OVE EN 50657

Ausgabe: 2017-12-01

Bahnanwendungen – Anwendungen für Schienenfahrzeuge – Software auf Schienenfahrzeugen

Railways Applications –
Rolling stock applications – Software on Board Rolling Stock

Applications ferroviaires –
Applications du matériel roulant – Logiciels embarqués

Medieninhaber und Hersteller:
OVE Österreichischer Verband für Elektrotechnik

OVE Österreichischer Verband für Elektrotechnik
Eschenbachgasse 9, 1010 Wien
E-Mail: verkauf@ove.at
Internet: http://www.ove.at
Webshop: www.ove.at/webshop
Tel.: +43 1 587 63 73
Fax: +43 1 587 63 73-99

ICS 35.080, 35.240.60

Ident (IDT) mit EN 50657:2017

zuständig OVE/TK TM
Traktion und Motorik

Nationales Vorwort

Diese Europäische Norm EN 50657:2017 hat den Status einer nationalen elektrotechnischen Norm gemäß ETG 1992. Bei ihrer Anwendung ist dieses Nationale Vorwort zu berücksichtigen.

Für den Fall einer undatierten normativen Verweisung (Verweisung auf einen Standard ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste Ausgabe dieses Standards.
Für den Fall einer datierten normativen Verweisung bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Standards.

Der Rechtsstatus dieser nationalen elektrotechnischen Norm ist den jeweils geltenden Verordnungen zum Elektrotechnikgesetz zu entnehmen.

Bei mittels Verordnungen zum Elektrotechnikgesetz verbindlich erklärten rein österreichischen elektrotechnischen Normen ist zu beachten:

- Hinweise auf Veröffentlichungen beziehen sich, sofern nicht anders angegeben, auf den Stand zum Zeitpunkt der Herausgabe dieser rein österreichischen elektrotechnischen Norm. Zum Zeitpunkt der Anwendung dieser rein österreichischen elektrotechnischen Norm ist der durch die Verordnungen zum Elektrotechnikgesetz oder gegebenenfalls auf andere Weise festgelegte aktuelle Stand zu berücksichtigen.
- Informative Anhänge und Fußnoten sowie normative Verweise und Hinweise auf Fundstellen in anderen, nicht verbindlichen Texten werden von der Verbindlicherklärung nicht erfasst.

Europäische Normen (EN) von CENELEC werden gemäß den CENELEC-Regeln durch Veröffentlichung eines identen Titels und Textes in das Gesamtwerk der nationalen elektrotechnischen Normen übernommen, wobei der Nummerierung der Zusatz OVE vorangestellt wird.

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 50657

August 2017

ICS 35.080; 35.240.60

Deutsche Fassung

Bahnanwendungen – Anwendungen für Schienenfahrzeuge – Software auf Schienenfahrzeugen

Railways Applications –
Rolling stock applications –
Software on Board Rolling Stock

Applications ferroviaires –
Applications du matériel roulant –
Logiciels embarqués

Diese Europäische Norm wurde von CENELEC am 2017-05-08 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

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

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees 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, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

Ref. Nr. EN 50657:2017 D

EN 50657:2017

Inhalt

Seite

EN 50657:2017

Seite

Seite

Bilder

Tabellen

Seite

Europäisches Vorwort

Dieses Dokument (EN 50657:2017) wurde vom CLC/SC 9XB „Elektrische, elektronische und elektromechanische Einrichtungen auf Schienenfahrzeugen einschließlich Software“ ausgearbeitet.

Nachstehende Daten wurden festgelegt:

– spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2018-05-08

– spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-05-08

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] 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 CENELEC erteilt haben, und unterstützt grundlegende Anforderungen von EU-Richtlinien.

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

Dieses Dokument adaptiert EN 50128:2011 (ausgearbeitet vom CENELEC-Unterkomitee SC9XA „Kommunikations-, Signal- und Verarbeitungssysteme“) für die Anwendung im Bereich von Schienenfahrzeugen. Es verwendet die gleiche Gliederung und Abschnittsnummerierung wie EN 50128:2011. Falls Anforderungen von EN 50128:2011 nicht auf Schienenfahrzeuge zutreffen, ist der entsprechende Text durch „Absichtlich leer gelassen“ ersetzt worden.

Die wesentlichen Änderungen gegenüber EN 50128:2011 sind in Anhang E aufgeführt.

EN 50657:2017

Einleitung

Diese Europäische Norm steht in Verbindung mit der Normenreihe EN 50126 „Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)“ und sollte in Verbindung mit dieser Normenreihe gelesen werden.

