

DIN EN 16590-3

ICS 35.240.99; 65.060.01

Ersatz für
DIN EN 16590-3:2014-11

**Traktoren und Maschinen für die Land- und Forstwirtschaft –
Sicherheitsbezogene Teile von Steuerungen –
Teil 3: Serienentwicklung, Hardware, Software (ISO 25119-3:2010
modifiziert);
Deutsche Fassung EN 16590-3:2014**

Tractors and machinery for agriculture and forestry –
Safety-related parts of control systems –
Part 3: Series development, hardware and software (ISO 25119-3:2010 modified);
German version EN 16590-3:2014

Tracteurs et matériels agricoles et forestiers –
Parties des systèmes de commande relatives à la sécurité –
Partie 3: Développement en série, matériels et logiciels (ISO 25119-3:2010 modifié);
Version allemande EN 16590-3:2014

Gesamtumfang 67 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 16590-3:2014.

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.

Änderungen

Gegenüber DIN EN 16590-3:2014-11 wurden folgende Korrekturen vorgenommen:

- a) Unterabschnitt 5.2: Bild 1 wurde modifiziert, d. h. angepasst an die englische Referenzfassung;
- b) Unterabschnitt 7.5.4.1: In Tabelle 4 wurde der Wert in Zeile 3.1 der letzten Spalte, sowie in Zeile 4.4 der Wert in der vorletzten Spalte korrigiert;
- c) Unterabschnitt B.2.24: Die ANMERKUNG wurde entfernt.

Frühere Ausgaben

DIN EN 16590-3: 2014-11

Deutsche Fassung

Traktoren und Maschinen für die Land- und Forstwirtschaft —
Sicherheitsbezogene Teile von Steuerungen —
Teil 3: Serienentwicklung, Hardware, Software
(ISO 25119-3:2010 modifiziert)

Tractors and machinery for agriculture and forestry —
Safety-related parts of control systems —
Part 3: Series development, hardware and software
(ISO 25119-3:2010 modified)

Tracteurs et matériels agricoles et forestiers —
Parties des systèmes de commande relatives
à la sécurité —
Partie 3: Développement en série, matériels et logiciels
(ISO 25119-3:2010 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 Systementwurf	8
5.1 Ziele	8
5.2 Allgemeines	8
5.3 Voraussetzungen	9
5.4 Anforderungen	9
5.4.1 Gliederung der Sicherheitsanforderungen	9
5.4.2 Funktionales Sicherheitskonzept.....	10
5.4.3 Technisches Sicherheitskonzept.....	11
6 Hardware.....	13
6.1 Ziele	13
6.2 Allgemeines	13
6.3 Voraussetzungen	14
6.4 Anforderungen	14
6.5 Hardware-Kategorien	15
6.6 Arbeitsprodukte	16
7 Software	16
7.1 Software-Entwicklungsplanung	16
7.1.1 Ziele	16
7.1.2 Allgemeines	16
7.1.3 Voraussetzungen	16
7.1.4 Anforderungen	17
7.1.5 Arbeitsprodukte	19
7.2 Spezifikation der Sicherheitsanforderungen an die Software	19
7.2.1 Ziele	19
7.2.2 Allgemeines	19
7.2.3 Voraussetzungen	20
7.2.4 Anforderungen	20
7.2.5 Arbeitsprodukte	23
7.3 Software-Architektur und -entwurf	23
7.3.1 Ziele	23
7.3.2 Allgemeines	23
7.3.3 Voraussetzungen	23
7.3.4 Anforderungen	24
7.3.5 Arbeitsprodukte	26
7.4 Entwurf und Implementierung von Softwaremodulen	26
7.4.1 Ziele	26
7.4.2 Allgemeines	26
7.4.3 Voraussetzungen	26
7.4.4 Anforderungen	26
7.4.5 Arbeitsprodukte	35
7.5 Testen von Softwaremodulen.....	35
7.5.1 Ziele	35
7.5.2 Allgemeines	35
7.5.3 Voraussetzungen	36

7.5.4	Anforderungen.....	36
7.5.5	Arbeitsprodukte.....	44
7.6	Software Integrationstest	44
7.6.1	Ziele.....	44
7.6.2	Allgemeines	44
7.6.3	Voraussetzungen.....	44
7.6.4	Anforderungen.....	45
7.6.5	Arbeitsprodukte.....	47
7.7	Software-Sicherheitsvalidierung	47
7.7.1	Ziele.....	47
7.7.2	Allgemeines	47
7.7.3	Voraussetzungen.....	47
7.7.4	Anforderungen.....	48
7.7.5	Arbeitsprodukte.....	49
7.8	Softwarebasierte Parametrierung.....	49
7.8.1	Ziel.....	49
7.8.2	Allgemeines	50
7.8.3	Voraussetzungen.....	50
7.8.4	Anforderungen.....	50
7.8.5	Arbeitsprodukte.....	51
Anhang A (informativ) Beispiel einer Agenda für die Beurteilung der funktionalen Sicherheit bei		
	AgPL = e	52
A.1	Funktionen des Systems	52
A.2	Hardware	52
A.3	Sicherheitskonzept.....	52
A.4	Sicherheitsanalyse und Sicherheitsdaten	52
A.5	Sicherheitsentwurfsprozess für die Phasen des Lebenszyklus.....	53
A.6	Softwareentwicklung.....	53
A.7	Verifizierung und Tests.....	53
A.8	Dokumentation und Sicherheitsdokumentation	53
A.9	Zusammenfassung und Beurteilung	53
Anhang B (informativ) Unabhängigkeit durch Softwarepartitionierung.....		
B.1	Allgemeines	54
B.2	Begriffe und Abkürzungen	54
B.3	Ziele.....	58
B.4	Allgemeines	58
B.5	Anforderungen.....	58
B.5.1	Allgemeine Anforderungen	58
B.5.2	Mehrere Partitionen in einem einzelnen Mikrocontroller	59
B.5.3	Mehrere Partitionen im Rahmen eines Mikrocontroller-Netzwerks	61
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den		
grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG		64
Literaturhinweise		65

Vorwort

Dieses Dokument (EN 16590-3:2014) 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 25119-3:2010 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 (Stromschlag, Brand, Nennleistung von E/E/PES, die der aktiven und passiven Sicherheit dienen, usw.).

