

DIN EN ISO 13849-1/A1

ICS 13.110

Einsprüche bis 2013-11-13
Vorgesehen als Änderung von
DIN EN ISO 13849-1:2008-12

Entwurf

**Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze – Änderung 1
(ISO 13849-1:2006/DAM 1:2013);
Deutsche Fassung EN ISO 13849-1:2006/prA1:2013**

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design – Amendment 1 (ISO 13849-1:2006/DAM 1:2013);
German version EN ISO 13849-1:2006/prA1:2013

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception – Amendement 1
(ISO 13849-1:2006/DAM 1:2013);
Version allemande EN ISO 13849-1:2006/prA1:2013

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-09-13 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de 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/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 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 42 Seiten

Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN
Normenausschuss Maschinenbau (NAM) im DIN

Nationales Vorwort

Dieser Änderungs-Entwurf enthält sicherheitstechnische Festlegungen.

Dieses Dokument enthält die Deutsche Fassung des vom Technischen Komitee ISO/TC 199 „Safety of machinery“ des Internationalen Komitees für Normung (ISO) in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“ des Europäischen Komitees für Normung (CEN) entsprechend der Vereinbarung zwischen dem CEN und ISO über die technische Zusammenarbeit (Wiener Vereinbarung) ausgearbeiteten Änderungs-Entwurfs A1:2013 zur EN ISO 13849-1:2008. Die Sekretariate beider Technischer Komitees werden vom DIN (Deutschland) gehalten.

Die nationalen Interessen bei der Erarbeitung dieses Dokuments wurden vom Gemeinschaftsarbeitsausschuss „Steuerungen“ (NA 095-01-03 GA) des Normenausschusses Sicherheitstechnische Grundsätze (NASG) mit dem NAM und der DKE im DIN wahrgenommen.

Es ist vorgesehen, diese Änderung bei der Veröffentlichung nicht separat, sondern als konsolidierte Fassung herauszugeben.

Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze – Änderung 1 (ISO 13849- 1:2006/DAM 1:2013)

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1 : Principes généraux de conception – Amendement 1 (ISO 13849-1:2006/DAM 1:2013)

Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design – Amendment 1 (ISO 13849-1:2006/DAM 1:2013)

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp: Änderung
Dokumentstufe: parallele Umfrage
Dokumentsprache: D

STD Version 2.5a

Inhalt

	Seite
Vorwort	3
1 Änderung zum Vorwort	4
2 Änderung zur Einleitung	4
3 Änderung zum Anwendungsbereich	4
4 Änderung zu Normative Verweisungen	4
5 Änderung zu Begriffe	5
6 Änderung zu 4 Gestaltungsaspekte	6
7 Änderung zu 5 Sicherheitsfunktionen	12
8 Änderung zu 6 Die Kategorien und deren Beziehung zur MTTF_d jedes Kanals, DC_{avg} und CCF	13
9 Änderung zu 7 Berücksichtigung von Fehlern, Fehlerausschluss	16
10 Änderung zu 9 Instandhaltung	16
11 Änderung zu 11 Benutzerinformation	16
12 Änderung zu Anhang A	17
13 Änderung zu Anhang C	19
14 Änderung zu Anhang D	24
15 Änderung zu Anhang E	25
16 Änderung zu Anhang F	25
17 Änderung zu Anhang G	27
18 Änderung zu Anhang I	27
Anhang I (informativ) Beispiele	28
Literaturhinweise	40

Vorwort

Dieses Dokument (EN ISO 13849-1:2008/prA1:2013) wurde vom Technischen Komitee ISO/TC 199 „Safety of machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 114 „Sicherheit von Maschinen“ erarbeitet, dessen Sekretariat vom DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

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

Dieses Dokument ist als Änderung zu EN ISO 13849-1:2008 vorgesehen.

Anerkennungsnotiz

Der Text von ISO 13849-1:2006/DAM 1:2013 wurde vom CEN als EN ISO 13849-1:2008/prA1:2013 ohne irgendeine Abänderung genehmigt.

