT
3.2. BEDIENERPLÄTZE	—	
3.2.1. Fahrerplatz		NICHT ABGEDECKT
3.2.2. Sitze		NICHT ABGEDECKT
3.2.3. Plätze für andere Personen		NICHT ABGEDECKT
3.3. STEUERUNG	—	
3.3.1. Stellteile		NICHT ABGEDECKT
3.3.2. Ingangsetzen/Verfahren		NICHT ABGEDECKT
3.3.3. Stillsetzen/Bremsen		NICHT ABGEDECKT
3.3.4. Verfahren mitgängergeführter Maschinen		NICHT ABGEDECKT
3.3.5. Störung des Steuerkreises		NICHT ABGEDECKT
3.4. SCHUTZMASSNAHMEN GEGEN MECHANISCHE GEFÄHRDUNGEN	—	
3.4.1. Unkontrollierte Bewegungen		NICHT ABGEDECKT
3.4.2. Bewegliche Übertragungselemente		NICHT ABGEDECKT
3.4.3. Überrollen und Umkippen		NICHT ABGEDECKT
3.4.4. Herabfallende Gegenstände		NICHT ABGEDECKT
3.4.5. Zugänge		NICHT ABGEDECKT
3.4.6. Anhängavorrichtungen		NICHT ABGEDECKT
3.4.7. Kraftübertragung zwischen einer selbstfahrenden Maschine (oder einer Zugmaschine) und einer angetriebenen Maschine		NICHT ABGEDECKT
3.5 SCHUTZMASSNAHMEN GEGEN SONSTIGE GEFÄHRDUNGEN	—	
3.5.1. Batterien		NICHT ABGEDECKT
3.5.2. Brand		NICHT ABGEDECKT
3.5.3. Emission von gefährlichen Stoffen		NICHT ABGEDECKT
3.6. INFORMATIONEN UND ANGABEN	—	
3.6.1. Zeichen, Signaleinrichtungen und Warnhinweise		NICHT ABGEDECKT
3.6.2. Kennzeichnung		NICHT ABGEDECKT
3.6.3. Betriebsanleitung	—	
3.6.3.1. Vibrationen		NICHT ABGEDECKT
3.6.3.2. Mehrere Verwendungsmöglichkeiten		NICHT ABGEDECKT

Tabelle ZA.2 — Anwendbare Normen, die die Konformitätsvermutung gemäß diesem Anhang ZA begründen

Spalte 1 Verweisung in Abschnitt 2	Spalte 2 Ausgabe der Internationalen Norm	Spalte 3 Titel	Spalte 4 Entsprechende Ausgabe der Europäischen Norm
ISO 25119-1	ISO 25119-1:2018 ISO 25119-1:2018/ A1:2020	Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development	EN ISO 25119-1:2023 EN ISO 25119-1:2023/ A1:2023
ISO 25119-2:2019	ISO 25119-2:2019	Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase	EN ISO 25119-2:2023
ISO 25119-4:2018	ISO 25119-4:2018 ISO 25119-4:2018/ A1:2020	Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes	EN ISO 25119-4:2023 EN ISO 25119-4:2023/ A1:2023

Die in Spalte 1 von Tabelle ZA.2 aufgeführten Dokumente werden in diesem Dokument teilweise oder als Ganzes normativ zitiert, d. h. sie sind für seine Anwendung erforderlich. Das Erreichen der Konformitätsvermutung unterliegt der Anwendung der in Spalte 4 aufgeführten Normausgabe oder, wenn keine Ausgabe einer Europäischen Norm existiert, der in Spalte 2 von Tabelle ZA.2 angegebenen Ausgabe der Internationalen Norm.

WARNHINWEIS 1 — Die Konformitätsvermutung bleibt nur bestehen, solange 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 ist 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.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen, sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe 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 zweite Ausgabe ersetzt die erste Ausgabe (ISO 25119-3:2010), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Die Einleitung wurde geändert, um spezifische Informationen zu Sicherheitsnormen hinzuzufügen;
- Die Voraussetzungen für die Funktionssicherheit wurden festgelegt;
- Abschnitt 5 wurde geändert, um:
 - die Voraussetzungen für die Funktionssicherheit festzulegen und
 - die allgemeinen Anforderungen technischer Sicherheitskonzepte zu vereinfachen;
- Zusätzliche Anweisungen wurden im gesamten Dokument hinzugefügt, um die Konsistenz der Prüfspezifikationen und Berichte zu verifizieren;
- Anhang B wurde in einen normativen Anhang geändert;
- Das Dokument wurde redaktionell überarbeitet.