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 separat von der oder in die Steuerung integriert 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 enthält allgemeine Gestaltungsleitsätze für Serienentwicklung, Hardware und Software 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 von SRP/CS-Systemen, die zur Ausführung sicherheitsrelevanter Funktionen 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 16590-2:2014, *Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Konzeptphase*

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 Begriffe nach EN 16590-1:2014.

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	rechnergestützter Entwurf (en: computer-aided-design)
Cat	Hardware-Kategorie (en: hardware category)
CCF	Ausfall 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 (en: electrical/electronic/programmable electronic systems)
EMV	elektromagnetische Verträglichkeit (en: EMC, electromagnetic compatibility)
EPROM	löschrbarer, 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)
UML	vereinheitlichte Modellierungssprache (en: Unified Modeling Language)

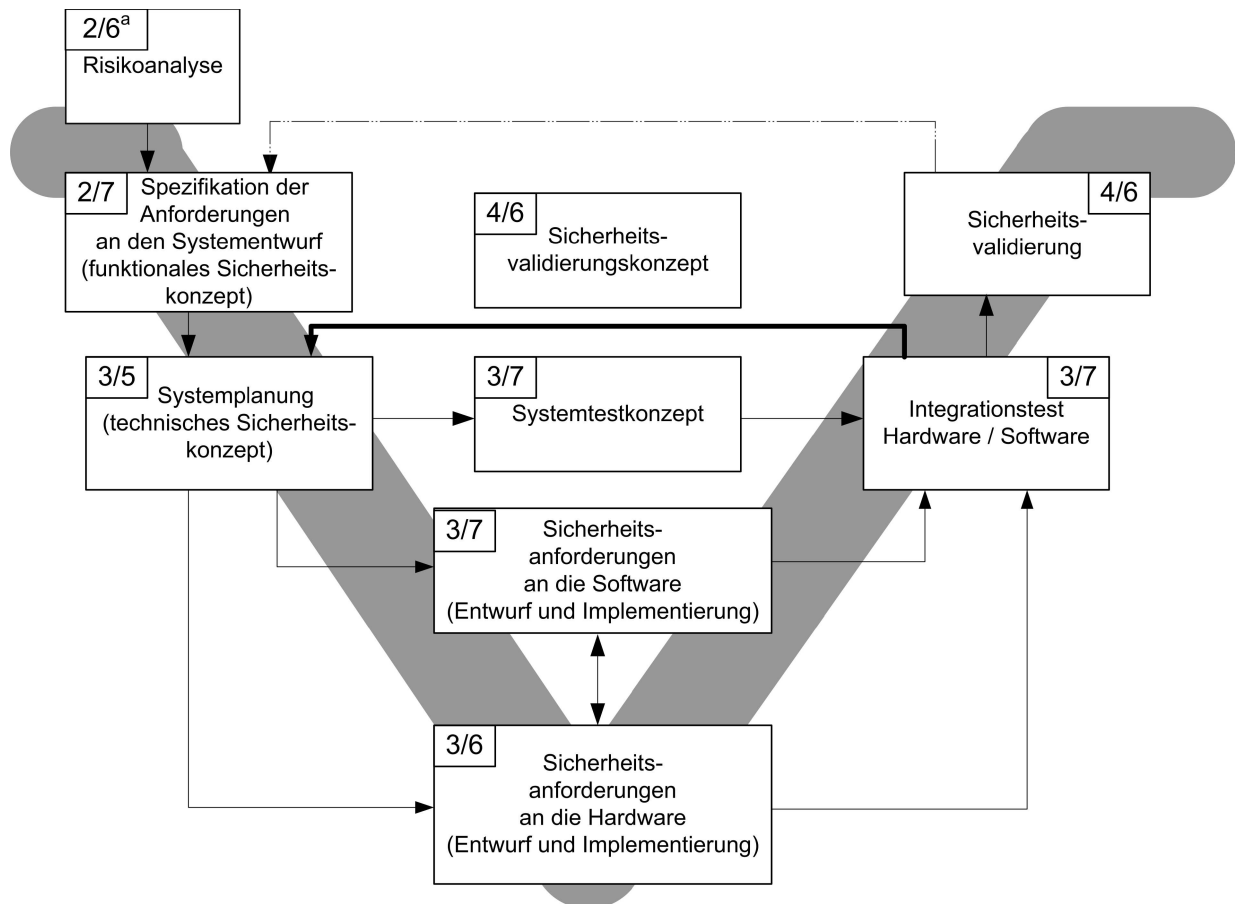
5 Systementwurf

5.1 Ziele

Ziel ist die Definition eines Entwicklungsprozesses 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 spezifiziert. Die verschiedenen Ebenen der Sicherheitsanforderungen sind in Bild 1 dargestellt. Für eine Gesamtdarstellung des Verfahrens zur Entwicklung der Sicherheitsanforderungen siehe auch 5.4 dieser Norm. Zur Unterstützung des Managements der Sicherheitsanforderungen wird die Anwendung geeigneter Werkzeuge für das Anforderungs-Management empfohlen.



Legende

- Folge
- ← Bestätigung
- ←... Validierung

^a Die erste der beiden durch einen Schrägstrich getrennten Ziffern verweist auf den entsprechenden Teil der EN 16590, die zweite Ziffer bezeichnet den Abschnitt im Normenteil: 2/6 bedeutet EN 16590-2:2014/Abschnitt 6, 3/5 bedeutet EN 16590-3:2014/Abschnitt 5, usw.

Bild 1 — Gliederung der Sicherheitsanforderungen

5.3 Voraussetzungen

Vor dem Beginn, das System zu entwerfen, müssen zuerst die Anforderungen an die Funktion des Sicherheitssystems, an die Anwendung und an die Betriebsumgebung definiert sein.

