SLOVENSKI STANDARD

SIST EN ISO 13849-1:2008

01-oktober-2008

Nadomešča:

SIST EN ISO 13849-1:2007

Varnost strojev - Z varnostjo povezani deli krmilnih sistemov - 1. del: Splošna načela za načrtovanje (ISO 13849-1:2006)

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006)

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception (ISO 13849-1:2006)

Ta slovenski standard je istoveten z: **EN ISO 13849-1:2008**

ICS:

13.110	Varnost strojev	Safety of machinery

SIST EN ISO 13849-1:2008 **en**

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO 13849-1

Juni 2008

ICS 13.110

Ersatz für EN ISO 13849-1:2006

Deutsche Fassung

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006)

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception (ISO 13849-1:2006)

Diese Europäische Norm wurde vom CEN am 18.Mai 2008 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzen Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

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

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, 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.

EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

Inhalt

Seite

Vorwort

Der Text von ISO 13849-1:2006 wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery" der Internationalen Organisation für Standardisierung (ISO) erarbeitet und wurde als EN ISO 13849-1:2008 vom Technischen Komitee CEN/TC 114 „Safety of machinery" übernommen, dessen Sekretariat vom DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2008, und etwaige entgegenstehende nationale Normen müssen bis November 2009 zurückgezogen werden.

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

Dieses Dokument ersetzt EN ISO 13849-1:2006.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben, und unterstützt grundlegende Anforderungen der EG-Richtlinien.

Zum Zusammenhang mit EG-Richtlinien siehe informativen Anhang ZA und ZB, der Bestandteil dieses Dokuments ist.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 13849-1:2006 wurde vom CEN als EN ISO 13849-1:2008 ohne irgendeine Abänderung genehmigt.

Einleitung

Die Struktur von Sicherheitsnormen auf dem Gebiet der Maschinen ist wie folgt.

a) Typ-A-Normen (Sicherheitsgrundnormen) behandeln Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die auf Maschinen angewandt werden können.

b) Typ-B-Normen (Sicherheitsfachgrundnormen) behandeln einen Sicherheitsaspekt oder eine Art von Schutzeinrichtungen, die für eine ganze Reihe von Maschinen verwendet werden können:

   — Typ-B1-Normen für bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Lärm);

   — Typ-B2-Normen für Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen, druckempfindliche Schutzeinrichtungen, trennende Schutzeinrichtungen).

c) Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen an eine bestimmte Maschinen oder eine Gruppe von Maschinen.

Dieser Teil der ISO 13849 ist eine Typ-B1-Norm wie in ISO 12100-1 dargelegt.

Wenn sich die Bestimmungen einer Typ-C-Norm von denen unterscheiden, die in einer Typ-A- oder Typ-B-Norm dargelegt sind, haben die Bestimmungen der Typ-C-Norm Vorrang vor anderen Normen für Maschinen, die nach den Bestimmungen der Typ-C-Norm entworfen und hergestellt worden sind.

Mit diesem Teil der ISO 13849 ist beabsichtigt, für diejenigen einen Leitfaden zu geben, die an der Gestaltung und Beurteilung von Steuerungen beteiligt sind und für Technische Komitees, die Typ-B2- und Typ-C-Normen erarbeiten, mit der Vermutung, mit den wesentlichen Sicherheitsanforderungen des Anhangs I der Maschinenrichtlinie 98/37/EG, der Maschinen-Richtlinie, übereinzustimmen. Sie gibt keine besondere Anleitung zur Übereinstimmung mit anderen EG-Richtlinien.

Als Teil einer Gesamtrisikominderung an einer Maschine wird ein Konstrukteur oft Maßnahmen durch die Anwendung von Schutzeinrichtungen zur Risikoreduzierung ergreifen, die eine oder mehrere Sicherheitsfunktionen verwenden.

Teile einer Maschinensteuerung, die Sicherheitsfunktionen liefern sollen, werden sicherheitsbezogene Teile einer Steuerung (SRP/CS) genannt, und diese Teile können entweder aus Hardware und Software bestehen und separater oder integraler Bestandteil der Maschinensteuerung sein. Zusätzlich zur Bereitstellung von Sicherheitsfunktionen kann ein SRP/CS auch Betriebsfunktionen liefern (z. B. eine Zweihandsteuerung zum Start eines Prozesses).

