

	DIN EN 61508-4 (VDE 0803-4)	
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	
ICS 35.240.50 Ersatz für DIN EN 61508-4 (VDE 0803-4):2002-11 Siehe jedoch Anwendungsbeginn Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations (IEC 61508-4:2010); German version EN 61508-4:2010 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations (CEI 61508-4:2010); Version allemande EN 61508-4:2010 Gesamtumfang 54 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2010-05-01 angenommene Europäische Norm als DIN-Norm ist 2011-02-01.

Daneben darf DIN EN 61508-4 (VDE 0803-4):2002-11 noch bis 2013-05-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61508-4 (VDE 0803-4):2009-06.

Für diese 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 (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Änderungen

Gegenüber DIN EN 61508-4 (VDE 0803-4):2002-11 wurden folgende Änderungen vorgenommen:

- a) Aufnahme von Begriffen, die für die Behandlung der ASICs nach DIN EN 61508-2 (VDE 0803-2) erforderlich sind;
- b) Hinzufügung von Begriffen zur systematischen Eignung von Software nach DIN EN 61508-3 (VDE 0803-3);
- c) neue Begriffe und neue Definitionen für vorhandene Begriffe zur Klarstellung der vorhandenen Anforderungen, wie z. B. systematische Eignung, Gesamtsicherheitsfunktionen, Ausfall eines unbeteiligten Bauteils und Ausfall ohne Auswirkung.

Frühere Ausgaben

DIN EN 61508-4 (VDE 0803-4): 2002-11

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 Abschnietsnummer, 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.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60050-351:2006	*)	–
EN 60601 (alle Teile)	IEC 60601 (alle Teile)	DIN EN 60601 (VDE 0750-1) (alle Teile)	VDE 0750-1
EN 61131-3:2003	IEC 61131-3:2003	DIN EN 61131-3:2003-12	–
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7
EN 61511 (alle Teile)	IEC 61511 (alle Teile)	DIN EN 61511 (VDE 0810-1) (alle Teile)	VDE 0810-1
EN 61800-5-2	IEC 61800-5-2	DIN EN 61800-5-2 (VDE 0160-105-2)	VDE 0160-105-2
EN 62061	IEC 62061	DIN EN 62061 (VDE 0113-50)	VDE 0113-50
–	IEC 60050-191:1990	*)	–
–	IEC/TR 62059-11	–	–
–	IEC Guide 104:1997	–	–
–	ISO/IEC 2382-1:1993	–	–
–	ISO/IEC 2382-14 :1997	–	–
–	ISO/IEC Guide 51 :1999	–	–
–	ISO 8402:1994	–	–
EN ISO 9000:2005	ISO 9000:2005	DIN EN ISO 9000:2005-12	–

*) „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: <http://www.dke.de/dke-iev>.

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60601 (VDE 0750-1) (alle Teile), *Klassifikation und Kennzeichnung von Dokumenten für Anlagen, Systeme und Ausrüstungen*

DIN EN 61131-3:2003-12, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (IEC 61131-3:2003); Deutsche Fassung EN 61131-3:2003*

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010*

DIN EN 61508-2 (VDE 0803-2):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010*

DIN EN 61508-3 (VDE 0803-3):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010*

DIN EN 61508-5 (VDE 0803-5):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010*

DIN EN 61508-6 (VDE 0803-6):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010*

DIN EN 61508-7 (VDE 0803-7):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010*

DIN EN 61511 (VDE 0810-1) (alle Teile), *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie*

DIN EN 61800-5-2 (VDE 0160-105-2), *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit*

DIN EN 62061 (VDE 0113-50), *Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*

DIN EN ISO 9000:2005-12, *Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2005); Dreisprachige Fassung EN ISO 9000:2005*

Anhang NC

(informativ)

Fachwörterliste mit Benennungen aus den Normen der Reihe IEC 61508

Diese Fachwörterliste enthält die wichtigsten Benennungen aus den Normen der Reihe IEC 61508 und die für die DIN EN 61508 (VDE 0803) verwendeten Übersetzungen.