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

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

Ⓐ Vorwort der Änderung 1 Ⓐ

Ⓐ ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (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 Normungsthemen 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 Directives, 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 Directives, Teil 2, erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist 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.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe 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*, in Zusammenarbeit mit dem Europäischen Komitee für Normung (CEN), Technisches Komitee CEN/TC 144, „*Traktoren und Maschinen für die Land- und Forstwirtschaft*“ in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

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

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

Einleitung

ISO 25119 (alle Teile) beschreibt einen 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 von 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 Steuerung oder in diese 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 Gefährdung (oder Gefährdungssituation) 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-Level. 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 infolge gemeinsamer Ursache), von den Entwurfsverfahren, von der Beanspruchung im Betrieb, von Umweltbedingungen und von Arbeitsabläufen. Es werden drei Arten von Ausfällen berücksichtigt, die E/E/PES-Funktionsstörungen hervorrufen können, welche zu potentiellen Gefährdungssituationen führen: systematische Ausfälle, Ausfälle infolge gemeinsamer Ursache und Zufallsausfälle.

ISO 25119 (alle Teile) legt einen Ansatz auf Basis einer Klassifikation der Architektur 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 können auf Steuerungen aller Arten fahrbarer Maschinen angewendet werden: von einfachen Systemen (z. B. Anlassventilen) bis hin zu komplexen Systemen (z. B. Steer-by-Wire) sowie Steuerungen von Schutzeinrichtungen (z. B. Verriegelungsvorrichtungen, druckempfindliche Einrichtungen).

ISO 25119 (alle Teile) übernimmt für die Ermittlung der Risiken einen risikobasierten Ansatz und bietet zugleich ein Mittel zur Festlegung des erforderlichen Performance-Levels für die von den sicherheitsrelevanten E/E/PES-Kanälen auszuführenden Sicherheitsfunktionen. Sie legt mit den Performance-Levels verbundene Anforderungen an den gesamten E/E/PES-Lebenszyklus (Entwicklung, Validierung, Fertigung, Betrieb, Wartung, Außerbetriebnahme) fest, die zur Erzielung der erforderlichen Funktionssicherheit für E/E/PES und der zugehörigen Performance-Level notwendig sind.

Sicherheitsnormen im Bereich Maschinenbau sind in folgende Arten untergliedert:

- a) Typ-A-Normen (Sicherheitsgrundnormen) enthalten Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die für alle Maschinen angewendet werden können.
- b) Typ-B-Normen (Sicherheitsfachgrundnormen) 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, Lärm);
 - Typ-B2-Normen behandeln Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen, druckempfindliche Schutzeinrichtungen, trennende Schutzeinrichtungen).
- c) Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen an eine bestimmte Maschine oder Gruppe von Maschinen.

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

Dieses Dokument ist insbesondere für die folgenden interessierten Kreise von Relevanz, die die Marktakteure im Hinblick auf die Sicherheit von Maschinen repräsentieren:

- Maschinenhersteller (kleine, mittlere und große Unternehmen);
- Organisationen des Arbeits- und Gesundheitsschutzes (Gesetzgeber, Unfallversicherungen, Marktaufsicht usw.).

Andere interessierte Kreise können durch das in diesem Dokument (durch die oben genannten interessierten Kreise) festgeschriebenen Sicherheitsniveau betroffen sein. Es handelt sich dabei um:

- Maschinenanwender/Arbeitgeber (kleine, mittlere und große Unternehmen);
- Maschinenanwender/Arbeitnehmer (z. B. Gewerkschaften, Organisationen für Personen mit spezifischen Bedürfnissen);
- Dienstleistungsanbieter, z. B. für die Wartung (kleine, mittlere und große Unternehmen);
- Verbraucher (falls die behandelten Maschinen für die Nutzung durch Verbraucher bestimmt sind).

Den oben genannten interessierten Kreisen wurde die Möglichkeit eingeräumt, sich an der Erarbeitung dieses Dokuments zu beteiligen.

Des Weiteren ist dieses Dokument an Normungsinstitute gerichtet, die Typ-C-Normen erarbeiten.

