

DIN EN 16590-2

ICS 35.240.99; 65.060.01

**Traktoren und Maschinen für die Land- und Forstwirtschaft –
Sicherheitsbezogene Teile von Steuerungen –
Teil 2: Konzeptphase (ISO 25119-2:2010 modifiziert);
Deutsche Fassung EN 16590-2:2014**

Tractors and machinery for agriculture and forestry –
Safety-related parts of control systems –
Part 2: Concept phase (ISO 25119-2:2010 modified);
German version EN 16590-2:2014

Tracteurs et matériels agricoles et forestiers –
Parties des systèmes de commande relatives à la sécurité –
Partie 2: Phase de projet (ISO 25119-2:2010 modifié);
Version allemande EN 16590-2:2014

Gesamtumfang 48 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 16590:2014.

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 2: Konzeptphase
(ISO 25119-2:2010 modifiziert)

Tractors and machinery for agriculture and forestry —
Safety-related parts of control systems —
Part 2: Concept phase
(ISO 25119-2:2010 modified)

Tracteurs et matériels agricoles et forestiers —
Parties des systèmes de commande relatives
à la sécurité —
Partie 2: Phase de projet
(ISO 25119-2:2010 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	7
5 Konzept — Definition der Betrachtungseinheit.....	8
5.1 Ziele	8
5.2 Voraussetzungen	8
5.3 Anforderungen.....	9
5.3.1 Betrachtungseinheit und Umgebungsbedingungen.....	9
5.3.2 Grenzen der Betrachtungseinheit und ihre Schnittstellen zu anderen Betrachtungseinheiten.....	9
5.3.3 Gefährdungsquellen.....	9
5.3.4 Weitere Festlegungen	10
5.3.5 Arbeitsprodukte	10
6 Risikoanalyse und Methodenbeschreibung	10
6.1 Ziele	10
6.2 Voraussetzungen.....	10
6.3 Anforderungen.....	11
6.3.1 Verfahren zur Erstellung einer Risikoanalyse	11
6.3.2 Aufgaben bei der Risikoanalyse	11
6.3.3 Teilnehmer an der Risikoanalyse.....	11
6.3.4 Beurteilung und Klassifizierung eines potentiellen Schadens.....	11
6.3.5 Beurteilung der Aufenthaltsdauer in der beobachteten Situation.....	12
6.3.6 Beurteilung einer möglichen Schadensvermeidung.....	12
6.3.7 Herleitung des geforderten Performance Levels AgPL _r	13
6.4 Arbeitsprodukte	14
7 Systementwurf	14
7.1 Ziele	14
7.2 Voraussetzungen.....	14
7.3 Anforderungen.....	14
7.3.1 Zuweisung des AgPL	14
7.3.2 Erreichen des geforderten landwirtschaftlichen Performance Levels AgPL _r	15
7.3.3 Erreichen des Performance Levels.....	16
7.4 Arbeitsprodukte	16
Anhang A (normativ) Vorgesehene Architekturen für sicherheitsbezogene Teile von Steuerungen.....	17
A.1 Allgemeines.....	17
A.2 Kategorie B (elementar)	17
A.3 Kategorie 1	18
A.4 Kategorie 2	18
A.5 Kategorie 3	19
A.6 Kategorie 4	21