Englische Benennung	Deutsche Benennung
1oo2 1out of 2	1oo2
activity	Tätigkeit
actuator	Aktor
allocation of requirements	Zuordnung von Anforderungen
animation	Animation
application	Anwendung
application software	Anwendungssoftware
application specific integrated circuit	anwendungsspezifischer integrierter Schaltkreis
appropriate pedigree	angemessene Herkunft
architectural constraints	Einschränkungen hinsichtlich der Architektur
architecture	Architektur
as low as reasonably practicable (ALARP)	so niedrig wie vernünftigerweise möglich
assertion programming	siehe failure assertion programming
assessment	Beurteilung
assessor	beurteilende Person
average frequency of a dangerous failure	mittlere Häufigkeit eines gefahrbringenden Ausfalls
average probability of dangerous failure on demand (PFDavg)	mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung
average probability of dangerous failure per hour (PFHavg)	mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFHavg)
average rate of safe failures	mittlere Rate sicherer Ausfälle
avoid (a hazardous event)	vermeiden
basic process control system (BPCS)	Betriebs- und Überwachungseinrichtungen, PLT-Betriebs- und Überwachungseinrichtungen
cell based ASIC	Cell-based-ASIC
channel	Kanal
code	Programm (oder Code)
coding guideline	Programmierrichtlinie
coding rule	Programmierregel
coding standard	Programmierrichtlinie
commercially available	im Handel erhältlich
common cause analysis	Analyse gemeinsamer Ursachen
common cause failure	Ausfall infolge gemeinsamer Ursache
comparator	Vergleicher
compatibility	Verträglichkeit
competence	Kompetenz
competent	kompetent
complex programmable logic device (CPLD)	komplexer programmierbarer Logikbaustein (CPLD)
compliance	Konformität, auch Übereinstimmung
compliance route	Konformitätspfad
compliant item	konformes Objekt
component	Bauteil (auch Komponente)
confidence level	Konfidenzniveau

confidence limit	Konfidenzgrenze
configuration management	Konfigurationsmanagement
conformance	Übereinstimmung
consequence	Auswirkung
continuous mode	Betriebsart mit kontinuierlicher Anforderung
control als Managmenttätigkeit	lenken
control als Oberbegriff von Regeln und Steuern	meistens steuern, in bestimmten Fällen auch Regeln, z. B. „temperature control = „Temperaturregelung“
control of faults oder faults control	Fehlerbeherrschung
control system	Leit- oder Steuerungssystem Regelsystem
core based ASIC	Core-based-ASIC
correct	ordnungsgemäß, richtig, korrekt
corrective maintenance	Instandsetzung
correctness	Korrektheit
cross monitoring	wechselseitige Überwachung
dangerous failure	gefährbringender Ausfall
dangerous failure on demand	gefährbringender Ausfall bei Anforderung
dangerous failure rate	Rate gefährbringender Ausfälle
data	Daten
data driven categories	datengesteuerte Kategorien
data driven system	datengesteuertes System
data failure	Datenfehler
data logging system	Datenaufzeichnungssystem
decommissioning	Außerbetriebnahme
demand mode	Anforderungsbetriebsart
demand rate	Anforderungsrate
demonstrate	darlegen, auch zeigen, nachweisen
dependent failure	abhängiger Ausfall
design	Entwurf
design review	Entwurfsüberprüfung
detected	erkannt
diagnostic coverage (DC)	Diagnosedeckungsgrad
diagnostic test interval	Diagnose-Testintervall
diagnostic test rate	Diagnose-Testrate
diagnostics	Diagnose
disposal	Ausmusterung
disturbance level	Störgrade
diversity	Diversität
domain specific specification	fachspezifische Spezifikation
dynamic testing	dynamisches Testen nicht dynamisches Prüfen
E/E/PE design requirements specification	Spezifikation der E/E/PE-Entwurfsanforderungen
E/E/PE device	E/E/PE-Gerät
E/E/PE safety functions requirements specification	Spezifikation der Anforderungen an die E/E/PE-Sicherheitsfunktionen
E/E/PE safety-related system	sicherheitsbezogenes E/E/PE-System
E/E/PE safety-related system design documentation	Dokumentation des Entwurfs des sicherheitsbezogenen E/E/PE-Systems
E/E/PE safety-related system operation and maintenance procedures	Betriebs- und Instandhaltungsverfahren für das sicherheitsbezogene E/E/PE-System
E/E/PE system ...	... des E/E/PE-Systems
E/E/PE system application engineering	Anwendungengineering des Systems
E/E/PE system design and development verification	Verifikation des Entwurfs und der Entwicklung des E/E/PE-Systems
E/E/PE system design requirements	Anforderungen an den Entwurf des E/E/PE-Systems