5.4 Anforderungen

5.4.1 Gliederung der Sicherheitsanforderungen

Das funktionale Sicherheitskonzept spezifiziert das grundlegende Funktionieren des Sicherheitssystems, mit dem die Sicherheitsziele erfüllt werden müssen. Die Grundzuordnung der funktionalen Sicherheitsanforderungen zur Systemarchitektur wird vom technischen Sicherheitskonzept in Form technischer Sicherheitsanforderungen spezifiziert. Diese Systemarchitektur umfasst Hardware und Software.

Die Sicherheitsanforderungen an die Hardware verfeinern und konsolidieren die Anforderungen des technischen Sicherheitskonzepts. Abschnitt 6 beschreibt, wie die Hardware-Anforderungen im Einzelnen zu spezifizieren sind.

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

Dieser Abschnitt enthält Richtlinien für den bei der Spezifizierung der Anforderungen des Sicherheitskonzepts während des Systementwurfs anzuwendenden Ansatz. Diese Verfahrensrichtlinien liefern eine Grundlage für einen fehlerfreien Systementwurf.

5.4.2 Funktionales Sicherheitskonzept

5.4.2.1 Allgemeine Anforderungen des funktionalen Sicherheitskonzepts

Sicherheitsfunktionen werden in der Regel während der System-Risikoanalyse identifiziert. Das Dokument des funktionalen Sicherheitskonzepts enthält die funktionalen Sicherheitsanforderungen an das System.

Bei der Umsetzung jeder Anforderung des Sicherheitskonzepts muss Folgendes beachtet werden.

— Durchführbarkeit

Bei der Auflistung der funktionalen Sicherheitsanforderungen muss auf die Durchführbarkeit hinsichtlich der Umgebungseinschränkungen, wie z. B. vorhandene Technik sowie finanzielle und zeitliche Ressourcen, geachtet werden. Die für die Umsetzung Zuständigen müssen die technischen Sicherheitsanforderungen verstehen und akzeptieren.

— Eindeutigkeit

Die funktionalen Sicherheitsanforderungen müssen so genau und eindeutig wie möglich formuliert werden.

ANMERKUNG Eine funktionale Sicherheitsanforderung ist eindeutig formuliert, wenn sie nur eine Interpretation durch den erwarteten Leser zulässt.

— Widerspruchsfreiheit

Funktionale Sicherheitsanforderungen dürfen sich weder selbst (interne Widerspruchsfreiheit) noch anderen Anforderungen widersprechen (externe Widerspruchsfreiheit).

Analysen der Anforderungen und Vergleiche zwischen verschiedenen Anforderungen sind notwendig, um die externe Widerspruchsfreiheit zu gewährleisten. Dies ist eine Aufgabe des Anforderungsmanagements.

— Vollständigkeit

Das funktionale Sicherheitskonzept muss alle einschlägigen Normen, Standards und gesetzlichen Vorschriften berücksichtigen.

Das funktionale Sicherheitskonzept muss alle entsprechenden, aus der Risikoanalyse nach EN 16590-2 resultierenden Sicherheitsanforderungen berücksichtigen.

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

- 1) müssen die Version des funktionalen Sicherheitskonzepts und die Version der entsprechenden zugrunde liegenden Quellen angegeben werden;
- 2) müssen die Anforderungen aus dem Änderungsmanagement (siehe EN 16590-4:2014, Abschnitt 10) erfüllt werden; daher müssen die funktionalen Sicherheitsanforderungen so aufgegliedert und formuliert werden, dass ein Änderungsprozess unterstützt wird;
- 3) müssen die funktionalen Sicherheitsanforderungen einem Review unterzogen werden (siehe EN 16590-4:2014, Abschnitt 6).

Beim funktionalen Sicherheitskonzept müssen alle Phasen des Lebenszyklus (einschließlich Produktion, Betrieb durch den Kunden, Kundendienst und Außerbetriebnahme) betrachtet werden.

5.4.2.2 Spezifikation des funktionalen Sicherheitskonzepts

Dieser Abschnitt enthält Angaben, die im funktionalen Sicherheitskonzept zu machen sind. Die funktionalen Sicherheitskonzepte können von den während einer Risikoanalyse ausgewerteten Maschinenausfallszenarios abgeleitet werden.

Jede Beschreibung eines Ausfallszenarios muss Folgendes enthalten:

- Umgebungsbedingungen (Fahren auf einer vereisten Straße, bergauf, bergab, Wetter, usw.);
- Maschinenbedingungen (Motor läuft, Gang eingelegt, Stillstand, usw.);
- der daraus resultierende AgPL;
- Beschreibungen des sicheren Zustands (Motorabschaltung, Ventil aus, Getriebe in Parkstellung, Funktionserhalt bei reduzierter Leistung, usw.).

5.4.3 Technisches Sicherheitskonzept

5.4.3.1 Allgemeine Anforderungen des technischen Sicherheitskonzepts

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

Jedem technischen Sicherheitskonzept müssen (z. B. durch Querverweis) übergeordnete Sicherheitsanforderungen zugeordnet werden. Übergeordnete Sicherheitsanforderungen können sein:

- andere technische Sicherheitsanforderungen;
- funktionale Sicherheitsanforderungen; oder
- Sicherheitsziele.

ANMERKUNG 1 Die Rückverfolgbarkeit kann durch Nutzung geeigneter Anforderungsmanagement-Werkzeuge sehr erleichtert werden.

Genau wie beim *funktionalen* Sicherheitskonzept muss bei der Umsetzung jeder Anforderung des technischen Sicherheitskonzepts auf dessen Durchführbarkeit, Eindeutigkeit, Widerspruchsfreiheit und Vollständigkeit geachtet werden.

— **Durchführbarkeit**

Bei der Auflistung der technischen Sicherheitsanforderungen muss auf die Durchführbarkeit hinsichtlich der Umgebungseinschränkungen, wie z. B. vorhandene Technik sowie finanzielle und zeitliche Ressourcen, geachtet werden. Die für die Umsetzung Zuständigen müssen die technischen Sicherheitsanforderungen verstehen und akzeptieren.

— **Eindeutigkeit**

Die technischen Sicherheitsanforderungen müssen so genau und eindeutig wie möglich formuliert werden.