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

Für Maschinen, die in den Anwendungsbereich einer Typ-C-Norm fallen und die nach deren Anforderungen konstruiert und gebaut worden sind, haben die Anforderungen dieser Typ-C-Norm Vorrang.

1 Anwendungsbereich

Dieses Dokument legt allgemeine Grundlagen und Leitsätze für die Gestaltung und Entwicklung sicherheitsbezogener Teile von Steuerungen (SRP/CS) in land- und forstwirtschaftlichen Traktoren, selbstfahrenden Aufsitzmaschinen sowie landwirtschaftlich genutzten Anbau-, Aufsattel- und Anhängemaschinen dar. Es kann auch auf fahrbare kommunale Geräte (z. B. Straßenkehrmaschinen) angewendet werden.

Dieses Dokument ist nicht anwendbar für:

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

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

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

Dieses Dokument ist für sicherheitsbezogene Teile elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES) als Teil mechatronischer Systeme anwendbar. Es behandelt die möglichen Gefahren durch Fehlfunktionen von sicherheitsbezogenen E/E/PES einschließlich der Wechselwirkungen dieser Systeme. Es behandelt keine Gefährdungen in Verbindung mit Stromschlag, Feuer, Rauch, Hitze, Strahlung, Toxizität, Entflammbarkeit, Reaktivität, Korrosion, Freisetzung von Energie usw., außer wenn diese 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 Gefährdungen beteiligt sind.

Im Anwendungsbereich dieses Dokuments enthaltene Beispiele sind:

- SRP/CS, die den Stromfluss in elektrischen Hybridsystemen begrenzen, um Isolierungsausfälle und Gefährdungen durch elektrischen Schlag zu verhindern;
- elektromagnetische Störungen mit SRP/CS;
- für Brandschutzzwecke gestaltete SRP/CS.

Im Anwendungsbereich dieses Dokuments nicht enthaltene Beispiele sind:

- Isolierungsausfälle durch Reibung, die zu Gefährdungen durch elektrischen Schlag führen;
- elektromagnetische Nennstrahlung, die nahe gelegene Maschinensteuerungssysteme beeinflusst;
- Korrosion, die zu einer Überhitzung von Stromkabeln führt.

Dieses Dokument ist nicht anwendbar für Nicht-E/E/PES-Systeme (z. B. hydraulische, mechanische und pneumatische).

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

Dieses Dokument ist nicht anwendbar 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, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

[A1] ISO 25119-2:2019 **[A1]**, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

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*

[A1] ISO 25119-4:2018/AMD 1:2020, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes — Amendment 1* **[A1]**

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.

AgPL	landwirtschaftlicher Performance-Level (en: agricultural performance level)
AgPL _r	geforderter landwirtschaftlicher Performance-Level (en: required agricultural performance level)
CAD	computergestützte Konstruktion (en: computer-aided design)
Kat	Hardwarekategorie
CCF	Ausfall infolge gemeinsamer Ursache (en: common-cause failure)
DC	Diagnosedeckungsgrad (en: diagnostic coverage)
DC _{avg}	durchschnittlicher Diagnosedeckungsgrad (en: average diagnostic coverage)
ECU	elektronische Steuereinheit (en: electronic control unit)
ETA	Ereignisbaumanalyse (en: event tree analysis)
E/E/PES	elektrische/elektronische/programmierbare elektronische Systeme
EMV	elektromagnetische Verträglichkeit (en: electromagnetic compatibility, EMC)
FMEA	Ausfallart- und -einflussanalyse (en: failure mode and effects analysis)
FSM	Funktionssicherheitsmanagement
FTA	Fehlerbaumanalyse (en: fault tree analysis)
HARA	Gefährdungsanalyse und Risikobeurteilung (en: hazard analysis and risk assessment)

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
RAM	Arbeitsspeicher (en: random-access memory)
SOP	Produktionsanlauf (en: start of production)
SRL	Software-Anforderungs-Level (en: software requirement level)
SRP	sicherheitsbezogene Teile (en: safety-related parts)
SRP/CS	sicherheitsbezogene Teile von Steuerungen (en: safety-related parts of control systems)
UML	vereinheitlichte Modellierungssprache (en: unified modelling language)