E/E/PE system design requirements specification	Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems
E/E/PE system functional safety assessment	Beurteilung der funktionalen Sicherheit des E/E/PE-Systems
E/E/PE system installation, commissioning, operation and maintenance procedures	Installations-, Inbetriebnahme-, Betriebs- und Instandhaltungsverfahren für das E/E/PE-System
E/E/PE system integration test plan	Plan der Integrationstests des E/E/PE-Systems
E/E/PE system integration verification	Verifikation der Integration des E/E/PE-Systems
E/E/PE system operation and maintenance procedures	Betriebs- und Instandhaltungsverfahren für das E/E/PE-System
E/E/PE system safety function description	Beschreibung der Sicherheitsfunktion des E/E/PE-Systems
E/E/PE system safety functions requirements specification	Spezifikation der Anforderungen an die Sicherheitsfunktionen des E/E/PE-Systems
E/E/PE system safety integrity description	Beschreibung der Sicherheitsintegrität des E/E/PE-Systems
E/E/PE system safety integrity requirements specification	Spezifikation der Anforderungen an die Sicherheitsintegrität des E/E/PE-Systems
E/E/PE system safety lifecycle	Sicherheitslebenszyklus des E/E/PE-Systems
E/E/PE system safety lifecycle phases	Phasen des Sicherheitslebenszyklus des E/E/PE-Systems
E/E/PE system safety lifecycle requirements	Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems
E/E/PE system safety requirements specification	Spezifikation der Anforderungen an die Sicherheit des E/E/PE-Systems
E/E/PE system safety validation	Validierung der Sicherheit des E/E/PE-Systems
E/E/PE system safety validation planning	Planung der Validierung der Sicherheit des E/E/PE-Systems
E/E/PE system safety validation testing	Tests zur Validierung der Sicherheit des E/E/PE-Systems
E/E/PE system verification planning	Planung der Verifikation des E/E/PE-Systems
electrical/electronic/programmable electronic (E/E/PE)	elektrisch/elektronisch/programmierbar elektronisch (E/E/PE)
electrical/electronic/programmable electronic (E/E/PE) safety-related system	Sicherheitsbezogenes elektrisches/elektronisches/programmierbar elektronisches (E/E/PE) System
electrical/electronic/programmable electronic system (E/E/PES)	elektrisch/elektronisch/programmierbar elektronisches System (E/E/PES)
element (hardware element / software element)	Element
element safety function	Elementsicherheitsfunktion
embedded software	Embedded-Software
encapsulation of domain knowledge	Kapselung des Fachwissens
entity	Einheit
environment	Umgebung
equipment	Einrichtung, Betriebsmittel
equipment under control (EUC)	die EUC-Einrichtung
error	Abweichung
error probability	Fehlerwahrscheinlichkeit
EUC control system	EUC-Leit- oder Steuerungssystem
EUC risk	EUC-Risiko
exposure time	Aufenthaltsdauer
factory acceptance testing (FAT)	Werksendprüfung
fail safe	Fail-safe
fail safe concept	Fail-safe-Konzept
failure	Ausfall, aber bei Software failure = Versagen
failure assertion programming	Assertion-Programmierung (en: failure assertion programming)