Die Fähigkeit sicherheitsbezogener Teile von Steuerungen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird einer von fünf Stufen zugeordnet, den so genannten Performance Level (PL). Diese Performance Level werden definiert in Form der Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (siehe Tabelle 3).

Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion hängt von mehreren Faktoren ab, einschließlich der Hardware- und Softwarestruktur, dem Umfang der Fehler-Detektionsmechanismen [Diagnosedeckungsgrad (DC)], der Zuverlässigkeit von Bauteilen [mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_d$)], den Ausfällen infolge gemeinsamer Ursache (CCF)], dem Gestaltungsprozess, der Belastung im Betrieb, den Umgebungsbedingungen und den betrieblichen Einsatzbedingungen.

Um den Konstrukteur zu unterstützen und als Hilfe zur Bestimmung des erreichten PL, stellt diese Norm eine Methode auf Basis einer Kategorisierung von Strukturen nach speziellen Entwurfskriterien und spezifiziertem Verhalten bei Fehlerbedingungen bereit. Diese Kategorien werden einer von fünf Stufen zugeordnet, genannt Kategorien B, 1, 2, 3 und 4.

Die Performance Level und Kategorien können angewendet werden für sicherheitsbezogene Teile von Steuerungen, wie:

— nicht trennende Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen), berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken), druckempfindliche Schutzeinrichtungen,

— Steuerungsbaugruppen (z. B. die Logik für Steuerungsfunktionen, Datenverarbeitung, Überwachung usw.), und

— Leistungsschaltelemente (z. B. Relais, Ventile usw.)

als auch Sicherheitsfunktionen ausführende Steuerungen in allen Arten von Maschinen — von einfachen (z. B. einer kleinen Küchenmaschine oder automatischen Türen und Toren) bis zu einer Fertigungsanlage (z. B. Verpackungsmaschinen, Druckmaschinen, Pressen).

Dieser Teil der 13849 liefert eine verständliche Basis, auf der die Gestaltung und Leistungsfähigkeit jeder Anwendung eines SRP/CS (und der Maschine) beurteilt werden kann, z. B. durch Dritte, innerhalb einer Organisation oder durch eine unabhängige Prüfstelle.

Informationen zur empfohlenen Anwendung der IEC 62061 und dieses Teils der ISO 13849

Die IEC 62061 und dieser Teil der ISO 13849 legen Anforderungen für den Entwurf und die Realisierung sicherheitsbezogener Steuerungssysteme von Maschinen fest. Der Anwender einer von beiden Normen kann in Übereinstimmung mit deren Anwendungsbereichen annehmen, die relevanten und erforderlichen Sicherheitsanforderungen zu erfüllen. Die folgende Tabelle fasst die Anwendungsbereiche der IEC 62061 und dieses Teils der ISO 13849 zusammen.

Tabelle 1 — Empfohlene Anwendung der IEC 62061 und ISO 13849-1

	Technologie für die Implementierung der sicherheitsbezogenen Steuerungsfunktion(en)	ISO 13849-1	IEC 62061
A	Nicht elektrisch, z. B. hydraulisch	X	Nicht enthalten
B	Elektromechanisch, z. B. Relais und/oder nicht komplexe Elektronik	Beschränkt auf die vorgesehenen Architekturen[a] und bis PL = e	Alle Architekturen und bis SIL 3
C	Komplexe Elektronik, z. B. programmierbar	Beschränkt auf die vorgesehenen Architekturen[a] und bis PL = d	Alle Architekturen und bis SIL 3
D	A kombiniert mit B	Beschränkt auf die vorgesehenen Architekturen[a] und bis PL = e	X[c]
E	C kombiniert mit B	Beschränkt auf die vorgesehenen Architekturen[a] und bis PL = d	Alle Architekturen und bis SIL 3
F	C kombiniert mit A, oder C kombiniert mit A und B	X[b]	X[c]

X zeigt, dass dieses Merkmal in der Norm der entsprechenden Tabellenüberschrift behandelt wird.

a Um ein einfaches Verfahren zur Berechnung des Performance Levels zu ermöglichen, sind vorgesehene Architekturen in 6.2 beschrieben.

b Für komplexe Elektronik: Verwendung der vorgesehenen Architekturen nach diesem Teil der ISO 13849 bis PL = d oder irgendeine Architektur nach IEC 62061.

c Für nicht elektrische Technologie, Verwendung der Teile nach diesem Teil der ISO 13849 als Teilsysteme.