Anhang B (informativ) Vereinfachtes Verfahren zur Abschätzung der Kanal-MTTF_{dc}	24
B.1 Allgemeines	24
B.2 MTTF _d -Werte für Bauteile	24
B.2.1 Bestimmung der MTTF _d -Werte für Bauteile	24
B.2.2 MTTF _d für Bauteile von B ₁₀	25
B.3 „Parts Count“-Verfahren	25
B.4 Berechnung der symmetrischen MTTF _{dc} für Zweikanalarchitekturen	26
Anhang C (informativ) Bestimmung des Diagnosedeckungsgrads (DC)	27
C.1 Allgemeines	27
C.2 Schätzung des geforderten DC	27
C.3 Schätzung des Kanal-DC	30
C.4 Berechnung des Kanal-DC	30
C.5 Berechnung des DC	31
Anhang D (informativ) Schätzung von Ausfällen gemeinsamer Ursache (CCF)	32
Anhang E (informativ) Systematischer Ausfall	34
E.1 Allgemeines	34
E.2 Anforderungen an die Beherrschung systematischer Ausfälle	34
E.3 Anforderungen an das Vermeiden systematischer Ausfälle	35
Anhang F (informativ) Merkmale von Sicherheitsfunktionen	37
F.1 Allgemeines	37
F.2 Anlaufverriegelung	37
F.3 Stoppfunktion	37
F.4 Manuelle Rückstellung	37
F.5 Anlauf und Wiederanlauf	38
F.6 Ansprechzeit	38
F.7 Sicherheitsbezogene Parameter	38
F.8 Externe Steuerfunktion	38
F.9 Muting (Aussetzung von Sicherheitsfunktionen von Hand)	39
F.10 Warnung des Maschinenführers	39
Anhang G (informativ) Beispiel einer Risikoanalyse	40
G.1 Arbeitsablauf	40
G.2 Beispiel einer Risikoanalyse eines Elektro-Hydraulikgetriebes für eine selbstfahrende Arbeitsmaschine (Futtererntemaschine) — Auszug aus einer vollständigen Risikoanalyse	40
G.2.1 Systembeschreibung	40
G.2.2 Umgebungsbedingungen	41
G.2.3 Systemzustände und Übergänge	41
G.2.4 Systemfehler	42
G.3 Beurteilung	43
G.3.1 Systemfehler — Unbeabsichtigtes Anhalten	43
G.3.2 Systemfehler — Trotz Anweisung keine Bewegung	44
G.4 Ergebnisse	44
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG	45
Literaturhinweise	46

Vorwort

Dieses Dokument (EN 16590-2:2014) 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 25119-2:2010 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 den 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.

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 beschreibt die Konzeptphase der Entwicklung sicherheitsbezogener Teile von Steuerungen (SRP/CS) in land- und forstwirtschaftlichen Traktoren, selbstfahrenden Aufsitzmaschinen sowie Anbau-, Aufsattel- und Anhängemaschinen für landwirtschaftliche Geräte. Sie kann auch auf 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 bestimmte Maschinen anzuwenden sind.

Maschinensicherheitsnormen (Typ-C-Normen) können entweder 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 und pneumatische).

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 16590-1:2014, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 16590-1:2014.

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

ADC	Analog/Digital-Wandler (en: analog to digital converter)
AgPL	landwirtschaftlicher Performance Level (en: agricultural performance level)
AgPL _r	geforderter landwirtschaftlicher Performance Level (en: required agricultural performance level)
CAD	rechnergestützter Entwurf (en: computer-aided-design)
Cat	Hardware-Kategorie (en: hardware category)
CCF	Ausfall gemeinsamer Ursache (en: common cause failure)
CRC	zyklische Redundanzprüfung (en: cyclic redundancy check)
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 (en: electrical/electronic/programmable electronic systems)
EMV	elektromagnetische Verträglichkeit (en: EMC, electromagnetic compatibility)
EPROM	löscher, programmierbarer schreibgeschützter Speicher (en: erasable programmable read-only memory)
EUC	gesteuertes Gerät (en: equipment under control)
FMEA	Ausfallarten- und Auswirkungsanalyse (en: failure mode and effects analysis)
FMECA	Ausfallarten- und Gefährlichkeitsanalyse (en: failure mode effects and criticality analysis)
FSM	Funktionssicherheitsmanagement (en: functional safety management)
FTA	Fehlerbaumanalyse (en: fault tree analysis)
HAZOP	Gefährdungs- und Bedienbarkeitsuntersuchung (en: hazard and operability study)
HIL	Hardware in the Loop (en: 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 (en: programmable electronic system)
QM	Qualitätssicherungsmaßnahmen (en: quality measures)
RAM	Direktzugriffsspeicher (en: random-access memory)
SOP	Produktionsanlauf (en: start of production)
SRL	Anforderungsniveau an die Software (en: software requirement level)
SRP	sicherheitsbezogene Teile (en: safety related parts)
SRP/CS	sicherheitsbezogene Teile von Steuerungen (en: safety-related parts of control systems)
SRS	sicherheitsbezogenes System (en: safety related system)

