

DIN EN ISO 13849-1

ICS 13.110

Entwurf

Einsprüche bis 2020-09-17
Vorgesehen als Ersatz für
DIN EN ISO 13849-1:2016-06

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1:2020);
Deutsche und Englische Fassung prEN ISO 13849-1:2020**

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design (ISO/DIS 13849-1:2020);
German and English version prEN ISO 13849-1:2020

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception (ISO/DIS 13849-1:2020);
Version allemande et anglaise prEN ISO 13849-1:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-07-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nasg@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 304 Seiten

DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG)



Nationales Vorwort

Dieses Dokument (prEN ISO 13849-1:2020) wurde vom Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen und Geräten“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche/nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 095-01-03 GA „Gemeinschaftsarbeitsausschuss NASG/NAM/DKE: Steuerungen“ im DIN-Normenausschuss Sicherheitstechnische Grundsätze (NASG).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

IEC 60204-1:2016	siehe	DIN EN 60204-1 (VDE 0113-1):2019-06
IEC 60447	siehe	DIN EN 60447 (VDE 0196)
IEC 60529	siehe	DIN EN 60529 (VDE 0470-1)
IEC 60812	siehe	DIN EN 60812
IEC 60947 (all parts)	siehe	DIN EN 60947 (alle Teile)
IEC 61000-6-7:2014	siehe	DIN EN 61000-6-7 (VDE 0839-6-7):2015-12
IEC 61078:2016	siehe	DIN EN 61078:2018-03
IEC 61131-3	siehe	DIN EN 61131-3
IEC 61300 (all parts)	siehe	DIN EN 61300-1 (VDE 0885-300) (alle Teile)
IEC 61310 (all parts)	siehe	DIN EN 61310 (VDE 0113) (alle Teile)
IEC 61326-3-1:2017	siehe	DIN EN 61326-3-1 (VDE 0843-20-3-1):2018-04
IEC 61496-1	siehe	DIN EN 61496-1 (VDE 0113-201)
IEC 61508-1:2010	siehe	DIN EN 61508-1 (VDE 0803-1):2011-02
IEC 61508-2:2010	siehe	DIN EN 61508-2 (VDE 0803-2):2011-02
IEC 61508-3:2010	siehe	DIN EN 61508-3 (VDE 0803-3):2011-02
IEC 61508-4:2010	siehe	DIN EN 61508-4 (VDE 0803-4):2011-02
IEC 61508-6:2000	siehe	DIN EN 61508-6 (VDE 0803-6):2003-06
IEC 61800-3	siehe	DIN EN 61800-3 (VDE 0160-103)

IEC 61800-5-2:2016	siehe	DIN EN 61800-5-2 (VDE 0160-105-2):2017-11
IEC 61810 (all parts)	siehe	DIN EN IEC 61810-10 (VDE 0435) (alle Teile)
IEC 62046:2018	siehe	DIN EN IEC 62046 (VDE 0113-211):2019-03
IEC 62061:2015	siehe	DIN EN 62061 (VDE 0113-50):2016-05
ISO 4413	siehe	DIN EN ISO 4413
ISO 4414	siehe	DIN EN ISO 4414
ISO 7731	siehe	DIN EN ISO 7731
ISO 9001	siehe	DIN EN ISO 9001
ISO 10218-1	siehe	DIN EN ISO 10218-1
ISO 10218-2	siehe	DIN EN ISO 10218-2
ISO 11161	siehe	DIN EN ISO 11161
ISO 12100:2010	siehe	DIN EN ISO 12100:2011-03
ISO 13849-2:2012	siehe	DIN EN ISO 13849-2:2013-02
ISO 13850	siehe	DIN EN ISO 13850
ISO 13851	siehe	DIN EN ISO 13851
ISO 13855:2010	siehe	DIN EN ISO 13855:2010-10
ISO 13856-1	siehe	DIN EN ISO 13856-1
ISO 13856-2	siehe	DIN EN ISO 13856-2
ISO 14118	siehe	DIN EN ISO 14118
ISO 14119	siehe	DIN EN ISO 14119
ISO/TR 14121-2:2012	siehe	DIN ISO/TR 14121-2:2013-02
ISO/TR 22100-2:2013	siehe	DIN ISO/TR 22100-2:2014-09
ISO/TR 23849	siehe	DIN ISO/TR 23849

