

DIN EN ISO 25119-4



ICS 35.240.99; 65.060.01

Entwurf

Einsprüche bis 2018-12-12
Vorgesehen als Ersatz für
DIN EN 16590-4:2014-11 und
DIN EN 16590-4
Berichtigung 1:2015-04

**Traktoren und Maschinen für die Land- und Forstwirtschaft –
Sicherheitsbezogene Teile von Steuerungen –
Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse
(ISO/FDIS 25119-4:2018);
Deutsche und Englische Fassung FprEN 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
(ISO/FDIS 25119-4:2018);
German and English version FprEN ISO 25119-4:2018

Tracteurs et matériels agricoles et forestiers –
Parties des systèmes de commande relatives à la sécurité –
Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien
(ISO/FDIS 25119-4:2018);
Version allemande et anglaise FprEN ISO 25119-4:2018

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 65 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

Er 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 25119-4:2018.

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 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 Traktoren und 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.

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 16590-4:2014-11 und DIN EN 16590-4 Berichtigung 1:2015-04 wurden folgende Änderungen vorgenommen:

- a) ISO 25119-4 wurde überarbeitet und an EN 16590-4 angepasst, sodass keine modifizierte Übernahme unter anderer Normnummer notwendig ist.

**Traktoren und Maschinen für die Land- und Forstwirtschaft —
Sicherheitsbezogene Teile von Steuerungen — Teil 4: Fertigung, Betrieb,
Modifikation und unterstützende Prozesse (ISO/FDIS 25119-4:2018)**

*Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 4 :
Procédés de production, de fonctionnement, de modification et d'entretien (ISO/FDIS 25119-4:2018)*

*Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production,
operation, modification and supporting processes (ISO/FDIS 25119-4:2018)*

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	9
5 Qualitätsmanagementsystem	10
6 Sicherheitsvalidierung und -verifizierung	10
6.1 Ziele	10
6.2 Allgemeines	10
6.3 Voraussetzungen	10
6.4 Anforderungen	11
6.4.1 Validierung und Verifizierung der SRP/CS-Gestaltung	11
6.4.2 Anwendungsbereich der Sicherheitsvalidierung und -verifizierung	11
6.4.3 Aktivitäten	11
6.4.4 Verifizierungs- und Validierungsplan	12
6.4.5 Validierungs- und Verifizierungsprüfspezifikation	12
6.5 Arbeitsprodukte	12
7 Konfigurationsmanagement	13
7.1 Ziele	13
7.2 Voraussetzungen	13
7.3 Anforderungen	13
7.4 Arbeitsprodukte	13
8 Produktfreigabe	13
8.1 Ziele	13
8.2 Allgemeines	13
8.3 Voraussetzungen	14
8.4 Anforderungen	15
8.4.1 Bedingungen für die Produktfreigabe	15
8.4.2 Dokumentation der Produktfreigabe	15
8.5 Arbeitsprodukte	15
9 Produktionsplanung, Produktion und Produktionsprüfung	15
9.1 Ziele	15
9.2 Allgemeines	15
9.3 Voraussetzungen	16
9.4 Anforderungen	16
9.4.1 Produktionsplan	16
9.4.2 Produktionsprüfplan	16
9.4.3 Personal	16
9.4.4 Prozessfähigkeit	16
9.4.5 Dokumentation	16
9.4.6 Nichterfüllung	17