failure mode	Ausfallart
failure rate	Ausfallrate
fault	Fehler
fault avoidance	Fehlervermeidung
fault tolerance	Fehlertoleranz
fault tree analysis (FTA)	Fehlerbaumanalyse (FTA)
faults control	Fehlerbeherrschung
feature (bei SW)	Eigenschaft
field programmable gate array (FPGA)	feldprogrammierbare Gatterlogik (FPGA)
final element synonym mit actuator	Stellglied synonym mit Aktor
fixed program language (FPL)	feste Programmiersprache
FMEA/failure modes and effects analysis	FMEA
forward traceability	Vorwärtsverfolgbarkeit
frequency	Häufigkeit
frequency of demands	Häufigkeit von Anforderungen
full custom ASIC	vollständig kundenspezifisches/r ASIC
full variability language (FVL)	Programmiersprache mit vollem Sprachumfang
functional safety	funktionale Sicherheit
functional safety assessment	Beurteilung der funktionalen Sicherheit
functional safety audit	Audit der funktionalen Sicherheit
functional safety planning	Planung der funktionalen Sicherheit
functional unit	Funktionseinheit
gate array	Gatterlogik
hardware (HW)	Hardware
hardware fault tolerance (HFT)	Hardware-Fehlertoleranz
hardware fault tolerance requirements	Anforderungen zur Fehlertoleranz der Hardware
hardware safety integrity	Sicherheitsintegrität der Hardware
hardware safety integrity level requirements	Anforderungen zum Sicherheits-Integritätslevel der Hardware
hardware safety integrity requirements	Anforderungen an die Sicherheitsintegrität der Hardware
harm	Schaden
harmful event	Schadensereignis
hazard	Gefährdung
hazard & risk analysis (H & RA)	Gefährdungs- und Risikoanalyse
hazardous event	Gefährlicher Vorfall
hazardous event rate (tolerable ...)	(tolerierbare) Rate gefährlicher Vorfälle
hazardous situation	Gefährdungssituation
high demand mode	Betriebsart mit hoher Anforderungsrate
high demand or continuous mode of operation	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung
human error	menschliches Versagen
human machine interface (HMI)	Mensch-Maschine-Schnittstelle
human reliability analysis (HRA)	Analyse menschlicher Zuverlässigkeit
immunity level	Störfestigkeit
impact analysis	Einflussanalyse
independent department	unabhängige Abteilung
independent organisation	unabhängige Organisation
independent person	unabhängige Person
independent protection layer	unabhängige Schutzebene
installation	Anlage, Errichtung
instantaneous availability	momentane Verfügbarkeit
instantaneous unavailability	momentane Nichtverfügbarkeit