5 Konzept — Definition der Betrachtungseinheit

5.1 Ziele

Diese Phase hat die Entwicklung eines ausreichenden Verständnisses für die Betrachtungseinheit zum Ziel, um alle im Sicherheitslebenszyklus festgelegten Aufgaben zufriedenstellend erfüllen zu können (siehe EN 16590-1:2014, Bild 2). Anhand dieses Sicherheitskonzepts muss ein geeignetes Verfahren zur Festlegung des Performance Levels angewendet werden. Zu den geeigneten Verfahren zählen die Risikoanalyse (im Folgenden beschrieben), andere Normen, gesetzliche Vorschriften und Fachkenntnisse von Prüfinstitutionen oder eine Kombination der Verfahren.

5.2 Voraussetzungen

Die notwendigen Voraussetzungen sind eine Beschreibung der Betrachtungseinheit, ihrer Schnittstellen, der bereits bekannten Anforderungen an die Sicherheit und Zuverlässigkeit, sowie des Anwendungsbereichs der Einheit.

5.3 Anforderungen

5.3.1 Betrachtungseinheit und Umgebungsbedingungen

Hinsichtlich einer sicherheitsbezogenen Umsetzung muss ein Konzept folgender Punkte ausgearbeitet werden:

- a) Umfang, Kontext und Zweck der Betrachtungseinheit;
- b) funktionale Anforderungen an die Betrachtungseinheit;
- c) sonstige Anforderungen bezüglich der Betrachtungseinheit und Umgebungsbedingungen, einschließlich
 - technische oder physikalische Anforderungen, z. B. Betriebs-, Umwelt- und Umgebungsbedingungen und Beschränkungen, und
 - gesetzliche Anforderungen, insbesondere sicherheitsbezogene Gesetze, Vorschriften und Normen (national und international);
- d) historische Anforderungen an Sicherheit und Zuverlässigkeit und Grad der erreichten Sicherheit und Zuverlässigkeit für ähnliche oder verwandte Betrachtungseinheiten.

5.3.2 Grenzen der Betrachtungseinheit und ihre Schnittstellen zu anderen Betrachtungseinheiten

Um ein Verständnis des Funktionierens der Betrachtungseinheit in ihrem Umfeld zu erlangen, müssen folgende Informationen in Erwägung gezogen werden:

- Grenzen der Betrachtungseinheit;
- ihre Schnittstellen und Wechselwirkungen mit anderen Betrachtungseinheiten und Bauteilen;
- Anforderungen bezüglich anderer Betrachtungseinheiten;
- Abbildung und Zuordnung relevanter Funktionen zu beteiligten Betrachtungseinheiten.

5.3.3 Gefährdungsquellen

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

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

5.3.4 Weitere Festlegungen

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

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

5.3.5 Arbeitsprodukte

Die Arbeitsprodukte des Konzepts/der Definition der Betrachtungseinheit sind

- a) Betrachtungseinheit und Umgebungsbedingungen,
- b) Grenzen der Betrachtungseinheit und ihrer Schnittstellen zu anderen Betrachtungseinheiten,
- c) Gefährdungsquellen, und
- d) weitere Festlegungen.

6 Risikoanalyse und Methodenbeschreibung

6.1 Ziele

Risiko wird beschrieben (siehe EN 16590-1:2014, Definition 3.39) als Kombination aus der Häufigkeit, mit der ein Schaden eintritt, und der Schwere dieses Schadens.