9.4.7	Lager- und Transportbedingungen.....	17
9.5	Arbeitsprodukte	17
10	Betriebsplanung und Instandhaltung (Betriebs-, Instandhaltungs-, Instandsetzungs- und Außerbetriebnahanweisungen)	17
10.1	Ziele	17
10.2	Allgemeines	17
10.3	Voraussetzungen	17
10.4	Anforderungen.....	18
10.4.1	Allgemeines	18
10.4.2	Wartungsplan	18
10.4.3	Reparaturanweisungen.....	18
10.4.4	Anweisungen für Servicetechniker.....	18
10.4.5	Anwenderinformationen.....	19
10.4.6	Beobachtung im Betrieb	19
10.4.7	Lager- und Transportbedingungen.....	19
10.4.8	Außerbetriebnahme und Demontage	19
10.5	Arbeitsprodukte	19
11	Modifikationen (Änderungsmanagement)	19
11.1	Ziel.....	19
11.2	Allgemeines	20
11.3	Voraussetzungen	20
11.4	Anforderungen.....	20
11.4.1	Verfahren zur Produktmodifikation und -verbesserung	20
11.4.2	Änderungsauftrag	22
11.4.3	Beurteilung der Auswirkung einer Modifikation	23
11.4.4	Änderungsbefugnis.....	23
11.5	Arbeitsprodukte	24
12	Verfahren für Lieferanten von SRP/CS, Teilsystemen und Komponenten.....	24
12.1	Ziele	24
12.2	Allgemeines	24
12.3	Voraussetzungen	24
12.4	Anforderungen.....	25
12.4.1	Allgemeines	25
12.4.2	Anwendungsbereich der Anforderungen.....	25
12.4.3	Lieferantenauswahl.....	25
12.4.4	Projektbeginn	25
12.4.5	Projektplanung.....	26
12.4.6	Projektdurchführung.....	26
12.4.7	Bestätigungsmaßnahmen für die funktionale Sicherheit des Entwicklungspartners.....	26
12.4.8	Systemvalidierung	26
12.5	Arbeitsprodukte	27
13	Technische Dokumentation.....	27
13.1	Ziele	27
13.2	Anforderungen.....	27
13.2.1	Dokumentenaufbewahrung.....	27
13.2.2	Dokumentenstruktur.....	27
Anhang A (informativ)	Checkliste zur technischen Dokumentation.....	29
Anhang ZA (informativ)	Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG.....	32
Literaturhinweise.....		33

Europäisches Vorwort

Dieses Dokument (FprEN ISO 25119-4:2018) 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 25119-4:2018 wurde von CEN als FprEN ISO 25119-4:2018 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 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.

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 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;
- der Anwendungsbereich wurde geringfügig verändert;
- und ein neuer Abschnitt 5 (Qualitätsmanagementsystem) wurde hinzugefügt;
- der vormalige Abschnitt 5 (Konfigurationsmanagement) wurde hinter Abschnitt 6 verschoben;
- Abschnitt 6 wurde geändert;
- das Beispiel für eine technische Dokumentationscheckliste wurde 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 kann unter www.iso.org/members.html gefunden 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 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, 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 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 Levels 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 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, Validierung, 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 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, Unfallverhütungsorganisationen, 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. Es 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 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 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 3600, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Operator's manuals — Content and format*

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 25119-2:2018, *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*

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: unter <https://www.iso.org/obp>
- IEC Electropedia: unter <http://www.electropedia.org/>

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

AgPL	landwirtschaftlicher Performance Level (en: agricultural performance level)
AgPLr	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
ETA	Ereignisbaumanalyse (en: event tree analysis)
E/E/PES	elektrische/elektronische/programmierbare elektronische Systeme
EMV	Elektromagnetische Verträglichkeit
FMEA	Fehlermöglichkeits- und Einflussanalyse (en: failure mode and effects analysis)
FSM	Funktionssicherheitsmanagement (en: functional safety management)

FTA	Fehlerbaumanalyse (en: fault tree analysis)
HARA	Gefahrenanalyse 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)
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 Dokuments müssen die Konformität mit den Abschnitten 7, 8, 9 und 11 nachweisen durch

- Anwendung der Qualitätsmanagementgrundsätze wie etwa in ISO 9001 unter Nutzung der Abschnitte 7, 8, 9 und 11 als Anleitung oder
- Anwendung der spezifischen Abschnitte in den Abschnitten 7, 8, 9 und 11 wie in diesem Dokument formuliert.

6 Sicherheitsvalidierung und -verifizierung

6.1 Ziele

Ein Ziel besteht darin, nachzuweisen, dass jede funktionale Sicherheitsanforderung ordnungsgemäß erfüllt wurde und für die Sicherheitsziele der UoO geeignet ist.