International Electrotechnical Vocabulary (IEV)	Internationales Elektrotechnisches Wörterbuch
limited variability configuration	eingeschränkte Möglichkeiten der Konfiguration
Limited variability language (LVL)	Programmiersprache mit eingeschränktem Sprachumfang
logic system, logic solver	Logiksystem
low demand mode	Betriebsart mit niedriger Anforderungsrate
low demand mode of operation	Betriebsart mit niedriger Anforderungsrate
low-complexity E/E/PE safety-related system	einfaches E/E/PE-sicherheitsbezogenes System
maintenance	Instandhaltung bei Software „Pflege“
malevolent or unauthorised action	böswillige oder nicht autorisierte Handlung
management of functional safety	Management der funktionalen Sicherheit
mean down time	mittlere Ausfalldauer
mean repair time	mittlere Reparaturdauer
mean time to restoration	mittlere Dauer bis zur Wiederherstellung
mean up time	mittlere ausfallfreie Betriebsdauer
mission time	Gebrauchsdauer
mitigation	Schadensbegrenzungsmaßnahmen
mode of operation	Betriebsart
modification	Modifikation
modify	modifizieren
modular approach	modularer Ansatz
module	Baugruppe bei Hardware Modul bei Software
necessary risk reduction	notwendige Risikominderung
no effect failure	Ausfall ohne Auswirkung
no part failure	Ausfall eines unbeteiligten Bauteils
non-programmable Programmable electronics (NPPE)	nicht programmierbar
notation	Aufzeichnungsart
objective acceptance criteria	objektive Akzeptanzkriterien
objective evidence	Nachweis nicht objektiver Nachweis
off-the-shelf dedicated-function product	handelsübliches Produkt mit vorgegebener Funktion
one out of N (1ooN)	Eins-aus-N (1ooN)
on-line	während des Betriebs
operational profile	Betriebsanforderungen
operator	Bediener
other risk reduction measure	andere risikomindernde Maßnahmen
overall safety function	Gesamtsicherheitsfunktion
overall safety lifecycle	Gesamt-Sicherheitslebenszyklus
overall safety lifecycle requirements	Anforderungen zum Gesamt-Sicherheitslebenszyklus
overall safety requirements allocation	Zuordnung der Anforderungen an die Gesamtsicherheit
overall safety validation	Validierung der Gesamtsicherheit
overt synonym zu detected	erkannt
performance requirements	Anforderungen an die Leistungsfähigkeit
PFD	siehe unter „Average probability of failure on demand (PFDavg)“
pre-existing software	bereits existierende Software
previous use	vorherige Verwendung
probability of dangerous failure on demand (PFD)	Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung (PFD)
probability of dangerous failure per hour (PFH)	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH)
probability of failure	Ausfallwahrscheinlichkeit
process industry	Prozessindustrie
process safety time	Prozesssicherheitszeit

programmable electronic	programmierbar elektronisch (PE) oder programmierbare Elektronik (PE)
programmable electronic system (PES)	programmierbares elektronisches System (PES)
programmable logic controller (PLC) =PC= Programmable Controller (61131)	speicherprogrammierbare Steuerungen (SPS)
programmable logic device (PLD)	programmierbarer Logikbaustein (PLD)
proof test	Wiederholungsprüfung
proof test interval	Intervall für die Wiederholungsprüfung
properties of software lifecycle phases	Eigenschaften der Softwarelebenszyklusphasen
proprietary configuration language	proprietäre Konfigurationssprache
proven in use (element)	betriebsbewährt
random hardware failure	zufälliger Hardwareausfall
reasonably foreseeable misuse	vernünftigerweise vorhersehbare Fehlanwendung
redundancy	Redundanz
reliability	Zuverlässigkeit
reliability block diagram	Zuverlässigkeitsblockdiagramm
required target failure measures	erforderliche Ausfallgrenzwerte
requirements for the avoidance of failures	Anforderungen zur Vermeidung von Ausfällen
requirements for the control of systematic faults	Anforderungen zur Beherrschung von systematischen Fehlern
requirements specification	Spezifikation der Anforderungen
requirements specification for the system and the software	Spezifikation der Anforderungen an das System und an die Software
residual risk	Restrisiko
retrofit	Nachrüstung
re-verification	Neuverifikation
review	Überprüfung
risk	Risiko
risk reduction	Risikominderung
route	Pfad
safe failure	ungefährlicher Ausfall
safe failure fraction (SFF)	Anteil sicherer Ausfälle (SFF)
safe state	sicherer Zustand
safety	Sicherheit
safety bag techniques	"externe Überwachungseinrichtungen"
safety function	Sicherheitsfunktion
safety function description	Beschreibung der Sicherheitsfunktion
safety functions requirements specification	Spezifikation der Anforderungen an die Sicherheitsfunktionen
safety instrumented function (SIF)	sicherheitstechnische Funktion
safety instrumented system (SIS)	das sicherheitstechnische System, das SIS
safety integrity	Sicherheitsintegrität
safety integrity description	Beschreibung der Sicherheitsintegrität
safety integrity level (SIL)	der Sicherheits-Integritätslevel
safety integrity level requirements	Anforderungen an den Sicherheits-Integritätslevel
safety integrity requirements specification	Spezifikation der Anforderungen an die Sicherheitsintegrität
safety lifecycle	Sicherheitslebenszyklus
safety manual for compliant items	Sicherheitshandbuch für konforme Objekte
safety performance	sicherheitstechnische Leistungsfähigkeit
safety requirements	Anforderungen an die Sicherheit
safety requirements specification	Spezifikation der Anforderungen an die Sicherheit
safety unavailability	sicherheitsbezogene Nichtverfügbarkeit
safety validation	Validierung der Sicherheit