Diese Europäische Norm konzentriert sich auf die anzuwendenden Verfahren, um Software zu erhalten, welche den Anspruch an die Software-Integrität erfüllt, der durch übergeordnete Betrachtungen an sie gestellt wird.

Diese Europäische Norm beschreibt eine Reihe von Anforderungen für die Entwicklung, Bereitstellung und Wartung von Software für Schienenfahrzeuganwendungen. Es werden Anforderungen hinsichtlich der Organisationsstruktur, der Beziehung zwischen Organisationen und der Aufteilung von Verantwortlichkeiten derjenigen festgelegt, die in Entwicklungs-, Bereitstellungs- und Wartungsmaßnahmen eingebunden sind. Gleichermaßen werden in dieser Europäischen Norm die Kriterien für die Qualifikation und für die Fachkenntnis des Personals angegeben.

Das Grundkonzept dieser Europäischen Norm basiert auf Software-Integritätsleveln. Diese Europäische Norm behandelt fünf Software-Integritätslevel, von denen die Basisintegrität (Basic Integrity) der niedrigste und 4 der höchste Level ist. Je größer das Risiko ist, das von einem Softwarefehler ausgeht, desto höher ist der Software-Integritätslevel.

ANMERKUNG 1 Der in dieser Europäischen Norm benutzte Begriff der „Basisintegrität“ (Basic Integrity) wurde erstmals in der Normenreihe EN 50126 eingeführt.

Diese Europäische Norm führt Techniken und Maßnahmen für fünf Software-Integritätslevel auf. Die geforderten Techniken und Maßnahmen für die Basisintegrität und die Sicherheits-Integritätslevel 1 bis 4 werden in den Tabellen im normativen Anhang A angegeben. In dieser Norm sind die geforderten Techniken für Level 1 dieselben wie die für Level 2 und die geforderten Techniken für Level 3 dieselben wie für Level 4. Diese Europäische Norm gibt keine Hinweise darauf, welcher Software-Integritätslevel für ein gegebenes Risiko angemessen ist. Diese Entscheidung hängt von vielen Faktoren ab, wie der Art der Anwendung, dem Ausmaß, in dem andere Systeme sicherheitsrelevante Funktionen übernehmen, und von sozialen und wirtschaftlichen Faktoren.

Es fällt in den Anwendungsbereich der Normenreihe EN 50126, die der Software zugewiesenen sicherheitsrelevanten Funktionen festzulegen.

Diese Europäische Norm beschreibt die Maßnahmen, die notwendig sind, um diese Anforderungen zu erfüllen.

Die Normenreihe EN 50126 fordert eine systematische Vorgehensweise zwecks:

a) Identifikation von Gefährdungen, Bewertung von Risiken und risikobasierte Entscheidungsfindung;

b) Identifikation der notwendigen Risikominderung, um die Risikoakzeptanzkriterien zu erfüllen;

c) Definition der übergreifenden System-Sicherheitsanforderungen für die Schutzmaßnahmen, die notwendig sind, um die erforderliche Risikominderung zu erreichen;

d) Auswahl einer passenden Systemarchitektur;

e) Planung, Überwachung und Steuerung der technischen Aktivitäten und der Managementaktivitäten, die erforderlich sind, um die System-Sicherheitsanforderungsspezifikation in ein sicherheitsrelevantes System mit einem validierten Sicherheits-Integritätslevel umzusetzen.

Mit der Aufteilung der Spezifikation in einen Entwurf sicherheitsrelevanter Systeme und Komponenten erfolgt eine weitergehende Zuordnung von Sicherheits-Integritätsleveln. Schließlich führt dies zu den erforderlichen Software-Integritätsleveln.

Der aktuelle Stand der Technik ist der, dass weder die Anwendung von Qualitätssicherungsverfahren (so genannte fehlervermeidende Maßnahmen und fehlererkennende Maßnahmen) noch die Anwendung

fehlertoleranter Softwareverfahren die absolute Sicherheit der Software garantieren können. Es ist kein Weg bekannt, die Fehlerfreiheit in einer vergleichsweise komplexen sicherheitsrelevanten Software zu beweisen, dies gilt insbesondere für Spezifikations- und Entwurfsfehler.

Die bei der Entwicklung von Software mit hoher Integrität anzuwendenden Prinzipien beinhalten, sind aber nicht beschränkt auf:

– Top-Down-Entwurfsverfahren;
– Modularität;
– Verifikation jeder Phase des Entwicklungslebenszyklus;
– verifizierte Komponenten und Komponentenbibliotheken;
– klare Dokumentation und Rückverfolgbarkeit;
– auditierbare Dokumente;
– Validierung;
– Begutachtung;
– Konfigurationsmanagement und Änderungsmanagement; und
– geeignete Betrachtung von Fragen der Organisation und der Kompetenz des Personals.