Ein weiteres Ziel besteht darin, nachzuweisen, dass jedes Sicherheitsziel wie ursprünglich gewünscht und festgelegt erreicht wurde und für die funktionale Sicherheit der UoO geeignet ist.

6.2 Allgemeines

Die vorhergehenden Verifizierungs- und Validierungsstufen (z. B. Überprüfungen, Sicherheitsanalysen und Komponenten- und Integrationsprüfungen) dienen dazu, nachzuweisen, dass die Ergebnisse jeder einzelnen Phase die relevanten, in ISO 25119-3 beschriebenen Entwurfs- und Implementierungssicherheitsanforderungen erfüllen.

6.3 Voraussetzungen

Die folgenden Voraussetzungen werden an diese Phase gestellt:

- Sicherheitsplan nach ISO 25119-1:2018, 6.4.6.3 — Termine, Ressourcen, Ausrüstung, Reifegrad usw.;
- Maschinenprüfplan — Teil des bestehenden Qualitätssicherungsprozesses;

- HARA nach ISO 25119-2:2018, Abschnitt 6 — Identifikation potenzieller Gefährdungen;
- funktionales Sicherheitskonzept nach ISO 25119-2:2018, Abschnitt 7 — Sicherheitsziele sowie sichere Zustände und funktionale Sicherheitsanforderungen;
- technisches Sicherheitskonzept nach ISO 25119-3:2018, Abschnitt 5 — Technische Sicherheitsanforderungen.

6.4 Anforderungen

6.4.1 Validierung und Verifizierung der SRP/CS-Gestaltung

Der Gestaltung der SRP/CS muss validiert/verifiziert werden (siehe ISO 25119-1:2018, Bild 1).

Die Validierung und Verifizierung muss nachweisen, dass jedes SRP/CS Folgendes erfüllt:

- die Anforderungen des festgelegten AgPL einschließlich gegebenenfalls:
 - a) Hardware-Kategorie, $MTTF_{DC}$, DC, CCF (siehe ISO 25119-2:2018, Anhänge A, B, C, D);
 - b) SRL (siehe ISO 25119-3:2018, Abschnitt 7);
- die Sicherheitsziele, sicheren Zustände und verbleibenden funktionalen und technischen Sicherheitsanforderungen;
- die Erfüllung der zugeordneten Sicherheitsfunktionen.

6.4.2 Anwendungsbereich der Sicherheitsvalidierung und -verifizierung

Innerhalb des Lebenszyklus muss eine Validierung und Verifizierung der Sicherheitsanforderungen zumindest für folgende Teile durchgeführt werden:

- komplettes System auf Maschinenebene (z. B. Prüfstandtests, Hardware-in-the-Loop-Tests, Prüfmaschine);
- Hardware;
- Software.

6.4.3 Aktivitäten

Für eine strukturierte Sicherheitsvalidierung und -verifizierung muss folgende Reihenfolge eingehalten werden:

- Validierungs- und Verifizierungsplanung;
- Validierungs- und Verifizierungsspezifikation;
- Validierungs- und Verifizierungsausführung;
- Dokumentation des Ergebnisses der Validierung und Verifizierung.

6.4.4 Verifizierungs- und Validierungsplan

Für die Sicherheitsziele, sicheren Zustände und funktionalen und technischen Sicherheitsanforderungen muss ein Validierungs- und Verifizierungsplan ausgearbeitet werden, der folgende Punkte umfasst:

- Validierung und Verifizierung und mögliche Varianten;
- Reifegrad des Systems;
- Validierungs- und Verifizierungsziele;
- Validierungs- und Verifizierungsverfahren;
- Erklärung der Unabhängigkeit zwischen dem für die Validierung/Verifizierung Verantwortlichen und dem Entwickler;
- erforderliche Ausrüstung und Umgebungsbedingungen, einschließlich Kalibrierungsspezifikationen für Werkzeuge;
- festgelegte Bezugnahme auf den Gesamtprojektplan;
- „Bestanden“/„Nicht bestanden“-Kriterien für alle Prüfungen.