safety validation of the E/E/PE safety-related systems	Validierung der Sicherheit der sicherheitsbezogenen E/E/PE-Systeme
safety-related software	sicherheitsbezogene Software
safety-related system	sicherheitsbezogenes System
security policy	IT-Sicherheitsregeln
security service	IT-Sicherheitsdienste
selfhealing	Selbstheilung
shut down	Abschaltung
site acceptance test (SAT)	Vor-Ort-Abnahme
smart instrument	intelligentes Feldgerät
soft-error	Soft-Error
software	Software
software compliant item	konformes Softwareobjekt
software configuration management	Software-Konfigurationsmanagement
software design lifecycle	Software-Entwicklungslebenszyklus
software element	Softwareelement
software failure	Softwareversagen
software failure	Softwareversagen
software lifecycle	Softwarelebenszyklus
software modification	Softwaremodifikation
software module	Softwaremodul
software module size	Softwaremodulgröße
software off-line support tool	Offline-Softwarewerkzeug
software on-line support tool	Online-Softwarewerkzeug
software programming language	Software-Programmiersprache
software requirements specification	Spezifikation der Anforderungen an die Software
software safety	Softwaresicherheit
software safety function	Funktion der Software bezüglich der Sicherheit
software safety integrity	Sicherheitsintegrität der Software
software safety integrity level	Software-Sicherheits-Integritätslevel
software safety lifecycle	Software-Sicherheitslebenszyklus
software safety requirements	Anforderungen an die Sicherheit der Software
software safety requirements specification	Spezifikation der Anforderungen an die Sicherheit der Software
software safety validation planning	Planung der Validierung der Sicherheit der Software
software systematic capability	systematische Eignung der Software
software tool	Softwarewerkzeug
source code	Source-Code
specification for the overall safety requirements	Spezifikation der Anforderungen an die Gesamtsicherheit
specification of the system requirements	Spezifikation der Anforderungen an das System
spurious action	Fehlauslösung
stateless design	zustandsloser Entwurf
subsystem	Teilsystem
system requirements	Anforderungen an das System
system requirements specification	Spezifikation der Anforderungen an das System
system software	Systemsoftware
systematic capability	systematische Eignung
systematic failure	systematischer Ausfall, systematisches Versagen (bei Software)
systematic fault	systematischer Fehler
systematic safety integrity	systematische Sicherheitsintegrität
target failure measure	Ausfallgrenzwert

target hardware safety integrity	Zielwert der Sicherheitsintegrität der Hardware
target risk	Grenzrisiko
test harness	Prüfeinrichtung
test performance criteria	Prüfschärfegrade
tolerable risk	tolerierbares Risiko
tool	Werkzeug (auch Software)
total average failure rate	mittlere Gesamtausfallrate
transmission error (bei Kommunikationssystemen)	Übertragungsfehler
undetected, unrevealed	unerkannt
use	Verwendung nicht Gebrauch
useful lifetime	Gebrauchsdauer
validation	Validierung
verification	Verifikation
voter	Mehrheitsentscheider, auch Ausgangsvergleicher
vulnerability analysis	Gefährdungsanalyse
vulnerability analysis	Schwachstellenanalyse
wrapper	Schutzmechanismus

