

	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:1998 + Corrigendum 1999) Deutsche Fassung EN 61508-5:2001	<u>DIN</u> EN 61508-5
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0803 Teil 5
ICS 25.040.40 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5:1998 + corrigendum 1999); German version EN 61508-5:2001 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité (CEI 61508-5:1998 + corrigendum 1999); Version allemande EN 61508-5:2001 Die Europäische Norm EN 61508-5:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 61508-5 wurde am 2001-07-03 angenommen. Nationales Vorwort Für die vorliegende Norm ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Norm-Inhalt war veröffentlicht als E DIN IEC 65A/183/CDV (VDE 0801 Teil 5):1996-05. Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet. Die Vornormen DIN V VDE 0801 (VDE 0801):1990-01 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben DIN V VDE 0801/A1 (VDE 0801/A1):1994-10 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben; Änderung 1:1994-10 DIN V 19250:1994-05 Leittechnik – Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen und DIN V 19251:1995-02 Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion enthalten Festlegungen, die den Festlegungen in den Normen der Reihe DIN EN 61508 (VDE 0803) entgegenstehen oder zu ihnen redundant sind. Die DKE beabsichtigt daher, die oben genannten Vornormen zum 01. August 2004 zurückzuziehen. Fortsetzung Seite 2 und 3 und 31 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-1:2001	IEC 61508-1:1998	DIN EN 61508-1 (VDE 0803 Teil 1):2002-11	VDE 0803 Teil 1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803 Teil 2): in Vorbereitung	VDE 0803 Teil 2
EN 61508-3:2001	IEC 61508-3:1998	DIN EN 61508-3 (VDE 0803 Teil 3): in Vorbereitung	VDE 0803 Teil 3
EN 61508-4:2001	IEC 61508-4:1998	DIN EN 61508-4 (VDE 0803 Teil 4):2002-11	VDE 0803 Teil 4
EN 61508-6:2001	IEC 61508-6:2000	DIN EN 61508-6 (VDE 0803 Teil 6): in Vorbereitung	VDE 0803 Teil 6
EN 61508-7:2001	IEC 61508-7:2000	DIN EN 61508-7 (VDE 0803 Teil 7): in Vorbereitung	VDE 0803 Teil 7
–	IEC Guide 104:1997	–	–
–	ISO/IEC Guide 51: 1990	DIN 820-120:2001-10	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-120, *Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC-Guide 51:1999)*.

DIN EN 61508-1 (VDE 0803 Teil 1, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme – Teil 1: Allgemeine Anforderungen IEC 61508-1:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-1:2001.

DIN EN 61508-2 (VDE 0803 Teil 2), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.

DIN EN 61508-3 (VDE 0803 Teil 3), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001.

DIN EN 61508-4 (VDE 0803 Teil 4), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001.

DIN EN 61508-6 (VDE 0803 Teil 6), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für die IEC 61508-2 und IEC 61508-3.

DIN EN 61508-7 (VDE 0803 Teil 7), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen.

– Leerseite –

**Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität
(safety integrity level)
(IEC 61508-5:1998 + Corrigendum 1999)**

Functional safety of electrical/electronic/programmable
electronic safety-related systems –
Part 5: Examples of methods for the determination of
safety integrity levels
(IEC 61508-5:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 5: Exemples de méthodes de détermination des
niveaux d'intégrité de sécurité
(CEI 61508-5:1998 + corrigendum 1999)

Diese Europäische Norm wurde von CENELEC am 2001-07-03 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, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Der Text der Internationalen Norm IEC 61508-5 einschließlich deren Corrigendum April 1999, ausgearbeitet von dem SC 65A "System aspects" des IEC TC 65 "Industrial-process measurement and control", wurde dem Einstufigen Annahmeverfahren unterworfen und von CENELEC am 2001-07-03 ohne irgendeine Abänderung als EN 61508-5 angenommen.

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): 2002-08-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2004-08-01

Anhänge, die als "normativ" bezeichnet sind, gehören zum Norminhalt.