Die Zuweisung von Systemanforderungen zu Softwarefunktionen findet auf Systemebene statt. Dies beinhaltet die Definition der geforderten Integritätslevel für die Softwarefunktionen. Die aufeinander folgenden funktionalen Schritte bei der Anwendung dieser Europäischen Norm werden in Bild 1 dargestellt und sind die folgenden:

a) definieren der Software-Anforderungsspezifikation und parallel dazu Überlegungen zur Softwarearchitektur anstellen. Mit der Softwarearchitektur wird die Sicherheitsstrategie für die Software und den Software-Integritätslevel entwickelt (7.2 und 7.3);
b) entwerfen, entwickeln und testen der Software entsprechend dem Software-Qualitätssicherungsplan, dem Software-Integritätslevel und dem Software-Lebenszyklus (7.4 und 7.5);
c) integrieren der Software auf der Zielhardware und Verifikation der Funktionalität (7.6);
d) abnehmen und bereitstellen der Software (7.7 und 9.1);
e) wenn während der Betriebslebensdauer eine Softwarewartung erforderlich ist, ist diese Europäische Norm in geeigneter Form erneut anzuwenden (9.2).

Einige Aktivitäten erstrecken sich über die gesamte Softwareentwicklung. Diese schließen Tests (6.1), Verifikation (6.2), Validierung (6.3), Begutachtung (6.4), Qualitätssicherung (6.5) sowie Änderungen und Änderungsmanagement (6.6) ein.

Es werden Anforderungen für Hilfswerkzeuge (6.7) und für Systeme festgelegt, die durch Anwendungsdaten (Abschnitt 8) konfiguriert werden.

Außerdem werden Anforderungen an die Unabhängigkeit der Rollen und die Kompetenz des an der Softwareentwicklung beteiligten Personals gestellt (5.1, 5.2 und Anhang B).

Diese Norm schreibt nicht die Anwendung eines bestimmten Software-Entwicklungslebenszyklus vor. In 5.3, Bild 3 und Bild 4, sowie in 7.1 sind jedoch ein Lebenszyklus und ein Satz von Dokumenten zur Erläuterung angegeben.

Es wurden Tabellen erstellt, die die verschiedenen Techniken/Maßnahmen entsprechend den Sicherheits-Integritätsleveln 1 bis 4 und für die Basisintegrität zuordnen. Die Tabellen befinden sich in Anhang A. Ein Literaturverzeichnis gibt, Bezug nehmend auf die Tabellen, eine kurze Beschreibung jeder Technik/Maßnahme mit Hinweisen auf weiterführende Informationsquellen. Das Literaturverzeichnis für die Techniken befindet sich in Anhang D.

Diese Europäische Norm legt nicht die Anforderungen an die Entwicklung, Implementierung, Wartung und/oder Anwendung von Sicherheitsrichtlinien (en: security policies) oder –diensten (en: security services)

fest, die zur Erfüllung der Sicherheitsanforderungen (en: security requirements) erforderlich sind, die von sicherheitsrelevanten Systemen benötigt werden können. Die IT-Sicherheit kann nicht nur den Betrieb, sondern auch die funktionale Sicherheit eines Systems beeinflussen. Für die IT-Sicherheit sollten entsprechende IT-Sicherheitsnormen angewendet werden.

ANMERKUNG 2 IEC-/ISO-Normen, die die IT-Sicherheit ausführlich behandeln, sind die Normenreihen ISO/IEC 27000, ISO/IEC TR 19791 und die Normenreihe IEC 62443.

Es kann notwendig sein, zwischen Maßnahmen gegen systematische Fehler und Maßnahmen gegen Sicherheitsbedrohungen (en: security threats) abzuwägen. Ein Beispiel dafür ist die Notwendigkeit schneller Sicherheits-Updates von Software bei Sicherheitsbedrohungen (en: security threats), wobei sicherheitsrelevante Software vor jedem Update sorgfältig entwickelt, getestet, validiert und freigegeben werden sollte.

