ÖVE/ÖNORM
EN 50128

Ausgabe: 2012-04-01

Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme

Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems

Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire

Medieninhaber und Hersteller:
OVE Österreichischer Verband für Elektrotechnik
Austrian Standards Institute

Verkauf von in- und ausländischen Normen und technischen Regelwerken durch
Austrian Standards Institute
Heinestraße 38, 1020 Wien
E-Mail: sales@as-plus.at
Internet: www.as-plus.at
Webshop: www.as-plus.at/shop
Tel.: +43 1 213 00-444
Fax: +43 1 213 00-818

Alle Regelwerke für die Elektrotechnik auch erhältlich bei
OVE Österreichischer Verband für Elektrotechnik
Eschenbachgasse 9, 1010 Wien
E-Mail: verkauf@ove.at
Internet: www.ove.at
Webshop: www.ove.at/webshop
Tel.: +43 1 587 63 73
Fax: +43 1 586 74 08

ICS	35.240.60; 45.020; 93.100
Ident (IDT) mit	EN 50128:2011
Ersatz für	siehe nationales Vorwort
zuständig	OVE/Komitee TK TM Traktion und Motorik

Nationales Vorwort

Diese Europäische Norm EN 50128:2011 hat sowohl den Status von ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK gemäß ETG 1992 als auch den einer ÖNORM gemäß NG 1971. 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 ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORM ist den jeweils geltenden Verordnungen zum Elektrotechnikgesetz zu entnehmen.

Bei mittels Verordnungen zum Elektrotechnikgesetz verbindlich erklärten ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORMEN ist zu beachten:

- Hinweise auf Veröffentlichungen beziehen sich, sofern nicht anders angegeben, auf den Stand zum Zeitpunkt der Herausgabe dieser ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORM. Zum Zeitpunkt der Anwendung dieser ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORM 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) werden gemäß den „Gemeinsamen Regeln“ von CEN/CENELEC durch Veröffentlichung eines identen Titels und Textes in das Gesamtwerk der ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORMEN übernommen, wobei der Nummerierung der Zusatz ÖVE/ÖNORM bzw. ÖNORM vorangestellt wird.

Erläuterung zum Ersatzvermerk

Gemäß Vorwort zur EN wird das späteste Datum, zu dem nationale Normen, die der vorliegenden Norm entgegenstehen, zurückgezogen werden müssen, mit dow (date of withdrawal) festgelegt. Bis zum Zurückziehungsdatum (dow) 2014-04-25 ist somit die Anwendung folgender Norm(en) noch erlaubt:

ÖVE/ÖNORM EN 50128:2002-01-01,
ÖVE/ÖNORM EN 50128/AC:2010-10-01.

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 50128

Juni 2011

ICS 35.240.60; 45.020; 93.100

Ersatz für EN 50128:2001

Deutsche Fassung

Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme

Railway applications –
Communication, signalling and processing systems –
Software for railway control and protection systems

Applications ferroviaires –
Systèmes de signalisation, de télécommunication et de traitement –
Logiciels pour systèmes de commande et de protection ferroviaire

Diese Europäische Norm wurde von CENELEC am 2011-04-25 angenommen. Die 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 Zentralsekretariat 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 Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, 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, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

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

Zentralsekretariat: Avenue Marnix 17, B-1000 Brüssel

Ref. Nr. EN 50128:2011 D

Inhalt

Seite

Bilder

Tabellen

Vorwort

Diese Europäische Norm wurde vom SC 9XA „Kommunikation, Signaltechnik und Datenverarbeitungssysteme“ des Technischen Komitees CENELEC/TC 9X „Elektrische und elektronische Anwendungen für Bahnen“ ausgearbeitet.

Sie wurde der formellen Abstimmung unterworfen und von CENELEC am 2011-04-25 als EN 50128 angenommen.

Dieses Schriftstück ersetzt EN 50128:2001.

Nachfolgend sind die wesentlichen Änderungen gegenüber EN 50128:2001 aufgeführt:

– Anforderungen an Softwaremanagement und -organisation, Festlegung von Rollen und Kompetenzen, Bereitstellung und Wartung wurden ergänzt;

– ein neuer Abschnitt zu Werkzeugen, der auf EN 61508-2:2010 beruht, wurde eingefügt;

– die Tabellen in Anhang A wurden aktualisiert.