ANMERKUNG 2 Eine technische Sicherheitsanforderung ist eindeutig formuliert, wenn sie nur eine Interpretation durch den erwarteten Leser zulässt.

— **Widerspruchsfreiheit**

Technische Sicherheitsanforderungen dürfen sich weder selbst (interne Widerspruchsfreiheit) noch anderen Anforderungen widersprechen (externe Widerspruchsfreiheit).

Analysen der Anforderungen und Vergleiche zwischen verschiedenen Anforderungen sind notwendig, um die externe Widerspruchsfreiheit sicherzustellen. Dies ist eine Aufgabe des Anforderungsmanagements.

— **Vollständigkeit**

Das technische Sicherheitskonzept muss folgende Quellen berücksichtigen:

- 1) alle Sicherheitsziele und funktionalen Sicherheitsanforderungen;
- 2) alle einschlägigen Normen, Standards und gesetzlichen Vorschriften;
- 3) die entsprechenden Ergebnisse von Sicherheitsanalyse-Werkzeugen (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:

- 4) müssen die Version des technischen Sicherheitskonzepts und die Version der entsprechenden zugrunde liegenden Quellen angegeben werden;
- 5) müssen die Anforderungen aus dem Änderungsmanagement (siehe EN 16590-4:2014, Abschnitt 10) erfüllt werden; daher müssen die technischen Sicherheitsanforderungen so aufgegliedert und formuliert werden, dass ein Änderungsprozess unterstützt wird;
- 6) müssen die technischen Sicherheitsanforderungen einem Review unterzogen werden (siehe EN 16590-4:2014, Abschnitt 6).

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

5.4.3.2 Spezifikation des technischen Sicherheitskonzepts

5.4.3.2.1 Allgemeines

Das technische Konzept muss Sicherheitsanforderungen an Hardware und Software enthalten, die für den Entwurf der Betrachtungseinheit ausreichend und von den in 5.4.3.1 enthaltenen Regeln bestimmt sind.

5.4.3.2.2 Zustände und Zeiten

Das Verhalten der Betrachtungseinheit und ihrer Module sowie deren Schnittstellen müssen für alle relevanten Betriebszustände spezifiziert werden, einschließlich

- Anlauf,
- Normalbetrieb,
- Abschaltung,
- Wiederanlauf nach einer Rückstellung, und
- vernünftigerweise vorhersehbare ungewöhnliche Betriebszustände (z. B. herabgesetzte Betriebszustände).

Insbesondere müssen das Ausfallverhalten und die erforderliche Reaktion darauf genau beschrieben werden. Zusätzliche Notbetriebsfunktionen können aufgenommen werden.

Das technische Sicherheitskonzept muss einen sicheren Zustand für jede funktionale Sicherheitsanforderung, den Übergang in den sicheren Zustand sowie die Aufrechterhaltung des sicheren Zustands spezifizieren. Insbesondere ist anzugeben, ob ein Ausschalten der Betrachtungseinheit direkt einen sicheren Zustand darstellt oder ob ein sicherer Zustand nur durch eine kontrollierte Abschaltung erreicht werden kann.

Im technischen Sicherheitskonzept muss für jede funktionale Sicherheitsanforderung die maximale Zeit zwischen dem Auftreten eines Fehlers und dem Erreichen eines sicheren Zustands (Fehlertoleranzzeit) angegeben werden. Alle daraus abgeleiteten Zeiten für Teilsysteme und Teilfunktionen müssen in den Anforderungen des Sicherheitskonzepts angegeben werden.

Kann durch eine direkte Abschaltung kein sicherer Zustand erreicht werden, muss die Zeit definiert werden, während der eine als Notbetrieb angegebene Sonderfunktion für alle Teilsysteme und Teilfunktionen aufrechterhalten werden muss (Notbetriebszeit). Diese als Notbetrieb angegebene Sonderfunktion muss in den Anforderungen des Sicherheitskonzepts dokumentiert werden.

5.4.3.2.3 Sicherheitsarchitektur, Schnittstellen und Randbedingungen

Die Sicherheitsarchitektur und ihre Teilmodule müssen beschrieben werden. Insbesondere müssen die technischen Maßnahmen angegeben werden. Im technischen Sicherheitskonzept müssen folgende Module (falls vorhanden) separat beschrieben werden:

- Sensorsystem, separat für jeden erfassten physischen Parameter;
- verschiedene digitale und analoge Ein- und Ausgabeeinheiten;
- Verarbeitung, separat für jedes Rechenwerk/jede diskrete Logikeinheit;
- Aktorsystem, separat für jeden Aktor;
- Anzeigen, separat für jede Anzeigeeinheit;
- verschiedene elektromechanische Bauteile;
- Signalübertragung zwischen den Modulen;
- Signalübertragung von/zu Systemen außerhalb der Betrachtungseinheit;
- Stromversorgung.

Die Schnittstellen zwischen den Modulen der Betrachtungseinheit, Schnittstellen zu anderen Systemen und Funktionen in der Maschine sowie Benutzerschnittstellen müssen angegeben werden.

Beschränkungen und Randbedingungen der Betrachtungseinheit müssen angegeben werden. Dies gilt insbesondere für Extremwerte aller Umgebungsbedingungen in allen Phasen des Lebenszyklus.

6 Hardware

6.1 Ziele

Ziel ist es, akzeptable Hardware-Architekturen für sicherheitsbezogene Steuerungen zu definieren.

6.2 Allgemeines

Die Verbesserung des Hardware-Aufbaus der sicherheitsbezogenen Teile einer Steuerung kann Maßnahmen zur Vermeidung, Erkennung oder Tolerierung von Fehlern liefern. Zu den praktischen Maßnahmen können Redundanz, Diversität und Überwachung zählen.

Im Allgemeinen müssen folgende Fehlerkriterien berücksichtigt werden.

- Wenn infolge eines Fehlers weitere Bauteile ausfallen, müssen der erste Fehler und all diese Folgefehler als Einzelfehler betrachtet werden.
- Zwei oder mehr separate Fehler mit gemeinsamer Ursache müssen als Einzelfehler betrachtet werden (dies ist als *Ausfall gemeinsamer Ursache* bekannt).
- Das gleichzeitige Auftreten zweier voneinander unabhängiger Fehler gilt als höchst unwahrscheinlich.