Die Eintrittshäufigkeit betrachtet in der Regel die Wahrscheinlichkeit, einer Gefahrensituation ausgesetzt zu werden.

Bei der Betrachtung von Systemen muss generell eine mögliche Reaktion des Maschinenführers, welche in vielen Fällen einen Schaden vermeiden kann, berücksichtigt werden.

Die in 6.2 bis 6.4 beschriebene Vorgehensweise liefert eine Anleitung zur Bestimmung des Performance Levels (AgPL).

6.2 Voraussetzungen

Für diese Phase sind keine Voraussetzungen zu erfüllen.

6.3 Anforderungen

6.3.1 Verfahren zur Erstellung einer Risikoanalyse

Die Risikoanalyse muss den gesamten Anwendungsbereichs berücksichtigen. Werden in späteren Phasen des Sicherheitslebenszyklus Entscheidungen getroffen, welche die Festlegung des Anwendungsbereichs verändern, so muss erneut eine Risikoanalyse durchgeführt werden.

Die Architektur der SRP/CS darf nicht als Teil der Risikoanalyse betrachtet werden.

6.3.2 Aufgaben bei der Risikoanalyse

Die Betriebsbedingungen, unter denen die Einheit bei korrekter Anwendung Gefahren (einschließlich vernünftigerweise vorhersehbarer menschlicher Bedienungsfehler und bei Ausfall der Einheit) auslösen kann, müssen betrachtet werden.

6.3.3 Teilnehmer an der Risikoanalyse

An der Erstellung einer Risikoanalyse sind mehrere Personen aus verschiedenen Abteilungen, z. B. Elektronik- oder Elektroentwicklung, Prüfung oder Validierung, Maschinen- oder Hydraulikentwurf, Kundendienst, externe Berater (z. B. TÜV), beteiligt.

6.3.4 Beurteilung und Klassifizierung eines potentiellen Schadens

Die potentiellen Auswirkungen können durch Betrachtung der möglichen Störungen und systematischen Ausfälle unter relevanten Betriebsbedingungen hergeleitet werden. Die potentielle Schwere des Schadens muss so genau wie möglich für jedes relevante Szenario beschrieben werden.

Bei der Beschreibung der Schäden muss eine gewisse Kategorisierung angewendet werden. Daher wird die Schwere des Schadens eingeteilt in vier Kategorien: S0, S1, S2 und S3 (siehe Tabelle 1).

Der Führer des betroffenen Fahrzeugs und andere Parteien (z. B. Hilfspersonal, andere Fahrzeug-/Maschinenführer, Umstehende, usw.) müssen in einer detaillierten Beschreibung des Schadens genannt werden.

Der Schwerpunkt einer Untersuchung des Risikos für Sicherheitsfunktionen liegt auf dem Ursprung von Körperverletzungen. Kann bei der Analyse eines potentiellen Schadens nachgewiesen werden, dass der Schaden eindeutig auf Sachen beschränkt ist und nicht zu einer Körperverletzung führt, wäre dies kein Grund für die Einstufung als sicherheitsbezogene Funktion. Die Einführung einer Schadensklassifikation S0 berücksichtigt diese Tatsache. Für die der Schadensklasse S0 zugewiesenen Funktionen braucht keine weitere Risikobeurteilung durchgeführt zu werden.

Tabelle 1 — Beispiele für Beschreibungen von Verletzungen

S0	S1	S2	S3
Keine bedeutsamen Verletzungen, Erste-Hilfe-Maßnahmen genügen	Leichte und mäßige Verletzungen, medizinische Versorgung erforderlich, vollständige Genesung	Schwere und lebensbedrohende Verletzungen (Überleben wahrscheinlich), dauerhafte Einschränkung der Arbeitsfähigkeit	Lebensbedrohliche Verletzungen (Überleben ungewiss), schwere Behinderung