1 Änderung zum Vorwort

Letzter Absatz:

Die Verweisung „ISO 13849-100“ ist zu streichen, da der Teil 100 zurückgezogen wurde.

2 Änderung zur Einleitung

Absatz nach der Auflistung:

Die Verweisung „ISO 12100-1“ ist durch „ISO 12100“ zu ersetzen.

Fünfter Absatz:

Die Verweisung „Maschinenrichtlinie 98/37/EG, der Maschinen-Richtlinie“ ist durch „Richtlinie 2006/42/EG über Maschinen“ zu ersetzen.

Tabelle 1 und der Absatz vor Tabelle 1:

Tabelle 1 und der Absatz vor der Tabelle 1 sind durch folgenden Absatz zu ersetzen:

„Die IEC 62061 und dieser Teil der ISO 13849 legen Anforderungen für den Entwurf und die Realisierung sicherheitsbezogener Steuerungen von Maschinen fest. Durch die Anwendung einer der beiden Internationalen Normen kann in Übereinstimmung mit deren Anwendungsbereichen angenommen werden, dass die relevanten und erforderlichen Sicherheitsanforderungen erfüllt sind. ISO/TR 23849 enthält Hinweise zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen.“

Der folgende neue Tabellentitel ist nach diesem neuen Absatz zu ergänzen, um eine neue Benummerung aller Tabellen und deren Verweise zu vermeiden:

„Tabelle 1 — gestrichen“

3 Änderung zum Anwendungsbereich

Die ANMERKUNG 5 ist durch folgende neue ANMERKUNG 5 zu ersetzen:

„ANMERKUNG 5 ISO 13849-1 behandelt die Betriebsart mit hoher Anforderungsrate und die Betriebsart mit kontinuierlicher Anforderungsrate.“

4 Änderung zu Normative Verweisungen

Folgende Verweisungen sind zu streichen:

„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 14121, *Safety of machinery — Principles of risk assessment“*

Folgende Verweisung ist zu ergänzen:

„ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction“*

5 Änderung zu Begriffe

3.1 Begriffe

Die Verweisung „ISO 12100-1“ ist durch „ISO 12100“ zu ersetzen.

3.1.6

In der ANMERKUNG ist die Verweisung „(siehe ISO 12100-1:2003, 3.34)“ durch „(siehe ISO 12100:2010, 3.36)“ zu ersetzen.

3.1.10

Die Quelle der Definition „[ISO 12100-1:2003, 3.5]“ ist durch „[ISO 12100:2010, 3.5]“ zu ersetzen.

3.1.11

Die Quelle der Definition „[ISO 12100-1:2003, 3.6]“ ist durch „[ISO 12100:2010, 3.6, modifiziert]“ zu ersetzen.

3.1.12

Die Quelle der Definition „[ISO 12100-1:2003, 3.9]“ ist durch „[ISO 12100:2010, 3.10]“ zu ersetzen.

3.1.13

Die Quelle der Definition „[ISO 12100-1:2003, 3.11]“ ist durch „[ISO 12100:2010, 3.12]“ zu ersetzen.

3.1.14

In der ANMERKUNG ist die Verweisung „ISO 12100-1:2003, Begriff 3.12“ durch „ISO 12100:2010, Begriff 3.13“ zu ersetzen.

3.1.15

Die Quelle der Definition „[ISO 12100-1:2003, 3.13]“ ist durch „[ISO 12100:2010, 3.17]“ zu ersetzen.

3.1.16

Die Quelle der Definition „[ISO 12100-1:2003, 3.14]“ ist durch „[ISO 12100:2010, 3.15]“ zu ersetzen.

3.1.17

Die Quelle der Definition „[ISO 12100-1:2003, 3.16]“ ist durch „[ISO 12100:2010, 3.16]“ zu ersetzen.

3.1.18

Die Quelle der Definition „[ISO 12100-1:2003, 3.22]“ ist durch „[ISO 12100:2010, 3.23]“ zu ersetzen.

3.1.19

Die Quelle der Definition „[ISO 12100-1:2003, 3.23]“ ist durch „[ISO 12100:2010, 3.24]“ zu ersetzen.