1 Anwendungsbereich

Dieser Teil der ISO 13849 stellt Sicherheitsanforderungen und einen Leitfaden für die Prinzipien der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS) bereit, einschließlich der Entwicklung von Software. Für diese Teile der SRP/CS werden Eigenschaften, einschließlich des Performance Levels, festgelegt, die zur Ausführung der entsprechenden Sicherheitsfunktionen erforderlich sind. Er ist anzuwenden auf SRP/CS aller Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch usw.).

Er legt nicht fest, welche Sicherheitsfunktionen oder Performance Level für einen speziellen Fall verwendet werden.

Dieser Teil der ISO 13849 stellt spezielle Anforderungen für SRP/CS mit programmierbar elektronischen Systemen bereit.

Er stellt keine speziellen Anforderungen an den Entwurf von Produkten, die Teile von SRP/CS sind. Trotzdem können die angegebenen Prinzipien, wie Kategorien oder Performance Level, verwendet werden.

ANMERKUNG 1 Beispiele von Produkten, die Teile von SRP/CS sind: Relais, Magnetventile, Positionsschalter, PLC(en), Antriebssteuerungen, Zweihandschaltungen, druckempfindliche Schutzeinrichtungen. Für den Entwurf solcher Produkte ist es wichtig, sich auf spezielle anwendbare Internationale Normen zu beziehen, z. B. ISO 13851, ISO 13856-1 und ISO 13856-2.

ANMERKUNG 2 Für die Definition des *erforderlichen Performance Levels,* siehe 3.1.24.

ANMERKUNG 3 Die in diesem Teil der ISO 13849 bereitgestellten Anforderungen für programmierbare elektronische Systeme sind kompatibel mit der Methodik für Gestaltung und Entwicklung sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungen für Maschinen in der IEC 62061.

ANMERKUNG 4 Für sicherheitsbezogene Embedded-Software in Komponenten mit PL_r = e, siehe IEC 61508-3:1998, Abschnitt 7.

ANMERKUNG 5 Siehe auch Tabelle 1.

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).

ISO 12100-1:2003, *Safety of machinery —Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

ISO 12100-2:2003, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles*

ISO 13849-2:2003, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

ISO 14121[1)], *Safety of machinery — Principles of risk assessment*

IEC 60050-191:1990, *International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service* and IEC 60050-191: -am 1:1999 and IEC 60050-191-am2:2002:1999, *Amendment 1 and Amendment 2, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service*

1) Noch zu veröffentlichen (Überarbeitung von ISO 14121:1999).

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements,* and IEC 61508-3 Corr. 1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations,* and IEC 61508-4 Corr. 1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

3 Begriffe, Formelzeichen und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100-1, IEC 60050-191 und die folgenden Begriffe.

3.1.1
sicherheitsbezogenes Teil einer Steuerung
SRP/CS
Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt

ANMERKUNG 1 Die Kombination sicherheitsbezogener Teile einer Steuerung beginnt an dem Punkt, an dem sicherheitsbezogene Signale erzeugt werden (einschließlich z. B. Betätiger und Rolle eines Positionsschalters) und endet an den Ausgängen der Leistungssteuerungselemente (einschließlich z. B. Hauptkontakte eines Schützes).

ANMERKUNG 2 Werden Überwachungssysteme zur Diagnose verwendet, werden sie wie SRP/CS behandelt.

3.1.2
Kategorie
Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstandes gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, der Fehlererkennung und/oder ihrer Zuverlässigkeit

3.1.3
Fehler
Zustand einer Einheit, charakterisiert durch die Unfähigkeit, eine geforderte Funktion auszuführen, ausgenommen der Unfähigkeit während vorbeugender Wartung oder anderer geplanter Handlungen, oder aufgrund des Fehlens externer Mittel

ANMERKUNG 1 Ein Fehler ist oft das Resultat eines Ausfalls der Einheit selbst, kann aber ohne vorherigen Ausfall bestehen.