6.3 Voraussetzungen

Voraussetzung ist der für jede Sicherheitsfunktion, die von der Hardware zu realisieren ist, festgelegte AgPL_r.

6.4 Anforderungen

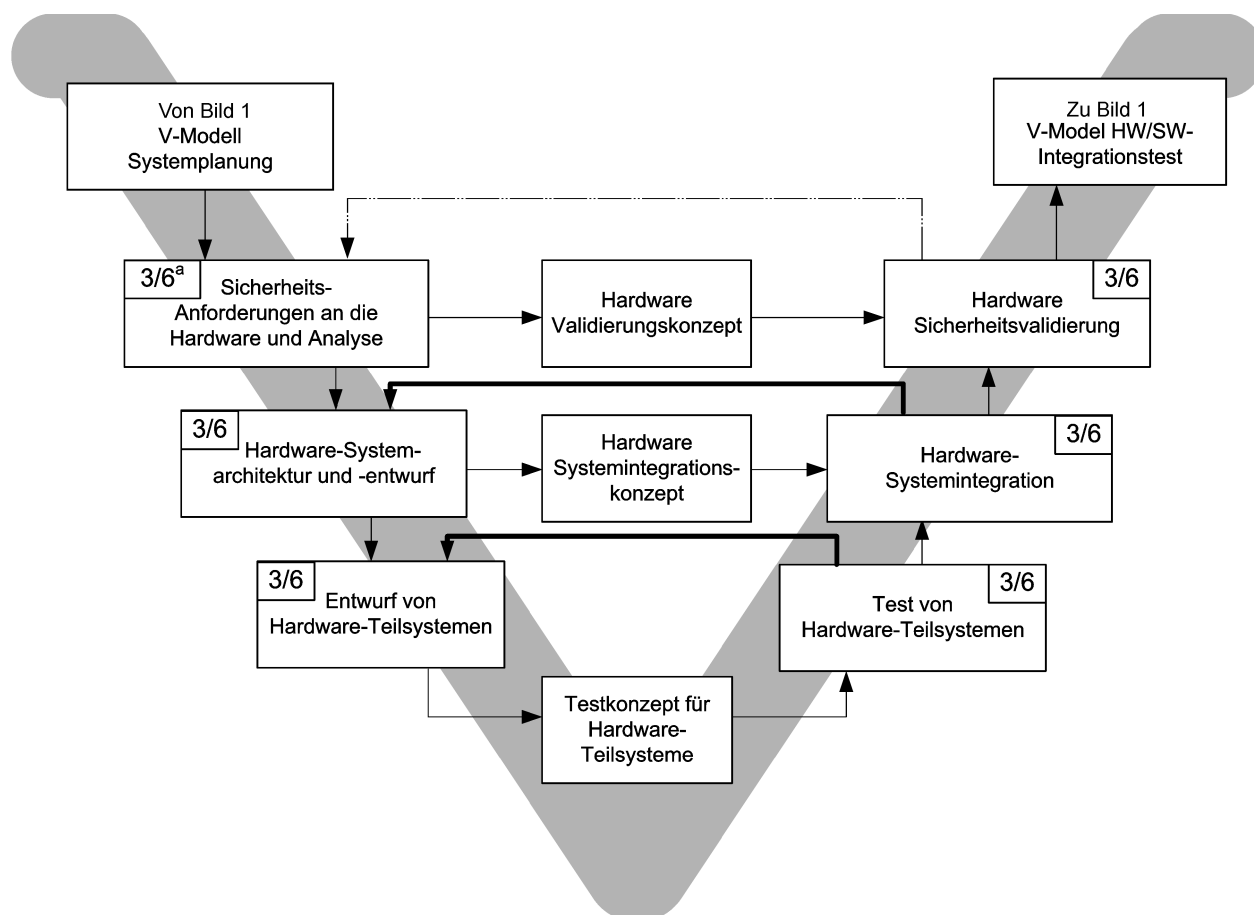
Der Hardware-Entwicklungsprozess beginnt auf der Systemebene, auf der die Sicherheitsfunktionen und zugehörigen Anforderungen identifiziert werden (siehe Bild 2).

Die Hardware-Sicherheitsanalyse muss für die Identifizierung des Performance Levels (AgPL_r) für jede Systemsicherheitsfunktion angewendet werden (siehe EN 16590-2).

Der Konstrukteur fasst Funktionen in entsprechenden Architekturen (Hardware-Kategorie) mit zugehörigem MTTF_{dc}, DC und CCF zusammen.

Das System kann in Teilsysteme zerlegt werden, um die Entwicklung zu vereinfachen.

Jede Phase des Entwicklungszyklus muss validiert werden.



Legende

- Folge
- ← Bestätigung
- ← Validierung

a Die erste der beiden, durch einen Schrägstrich getrennten Ziffern verweist auf diesen Teil der EN 16590, die zweite Ziffer bezeichnet den Abschnitt 6.

Bild 2 — V-Modell für die Hardware-Entwicklung

Die Vorgehensweise für den Entwurf der Hardware-Systemarchitektur umfasst die folgenden Schritte:

- Wahl der Hardware-Kategorie (siehe EN 16590-2:2014, Anhang A);
- Identifizierung der Betriebsumgebung und der Beanspruchungshöhe von Bauteilen;
- Auswahl der Bauteile;
- Berechnung und Verifizierung, ob die $MTTF_{dC}$ dem geforderten Level entspricht (siehe EN 16590-2:2014, Anhang B);
- Bestimmung und Verifizierung, ob der DC dem geforderten Level entspricht (siehe EN 16590-2:2014, Anhang C);
- Betrachtung von CCF (siehe EN 16590-2:2014, Anhang D);
- Betrachtung der systematischen Ausfälle (siehe EN 16590-2:2014, Anhang E);
- Betrachtung anderer Sicherheitsfunktionen (siehe EN 16590-2:2014, Anhang F).