6.4.5 Validierungs- und Verifizierungsprüfspezifikation

Folgende Verfahren und Maßnahmen müssen angewendet und festgelegt werden:

- Prüfungen (Black-Box-Prüfung, Hardware-in-the-Loop-Prüfung [HIL], Maschinenprüfungen, Feldprüfungen usw.);
- Analyse (z. B. Simulation);
- Prüfungen der relevanten Dokumente (Input von der Hardware/Software, z. B. FMEA, Schaltplan).

6.5 Arbeitsprodukte

Folgende Arbeitsprodukte müssen während dieser Phase geliefert werden:

- a) ausführlicher Validierungs- und Verifizierungsplan;
- b) Prüfspezifikation;
- c) Validierungs- und Verifizierungsdokumentation, die den Nachweis enthalten muss, dass die Validierungs- und Verifizierungsziele erreicht wurden für
 - 1) das vollständige System auf Systemebene oder gegebenenfalls auf Maschinenebene,
 - 2) Hardware und
 - 3) Software.

7 Konfigurationsmanagement

7.1 Ziele

Das erste Ziel muss sein, sicherzustellen, dass die SRP/CS und die zugehörige technische Dokumentation für eine Sicherheitsfunktion jederzeit eindeutig identifiziert und vervielfältigt werden können.

Das zweite Ziel ist, sicherzustellen, dass die Beziehungen und Unterschiede zwischen früheren und aktuellen Versionen der SRP/CS und der damit verbundenen technischen Dokumentation verfolgt werden können.

7.2 Voraussetzungen

Siehe Arbeitsprodukte für jede Phase des Sicherheitslebenszyklus.

7.3 Anforderungen

Softwarewerkzeuge und Softwareentwicklungsumgebungen müssen dem Konfigurationsmanagement unterworfen werden.

Die SRP/CS-Spezifikationen und die damit verbundene technische Dokumentation müssen dem Konfigurationsmanagement unterliegen.

Die Konfigurationsmanagementdaten müssen in Übereinstimmung mit der Dokumentenaufbewahrungspolitik des Unternehmens verwahrt werden.

Alle Varianten/Versionen des E/E/PES-Systems, die ein SRP/CS enthalten, müssen eindeutig gekennzeichnet werden. Die Kennzeichnung könnte in Form einer Seriennummer oder eines Datumscode erfolgen.

7.4 Arbeitsprodukte

Das anwendbare Arbeitsprodukt muss die Auflistung der SRP/CS mit Verweisung auf die zugehörige technische Dokumentation für eine gegebene Konfiguration sein.

8 Produktfreigabe

8.1 Ziele

Ziel dieser Phase ist, die Bedingungen für die „Produktfreigabe“ als Abschluss der Entwicklung von E/E/PES-Systemen zu spezifizieren. Die Produktfreigabe bestätigt, dass das Produkt die Anforderungen an die funktionale Sicherheit in der Maschine erfüllt.

8.2 Allgemeines

Bild 1 zeigt die notwendigen Bestätigungen der Entwicklungsstufen eines E/E/PES-Systems und die Reihenfolge ihrer Vervollständigung, bis abschließend alle Bedingungen für eine Produktfreigabe erfüllt sind.

