

DIN EN 16590-1

ICS 35.240.99; 65.060.01

**Traktoren und Maschinen für die Land- und Forstwirtschaft –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze
(ISO 25119-1:2010 modifiziert);
Deutsche Fassung EN 16590-1:2014**

Tractors and machinery for agriculture and forestry –
Safety-related parts of control systems –
Part 1: General principles for design and development (ISO 25119-1:2010 modified);
German version EN 16590-1:2014

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 25119-1:2010 modifié);
Version allemande EN 16590-1:2014

Gesamtumfang 34 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen.

Sie beinhaltet die Deutsche Fassung der vom Technischen Komitee CEN/TC 144 „Traktoren und land- und forstwirtschaftliche Maschinen“ (Sekretariat: AFNOR, Frankreich) im Europäischen Komitee für Normung (CEN) ausgearbeiteten EN 16590-1:2014.

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

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).

Die im Abschnitt 2 und den Literaturhinweisen zitierten Europäischen Normen sind als DIN-EN- bzw. DIN-EN-ISO-Normen mit gleicher Zählnummer veröffentlicht.

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

Deutsche Fassung

Traktoren und Maschinen für die Land- und Forstwirtschaft —
Sicherheitsbezogene Teile von Steuerungen —
Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze
(ISO 25119-1:2010 modifiziert)

Tractors and machinery for agriculture and forestry —
Safety-related parts of control systems —
Part 1: General principles for design and development
(ISO 25119-1:2010 modified)

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 25119-1:2010 modifié)

Diese Europäische Norm wurde vom CEN am 23. Februar 2014 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 Management-Zentrum des CEN-CENELEC 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 Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, 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: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	7
2 Normative Verweisungen.....	7
3 Begriffe	7
4 Abkürzungen	14
5 Management während des gesamten Sicherheitslebenszyklus.....	15
5.1 Ziele	15
5.2 Allgemeines.....	15
5.2.1 Einführung in das Konzept des Sicherheitslebenszyklus.....	15
5.2.2 Externe funktionale Sicherheitsmaßnahmen.....	15
5.3 Voraussetzungen.....	16
5.4 Anforderungen — Aktivitäten des funktionalen Sicherheitsmanagements über alle Lebenszyklen hinweg.....	17
5.4.1 Kultur der funktionalen Sicherheit.....	17
5.4.2 Ständige Verbesserung.....	17
5.4.3 Schulung und Qualifizierung.....	18
5.4.4 Sicherheitsmanagement während der Entwicklung	18
5.4.5 Zuweisung der Verantwortlichkeiten für die Sicherheit	18
5.4.6 Zuweisung der Aufgaben.....	18
5.4.7 Planung aller Sicherheitsmanagement-Aktivitäten während der Entwicklung.....	19
5.5 Arbeitsprodukte	21
6 Beurteilung der funktionalen Sicherheit	21
6.1 Ziele	21
6.2 Allgemeines.....	21
6.3 Voraussetzungen.....	22
6.4 Anforderungen.....	22
6.4.1 Hinweise für die Beurteilung der funktionalen Sicherheit	22
6.4.2 Verifizierungsmaßnahmen.....	22
6.5 Arbeitsprodukte	24
7 Sicherheitsmanagement-Aktivitäten nach Produktionsanlauf (SOP)	24
7.1 Ziele	24
7.2 Allgemeines.....	25
7.3 Voraussetzungen.....	25
7.4 Anforderungen.....	25
7.4.1 Produktionsmanagement und Modifikationsprozeduren.....	25
7.4.2 Aufgaben zur Vorbereitung und Durchführung der Fertigung und End-of-Line-Kontrollen	25
7.4.3 Aufgaben für sicheren Betrieb und Außerbetriebnahme der Maschine	25
7.5 Arbeitsprodukte	25
8 Produktion und Installation sicherheitsbezogener Systeme	25
8.1 Ziele	25
8.2 Allgemeines.....	26
8.3 Voraussetzungen.....	26
8.4 Anforderungen.....	26
8.4.1 Produktionsplan.....	26

8.4.2	Prüfplan	26
8.4.3	Produktion und Prüfung	26
8.4.4	Prozessfähigkeit	27
8.4.5	Dokumentation	27
8.4.6	Nichterfüllung	27
8.4.7	Rückverfolgbarkeit	27
8.4.8	Lager- und Transportbedingungen	27
8.4.9	Modifikation	27
8.5	Arbeitsprodukte	27
Anhang A (informativ) Beispiel für die Gliederung eines projektspezifischen Sicherheitsplans.....		28
A.1	Allgemeines	28
A.2	Änderungsprotokoll	28
A.3	Ziel des Gesamtprojekts	28
A.4	Terminplan	28
A.5	Projektorganisation	28
A.5.1	Projektteam-Organisation	28
A.5.2	Projektteammitglieder.....	29
A.5.3	Sicherheitsmanagement.....	29
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG		31
Literaturhinweise		32