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

Nachstehende Daten wurden festgelegt:

– spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2012-04-25

– spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2014-04-25

Diese Europäische Norm sollte in Verbindung mit EN 50126-1:1999 „*Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) – Teil 1: Grundlegende Anforderungen und genereller Prozess*“ und EN 50129:2003 „*Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik*“ gelesen werden.

Einleitung

Diese Europäische Norm ist Teil einer Gruppe verwandter Normen. Die anderen sind EN 50126-1:1999 „*Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) – Teil 1: Grundlegende Anforderungen und genereller Prozess*“ und EN 50129:2003 „*Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik*“.

EN 50126-1 behandelt Systemfragen im weitesten Sinn, während EN 50129 den Abnahmeprozess für einzelne Systeme behandelt, die innerhalb des gesamten Eisenbahnsteuerungs- und Überwachungssystems existieren können. Diese Europäische Norm konzentriert sich auf die anzuwendenden Verfahren, um Software zu erhalten, welche den Anspruch an die Sicherheitsintegrität erfüllt, der durch übergeordnete Betrachtungen an sie gestellten wird.

Diese Europäische Norm beschreibt eine Reihe von Anforderungen, denen die Entwicklung, Bereitstellung und Wartung von sicherheitsrelevanter Software für Eisenbahnsteuerungs- und Überwachungsanwendungen entsprechen muss. 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-Sicherheits-Integritätslevel. Diese Europäische Norm behandelt fünf Software-Sicherheits-Integritätslevel, von denen 0 die niedrigste und 4 der höchste Level ist. Je größer das Risiko ist, das von einem Softwarefehler ausgeht, desto höher ist der Software-Sicherheits-Integritätslevel.

Diese Europäische Norm führt Techniken und Maßnahmen für 5 Software-Sicherheits-Integritätslevel auf. Die geforderten Techniken und Maßnahmen für die Software-Sicherheits-Integritätslevel 0 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-Sicherheits-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 Sicherheitsfunktionen übernehmen, und von sozialen und wirtschaftlichen Faktoren.

Es fällt in den Anwendungsbereich von EN 50126-1 und EN 50129 die der Software zugewiesenen Sicherheitsfunktionen festzulegen.

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

EN 50126-1 und EN 50129 fordern 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 einer übergreifenden Spezifikation der 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 und Managementaktivitäten, die erforderlich sind, um die Spezifikation der System-Sicherheitsanforderungen in ein sicherheitsrelevantes System mit einer validierten Sicherheitsintegrität umzusetzen.

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

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

toleranter Software-Verfahren 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 Sicherheitsintegrität anzuwendenden Prinzipien beinhalten, sind aber nicht beschränkt auf:

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

Die Spezifikation der System-Sicherheitsanforderungen identifiziert alle der Software zugeordneten Sicherheitsfunktionen und die System-Sicherheits-Integritätslevel. 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 die Überlegungen zur Software-Architektur. In der Software-Architektur wird die grundlegende Sicherheitsstrategie für die Software und dem Software-Sicherheits-Integritätslevel entwickelt (7.2 und 7.3);
b) Entwerfen, entwickeln und testen der Software entsprechend dem Software-Qualitätssicherungsplan, dem Software-Sicherheits-Integritätslevel und dem Software-Lebenszyklus (7.4 und 7.5);
c) Integration der Software auf der Zielhardware und Verifikation der Funktionalität (7.6);
d) Abnahme und Bereitstellung der Software (7.7 und 9.1);
e) Wenn innerhalb der Betriebslebensdauer eine Software-Wartung erforderlich ist, ist diese Europäische Norm in geeigneter Form erneut anzuwenden (9.2).

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

Es werden Anforderungen für Hilfswerkzeuge (6.7) und für Systeme festgelegt, die durch Anwendungsdaten oder Algorithmen (Abschnitt 8) konfigurierbar sind.

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

Die Norm schreibt nicht den Gebrauch eines bestimmten Software-Entwicklungslebenszyklus vor. Ein empfohlener Lebenszyklus und ein Satz von Dokumenten sind jedoch angegeben (5.3, Bild 3 und Bild 4 und 7.1).