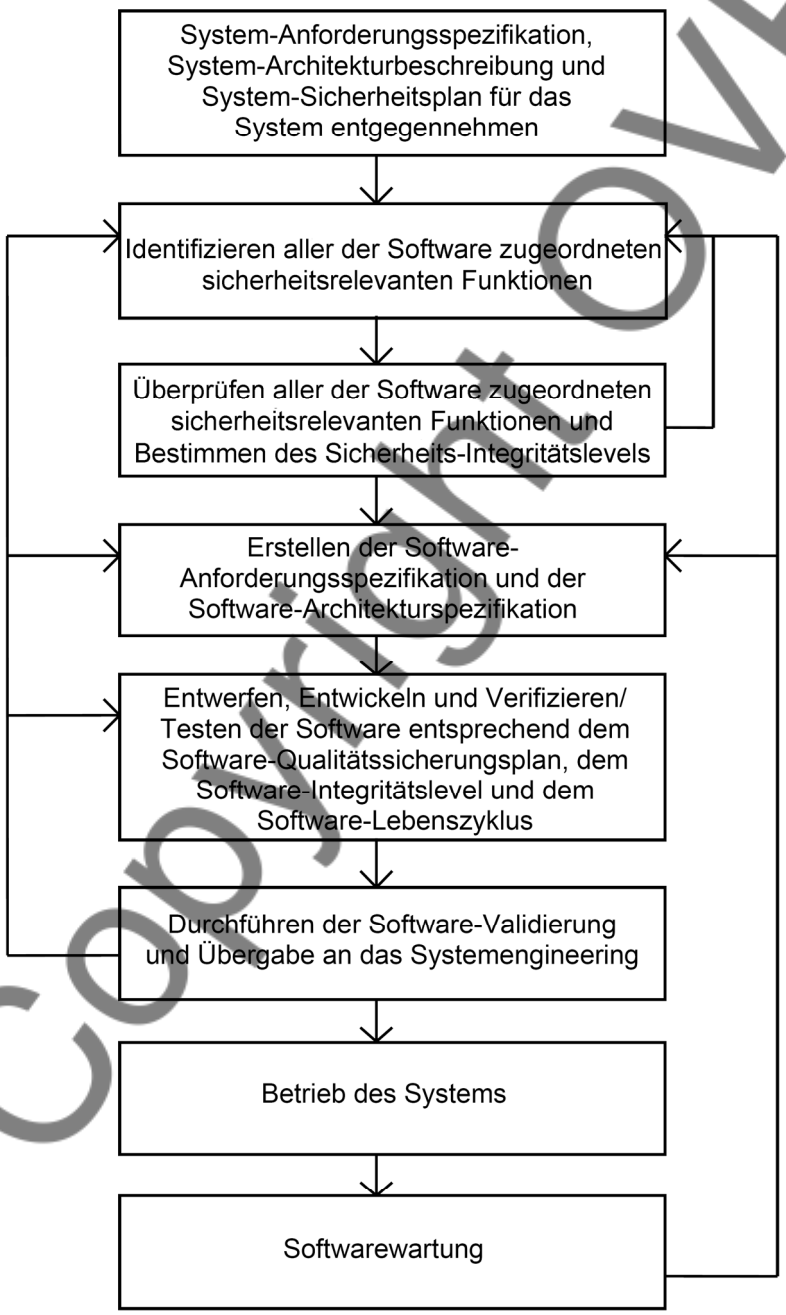

Bild 1 – Software, Übersicht über das Vorgehen

1 Anwendungsbereich

1.1 Diese Europäische Norm spezifiziert den Prozess und die technischen Anforderungen für die Entwicklung von Software für programmierbare elektronische Systeme für Schienenfahrzeuganwendungen.

Nicht zum Anwendungsbereich dieser Norm gehört Software, die:

– Teil einer zugseitigen, signaltechnischen Einrichtung ist (Anwendungen des CENELEC-Unterkomitees SC 9XA);

– keinen Beitrag zu betrieblichen Funktionen von Schienenfahrzeugen leistet und von diesen getrennt ist.

1.2 Diese Europäische Norm ist ausschließlich auf Software und die Wechselwirkung zwischen Software und dem System anwendbar, zu dem die Software gehört.

1.3 Unterabschnitt absichtlich leer gelassen.[N1)]

1.4 Diese Europäische Norm gilt für sicherheitsrelevante und nicht-sicherheitsrelevante Software, einschließlich z. B.:

– Anwendungsprogrammierung;

– Betriebssysteme;

– unterstützende Werkzeuge;

– Firmware.

Anwendungsprogrammierung umfasst Programmierung in Hochsprache, Maschinensprache und speziellen Anwendungssprachen (z. B. SPS-Kontaktplan).

1.5 Die Nutzung vorher entwickelter Software und von Werkzeugen wird in dieser Europäischen Norm ebenfalls angesprochen. Derartige Software darf eingesetzt werden, wenn die spezifischen Anforderungen in 7.3.4.7 und 6.5.4.16 für vorher entwickelte Software und für Werkzeuge in 6.7 erfüllt sind.