5 Systementwurf

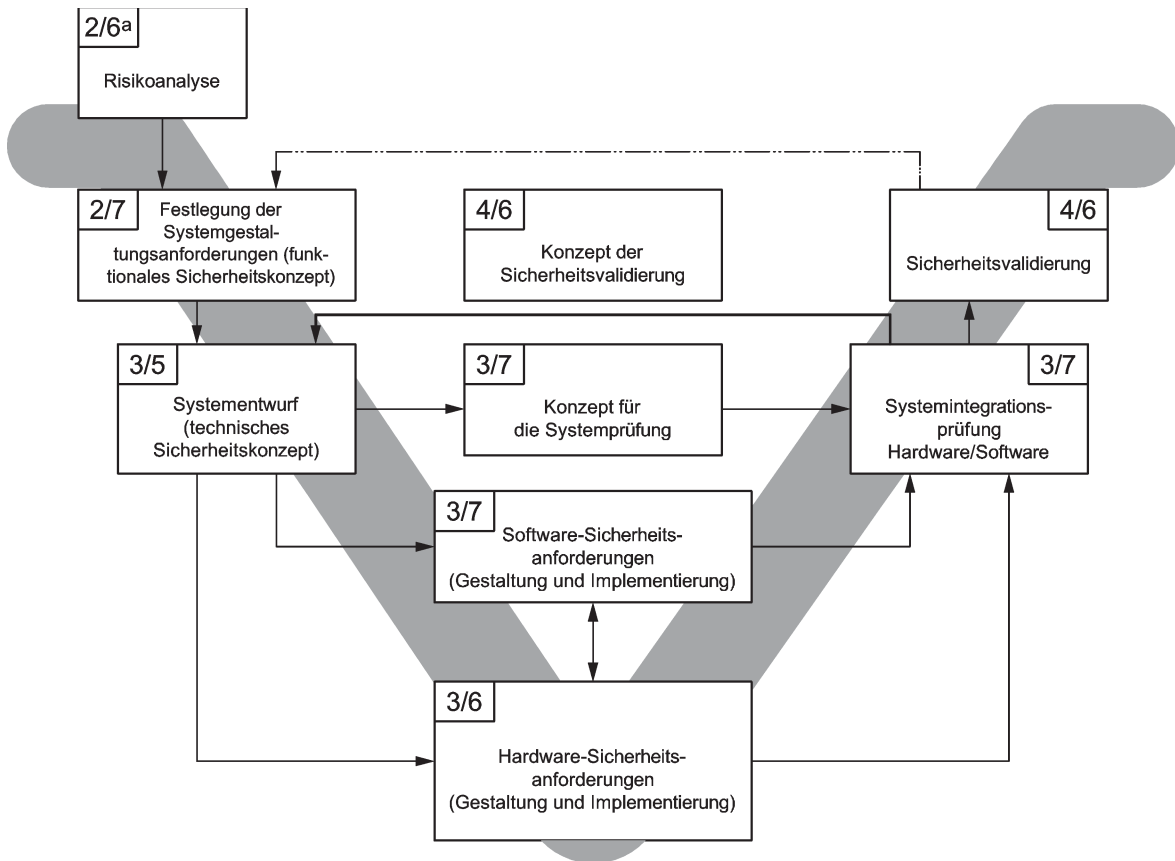
5.1 Ziele

Ziel ist die Definition einer Systemgestaltung zur Herstellung eines Entwurfs, der die Sicherheitsanforderungen an das sicherheitsbezogene Gesamtsystem erfüllt.

5.2 Allgemeines

Sicherheitsanforderungen machen alle Anforderungen aus, die das Erreichen und Sicherstellen der funktionalen Sicherheit zum Ziel haben. Während des Sicherheitslebenszyklus werden die Sicherheitsanforderungen in immer näheren Einzelheiten in hierarchischen Ebenen detailliert und festgelegt. Die verschiedenen Ebenen der Sicherheitsanforderungen sind in Bild 1 dargestellt. Für eine Gesamtdarstellung des Verfahrens zur Entwicklung der Sicherheitsanforderungen siehe auch 5.4. Zur Unterstützung des Managements der Sicherheitsanforderungen wird die Anwendung geeigneter Werkzeuge für das Anforderungsmanagement empfohlen.

Anhang A bietet eine Anleitung für ein Beispielpogramm für die Beurteilung der Funktionssicherheit in Verbindung mit einem AgPL = e.