[IEC 60050-191:1990, 05-01]

ANMERKUNG 2 In diesem Teil der ISO 13849 bedeutet der Begriff „Fehler“ *zufälliger Fehler*.

3.1.4
Ausfall
Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

ANMERKUNG 1 Nach einem Ausfall hat die Einheit einen Fehler.

ANMERKUNG 2 Der „Ausfall“ ist ein Ereignis, im Unterschied zum „Fehler“, dieser ist ein Zustand.

ANMERKUNG 3 Der so definierte Begriff kann nicht angewendet werden auf Einheiten, die nur aus Software bestehen.

[IEC 60050-191:1990, 04-01]

ANMERKUNG 4 Ausfälle, die nur die Verfügbarkeit des zu steuernden Prozesses betreffen, liegen nicht im Anwendungsbereich dieses Teils der ISO 13849.

3.1.5
gefahrbringender Ausfall
Ausfall der das Potential hat, das SRP/CS in einen gefährlichen Zustand oder eine Fehlfunktion zu bringen

ANMERKUNG 1 Ob dieses Potential bemerkt werden kann oder nicht, hängt von der Architektur des Systems ab; in einem redundanten System wird ein gefährlicher Hardwareausfall weniger wahrscheinlich zu einem gefährlichen Ausfall des Gesamtsystems führen.

ANMERKUNG 2 Abgeleitet von IEC 61508-4:1998, Begriff 3.6.7.

3.1.6
Ausfall infolge gemeinsamer Ursache
CCF
Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle nicht auf gegenseitiger Ursache beruhen

[IEC 60050-191-am 1:1999, 04-23]

ANMERKUNG Ausfälle infolge gemeinsamer Ursache sollten nicht verwechselt werden mit gleichartigen Ausfällen (siehe ISO 12100-1:2003, 3.34).

3.1.7
systematischer Ausfall
Ausfall mit deterministischem Bezug zu einer bestimmten Ursache, der nur durch Änderung der Gestaltung oder des Herstellungsprozesses, Betriebsverfahren, Dokumentation oder zugehörenden Faktoren, beseitigt werden kann

ANMERKUNG 1 Instandsetzung ohne Änderung wird üblicherweise den Grund des Ausfalls nicht beseitigen.

ANMERKUNG 2 Ein systematischer Ausfall kann hervorgerufen werden durch Simulation der Ausfallursache.

[IEC 60050-191:1990, 04-19]

ANMERKUNG 3 Beispielursachen systematischer Ausfälle beinhalten menschliches Versagen in:

— der Spezifikation der Sicherheitsanforderungen,

— der Gestaltung, der Herstellung, der Installation, des Betriebs der Hardware und

— der Gestaltung, Realisierung usw. der Software.

3.1.8
Muting
vorübergehende automatische Unterdrückung einer (der) Sicherheitsfunktion(en) durch das SRP/CS

3.1.9
manuelle Rückstellung
interne Funktion des SRP/CS zum manuellen Wiederherstellen einer oder mehrerer Sicherheitsfunktionen, vor dem Neustart einer Maschine verwendet

3.1.10
Schaden
physische Verletzung oder Schädigung der Gesundheit

[ISO 12100-1:2003, 3.5]

3.1.11
Gefährdung
potentielle Schadensquelle

ANMERKUNG 1 Eine Gefährdung kann spezifiziert werden, um damit den Ursprung (z. B. mechanische Gefährdung, elektrische Gefährdung) oder die Art des zu erwartenden Schadens (z. B. Gefährdung durch elektrischen Schlag, Gefährdung durch Schneiden, Gefährdung durch Vergiftung, Gefährdung durch Feuer) näher zu bezeichnen.