Vorwort

Dieses Dokument (EN 16590-1:2014) wurde vom Technischen Komitee CEN/TC 144 „Traktoren und land- und forstwirtschaftliche Maschinen“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Oktober 2014, und etwaige entgegenstehende nationale Normen müssen bis Oktober 2014 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinien.

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

EN 16590, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen*, besteht aus den folgenden Teilen:

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

Auf Änderungen im Vergleich zu ISO 25119-1:2010 wird durch eine senkrechte Linie am Seitenrand hingewiesen.

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

Einleitung

EN 16590 beschreibt den Ansatz der Gestaltung und Bewertung für alle Aktivitäten bezüglich des Sicherheitslebenszyklus für sicherheitsbezogene Systeme, bestehend aus elektrischen und/oder elektronischen und/oder programmierbaren elektronischen Systemen (E/E/PES), welche für land- und forstwirtschaftliche Traktoren, selbstfahrende Aufsitzmaschinen sowie Anbau-, Aufsattel- und Anhängemaschinen für landwirtschaftliche Geräte verwendet werden. Sie ist auch auf kommunale Geräte anwendbar. Sie behandelt potentielle, durch das Funktionsverhalten von E/E/PES-sicherheitsrelevanten Systemen verursachte Gefahren, im Unterschied zu Gefahren, die durch die E/E/PES-Geräte selbst entstehen (z. B. Stromschlag, Brand, Nennleistung von E/E/PES, die der aktiven und passiven Sicherheit dienen).

Den Steuerungssystemen der betroffenen Geräte werden häufig kritische Funktionen zugewiesen. Diese werden als die *sicherheitsbezogenen Teile von Steuerungen* (SRP/CS) bezeichnet. Diese Teile können aus Hardware und Software bestehen, können separate oder in die Steuerung integrierte Teile sein und entweder allein kritische Funktionen 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 Schutzmaßnahmen (sowohl SRP/CS als auch Nicht-SRP/CS) erreicht werden, wobei das Endergebnis das Erzielen eines sicheren Zustands ist.

EN 16590 unterteilt die Fähigkeit sicherheitsbezogener Teile, eine kritische Funktion unter vorhersehbaren Bedingungen auszuführen, in fünf Stufen, sogenannte Performance Levels. Der Performance Level eines gesteuerten Kanals hängt von mehreren Faktoren und vom Systemaufbau (Kategorie) ab, 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 sind zu berücksichtigen: systematische Ausfälle, Ausfälle gemeinsamer Ursache und Zufallsausfälle.

Darüber hinaus legt EN 16590 einen Ansatz auf Basis einer Klassifikation der Strukturen mit verschiedenen Konstruktionsmerkmalen und einem bestimmten Verhalten im Fehlerfall fest, um den Konstrukteur während des Entwurfs anzuleiten und die Beurteilung des erreichten Performance Levels zu erleichtern.

Die Performance Levels 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).

EN 16590 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 sicherheitsbezogenen Funktionen. 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 dem zugehörigen Performance Level 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.

Dieser Teil von EN 16590 ist eine Typ-B1-Norm entsprechend EN ISO 12100.

Für Maschinen, die vom Anwendungsbereich einer maschinenspezifischen Typ-C-Norm behandelt werden und entsprechend den Bestimmungen dieser Norm gestaltet und erstellt wurden, haben die Festlegungen der Typ-C-Norm Vorrang vor den Bestimmungen dieser Typ-B-Norm.

1 Anwendungsbereich

Dieser Teil der EN 16590 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 kommunale Geräte (z. B. Straßenkehrmaschinen) angewendet werden. Sie beschreibt Merkmale und Kategorien, die zur Ausführung sicherheitsrelevanter Funktionen durch SRP/CS-Systeme erforderlich sind.

Dieser Teil der EN 16590 gilt für sicherheitsbezogene Teile elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES) als Teil mechatronischer Systeme. Sie schreibt jedoch nicht vor, welche Sicherheitsfunktionen, Kategorien oder Performance Levels für die jeweilige Maschine anzuwenden sind.