3.1.20

Die Quelle der Definition „[ISO 12100-1:2003, 3.28]“ ist durch „[ISO 12100:2010, 3.30]“ zu ersetzen.

3.1.27

In der ANMERKUNG ist die Verweisung „ISO 12100-1:2003, Begriff 3.18“ durch „ISO 12100:2010, Begriff 3.19“ zu ersetzen.

Folgender neuer **Begriff 3.1.38** ist zu ergänzen:

„3.1.38

Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderungsrate

Betriebsart, bei der die Häufigkeit der Anforderungen an SRP/CS mehr als einmal pro Jahr beträgt“

3.2 Formelzeichen und Abkürzungen

In Tabelle 2 ist Folgendes zu ergänzen:

PFH _D	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde	Tabelle 3
------------------	--	-----------

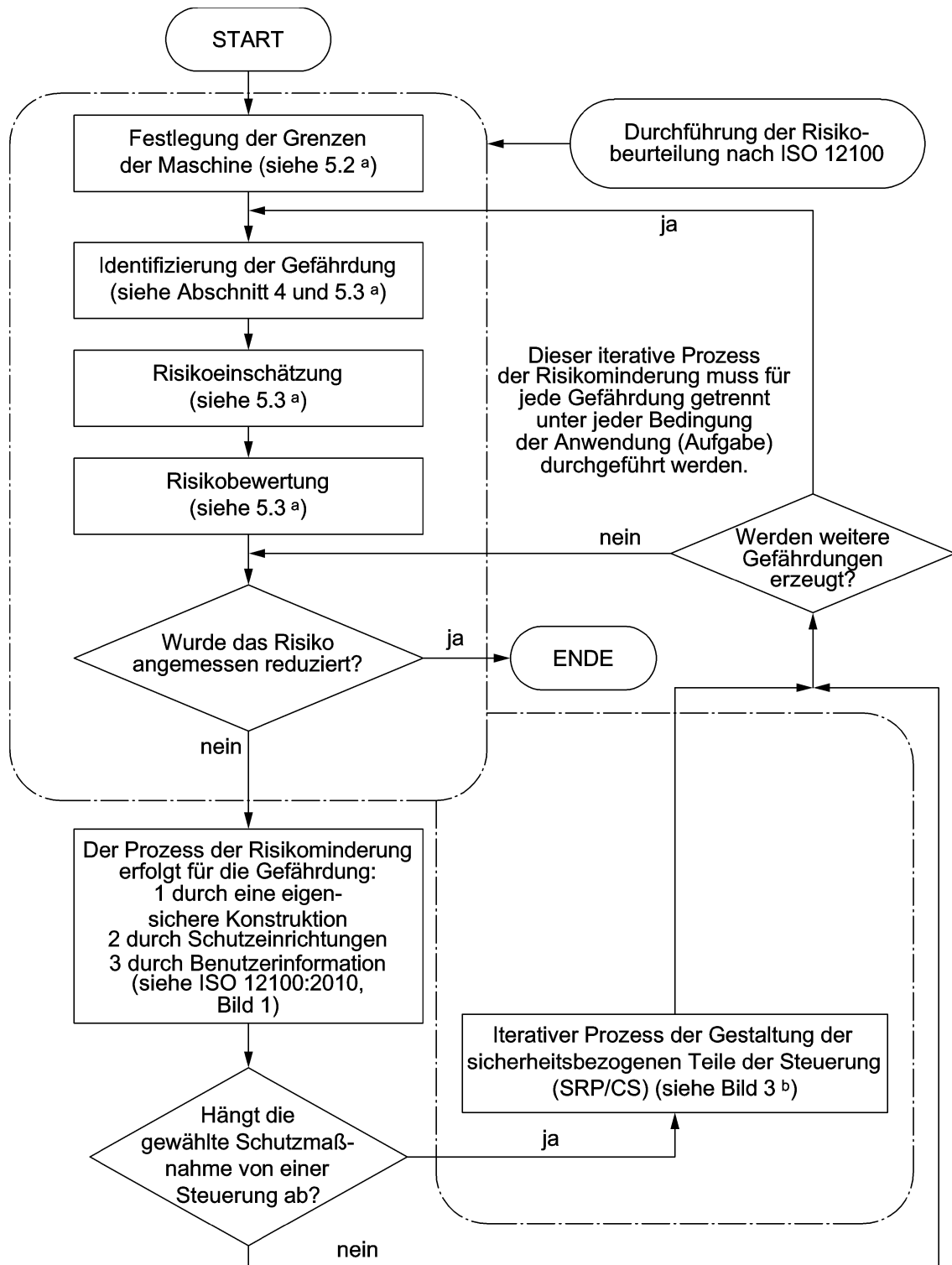
6 Änderung zu 4 Gestaltungsaspekte

4.1 Sicherheitsziele in der Gestaltung

Erster Absatz:

Die Verweisung „und ISO 14121“ im ersten Satz ist zu streichen.

Bild 1 ist durch folgendes Bild zu ersetzen (dieses neue Bild enthält keine fachlichen Änderungen sondern aktualisierte Verweisungen).



a Bezieht sich auf ISO 12100:2010.

b Bezieht sich auf diesen Teil der ISO 13849.

4.2.1 Allgemeines

Erster Absatz:

Um die Verweisungen zu aktualisieren, ist der erste Satz wie folgt zu ersetzen:

„Die Strategie zur Risikominderung an einer Maschine wird in der ISO 12100:2010, Abschnitt 6, genannt.“

Zweiter Absatz:

Um die Verweisungen zu aktualisieren, sind die drei Spiegelstriche wie folgt zu ersetzen:

”

- Beseitigung von Gefährdungen oder Risikominderung durch den Entwurf (siehe ISO 12100:2010, 6.2);
- Risikominderung durch Schutzeinrichtungen und mögliche ergänzende Schutzmaßnahmen (siehe ISO 12100:2010, 6.3);
- Risikominderung durch Bereitstellung einer Benutzerinformation über das Restrisiko (siehe ISO 12100:2010, 6.4).

“

4.2.2 Beitrag der Risikominderung durch das Steuerungssystem

Erster Absatz, vierter Satz:

Das Wort „Schutzeinrichtung“ ist durch „verriegelte trennende Schutzeinrichtung“ zu ersetzen.

Dritter Absatz, zweiter Satz:

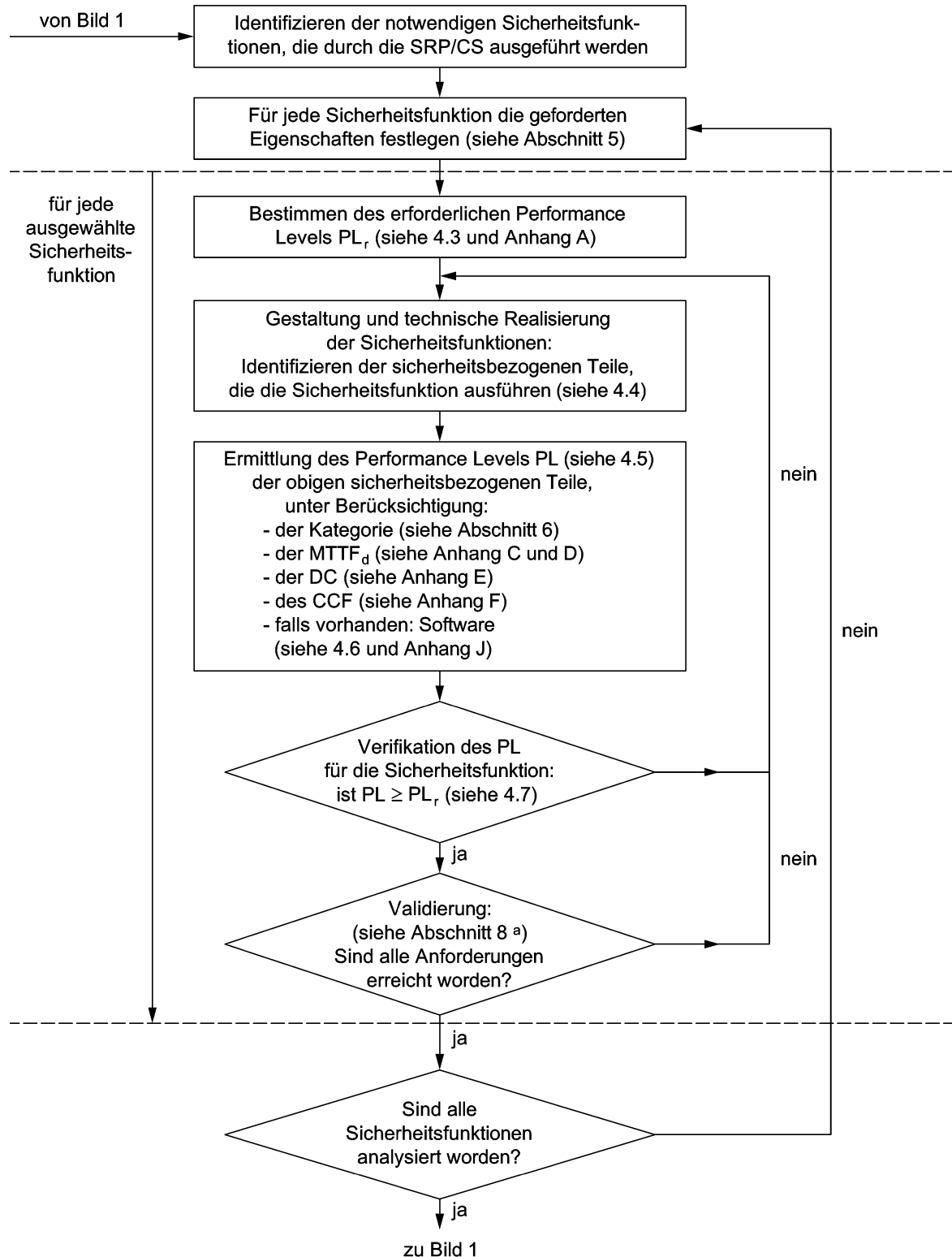
Der Satz ist in folgenden zu ändern: „Fünf Performance Level sind festgelegt, vom niedrigsten PL a bis zum höchsten PL e, mit definierten Bereichen der Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (siehe Tabelle 3).“

Vierter Absatz, nach Tabelle 3:

„(siehe ISO 14121)“ *ist durch* „(siehe ISO 12100)“ *zu ersetzen.*

Bild 3:

Die Verweisungen sind zu ändern, indem am Ende von Bild 3 „zu Bild 1 (ISO 12100)“ durch „zu Bild 1“ ersetzt wird.



^a ISO 13849-2 enthält weitere Hilfe zur Validierung.

4.5.1 Performance Level PL

ANMERKUNG 2 ist durch folgende neue ANMERKUNG 2 zu ersetzen:

„ANMERKUNG 2 Für den Entwurf komplexer Steuerungssysteme, wie PES zur Durchführung von Sicherheitsfunktionen, kann die Anwendung anderer einschlägiger Normen angemessen sein (z. B. IEC 61508 oder IEC 61496).“

Folgender neuer Absatz ist nach Tabelle 4 zu ergänzen:

„Obwohl es einen Zusammenhang zwischen den PLs der vorliegenden Norm und den SILs nach IEC 61508 und IEC 62061 gibt, ist es erlaubt, nur eine der beiden Normen anzuwenden; es ist jedoch nicht zulässig, die Anforderungen von ISO 13849-1 mit denen von IEC 61508/IEC 62061 (siehe auch ISO/TR 23849) bei der Auslegung von sicherheitsbezogenen Teilen von Steuerungen (SRP/CS) zu vermischen.“

4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF_d)

Zweiter Absatz:

Folgende neue ANMERKUNG ist zu ergänzen:

„ANMERKUNG Für eine Kombination von mehr als drei Teilsystemen (SRP/CS) in Kategorie 4, wird der Höchstwert von MTTF_d auf 2 500 Jahre für jedes Teilsystem (SRP/CS) erhöht. Dies ist darauf zurückzuführen, dass die anderen quantifizierbaren Aspekte, Struktur und DC, sich in Kategorie 4 auf ihrem Höchststand befinden, was in Kategorie 4 eine Kombination von mehr als drei Teilsystemen (SRP/CS) erlaubt und PL e nach 6.3 erreicht.“