Anhänge, die als "informativ" bezeichnet sind, enthalten nur Informationen.

In dieser Norm ist Anhang ZA normativ und sind Anhänge A, B, C, D, E und F informativ.

Der Anhang ZA wurde von CENELEC hinzugefügt.

Die IEC 61508 ist eine Sicherheitsgrundnorm zur funktionalen Sicherheit von elektrischen, elektronischen und programmierbar elektronischen sicherheitsbezogenen Systemen. Der Anwendungsbereich lautet :

„Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbar elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist es, für ein bestimmtes Anwendungsgebiet die Entwicklung einer entsprechenden Internationalen Norm durch das jeweils verantwortliche Komitee zu ermöglichen. Dies wird es erlauben, alle wichtigen Einflussgrößen dieses Anwendungsgebietes vollständig zu berücksichtigen und damit dessen besonderen Erfordernissen nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung eines elektrischen/elektronischen/programmierbar elektronischen (E/E/PE) sicherheitsbezogenen Systems für dessen Anwendungsgebiet noch keine Internationale Norm besteht, zu ermöglichen.“

Der CENELEC-Bericht R0BT-004, der auf der 103. Sitzung des technischen Büros im März 2000 angenommen wurde, geht davon aus, dass einige IEC-Normen, die bereits veröffentlicht sind oder gerade erarbeitet werden, Implementierung der IEC 61508 für ein bestimmtes Anwendungsgebiet darstellen, z. B.:

- IEC 61511, Functional safety – Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

Für das Anwendungsgebiet des Eisenbahnwesens wurde ebenfalls eine Reihe Europäischer Normen erstellt (EN 50126, EN 50128 und prEN 50129).

ANMERKUNG EN 50126 und EN 50128 beruhen auf früheren Entwürfen der IEC 61508. prEN 50129 beruht auf den Grundsätzen der jetzt gültigen Fassung der IEC 61508.

Diese Aufzählung schließt nicht aus, dass weitere Implementierungen der IEC 61508 für bestimmte Anwendungsgebiete, die sich gerade in der Erarbeitung oder Veröffentlichung innerhalb IEC oder CENELEC befinden, erscheinen.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61508-5:1998 einschließlich deren Corrigendum April 1999 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	10
3 Begriffe und Abkürzungen	10
Anhang A (informativ) Risiko und Sicherheitsintegrität – Allgemeine Konzepte	11
A.1 Allgemeines	11
A.2 Notwendige Risikominderung	11
A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme	11
A.4 Sicherheitsintegrität	12
A.5 Risiko und Sicherheitsintegrität	15
A.6 Sicherheits-Integritätslevel und Software-Sicherheits-Integritätslevel	15
A.7 Zuordnung von Sicherheitsanforderungen	15
Anhang B (informativ) Konzepte für ALARP und tolerierbares Risiko	17
B.1 Allgemeines	17
B.2 ALARP-Modell	17
B.2.1 Einleitung	17
B.2.2 Grenzwert für das tolerierbare Risiko	18
Anhang C (informativ) Festlegung der Sicherheits-Integritätsleveln – Eine quantitative Methode	20
C.1 Allgemeines	20
C.2 Allgemeine Methode	20
C.3 Beispielrechnung	21
Anhang D (informativ) Bestimmung der Sicherheits-Integritätslevel – Eine qualitative Methode: Risikograph	23
D.1 Allgemeines	23
D.2 Aufbau des Risikographen	23
D.3 Mögliche andere Risikoparameter	24
D.4 Anwendung des Risikographen: allgemeines Schema	24
D.5 Beispiel eines Risikographen	24
Anhang E (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls	28
E.1 Allgemeines	28
E.2 Matrix des Ausmaßes des gefährlichen Vorfalls	28
Anhang F (informativ) Literaturhinweise	30
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	31
Bilder	
Bild 1 – Gesamtrahmen der Betrachtung dieser Norm	9
Bild A.1 – Risikominderung: allgemeine Konzepte	14
Bild A.2 – Risiko- und Sicherheitsintegritätskonzepte	14
Bild A.3 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE-	