ANMERKUNG 2 Die Gefährdung im Sinne dieser Definition

— ist entweder bei der bestimmungsgemäßen Verwendung der Maschine dauerhaft vorhanden (z. B. Bewegung von gefährdenden beweglichen Teilen, Lichtbogen beim Schweißen, ungesunde Körperhaltung, Geräuschemission, hohe Temperatur);

— oder kann unerwartet auftreten (z. B. Explosion, Gefährdung durch Quetschen als Folge eines unbeabsichtigten/unerwarteten Anlaufs, Herausschleudern als Folge eines Bruchs, Stürzen als Folge von Beschleunigung/Abbremsen).

[ISO 12100-1:2003, 3.6]

3.1.12
Gefährdungssituation
Sachlage, bei der eine Person mindestens einer Gefährdung ausgesetzt ist, diese Situation führt unmittelbar oder über einen Zeitraum hinweg zu einem Schaden

[ISO 12100-1:2003, 3.9]

3.1.13
Risiko
Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[ISO 12100-1:2003, 3.11]

3.1.14
Restrisiko
verbleibendes Risiko, nachdem Schutzmaßnahmen ergriffen wurden

(Siehe Bild 2)

ANMERKUNG In Anlehnung an ISO 12100-1:2003, Begriff 3.12.

3.1.15
Risikobeurteilung
Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst

[ISO 12100-1:2003, 3.13]

3.1.16
Risikoanalyse
Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der Gefährdung und Risikoeinschätzung

[ISO 12100-1:2003, 3.14]

3.1.17
Risikobewertung
auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden

[ISO 12100-1:2003, 3.16]

3.1.18
bestimmungsgemäße Verwendung einer Maschine
Verwendung einer Maschine in Übereinstimmung mit den in der Benutzerinformation bereitgestellten Informationen

[ISO 12100-1:2003, 3.22]

3.1.19
vernünftigerweise vorhersehbare Fehlanwendung
Verwendung einer Maschine in einer Weise, die vom Konstrukteur nicht vorgesehen ist, sich jedoch aus dem leicht vorhersehbaren menschlichen Verhalten ergeben kann

[ISO 12100-1:2003, 3.23]

3.1.20
Sicherheitsfunktion
Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

[ISO 12100-1:2003, 3.28]

3.1.21
Überwachung
Sicherheitsfunktion, die sicherstellt, dass eine Schutzmaßnahme eingeleitet wird, wenn die Fähigkeit eines Bauteils oder eines Elements seine Funktion auszuführen, vermindert wird oder die Betriebsbedingungen so verändert werden, dass eine Reduzierung des Betrags der Risikominderung entsteht

3.1.22
programmierbares elektronisches System
PES
System zur Steuerung, Schutz oder Überwachung, abhängig von seiner Funktion auf der Basis einer oder mehrerer programmierbarer elektronischer Geräte, einschließlich aller Elemente dieses Systems wie Stromversorgung, Sensoren und andere Eingabegeräte, Schütze und anderer Ausgabegeräte

ANMERKUNG In Anlehnung an IEC 61508-4:1998, Begriff 3.3.2.

3.1.23
Performance Level
PL
diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

ANMERKUNG Siehe 4.5.1.

3.1.24
erforderlicher Performance Level
PL_r
angewandter Performance Level (PL), um die erforderliche Risikominderung für jede Sicherheitsfunktion zu erreichen

ANMERKUNG Siehe Bilder 2 und A.1.

3.1.25
mittlere Zeit bis zum gefahrbringenden Ausfall
$MTTF_d$
Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall

ANMERKUNG In Anlehnung an IEC 62061:2005, Begriff 3.2.34.

3.1.26
Diagnosedeckungsgrad
DC
Maß für die Wirksamkeit der Diagnose, die bestimmt werden kann als Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und Ausfallrate der gesamten gefährlichen Ausfälle

ANMERKUNG 1 Der Diagnosedeckungsgrad kann für die Gesamtheit oder für Teile des sicherheitsbezogenen Systems gelten. Zum Beispiel könnte ein Diagnosedeckungsgrad für die Sensoren und/oder das Logiksystem und/oder die Stellglieder vorhanden sein.

ANMERKUNG 2 In Anlehnung an IEC 61508-4:1998, Begriff 3.8.6.

3.1.27
Schutzmaßnahme
Maßnahme zur vorgesehenen Minderung des Risikos

BEISPIEL 1 Umgesetzt vom Konstrukteur: inhärente Gestaltung, technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen, Benutzerinformation.