6.3.5 Beurteilung der Aufenthaltsdauer in der beobachteten Situation

Eine Risikoanalyse gibt die Auswirkungen möglicher Ausfälle unter bestimmten Arbeits- und Betriebs-situationen wieder. Diese Situationen reichen von täglichen Routinearbeiten bis zu extrem seltenen Situationen. Die Variable „E“ muss zur Kategorisierung der verschiedenen Aufenthaltshäufigkeiten oder -dauer verwendet werden. Fünf Kategorien, mit E0, E1, E2, E3 und E4 bezeichnet (siehe Tabelle 2), werden für Variable E verwendet. Hier ist die Variable E eine Schätzung, wie oft oder wie lange ein Maschinenführer oder ein Umstehender einer Gefahr ausgesetzt ist, wenn ein Ausfall zu einer Verletzung des Maschinenführers oder eines Umstehenden führen könnte. Die Exposition in einer vorherrschenden Situation wird bestimmt durch Aufenthaltshäufigkeit und -dauer, wobei die höchste ermittelte Kategorie bei der Bestimmung des AgPL_r zu verwenden ist.

ANMERKUNG Eine Gefährdung kann sich aus Kombinationen von Zuständen (z. B. umgebungsbedingt und/oder betriebsbedingt) der Maschine ergeben.

Tabelle 2 — Exposition gegenüber dem gefährlichen Vorfall

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

6.3.6 Beurteilung einer möglichen Schadensvermeidung

Zur Beurteilung einer möglichen Schadensvermeidung muss eingeschätzt werden, ob ein Durchschnitts-Maschinenführer, möglichst geschult, eine entstehende gefährliche Situation beherrscht und sie vermeiden kann, oder ob die Situation völlig unbeherrschbar ist. Sogar der Umstehende kann eine gefährliche Situation für sich selbst vermeiden. Auch hier wurden vier Kategorien gebildet, mittels derer die Vermeidung eines Schadens bewertet werden kann. Es ist zu beachten, dass die Beurteilung einer möglichen Schadensvermeidung nur die Funktion *ohne* zusätzliche Schutzmaßnahmen annimmt (Schadensvermeidung über das technische System hinaus). Die verwendeten Kategorien C0, C1, C2 und C3 stehen für eine Klassifizierung in „leicht beherrschbar“, „beherrschbar“, „im Allgemeinen beherrschbar“ und „nicht beherrschbar“ (siehe Tabelle 3).

Tabelle 3 — Mögliche Schadensvermeidung

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

6.3.7 Herleitung des geforderten Performance Levels $AgPL_r$

Wie in Bild 1 dargestellt, wird der geforderte Performance Level $AgPL_r$ durch Kombinieren der verschiedenen Werte für Schwere, Aufenthaltsdauer und Beherrschbarkeit für jede identifizierte Gefährdung abgeleitet.

Die geforderten Performance Levels $AgPL_r$ werden mit $AgPL = a$ bis $AgPL = e$ bezeichnet. $AgPL = a$ bezeichnet den niedrigsten und $AgPL = e$ den höchsten Level der Systemanforderungen. Neben diesen Levels gibt es die Bezeichnung QM (Qualitätssicherungsmaßnahme), deren implizite Forderung in der Durchführung der Entwicklung der entsprechenden Systemfunktionen nach den zugrundeliegenden Normen wie ISO 9001 besteht. Jedoch muss das zusammenhängende Risiko hinreichend gering sein, damit eine als QM klassifizierte Funktion explizit nicht in die Kategorie der sicherheitsbezogenen Funktion einbezogen wird.

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

Legende

S	Schwere
E	Exposition gegenüber dem gefährlichen Vorfall
C	Beherrschbarkeit
QM	Qualitätssicherungsmaßnahmen
a, b, c, d, e	geforderter landwirtschaftlicher Performance Level ($AgPL_r$)

Bild 1 — Ermittlung des $AgPL_r$

ANMERKUNG QM ist zur besseren Übersicht dargestellt. Siehe 6.3.7.