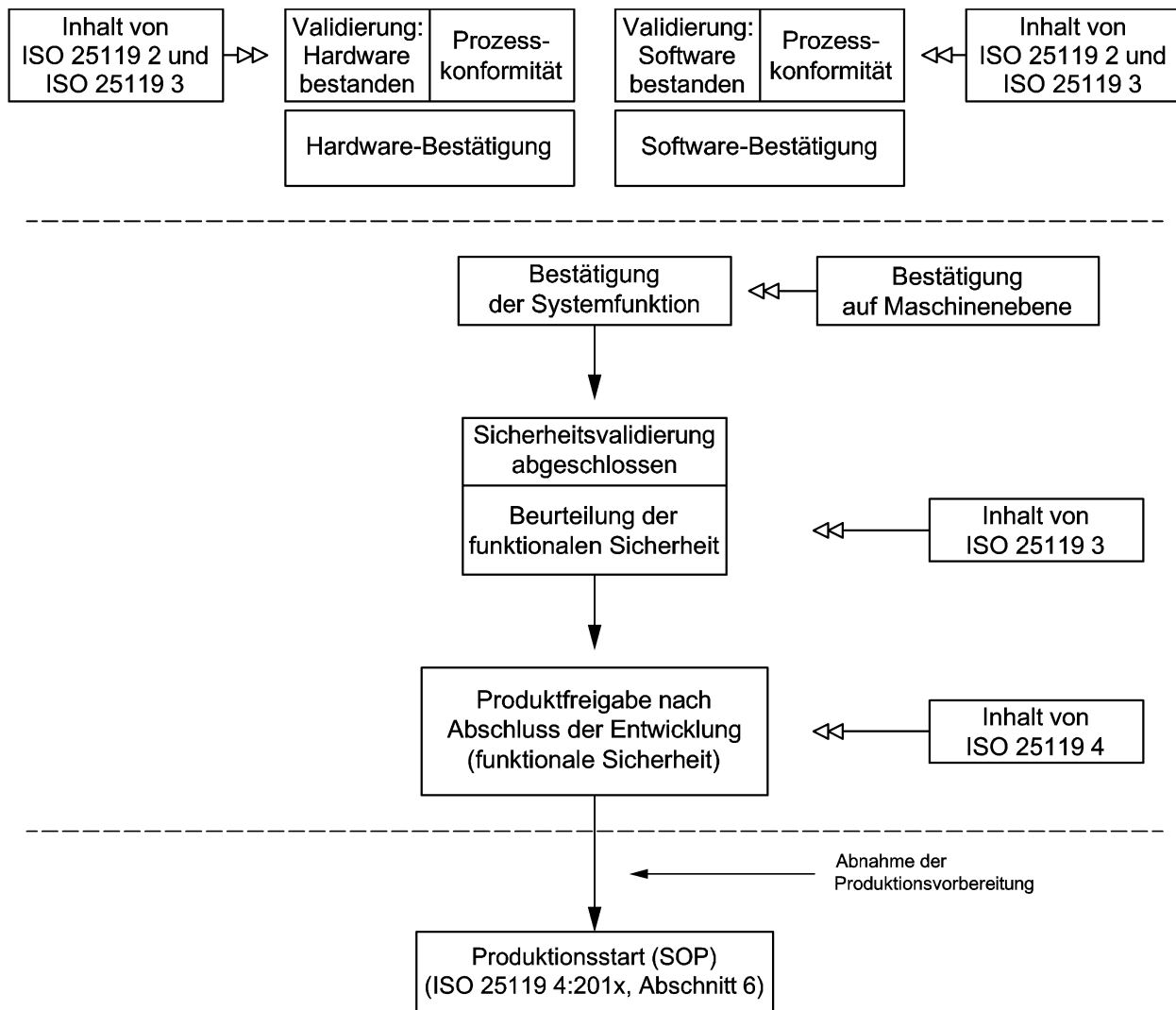


Bild 1 — Genehmigungshierarchie

8.3 Voraussetzungen

Die folgenden Voraussetzungen werden an diese Phase gestellt:

- Bestätigungsdokumentation: Hardware;
- Bestätigungsdokumentation: Software;
- Bestätigungsdokumentation auf Systemebene oder gegebenenfalls auf Maschinenebene;
- Dokumentation der Bewertung der funktionalen Sicherheit.

8.4 Anforderungen

8.4.1 Bedingungen für die Produktfreigabe

Die Produktfreigabe darf nur genehmigt werden, wenn folgende Ergebnisse aus vorherigen Stufen im Lebenszyklus vorliegen (siehe Anhang A):

- eine akzeptierte Bewertung;
- Hardware-Bestätigung;
- Software-Bestätigung;
- Systembestätigung auf Ebene des E/E/PES-Systems oder gegebenenfalls auf Maschinenebene (einschließlich Datenparametrisierung).