ANMERKUNG Für die vorstehenden Schritte ist eventuell eine Iteration erforderlich.

6.5 Hardware-Kategorien

Die sicherheitsbezogenen Teile von Steuerungen müssen den Anforderungen einer oder mehrerer der fünf in EN 16590-2:2014, Anhang A, beschriebenen Kategorien entsprechen.

Wird eine Sicherheitsfunktion durch eine integrierte Kombination aus mehreren Hardware-Kategorien realisiert, so ist die Sicherheitsfunktion AgPL durch die Gesamtkategorie begrenzt: $MTTF_{dC}$, DC, SRL, CCF, usw. (siehe Bild 3).

Zur Bestimmung des Gesamt-SRL siehe 7.3.4.7.

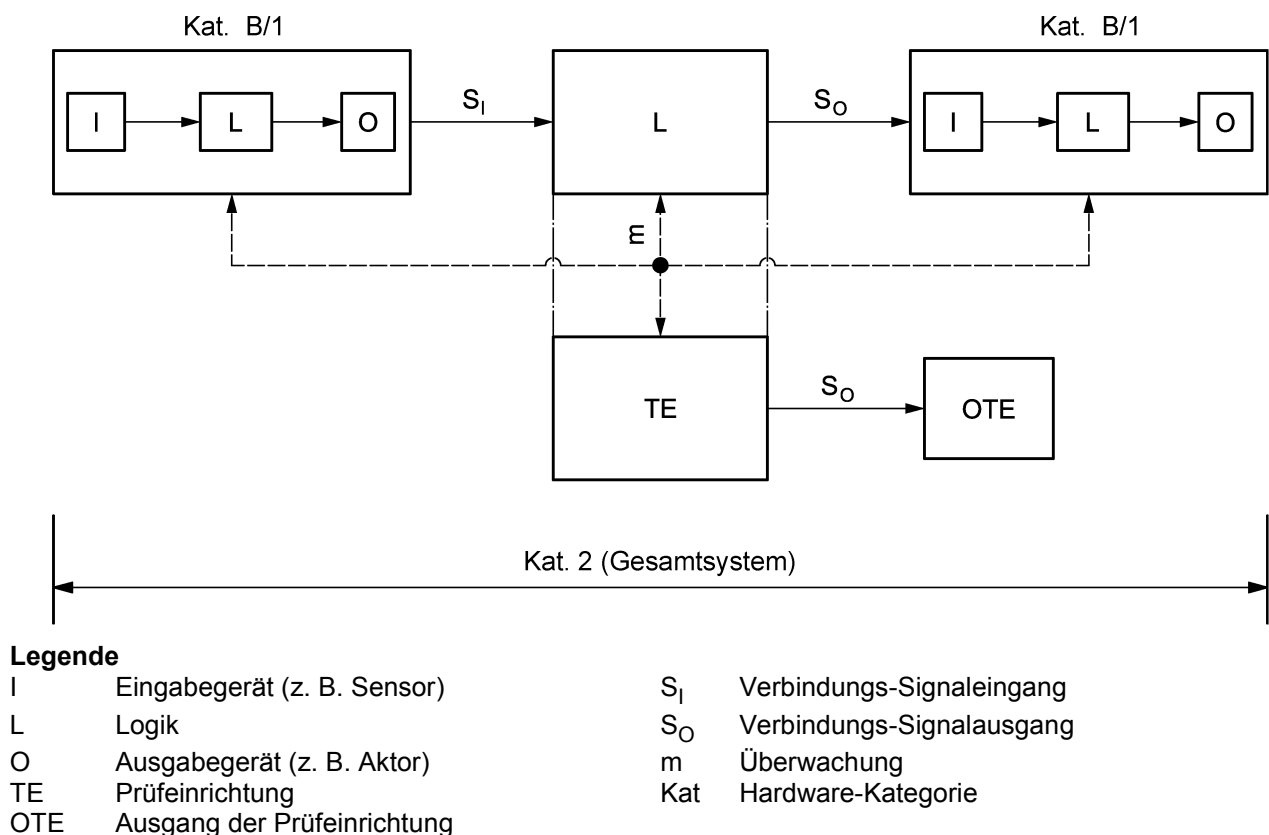


Bild 3 — Integriertes System mit maximalem AgPL für Kategorie 2

6.6 Arbeitsprodukte

Die folgenden Arbeitsprodukte sind auf die Hardwareentwicklung anwendbar:

- a) Testplan der Hardware-Sicherheitsvalidierung;
- b) Testspezifizierung der Hardware-Sicherheitsvalidierung;
- c) Testergebnisse der Hardware-Sicherheitsvalidierung;
- d) Hardware-Systemintegrations-Testplan/Hardware-Teilsysteme-Testplan;
- e) Testspezifikation der Hardware-Systemintegration;
- f) Hardware-Systemintegrations-Testergebnisse/Hardware-Teilsysteme-Testergebnisse.

7 Software

7.1 Software-Entwicklungsplanung

7.1.1 Ziele

Ziel ist es, die einzelnen Phasen der Softwareentwicklung festzulegen und zu planen. Dies umfasst den Prozess der Softwareentwicklung selbst, welche in diesem Abschnitt beschrieben ist, sowie die in EN 16590-4:2014, Abschnitt 10, beschriebenen notwendigen unterstützenden Verfahren.

7.1.2 Allgemeines

Bild 4 veranschaulicht den Prozess zur Entwicklung der Software. In den folgenden Absätzen und Tabellen wird jeder Kasten des Schemas näher erläutert.

Geeignete Methoden/Maßnahmen müssen entsprechend dem erforderlichen SRL gewählt werden. Angesichts der Vielzahl von Faktoren, welche die Sicherheitsintegrität der Software beeinflussen, kann kein Algorithmus für das Kombinieren der Methoden und Maßnahmen angegeben werden, welcher für jede mögliche Anwendung richtig ist. Für eine bestimmte Anwendung ist die passende Kombination von Methoden oder Maßnahmen im Laufe der Sicherheitsplanung anzugeben, wobei geeignete Methoden oder Maßnahmen entsprechend den Anforderungen von 7.1.4 auszuwählen sind.