	Seite
Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung	16
Bild B.1 – Tolerierbares Risiko und ALARP	18
Bild C.1 – Zuordnung der Sicherheitsintegrität: Beispiel für eine sicherheitsbezogene Schutz Einrichtung	22
Bild D.1 – Risikograph: Allgemeine Darstellung	25
Bild D.2 – Risikograph: Beispiel (zeigt nur allgemeine Prinzipien auf)	26
Bild E.1 – Matrix des Ausmaßes des gefährlichen Vorfalls: Beispiel (stellt nur die allgemeinen Prinzipien dar)	29
Tabellen	
Tabelle B.1 – Beispiel für die Risikoklassifizierung von Unfällen.....	19
Tabelle B.2 – Interpretation der Risikoklassen	19
Tabelle D.1 – Beispieldaten, die sich auf das Beispiel des Risikographen (Bild D.2) beziehen.....	27

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Bauteilen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme (PES)) werden in allen Anwendungsbereichen benutzt, um Nichtsicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerichtet eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen Entscheidungen getroffen werden.

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbar elektronischen Bauteilen bestehen (elektrische/elektronische/programmierbar elektronische Systeme (E/E/PES)) und die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

In den meisten Situationen wird Sicherheit durch eine Anzahl von Schutzsystemen erreicht, die auf vielerlei Technologien (zum Beispiel Mechanik, Hydraulik, Pneumatik, Elektrik, Elektronik, programmierbare Elektronik) basieren. Jede Sicherheitsstrategie muss deshalb nicht nur alle Elemente innerhalb eines Einzelsystems (zum Beispiel Sensoren, Steuereinheiten und Aktoren) betrachten, sondern auch all die sicherheitsbezogenen Systeme, die einzelne Teile einer Gesamtheit sind. Da sich diese Internationale Norm mit sicherheitsbezogenen elektrischen/elektronischen/programmierbar elektronischen (E/E/PE) Systemen beschäftigt, kann sie einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme, basierend auf anderen Technologien, betrachtet werden können.

Es ist berücksichtigt worden, dass eine große Vielfalt von E/E/PES-Anwendungen in vielfältigen Anwendungsbereichen vorliegt und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdeckt. In jeder speziellen Anwendung sind die erforderlichen Sicherheitsmaßnahmen von vielen anwendungsspezifischen Faktoren abhängig. Dadurch, dass diese Internationale Norm allgemein gehalten ist, wird die Formulierung solcher Maßnahmen in zukünftigen anwendungsspezifischen Internationalen Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten sicherheitsbezogenen Phasen des Gesamtsystems der E/E/PES und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Durchführung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PES benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PES befassen. Die Entwicklung anwendungsspezifischer Normen sollte innerhalb des Rahmens dieser Internationalen Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;
- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die notwendige funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu erreichen;
- verwendet Sicherheits-Integritätslevel für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen, die in dem sicherheitsbezogenen E/E/PE-System implementiert werden;
- verwendet einen auf dem Risiko basierenden Lösungsansatz für die Festlegung der Anforderungen der Sicherheits-Integritätslevel;
- setzt numerische Ausfallgrenzwerte für sicherheitsbezogene E/E/PE-Systeme, die mit Sicherheits-Integritätsleveln verbunden sind;

- setzt eine untere Grenze des Ausfallgrenzwertes für eine gefahrbringende Ausfallart, der für ein einzelnes sicherheitsbezogenes E/E/PE-System beansprucht werden kann. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze der mittleren Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen, auf 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen oder ununterbrochenen Anforderungsrate betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} pro Stunde festgelegt;

ANMERKUNG Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht auch notwendigerweise eine ein-kanalige Architektur.

- lässt einen weiten Bereich von Prinzipien, Techniken und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten gut definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.