Es wurden Tabellen erstellt, die die verschiedenen Techniken/Maßnahmen entsprechend den Software-Sicherheits-Integritätslevel 0 bis 4 bewerten. Die Tabellen befinden sich in Anhang A. Ein Literaturverzeichnis gibt, bezugnehmend auf die Tabellen, eine kurze Beschreibung jeder Technik/Maßnahme mit Hinweisen auf weiterführende Informationen. Das Literaturverzeichnis für die Techniken befindet sich in Anhang D.

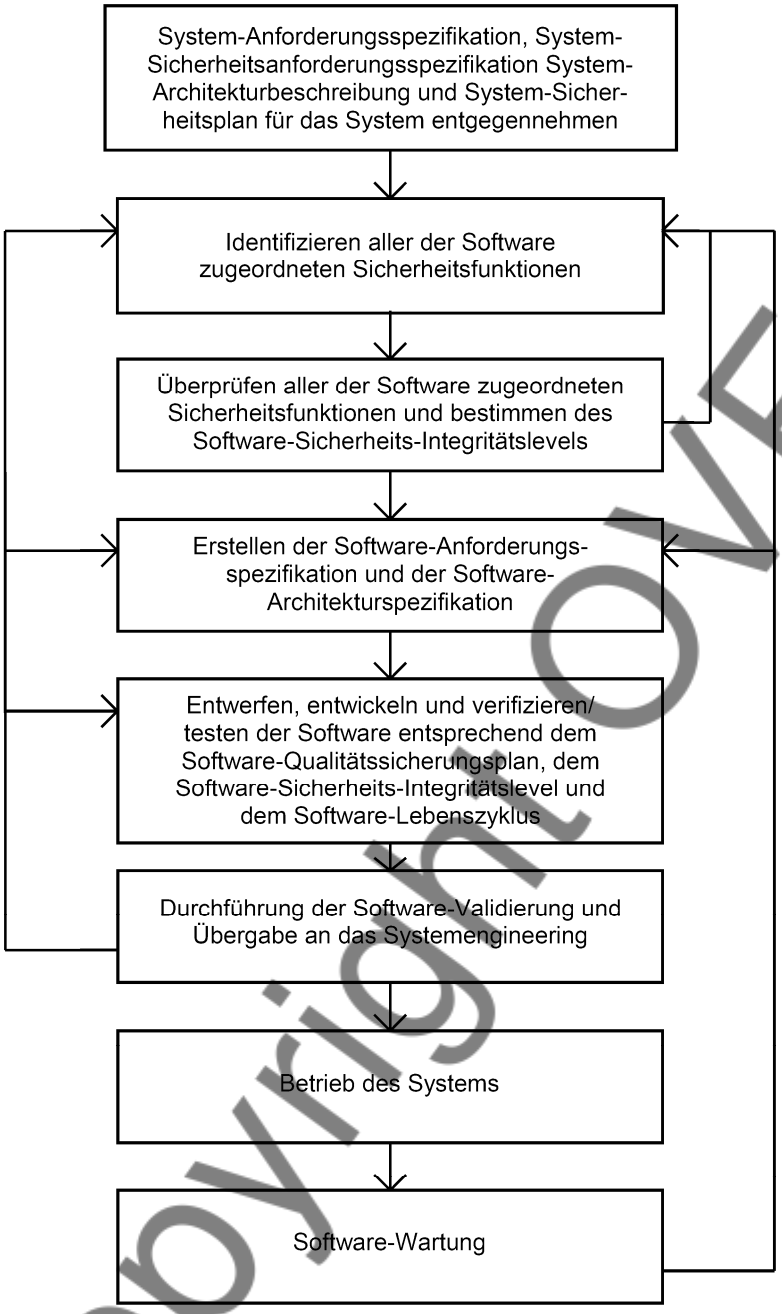

Bild 1 – Software, Übersicht über das Vorgehen

1 Anwendungsbereich

1.1 Diese Europäische Norm beschreibt den Prozess und die technischen Anforderungen für die Entwicklung von Software für programmierbare elektronische Systeme für die Anwendung auf dem Gebiet der Eisenbahnsteuerung und -überwachung. Sie hat das Ziel, in allen Bereichen angewendet zu werden, in denen Auswirkungen auf die Sicherheit bestehen. Diese Systeme können implementiert sein unter Verwendung dedizierter Mikroprozessoren, speicherprogrammierbarer Steuerungen, verteilter Multiprozessor-Systeme, großer Zentralrechner-Systeme oder anderer Architekturen.