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN ISO 13849-1:2016-06 wurden folgende Änderungen vorgenommen:

- a) Verweisungen überarbeitet und aktualisiert;
- b) normative Verweisungen und Begriffe und Definitionen überarbeitet;
- c) Integration eines Abschnitts zur Risikobeurteilung (Abschnitt 4);
- d) Beschreibung der Anforderungen an das Design und die verschiedenen Performance Levels (Abschnitt 6);
- e) detaillierte Anforderungen an die Spezifikation der Sicherheitsfunktion
- f) Integration eines neuen Abschnittes (7) zu Softwaresicherheit;
- g) Integration eines neuen Abschnittes (9) zu Ergonomieaspekten;
- h) detaillierte Beschreibung von Validierungsprozessen (Abschnitt 10);
- i) Integration von Anhang L zu Immunitätsanforderungen für elektromagnetische Kompatibilität;
- j) Integration von Anhang M mit zusätzlichen Informationen für das SRS-System;
- k) Integration von Anhang N zur Vermeidung von systematischen Fehlern im Software-Design.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 60204-1 (VDE 0113-1):2019-06, *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen (IEC 60204-1:2016, modifiziert); Deutsche Fassung EN 60204-1:2018*

DIN EN 60447 (VDE 0196), *Grund- und Sicherheitsregeln für die Mensch-Maschine-Schnittstelle, Kennzeichnung — Bedienungsgrundsätze*

DIN EN 60529 (VDE 0470-1), *Schutzarten durch Gehäuse (IP-Code)*

DIN EN 60812, *Analysetechniken für die Funktionsfähigkeit von Systemen — Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)*

DIN EN 60947 (alle Teile), *Niederspannungsschaltgeräte*

DIN EN 61000-6-7 (VDE 0839-6-7):2015-12, *Elektromagnetische Verträglichkeit (EMV) — Teil 6-7: Fachgrundnormen — Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind (IEC 61000-6-7:2014); Deutsche Fassung EN 61000-6-7:2015*

DIN EN 61078:2018-03, *Zuverlässigkeitsblockdiagramme (IEC 61078:2016); Deutsche Fassung EN 61078:2016*

DIN EN 61131-3, *Speicherprogrammierbare Steuerungen*

DIN EN 61300-1 (VDE 0885-300) (alle Teile), *Lichtwellenleiter*

DIN EN 61310 (VDE 0113) (alle Teile), *Sicherheit von Maschinen — Anzeigen, Kennzeichen und Bedienen*

DIN EN 61326-3-1 (VDE 0843-20-3-1):2018-04, *Elektrische Mess-, Steuer-, Regel- und Laborgeräte — EMV-Anforderungen — Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) — Allgemeine industrielle Anwendungen (IEC 61326-3-1:2017); Deutsche Fassung EN 61326-3-1:2017*

DIN EN 61496-1 (VDE 0113-201), *Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen — Teil 1: Allgemeine Anforderungen und Prüfungen*

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 1: 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 61508-4 (VDE 0803-4):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010*

DIN EN 61508-6 (VDE 0803-6):2003-06, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2000); Deutsche Fassung EN 61508-6:2001*

DIN EN 61800-3 (VDE 0160-103), *Drehzahlveränderbare elektrische Antriebe — Teil 3: EMV-Anforderungen einschließlich spezieller Prüfverfahren*

DIN EN 61800-5-2 (VDE 0160-105-2):2017-11, *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl — Teil 5-2: Anforderungen an die Sicherheit — Funktionale Sicherheit (IEC 61800-5-2:2016); Deutsche Fassung EN 61800-5-2:2017*