7.1.3 Voraussetzungen

Die Voraussetzungen in dieser Phase sind

- der auf Basis des ermittelten $AgPL_r$ geforderte SRL für jede umzusetzende Sicherheitsfunktion;
- der Projektplan (einschließlich des Systementwicklungsplans);
- der Systemverifizierungsplan;
- das technische Sicherheitskonzept;
- die Spezifikation des Systementwurfs; und
- der Sicherheitsplan.

7.1.4 Anforderungen

7.1.4.1 Bestimmung der Phasen

Für den Software-Entwicklungsprozess muss festgelegt werden, welche Phasen der Software-Entwicklung (siehe Bild 4) in welcher Reihenfolge auszuführen sind. Umfang und Komplexität des Projekts müssen berücksichtigt werden. Die Phasen können ohne Modifikation entsprechend Bild 4 ausgeführt werden. Es können jedoch auch einzelne Phasen miteinander kombiniert werden, sobald alle Arbeitsprodukte der kombinierten Phasen generiert sind.

ANMERKUNG Es ist sinnvoll, einzelne Phasen miteinander zu kombinieren, wenn die angewendete Methode eine eindeutige Unterscheidung zwischen den einzelnen Phasen schwierig macht. So können beispielsweise der Entwurf der Software-Architektur und die Software-Implementierung nacheinander mit demselben rechnergestützten Entwicklungswerkzeug generiert werden, wie dies im modellbasierten Entwicklungsprozess der Fall ist.

Andere Phasen können durch Verteilung der Aktivitäten und Aufgaben hinzugefügt werden.

BEISPIEL Die Anwendung der Daten kann als separate Phase vor der Sicherheitsvalidierung des elektronischen Steuergeräts eingefügt werden. Die Sicherheitsvalidierung des elektronischen Steuergeräts kann je nach Verteilung der Funktionen unterschiedlich — als Prüfung bestimmter elektronischer Steuergeräte oder als Prüfung des kombinierten Steuerungsnetzwerks — durchgeführt werden. So könnte sie am Prüfort der Bauteilsysteme oder im Laborfahrzeug durchgeführt werden.

7.1.4.2 Prozessflexibilität

Die Aktivitäten und Aufgaben können von einer Phase zu einer anderen verlagert werden.

7.1.4.3 Prozesszeitplan

Es muss ein Zeitplan erstellt werden, welcher die Beziehung zwischen den einzelnen Phasen der Software-Entwicklung und dem Produkt-Entwicklungsprozess einschließlich der Integrationsschritte auf Maschinenebene aufzeigt.

7.1.4.4 Anwendbarkeit

Nachdem die Sicherheitsanforderungen an die Software nach Tabelle 1 vollständig spezifiziert wurden, muss festgelegt werden, welche Sicherheitsanforderungen an die Software auf welche Integrationsschritte anzuwenden sind.

7.1.4.5 Unterstützende Verfahren

Unterstützende Verfahren müssen als Teil des Software-Entwicklungsprozesses geplant und implementiert werden:

- a) die Arbeitsprodukte müssen nach EN 16590-4:2014, Abschnitt 12, dokumentiert werden;
- b) Änderungen an der Software müssen nach EN 16590-4:2014, Abschnitt 10, behandelt werden;
- c) die Arbeitsprodukte müssen dem Konfigurations-Managementprozess unterzogen werden.

ANMERKUNG Das unterstützende Verfahren von vorstehend b) umfasst auch eine Strategie zur Behandlung der verschiedenen Verzweigungen der Software, welche sich aus Änderungen ergeben, einschließlich der Zusammenführung dieser Verzweigungen.