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 Diese Europäische Norm hat keine Bedeutung für Software, für die festgestellt wurde, dass sie keinen Einfluss auf die Sicherheit hat, d. h. Software, bei der Fehlfunktionen keine der identifizierten Sicherheitsfunktionen beeinträchtigen können.

1.4 Diese Europäische Norm gilt für jegliche sicherheitsrelevante Software, die in Eisenbahnsteuerungs- und -überwachungssystemen verwendet wird, einschließlich:

– Anwendungsprogrammierung;

– Betriebssysteme;

– unterstützende Werkzeuge;

– Firmware.

Anwendungsprogrammierung umfasst Programmierung in Hochsprache, Maschinensprache und speziellen Anwendungssprachen (z. B. ladder logic bei speicherprogrammierbaren Steuerungen).

1.5 Die Nutzung vorher entwickelter (pre-existing) 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 beliebigen Ausgabe dieser Europäischen Norm entwickelt worden ist, wird als konform betrachtet und unterliegt nicht den Anforderungen an vorher entwickelte (pre-existing) Software.

1.7 In dieser Europäischen Norm wird berücksichtigt, dass moderner Anwendungsentwurf häufig unter Einsatz generischer Software erfolgt, die als Basis für verschiedene Anwendungen geeignet ist. Diese generische Software wird anschließend durch Daten, Algorithmen oder beides konfiguriert, um damit die ausführbare Software für die Anwendung anzufertigen. Die allgemeinen Abschnitte 1 bis 6 und 9 dieser Europäischen Norm gelten sowohl für generische Software als auch für Anwendungsdaten oder -algorithmen. Der spezifische Abschnitt 7 gilt nur für generische Software, während Abschnitt 8 die spezifischen Anforderungen an Anwendungsdaten oder -algorithmen beschreibt.

1.8 Die Behandlung kommerzieller Themen ist nicht Zweck dieser Europäischen Norm. Diese sollten als ein wesentlicher Teil von vertraglichen Vereinbarungen angesehen werden. Alle Abschnitte dieser Europäischen Norm müssen in jeder kommerziellen Situation sorgfältig berücksichtigt werden.

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. Der Gutachter hat die in der Softwaredokumentation gegebenen Nachweise zu analysieren, um zu bestätigen, ob die Bestimmung der Art und des Umfangs von Änderung an der Software angemessen ist. Die Anwendung dieser Europäischen Norm bei Erweiterung und Wartung vorhandener Software wird jedoch dringend empfohlen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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 50126-1:1999, *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) – Teil 1: Grundlegende Anforderungen und genereller Prozess*

EN 50129:2003, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik*

EN ISO 9000, *Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000)*

EN ISO 9001, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001)*

ISO/IEC 90003:2004, *Software engineering – Guidelines for the application of ISO 9001:2000 to computer software*

ISO/IEC 9126 (Reihe), *Software engineering – Product quality*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1
Begutachtung
Analyseprozess zur Feststellung, ob die Software, die den Prozess, die Dokumentation, die System-, Subsystem-Hardware und/oder Softwarekomponenten umfassen kann, die spezifizierten Anforderungen erfüllt, und um zu beurteilen, ob die Software für ihren beabsichtigten Anwendungszweck geeignet ist. Die Begutachtung von Software richtet sich auf die sicherheitsrelevanten Eigenschaften eines Systems, ist jedoch nicht nur darauf beschränkt.

3.1.2
Gutachter
Einheit, die eine Begutachtung durchführt

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 bewiesen ist

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

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

– sie umfasst eine bestimmte Teilmenge der Software-Anforderungen;

– sie hat innerhalb des Konfigurations-Managementsystems eine eigenständige Versionierung oder sie ist Teil einer Sammlung von Komponenten (z. B. Untersystemen), die eine eigenständige Versionierung haben.