DIN EN 62061 (VDE 0113-50):2016-05, *Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005 + A1:2012 + A2:2015); Deutsche Fassung EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015*

DIN EN IEC 62046 (VDE 0113-211):2019-03, *Sicherheit von Maschinen — Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen (IEC 62046:2018); Deutsche Fassung EN IEC 62046:2018*

DIN EN IEC 61810-10 (VDE 0435) (alle Teile), *Elektromechanische Elementarrelais*

DIN EN ISO 4413, *Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile*

DIN EN ISO 4414, *Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile*

DIN EN ISO 7731, *Ergonomie — Gefahrensignale für öffentliche Bereiche und Arbeitsstätten — Akustische Gefahrensignale*

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 10218-1, *Industrieroboter — Sicherheitsanforderungen — Teil 1: Roboter*

DIN EN ISO 10218-2, *Industrieroboter — Sicherheitsanforderungen — Teil 2: Robotersysteme und Integration*

DIN EN ISO 11161, *Sicherheit von Maschinen — Integrierte Fertigungssysteme — Grundlegende Anforderungen*

DIN EN ISO 12100:2011-03, *Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010*

DIN EN ISO 13849-2:2013-02, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012*

DIN EN ISO 13850, *Sicherheit von Maschinen — Not-Halt-Funktion — Gestaltungsleitsätze*

DIN EN ISO 13851, *Sicherheit von Maschinen — Zweihandschaltungen — Funktionelle Aspekte und Gestaltungsleitsätze*

DIN EN ISO 13855:2010-10, *Sicherheit von Maschinen — Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (ISO 13855:2010); Deutsche Fassung EN ISO 13855:2010*

DIN EN ISO 13856-1, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schalmatten und Schalmplatten*

DIN EN ISO 13856-2, *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schalmleisten und Schalmstangen*

DIN EN ISO 14118, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf*

DIN EN ISO 14119, *Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl*

DIN ISO/TR 14121-2:2013-02, *Sicherheit von Maschinen — Risikobeurteilung — Teil 2: Praktischer Leitfaden und Verfahrensbeispiele (ISO/TR 14121-2:2012)*

DIN ISO/TR 22100-2:2014-09, *Sicherheit von Maschinen — Beziehung zu ISO 12100 — Teil 2: Wie ISO 12100 und ISO 13849-1 zusammenhängen (ISO/TR 22100-2:2013)*

DIN ISO/TR 23849, *Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen*

— Leerseite —

<i>Titel de:</i>	Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1:2020)
<i>Titel en:</i>	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (ISO/DIS 13849-1:2020)
<i>Titel fr:</i>	Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception (ISO/DIS 13849-1:2020)

Inhalt

	Seite
Europäisches Vorwort	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich	12
2 Normative Verweisungen	12
3 Begriffe	13
3.1 Begriffe	13
3.2 Symbole und Abkürzungen	22
4 Überblick	24
4.1 Anforderungen an die Risikobeurteilung und Risikominderung	24
4.2 Beitrag der Sicherheitsfunktion zur Risikominderung	26
4.3 Risikominderung mithilfe eines SRP/CS	27
4.4 Verfahren	29
4.5 Erforderliche Informationen	30
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen	30
5 Spezifikation der Sicherheitsfunktionen	31
5.1 Allgemeines	31
5.2 Spezifikation der Sicherheitsanforderungen (SRS, en: safety requirements specification)	31
5.2.1 Allgemeine Anforderungen	31
5.2.2 Zerlegung eines SRP/CS in Teilsysteme	34
5.2.3 Anforderungen an spezifische Sicherheitsfunktionen	36
5.3 Bestimmung des erforderlichen Performance Levels (PL _r) für jede Sicherheitsfunktion	41
5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen	41
6 Gestaltungsaspekte	41
6.1 Bewertung des erreichten Performance Levels PL	41
6.1.1 Allgemeine Übersicht der Performance Level PL	41
6.1.2 Zusammenhang zwischen PL und SIL	43
6.1.3 Architektur – Kategorien und deren Beziehung zur MTTF _D jedes Kanals, zum DC _{avg} und zum CCF	44
6.1.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF _D)	52
6.1.5 Diagnosedeckungsgrad (DC)	53
6.1.6 Ausfälle infolge gemeinsamer Ursache (CCF)	54
6.1.7 Systematische Ausfälle	54
6.1.8 Vereinfachtes Verfahren zur Abschätzung des PL	54
6.1.9 Alternatives Verfahren für die Bestimmung von PL und PFH _D ohne MTTF _D	56
6.1.10 Fehlerbetrachtung und Fehlerausschluss	58
6.1.11 Bewährtes Bauteil	59
6.2 Kombination von Teilsystemen zum Erreichen eines Gesamt-PL für die Sicherheitsfunktion	60
6.2.1 Allgemeines	60
6.2.2 Bekannte PFH _D -Werte	60
6.2.3 Unbekannte PFH _D -Werte	61
7 Software-Sicherheitsanforderungen	61
7.1 Allgemeines	61