1.6 Software, die nach einer gültigen Ausgabe der EN 50128 entwickelt worden ist, wird als konform zu dieser Norm betrachtet. Software, die vorher nach einer beliebigen Version von EN 50128 entwickelt wurde, wird ebenfalls als konform betrachtet und unterliegt nicht den Anforderungen an vorher entwickelte Software. Für SIL1-SIL4 Software im Geltungsbereich dieser Norm sind die in dieser Europäischen Norm enthaltenen Anforderungen äquivalent zu den SIL1-SIL4 Softwareanforderungen der EN 50128:2011.

1.7 In dieser Europäischen Norm wird berücksichtigt, dass ein moderner Anwendungsentwurf häufig Software verwendet, die als Basis für diverse Anwendungen geeignet ist. Diese Software wird anschließend durch Anwendungsdaten konfiguriert, um damit die ausführbare Software für die Anwendung anzufertigen. Diese Europäische Norm gilt für solche Software. Darüber hinaus werden spezifische Anforderungen an Anwendungsdaten angegeben.

1.8 Unterabschnitt absichtlich leer gelassen.[N1)]

1.9 Diese Europäische Norm gilt nicht rückwirkend. Sie gilt daher in erster Linie für Neuentwicklungen und in ihrer Gesamtheit für vorhandene Systeme nur dann, wenn diese größeren Änderungen unterworfen werden. Für kleinere Änderungen ist nur 9.2 anzuwenden. Die Anwendung dieser Europäischen Norm bei Erweiterung und Wartung bestehender Software wird jedoch empfohlen.

1.10 Die anwendbaren Abschnitte dieser Software-Norm gelten zusätzlich zur anwendbaren Hardware-Norm (z. B. EN 50129, EN 50155, EN 61508-2) auch für programmierbare Komponenten (z. B. FPGA und CPLD). Anforderungen dieser Software-Norm, die bereits von der anwendbaren Hardware-Norm abgedeckt werden, müssen nicht erneut adressiert werden.

[N1)] Nationale Fußnote: Die Gliederung bezieht sich auf EN 50128:2011, vgl. Anhang E.

Wenn die Möglichkeit eines umfassenden Tests der programmierbaren Logik für alle möglichen Eingangssignale und internen logischen Zustände besteht, gilt diese Europäische Norm nicht.

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 ISO 9000:2015, *Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2015)*

ISO/IEC 90003:2014, *Software engineering – Guidelines for the application of ISO 9001:2008 to computer software*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokumentes gelten die folgenden Begriffe.

3.1.1
Begutachtung
(en: assessment)
Prozess, um eine Beurteilung auf Basis von Nachweisen durchzuführen, ob ein Produkt, System oder Prozess den festgelegten Anforderungen entspricht

Anmerkung 1 zum Begriff: Hinsichtlich der Software kann die Begutachtung den Entwicklungsprozess, die Dokumentation, die System-, Subsystem-Hardware und/oder Softwarekomponenten umfassen. Die Begutachtung richtet sich auf die sicherheitsrelevanten Eigenschaften der begutachteten Software, ist jedoch nicht nur darauf beschränkt.

3.1.2
Gutachter
(en: assessor)
ernannte unabhängige Einheit, die eine Begutachtung durchführt

Anmerkung 1 zum Begriff: Dieser Begriff beruht auf EN 50126-1:2017, aber in der vorliegenden Europäischen Norm wird die Unabhängigkeit des Gutachters immer gefordert, siehe 5.1.2.

Anmerkung 2 zum Begriff: Die spezifische Bedeutung des Begriffs „Gutachter“ in dieser Norm ist in 5.1.2.4, 5.1.2.5, 5.1.2.6 und Anhang B, Tabelle B.8, festgelegt. Hierbei handelt es sich um eine softwarespezifische Rolle, die nicht mit verschiedenen Arten von Gutachtern verwechselt werden sollte, die in anderen Normen festgelegt sind.

3.1.3
kommerzielle Standard-Software
COTS
(en: commercial off-the-shelf software)
durch Markterfordernisse bestimmte Software, die kommerziell erhältlich ist und deren Einsatztauglichkeit durch ein breites Spektrum kommerzieller Anwender als hinreichend angesehen wird

[QUELLE: EN 50126-1:2017, 3.10, modifiziert]

3.1.4
Komponente
Bestandteil der Software, der in Bezug auf Softwarearchitektur und -entwurf über klar definierte Schnittstellen verfügt und ein bestimmtes Verhalten hat und die folgenden Kriterien erfüllt:

– er ist entsprechend den „Komponenten“ entwickelt (siehe Tabelle A.20);

– er umfasst eine bestimmte Teilmenge der Softwareanforderungen;