Maschinensicherheitsnormen (Typ-C-Normen) können Performance Levels und/oder Kategorien selbständig identifizieren oder sie sollten durch den Maschinenhersteller auf Basis einer Risikobeurteilung festgelegt werden.

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

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

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 16590-2:2014, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Konzeptphase*

EN 16590-3:2014, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 3: Serienentwicklung, Hardware, Software*

EN 16590-4:2014, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

landwirtschaftlicher Performance Level

AgPL

Level zur Beschreibung der Fähigkeit sicherheitsbezogener Teile, eine sicherheitsrelevante Funktion unter vorhersehbaren Bedingungen ausführen zu können

Anmerkung 1 zum Begriff: In EN 16590 ist die Performance für jede Gefährdungssituation 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

AgPL_r

Performance Level (AgPL) zum Erreichen der geforderten funktionalen Sicherheit für jede Sicherheitsfunktion

3.3

Kategorie

Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstands gegen Fehler und ihres nachfolgenden Verhaltens im Fehlerzustand, das durch die bauliche Anordnung der Teile und/oder ihre Zuverlässigkeit erreicht wird

3.4

Kanal

in Reihe geschaltete Kombination von Eingangs-, Logik- und Ausgangselementen

3.5

Ausfall gemeinsamer Ursache

CCF

Ausfälle mehrerer Einheiten aufgrund eines einzelnen Ereignisses, wenn diese Ausfälle nicht auf einer gegenseitigen Ursache beruhen

Anmerkung 1 zum Begriff: Ausfälle gemeinsamer Ursache sollten nicht mit mehreren *gleichartigen Ausfällen* verwechselt werden (siehe EN ISO 12100).

3.6

Beherrschbarkeit

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

3.7

erkannte gefahrbringende Ausfallrate

λ_{dd}

gefahrbringende Ausfallrate derjenigen Bauteile, bei denen eine Fehlererkennung erfolgte

3.8

gefahrbringender Ausfall

Ausfall, bei dem ein SRP/CS den geforderten Performance Level nicht mehr aufrechterhalten kann, auch wenn die sicherheitsbezogene Funktion von anderen (redundanten) Systembauteilen (aufgrund der Senkung des daraus resultierenden Performance Levels) aufrechterhalten wird

3.9

gefährliche Ausfallrate

λ_d

Anteil aller Bauteile, die je Zeiteinheit gefährlich ausfallen

3.10

Diagnosedeckungsgrad

DC

Anteil der Wahrscheinlichkeit erkannter gefahrbringender Ausfälle λ_{dd} und der Wahrscheinlichkeit der gesamten gefährlichen Ausfälle λ_d , wiedergegeben durch:

$$DC = \sum \lambda_{dd} / \sum \lambda_d$$

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

Anmerkung 2 zum Begriff: Der DC-Wert wird nach Tabelle 1 definiert.

Anmerkung 3 zum Begriff: Für SRP/CS, die aus mehreren Teilen bestehen, wird ein Durchschnittswert DC_{avg} für DC verwendet (siehe EN 16590-2:2014, Anhang C).

Tabelle 1 — Diagnosedeckungsgrad (DC)

Deckungsgrad	Bereich
Niedrig	$DC < 60 \%$
Mittel	$60 \% \leq DC < 90 \%$
Hoch	$90 \% \leq DC$

3.11

Diagnoseprüfintervall

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

3.12

E/E/PES-System-Architektur

Zuweisung sicherheitskritischer Funktionen 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 potentielle Gefahr besteht

3.15

Ausfall

Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion auszuführen

Anmerkung 1 zum Begriff: Ausfälle, die nicht die Verfügbarkeit des gesteuerten Prozesses betreffen, liegen nicht im Anwendungsbereich der EN 16590.

Anmerkung 2 zum Begriff: Nach einem Ausfall weist die Einheit einen Fehler auf.

Anmerkung 3 zum Begriff: „Ausfall“ ist ein Ereignis, im Unterschied zu einem „Fehler“, bei dem es sich um einen Zustand handelt.

Anmerkung 4 zum Begriff: Der so definierte Begriff gilt nicht für Einheiten, die nur aus Software bestehen.

3.16

Fehler

Zustand einer Einheit, 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 der Einheit selbst, kann aber auch ohne vorherigen Ausfall auftreten.

Anmerkung 2 zum Begriff: In EN 16590 bedeutet der Begriff ‚Fehler‘ *zufälliger* Fehler.

3.17

Funktion

definiertes Verhalten einer oder mehrerer elektronischer Steuereinheiten (ECU)