BEISPIEL 2 Umgesetzt vom Benutzer: durch Organisation (sichere Arbeitsverfahren, Beaufsichtigung, Betriebserlaubnis zur Ausführung von Arbeiten), Bereitstellung und Anwendung zusätzlicher Schutzeinrichtungen (persönliche Schutzausrüstung; Ausbildung).

ANMERKUNG In Anlehnung an ISO 12100-1:2003, Begriff 3.18.

3.1.28
Gebrauchsdauer
T_M
Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt

3.1.29
Testrate
r_t
Häufigkeit der automatischen Tests, um Fehler in einem SRP/CS zu bemerken, Kehrwert des Diagnose-Testintervalls

3.1.30
Anforderungsrate
r_d
Häufigkeit je Zeiteinheit von Anforderungen an eine sicherheitsbezogene Reaktion eines SRP/CS

3.1.31
Reparaturrate
r_r
Kehrwert der Zeitspanne zwischen der Erkennung eines gefahrbringenden Ausfalls, durch entweder einen Online-Test oder einer offensichtlichen Fehlfunktion des Systems, und Wiederanlauf nach System-/Bauteilaustausch.

ANMERKUNG Die Reparaturzeit beinhaltet nicht die Zeitspanne, die zur Fehlererkennung benötigt wird.

3.1.32
Maschinensteuerung
System, das auf Eingangssignale von Teilen der Maschine, des Benutzers, externer Steuerungseinrichtungen oder irgendeiner Kombination dieser, reagiert und Ausgangssignale erzeugt, damit sich die Maschine in der vorgesehenen Art und Weise verhält

ANMERKUNG Die Maschinensteuerung kann jede Technologie oder Kombination verschiedener Technologien verwenden (z. B. elektrische/elektronische, hydraulische, pneumatische, mechanische).

3.1.33
Sicherheits-Integritätslevel
SIL
diskrete Stufe (eine von vier möglichen) zur Spezifizierung der Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe und der Sicherheits-Integritätslevel 1 die niedrigste ist

[IEC 61508-4:1998, 3.5.6]

3.1.34
Programmiersprache mit eingeschränktem Sprachumfang
LVL
Typ einer Sprache, die die Fähigkeit hat, vordefinierte, anwendungsspezifische, Bibliotheksfunktionen zu kombinieren, um die Spezifikation der Sicherheitsanforderungen zu implementieren

ANMERKUNG 1 In Anlehnung an IEC 61511-1:2003, Begriff 3.2.80.1.2.

ANMERKUNG 2 Typische Beispiele von LVL (Kontaktplan, Funktions-Blockdiagramm) sind in IEC 61131-3 angegeben.

ANMERKUNG 3 Ein typisches Beispiel von einem System, das die LVL verwendet: PLC.

3.1.35
Programmiersprache mit nicht eingeschränktem Sprachumfang
FVL
Typ einer Sprache mit der Fähigkeit, einen großen Bereich von Funktionen und Anwendungen zu implementieren

BEISPIEL C, C++, Assembler.

ANMERKUNG 1 In Anlehnung an IEC 61511-1:2003, Begriff 3.2.80.1.3.

ANMERKUNG 2 Ein typisches Beispiel von Systemen für die Verwendung von FVL: Embedded-Systeme.

ANMERKUNG 3 Im Bereich der Maschinen wird FVL in Embedded-Software und gelegentlich in Anwendungssoftware eingesetzt.

3.1.36
Anwendungssoftware
Software, die speziell für die Anwendung vom Hersteller in die Maschine implementiert, und üblicherweise logische Sequenzen, Grenzwerte und Ausdrücke zum Steuern der entsprechenden Eingänge, Ausgänge, Berechnungen und Entscheidungen enthält, um die notwendigen Anforderungen des SRP/CS zu erfüllen

3.1.37
Embedded-Software
Firmware
Systemsoftware
Software, die als Teil des Systems durch den Steuerungshersteller geliefert wird und die durch den Anwender der Maschine nicht verändert werden kann

ANMERKUNG Üblicherweise wird Embedded-Software in FVL geschrieben.