8.4.2 Dokumentation der Produktfreigabe

Die Produktfreigabe muss schriftlich dokumentiert werden und mindestens folgende Punkte enthalten:

- Version(en) des freigegebenen E/E/PES-Systems;
- Konfiguration des freigegebenen E/E/PES-Systems;
- Verweisungen auf die zugehörigen Dokumente;
- Freigabedatum.

ANMERKUNG Das Freigabedokument für die funktionale Sicherheit kann entweder Teil des Dokuments für die Produktfreigabe des E/E/PES-Systems oder ein separates Dokument sein.

8.5 Arbeitsprodukte

Das anzuwendende Arbeitsprodukt muss die Produktfreigabedokumentation sein.

9 Produktionsplanung, Produktion und Produktionsprüfung

9.1 Ziele

Die Anforderungen an diese Phase haben zum Ziel, einen Produktions- und Installationsplan für SRP/CS zu entwickeln und sicherzustellen, dass die geforderte funktionale Sicherheit während des Produktionsprozesses vom jeweiligen Hersteller des Produkts oder der für den Prozess zuständigen Person oder Organisation (Maschinenhersteller, Lieferant, Unterlieferant usw.) aufrechterhalten wird.

9.2 Allgemeines

Durch Aufnahme sicherheitsrelevanter Merkmale in die Produktionsplanung und -kontrolle legt diese Phase die erforderlichen Schritte fest, um zu gewährleisten, dass die funktionale Sicherheit auch während des Produktionsprozesses aufrechterhalten wird.

9.3 Voraussetzungen

Die Voraussetzungen für Produktion und Prüfung sind:

- Montagehinweise (Dokumentation der Teile bzw. Funktionen, die von der Montage beeinflusst werden können);
- Prüfhinweise;
- Produktfreigabedokument;
- Prüfkriterien (zu prüfende sicherheitsrelevante Merkmale);
- Produktüberwachung — eine Produktüberwachung ist für sicherheitsrelevante Merkmale notwendig und stellt sicher, dass die sicherheitsrelevanten Merkmale von Komponenten entsprechend ihrer Spezifikationen beim Produktionsprozess des Maschinenherstellers gewahrt werden.

9.4 Anforderungen

9.4.1 Produktionsplan

Ein Produktionsplan muss unter Berücksichtigung der Montageanleitung Folgendes beinhalten:

- Identifikation der sicherheitsbezogenen Merkmale;
- Ablauf und Verfahren der Produktionsschritte;
- Montagegeräte/Werkzeuge.

9.4.2 Produktionsprüfplan

Ein Prüfplan muss Folgendes beinhalten:

- Identifikation der sicherheitsbezogenen Merkmale;
- Ablauf und Verfahren der Prüfschritte;
- Prüfeinrichtungen/-werkzeuge, Prüfkriterien und
- Häufigkeit der Produktionsprüfungen.

9.4.3 Personal

Produktion und Prüfung müssen von qualifiziertem Personal entsprechend den Produktions- und Prüfplänen durchgeführt werden.

9.4.4 Prozessfähigkeit

Die Prozessfähigkeit muss mittels der üblichen Anforderungen der Industrie gewährleistet sein.

9.4.5 Dokumentation

Die Durchführung von Prüfungen in Übereinstimmung mit dem Prüfplan muss dokumentiert werden. Die Prüfdokumentation muss mindestens folgende Angaben enthalten: Prüfdatum, Prüfer, eindeutige Teilekennzeichnung, Prüfergebnisse.

9.4.6 Nichterfüllung

Die Vorgehensweise bei einer Nichterfüllung eines Prüfkriteriums für sicherheitsbezogene Bereiche (SRP/CS) muss festgelegt werden. Nacharbeiten sind nur nach Vorliegen des Nachweises der geeigneten Prozesslenkung gestattet.