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 4: Begriffe und Abkürzungen
(IEC 61508-4:2010)

Functional safety of
electrical/electronic/programmable electronic
safety-related systems –
Part 4: Definitions and abbreviations
(IEC 61508-4:2010)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité –
Partie 4: Définitions et abréviations
(CEI 61508-4:2010)

Diese Europäische Norm wurde von CENELEC am 2010-05-01 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

© 2010 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61508-4:2010 D

Vorwort

Der Text des Schriftstücks 65A/551/FDIS, zukünftige 2. Ausgabe von IEC 61508-4, ausgearbeitet von dem SC 65A „System aspects“ des IEC/TC 65 „Industrial-process measurement, control and automation“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2010-05-01 als EN 61508-4 angenommen.

Diese Europäische Norm ersetzt EN 61508-4:2001.

Sie ist eine Sicherheits-Grundnorm nach IEC-Guide 104.

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): 2011-02-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2013-05-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61508-4:2010 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

[1] IEC 61511 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 61511 (nicht modifiziert).
[2] IEC 62061:2005	ANMERKUNG	Harmonisiert als EN 62061:2005 (nicht modifiziert).
[3] IEC 61800-5-2	ANMERKUNG	Harmonisiert als EN 61800-5-2.
[4] IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 (nicht modifiziert).
[5] IEC 61508-6:2010	ANMERKUNG	Harmonisiert als EN 61508-6:2010 (nicht modifiziert).
[6] IEC 61508-7:2010	ANMERKUNG	Harmonisiert als EN 61508-7:2010 (nicht modifiziert).
[8] IEC 61131-3:2003	ANMERKUNG	Harmonisiert als EN 61131-3:2003 (nicht modifiziert).
[10] ISO 8402:1994	ANMERKUNG	Harmonisiert als EN ISO 8402:1995 (nicht modifiziert).
[11] IEC 60601 Reihe	ANMERKUNG	Harmonisiert in der Reihe EN 60601 (teilweise modifiziert).
[14] IEC 61508-1:2010	ANMERKUNG	Harmonisiert als EN 61508-1:2010 (nicht modifiziert).
[15] IEC 61508-2:2010	ANMERKUNG	Harmonisiert als EN 61508-2:2010 (nicht modifiziert).
[16] IEC 61508-3:2010	ANMERKUNG	Harmonisiert als EN 61508-3:2010 (nicht modifiziert).
[18] ISO 9000:2005	ANMERKUNG	Harmonisiert als EN ISO 9000:2005 (nicht modifiziert).

Inhalt

	Seite
Anhang NC (informativ) Fachwörterliste mit Benennungen aus den Normen der Reihe IEC 61508.....	5
Vorwort.....	2
Einleitung	4
1 Anwendungsbereich	6
2 Normative Verweisungen	8
3 Begriffe und Abkürzungen	8
3.1 Sicherheitsbezogene Begriffe.....	9
3.2 Einrichtungen und Geräte.....	11
3.3 Systeme – allgemeine Aspekte	16
3.4 Systeme – sicherheitsbezogene Aspekte	18
3.5 Sicherheitsfunktionen und Sicherheitsintegrität	20
3.6 Fehler, Ausfall und Abweichung (siehe Bild 4).....	23
3.7 Lebenszyklustätigkeiten	30
3.8 Bestätigung von Sicherheitsmaßnahmen.....	31
Stichwortverzeichnis	36
Literaturhinweise.....	40
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	42
Bilder	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508.....	7
Bild 2 – Programmierbares elektronisches System.....	16
Bild 3 – Elektrisch/elektronisch/programmierbares elektronisches System (E/E/PE-System) – Struktur und Begriffe.....	17
Bild 4 – Ausfallmodell.....	25
Tabelle	
Tabelle 1 – In dieser Norm verwendete Abkürzungen	8

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Elementen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in den meisten Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) 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 diese 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 programmierbaren elektronischen (E/E/PE) Elementen bestehen 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 produkt- und anwendungsspezifischen internationalen Normen, die auf der Normenreihe IEC 61508 basieren, zu erleichtern.