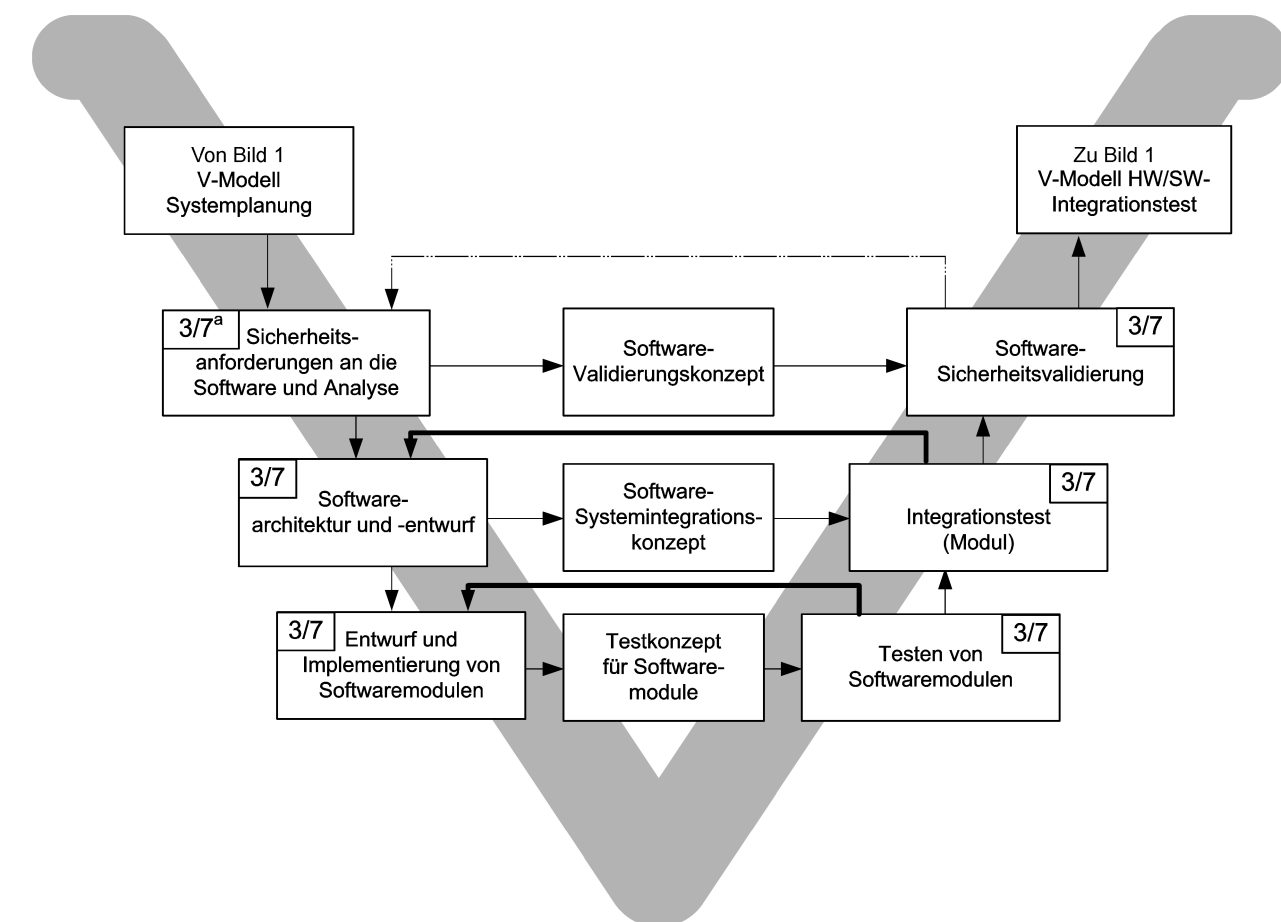
7.1.4.6 Phasen der Software-Entwicklung

Für jede Phase der Software-Entwicklung müssen die geeigneten Methoden und Maßnahmen, die entsprechenden Werkzeuge und die Richtlinien für die Umsetzung der Methoden, Maßnahmen und Werkzeuge je nach Sicherheitsintegritätsniveau (SRL) ausgewählt werden.

Diese Auswahl muss hinsichtlich ihrer Eignung für das Anwendungsgebiet begründet werden, und sie muss zu Beginn jeder Entwicklungsphase durchgeführt werden.

Bei der Auswahl der Methoden und Maßnahmen muss daran gedacht werden, dass neben der manuellen Codierung eine modellbasierte Entwicklung durchgeführt werden kann, bei der der Quellcode oder der Objektcode automatisch aus Modellen generiert wird.

ANMERKUNG Die Auswahl abgestimmter Methoden und Maßnahmen bietet die Möglichkeit, die Komplexität der Software-Entwicklung zu verringern.



Legende

- Folge
- ← Bestätigung
- ← Validierung

^a Die erste der beiden, durch einen Schrägstrich getrennten Ziffern verweist auf diesen Teil der EN 16590, die zweite Ziffer bezeichnet den Abschnitt 7.

Bild 4 — V-Modell für die Software-Entwicklung

7.1.4.7 Anwendung der Tabellen

Für jede Methode und Maßnahme der Softwareentwicklung enthalten die Tabellen 1 bis 6 eine Eintragung für jeden der vier SRL unter Verwendung der Symbole „+“ oder „o“.

- + Die Methode oder Maßnahme muss für diesen SRL verwendet werden. Wird diese Methode oder Maßnahme nicht verwendet, so muss der Grund dafür während der Planungsphase dokumentiert werden.
- o Es gibt keine Empfehlung zugunsten der oder gegen die Anwendung dieser Methode oder Maßnahme für diesen SRL.

In einer Tabelle kann rechts von „+“ ein „o“ erscheinen. In diesem Fall ist für den gleichen SRL eine striktere Maßnahme oder Methode verfügbar.

Es müssen die dem jeweiligen SRL entsprechenden Methoden und Maßnahmen gewählt werden. Alternative oder gleichwertige Methoden und Maßnahmen sind durch Buchstaben nach der Zahl gekennzeichnet. Es muss mindestens eine der alternativen oder gleichwertigen Methoden und Maßnahmen gewählt werden, die mit einem „+“ gekennzeichnet ist.

Ist eine spezielle Methode oder Maßnahme nicht in den Tabellen aufgeführt, so ist nicht anzunehmen, dass sie nicht berücksichtigt werden darf. Wird eine nicht aufgeführte Methode oder Maßnahme durch eine andere ersetzt, so muss diese eine gleiche oder höhere Wertigkeit haben.

7.1.5 Arbeitsprodukte

Das auf diese Phase anwendbare Arbeitsprodukt ist der Software-Projektplan entsprechend den Anforderungen in 7.1.4.2 bis 7.1.4.4 (siehe auch EN 16590-4:2014, Abschnitt 6).

7.2 Spezifikation der Sicherheitsanforderungen an die Software

7.2.1 Ziele

Das erste Ziel besteht in der Herleitung der Sicherheitsanforderungen an die Software einschließlich SRL aus den technischen Sicherheitsanforderungen.

Das zweite Ziel besteht in der Verifizierung, dass die Sicherheitsanforderungen an die Software dem technischen Sicherheitskonzept entsprechen.

7.2.2 Allgemeines

Die Spezifikation der Sicherheitsanforderungen an die Software muss von den Anforderungen des technischen Sicherheitskonzepts für das System abgeleitet und als Software-Sicherheitsanforderungen gekennzeichnet werden. Mindestens folgende Punkte müssen berücksichtigt werden:

- a) ausreichende Implementierung des technischen Sicherheitskonzepts in der Software;
- b) Systemkonfiguration und -architektur;
- c) Entwurf der Hardware des E/E/PES-Systems;
- d) Ansprechzeiten der Sicherheitsfunktionen;
- e) externe Schnittstellen, wie z. B. Kommunikationsschnittstellen;
- f) physische Anforderungen und Umgebungsbedingungen, soweit sie die Software beeinflussen;
- g) Anforderungen an eine sichere Software-Modifikation.

ANMERKUNG Hierbei wird berücksichtigt, dass zwischen der Hardware-Entwicklung des Systems und der Software-Entwicklung Iterationen vorhanden sind. Während des Prozesses der weiteren Spezifizierung und Detaillierung der Sicherheitsanforderungen an die Software und der Software-Architektur kann es zu Rückwirkungen auf die Hardware-Architektur kommen. Daher ist eine enge Zusammenarbeit zwischen der Hardware-Entwicklung und der Software-Entwicklung notwendig.