9.4.7 Lager- und Transportbedingungen

Eine eventuell erforderliche Sonderbehandlung und Verpackung von SRP/CS muss bei der Festlegung der Bedingungen für die Lagerung und den Transport des Produkts beachtet werden.

9.5 Arbeitsprodukte

Folgende Arbeitsprodukte müssen während dieser Phase geliefert werden:

- a) Dokumentation der durchgeführten Prüfungen in Übereinstimmung mit dem Prüfplan;
- b) Verfahren zur Behandlung von Konformitätsmängeln;
- c) Lager- und Transportbedingungen.

10 Betriebsplanung und Instandhaltung (Betriebs-, Instandhaltungs-, Instandsetzungs- und Außerbetriebnahanweisungen)

10.1 Ziele

Die Anforderungen an diese Phase haben zum Ziel, den Umfang von Wartungs-, Kundeninformations- und Instandsetzungsanweisungen von SRP/CS festzulegen, um die erforderliche funktionale Sicherheit im Betrieb, bei Feldüberwachung, Instandhaltung, Instandsetzung und Außerbetriebnahme zu bewahren.

10.2 Allgemeines

Dieser Abschnitt beinhaltet die Erfassung der Bereiche mit sicherheitsrelevanten Merkmalen zur Ausarbeitung von Reparaturanweisungen und Benutzerinformationen und zur Planung, Durchführung und Überwachung von Instandhaltungsarbeiten.

10.3 Voraussetzungen

Die Voraussetzungen für Betrieb, Planung und Instandhaltung sind:

- Produktfreigabe — Freigabedokument bezüglich der funktionalen Sicherheit;
- Qualitätsmanagementsystem (ein implementiertes, routinemäßig angewendetes Qualitätsmanagementsystem wie ISO 9001);
- Instandhaltungshinweise — Dokumentation der sicherheitsbezogenen Bereiche, die durch Instandhaltung beeinflusst werden können (Instandhaltungsaufgaben), und Hinweise zu den durch Feldanalysen erworbenen Erfahrungen;
- Konfigurationsmanagementplan — dokumentiertes Verfahren zum Konfigurationsmanagement.

10.4 Anforderungen

10.4.1 Allgemeines

Die Anforderungen an die funktionale Sicherheit während Instandhaltungs- und Reparaturarbeiten können sich von den im Betrieb erforderlichen Anforderungen unterscheiden und diese müssen berücksichtigt werden.

10.4.2 Wartungsplan

Mit dem Systementwurf muss gleichzeitig ein Wartungsplan erstellt werden, der Folgendes beinhaltet:

- Identifikation der Komponenten des SRP/CS, die einer regelmäßigen Wartung bedürfen, unter Berücksichtigung der relevanten freigegebenen Teilsystem- oder Systemkonfiguration und
- Reihenfolge, Verfahren (falls erforderlich Werkzeuge) und Festlegung der Zeitspanne und des Umfangs von Wartungsarbeiten für die festzulegende Betriebsdauer.

10.4.3 Reparaturanweisungen

Reparaturanweisungen müssen Folgendes beinhalten:

- Identifizierung der instandsetzungsfähigen Komponenten des SRP/CS;
- Arbeitsschritte und Arbeitsablauf, Verfahren und Werkzeuge (z. B. Programmier- und Diagnoseeinrichtungen, sofern anwendbar);
- die relevante freigegebene Konfiguration des Systems oder Teilsystems;
- die zulässige Deaktivierung von Teilsystemen/Systemen und die zusätzlichen an der Gesamtmaschine erforderlichen Einstellungen und
- Identifizierung der Ersatzteile des Herstellers und gegebenenfalls der genehmigten Ersatzteile.

10.4.4 Anweisungen für Servicetechniker

Instandsetzungs- und Wartungsarbeiten sollten:

- nur von ausreichend befugtem und geschultem Personal durchgeführt werden;
- in Übereinstimmung mit dem Wartungsplan oder entsprechend den Instandsetzungsanweisungen durchgeführt und dokumentiert werden.