7.2	Sicherheitsbezogene Embedded-Software (SRESW).....	62
7.3	Sicherheitsbezogene Anwendungssoftware (SRASW).....	64
7.4	Programmiersprache mit eingeschränktem Sprachumfang (LVL).....	67
7.4.1	Allgemeines	67
7.4.2	Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)	67
7.4.3	Entscheidung zwischen LVL oder FVL.....	68
7.5	Softwarebasierte Parametrisierung.....	69
7.5.1	Allgemeines	69
7.5.2	Einflüsse auf sicherheitsbezogene Parameter.....	70
7.5.3	Anforderungen an die softwarebasierte manuelle Parametrisierung	70
7.5.4	Verifizierung des Parametrisierungswerkzeugs.....	72
7.5.5	Ausführung der softwarebasierten manuellen Parametrisierung	72
8	Verifizierung, ob der erreichte PL dem PL _r entspricht.....	72
9	Ergonomische Aspekte der Gestaltung.....	73
10	Validierung	73
10.1	Grundsätze der Validierung	73
10.1.1	Allgemeines	73
10.1.2	Validierungsplan	75
10.1.3	Allgemeine Fehlerlisten	76
10.1.4	Spezielle Fehlerlisten.....	76
10.1.5	Angaben zur Validierung.....	76
10.2	Validierung durch Analyse.....	78
10.2.1	Allgemeines	78
10.2.2	Analysetechniken.....	78
10.3	Validierung durch Prüfung	79
10.3.1	Allgemeines	79
10.3.2	Messgenauigkeit	79
10.3.3	Zusätzliche Prüfanforderungen	80
10.3.4	Anzahl der Prüflinge	80
10.3.5	Prüfverfahren	80
10.4	Validierung der Spezifikation der Sicherheitsanforderungen (SRS)	81
10.5	Validierung der Sicherheitsfunktion	81
10.6	Validierung der Sicherheitsintegrität des SRP/CS.....	82
10.6.1	Validierung von Teilsystem(en)	82
10.6.2	Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle.....	84
10.6.3	Validierung der sicherheitsbezogenen Software	85
10.6.4	Validierung der Kombination von Teilsystemen.....	86
10.6.5	Überprüfung/Verifizierung der Sicherheitsintegrität	86
11	Instandhaltung.....	86
12	Technische Dokumentation.....	87
13	Benutzerinformation	87
13.1	Allgemeines	87
13.2	Informationen für den SRP/CS-Integrator	87
13.3	Informationen für den Benutzer.....	88
Anhang A (informativ)	Bestimmung des erforderlichen Performance Levels (PL _r)	90
A.1	Auswahl des PL _r	90
A.2	Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos	91
A.2.1	Schwere der Verletzung S1 und S2.....	91
A.2.2	Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2.....	91
A.2.3	Möglichkeit zur Vermeidung des Schadens	92
A.3	Überlagerte Gefährdungen	94