ANMERKUNG 1 In den Literaturhinweisen sind Beispiele von produkt- und anwendungsspezifischen internationalen Normen, die auf der Normenreihe IEC 61508 basieren, enthalten (siehe Hinweise [1], [2] und [3]).

In den meisten Situationen wird Sicherheit durch eine Anzahl von Systemen 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, welche die Gesamtheit von sicherheitsbezogenen Systemen bilden. Daher kann diese Internationale Norm, obwohl sie sich mit sicherheitsbezogenen E/E/PE-Systemen beschäftigt, auch einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme basierend auf anderen Technologien betrachtet werden können.

Es ist beachtet worden, dass eine große Vielfalt von Anwendungen in vielfältigen Anwendungsbereichen vorliegt, die sicherheitsbezogene E/E/PE-Systeme verwenden, und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdecken. 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 produkt- und anwendungsspezifischen internationalen Normen und in Überarbeitungen der bereits bestehenden Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme 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 produkt- und anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung produkt- und anwendungsspezifischer Internationaler Normen sollte innerhalb des Rahmens dieser 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 Anforderungen an die Sicherheit, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen,
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen an die Sicherheitsintegrität bestimmt werden können;

- führt Sicherheits-Integritätslevel für die Festlegung der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen ein, die von den sicherheitsbezogenen E/E/PE-Systemen zu implementieren sind;

ANMERKUNG 2 Diese Norm legt weder die Anforderungen an den Sicherheits-Integritätslevel für irgendeine Sicherheitsfunktion fest, noch bestimmt sie, wie der Sicherheits-Integritätslevel festgelegt wird. Stattdessen stellt sie einen risikobasierenden konzeptionellen Rahmen und Beispielverfahren bereit.

- legt Ausfallgrenzwerte für die von den sicherheitsbezogenen E/E/PE-Systemen auszuführenden Sicherheitsfunktionen fest, die mit den Sicherheits-Integritätsleveln verbunden sind,
- legt eine untere Grenze für die Ausfallgrenzwerte für eine Sicherheitsfunktion fest, die von einem einzelnen sicherheitsbezogenen E/E/PE-System ausgeführt wird. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze bei einer mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung von 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen Anforderungsrate oder mit kontinuierlicher Anforderung betrieben werden, ist die untere Grenze bei einer mittleren Häufigkeit eines gefahrbringenden Ausfalls von $10^{-9} [h^{-1}]$ festgelegt,

ANMERKUNG 3 Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht notwendigerweise eine einkanalige Architektur.

ANMERKUNG 4 Es kann für einfache Systeme möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigeren Zielwerten für die Sicherheitsintegrität zu erreichen, aber diese Grenzen werden als das betrachtet, was für relativ komplexe Systeme (zum Beispiel sicherheitsbezogene programmierbare elektronische Systeme) gegenwärtig erreicht werden kann.

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrungen und Urteilsvermögen beruhen, die durch praktische Erfahrung in der Industrie gewonnen wurden. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- führt die systematische Eignung ein, die für ein Element im Hinblick auf das Vertrauen gilt, dass die systematische Sicherheitsintegrität die Anforderungen des festgelegten Sicherheits-Integritätslevels erfüllt;
- lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht ausdrücklich das Fail-Safe-Konzept. „Fail-Safe“-Konzepte und „inhärent sichere“ Prinzipien können jedoch anwendbar sein, und der Einsatz solcher Konzepte ist zulässig, vorausgesetzt, dass die Anforderungen der zutreffenden Abschnitte in der Norm erfüllt werden.