4.5.3 Diagnosedeckungsgrad (DC)

Folgende neue ANMERKUNG ist nach Tabelle 6 zu ergänzen:

„ANMERKUNG Beispiele der Abschätzung des Diagnosedeckungsgrades (DC) sind in Anhang E enthalten.“

4.5.4 Vereinfachtes Verfahren zur Abschätzung eines PL

Die Überschrift von 4.5.4 ist durch folgende zu ersetzen:

„4.5.4 Vereinfachtes Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL (PFH_D)“

Fünfter Absatz:

Die Verweisung „(siehe auch ISO 12100-1:2003, Anhang A)“ ist durch „(siehe ISO 12100:2010, Anhang A)“ zu ersetzen.

Der dritte Spiegelstrich (Seite 26) ist durch folgenden zu ersetzen:

— für Kategorie 2, Anforderungsrate $\leq 1/100$ der Testrate; oder die Prüfung erfolgt unmittelbar nach Anforderung der Sicherheitsfunktion und die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung der Maschine in einen nicht gefahrbringenden Zustand (in der Regel wird die Maschine angehalten) ist kürzer als die Zeit zum Erreichen der Gefährdung (siehe auch ISO 13855);

Der vierte Spiegelstrich (Seite 26) ist durch folgenden zu ersetzen:

— für Kategorie 2, ist $MTTF_{d,TE}$ größer als die Hälfte der $MTTF_{d,L}$.

Siebter Absatz auf Seite 26:

Die Verweisung „(siehe auch ISO 12100-2:2003, Abschnitt 3 und IEC 60204-1:2000)“ ist durch „(siehe auch ISO 12100:2010, Abschnitt 3 und IEC 60204-1:2005)“ zu ersetzen.

4.6.2 Sicherheitsbezogene Embedded-Software (SRESW)

Die Auflistung auf Seite 29 (zweite Aufzählung in 4.6.2) ist zu ändern, indem im sechsten Spiegelstrich „Abgrenzung in nicht sicherheitsbezogene Software“ durch „Abgrenzung von nicht sicherheitsbezogener Software“ ersetzt wird.

Am Ende von 4.6.2, nach ANMERKUNG 2, ist folgender neuer Absatz zu ergänzen:

„Bauteile, für die die SRESW-Anforderungen nicht erfüllt sind, z. B. nicht sicherheitsbezogene PLCs, dürfen unter folgenden alternativen Bedingungen verwendet werden:

- das SRP/CS ist auf PL a oder PL b begrenzt und verwendet Kategorie B, 2 oder 3;
- das SRP/CS ist auf PL c oder PL d begrenzt und verwendet zwei Bauteile für zwei Kanäle in Kategorie 2 oder 3 und die beiden Bauteile verwenden unterschiedliche Embedded-Software oder verschiedene Technologien und eine entsprechende sicherheitsbezogene Anwendungssoftware (siehe 4.6.3), damit die Fehlererkennung den erforderlichen DC erfüllt (z. B. Kreuzvergleich);
- das SRP/CS ist auf PL c oder PL d begrenzt und verwendet zwei Bauteile für zwei Kanäle in Kategorie 2 oder 3 und verwendet zwei verschiedene Anwendungssoftwarekanäle, damit die Fehlererkennung den erforderlichen DC erfüllt (z. B. Kreuzvergleich).“

4.8 Ergonomische Aspekte der Gestaltung

Erster Absatz:

„ISO 12100-2“ ist durch „ISO 12100“ zu ersetzen und „IEC 60204-1:2000, Abschnitt 10“ ist durch „IEC 60204-1:2005, Abschnitt 10“ zu ersetzen.

Dritter Absatz:

Die Verweisung „ISO 12100-2:2003, 4.8“ ist durch „ISO 12100:2010, 6.2.8“ zu ersetzen.