Legende

- Folge
 ← Verifizierung
 ←... Validierung

a Die erste der beiden durch einen Schrägstrich getrennten Zahlen bezieht sich auf den jeweiligen Teil von ISO 25119 und die zweite Zahl bezieht sich auf den Abschnitt in diesem Dokument: d. h. 2/6 ist A ISO 25119-2:2019 A/Abschnitt 6, 3/5 ist ISO 25119-3:2018/Abschnitt 5 usw.

Bild 1 — Gliederung der Sicherheitsanforderungen

5.3 Voraussetzungen

Das funktionale Sicherheitskonzept (ISO 25119-2:2019, Abschnitt 7) ist die Voraussetzung.

5.4 Anforderungen

5.4.1 Gliederung der Sicherheitsanforderungen

Während der funktionalen Sicherheitskonzeptphase werden funktionale Sicherheitsanforderungen erstellt, um die grundlegende Funktion des Sicherheitssystems, mit dem die Sicherheitsziele erfüllt werden müssen, zu beschreiben. Die Grundzuordnung der funktionalen Sicherheitsanforderungen zur Systemarchitektur wird durch das technische Sicherheitskonzept in Form technischer Sicherheitsanforderungen festgelegt. Diese Systemarchitektur umfasst Hardware und Software.

Die Sicherheitsanforderungen an die Hardware verfeinern und konsolidieren die technischen Sicherheitsanforderungen. Abschnitt 6 beschreibt, wie die Hardwareanforderungen im Einzelnen festzulegen sind.

Die Sicherheitsanforderungen an die Software sind von den Anforderungen des technischen Sicherheitskonzepts und der zugrunde liegenden Hardware abgeleitet. Die in Abschnitt 7 festgelegten Software-Anforderungen sind zu berücksichtigen.

Dieser Abschnitt legt den Ansatz fest, nach dem die Anforderungen des technischen Sicherheitskonzepts während des Systementwurfs festzulegen sind und bietet somit eine Grundlage für einen fehlerfreien Systementwurf.

5.4.2 Technisches Sicherheitskonzept

5.4.2.1 Allgemeine Anforderungen des technischen Sicherheitskonzepts

Das Dokument des technischen Sicherheitskonzepts enthält die technischen Sicherheitsanforderungen an das System.

Jeder technischen Sicherheitsanforderung müssen (z. B. durch Querverweisung) übergeordnete Sicherheitsanforderungen zugeordnet werden. Übergeordnete Sicherheitsanforderungen können folgende sein:

- andere technische Sicherheitsanforderungen;
- funktionale Sicherheitsanforderungen.

ANMERKUNG Die Rückverfolgbarkeit kann durch Nutzung geeigneter Anforderungsmanagementwerkzeuge sehr erleichtert werden.

Bei der Implementierung jeder Anforderung des technischen Sicherheitskonzepts muss auf deren Durchführbarkeit, Eindeutigkeit, Konsistenz und Vollständigkeit geachtet werden.

Das technische Sicherheitskonzept muss Folgendes berücksichtigen:

- a) alle Sicherheitsziele und funktionalen Sicherheitsanforderungen;
- b) alle einschlägigen Normen, Standards und gesetzlichen Vorschriften;
- c) die entsprechenden Ergebnisse von Sicherheitsanalysewerkzeugen (FMEA, FTA usw.); die Sicherheitsanalyse bietet iterative Unterstützung für das technische Sicherheitskonzept während der Systementwicklung.

Die Vollständigkeit des technischen Sicherheitskonzepts nimmt während des Systementwurfs iterativ zu. Um die Vollständigkeit sicherzustellen:

- 1) müssen die Version des technischen Sicherheitskonzepts und die Versionen der entsprechenden zugrunde liegenden Quellen angegeben werden;
- 2) müssen die Anforderungen aus dem Änderungsmanagement (siehe ISO 25119-4:2018 [A1](#)) und ISO 25119-4:2018/AMD 1:2020 [A1](#), Abschnitt 11) erfüllt werden; daher müssen die technischen Sicherheitsanforderungen so aufgegliedert und formuliert werden, dass ein Modifikationsprozess unterstützt wird;
- 3) müssen die technischen Sicherheitsanforderungen (siehe ISO 25119-4:2018 [A1](#)) und ISO 25119-4:2018/AMD 1:2020 [A1](#), Abschnitt 6) überprüft werden.

Beim technischen Sicherheitskonzept müssen alle Phasen des Lebenszyklus (einschließlich Produktion, Betrieb durch den Kunden, Instandhaltung und Außerbetriebnahme) berücksichtigt werden.