DGUV
Deutsche Gesetzliche Unfallversicherung
Spitzenverband

Vierte Ausgabe der DIN EN ISO 13849-1

Die wesentlichen Neuerungen aus 2023 im Überblick

Übersicht

Die Internationale Organisation für Normung (ISO) hat eine Neufassung der Sicherheitsfachgrundnorm für Maschinensteuerungen, ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze“ [1], veröffentlicht. Mit dieser vierten Ausgabe liegt ein Vierteljahrhundert nach Erstveröffentlichung wieder eine komplett überarbeitete und modernisierte Fassung vor. Auch wenn bis zur Harmonisierung mit der EU-Norm EN 13849-1 noch Zeit vergeht und bis zu einer verpflichtenden Anwendung der Neufassung eine Übergangsfrist von drei Jahren besteht, lohnt sich ein frühzeitiger Blick auf die Neuerungen.

Während sich die Änderungen der dritten Ausgabe von 2016 auf Korrekturen zur Verbesserung der Lesbarkeit und Anwendbarkeit beschränkten, enthält die aktuelle Überarbeitung umfangreichere Anpassungen und Ergänzungen. So wurden die seit 1997 immer weiter gewachsenen und ergänzten Kernabschnitte „Gestaltungsaspekte“, „Sicherheitsfunktionen“ und „Kategorien“ systematisch neu gegliedert, um nach einem „Überblick“ zunächst die „Spezifikation der Sicherheitsfunktionen“ und dann den Entwicklungsablauf abzubilden. Auch die Rolle der Teilsysteme innerhalb einer Sicherheitskette ist nun präziser definiert – speziell im Hinblick auf die Integration von Teilsystemen, die nach IEC-Normen (IEC: International Electrotechnical Commission) der funktionalen Sicherheit mit einem Sicherheits-Integritätslevel (SIL) versehen sind. Der bisher in den zweiten Teil der Norm ausgelagerte abschließende Entwicklungsschritt der Validierung ist nun als Abschnitt 10 – inhaltlich weitgehend unverändert – in den ersten Teil übernommen worden, um seine Bedeutung im Kontext eines sicherheitsgerichteten Designs klar herauszustellen. Die detailliertere Darstellung der Anforderungen an sicherheitsgerichtete Software und die neu aufgenommenen Strategien zur praktischen Umsetzung der elektromagnetischen Störfestigkeit sind weitere wichtige Verbesserungen.

Der folgende Beitrag stellt die wesentlichen Änderungen im Einzelnen vor und gibt, wo notwendig, Empfehlungen zur Interpretation.

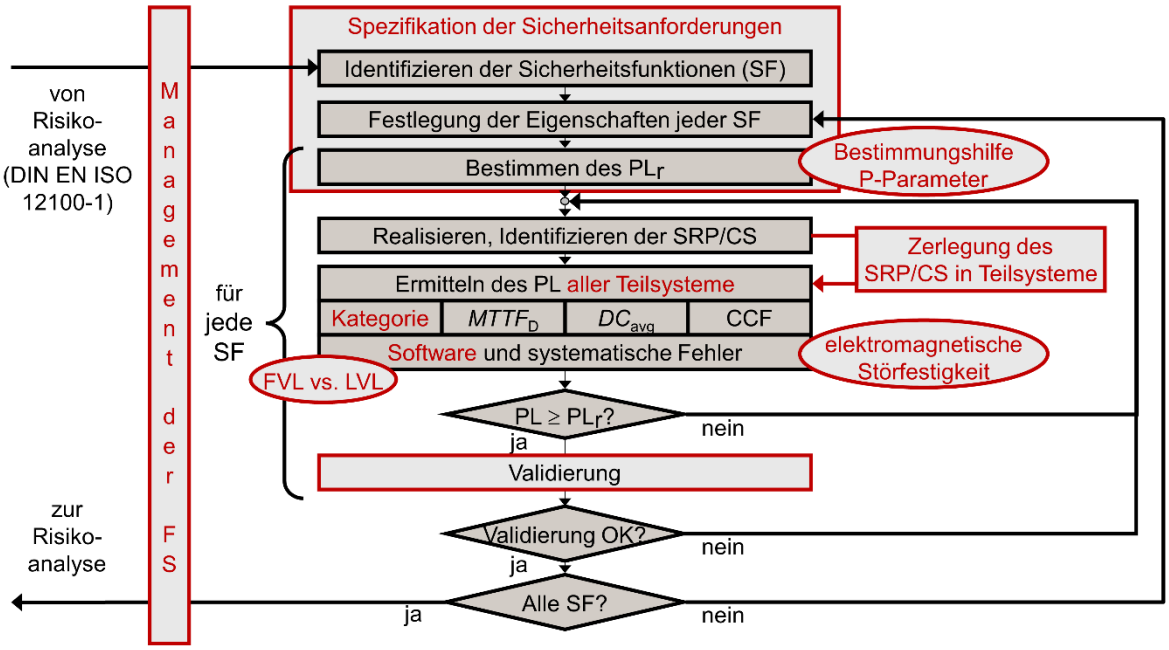

Abbildung: Wesentliche Änderungen entlang des Gestaltungsprozesses für SRP/CS in der vierten Ausgabe der Norm

1 Einleitung

Zum Anwendungsbereich der Norm wird in einer neuen Anmerkung klargestellt, dass die Inhalte der Norm sich an stationären Maschinen orientieren, andere wie z. B. mobile Maschinen aber ausdrücklich eingeschlossen sind.

Die Stellung der Norm im iterativen Prozess der Risikominderung nach DIN EN ISO 12100 wird nun ausführlicher dargestellt. Der informative Anhang A der Norm kann in diesem Kontext zur Bestimmung des erforderlichen Performance Levels PL_r herangezogen werden, wenn dieser nicht in einer Produktnorm (C-Norm) festgelegt wird.

Gegenüber der vorherigen Normausgabe wird genauer beschrieben, dass die Norm auch zur Integration von z.B. Logikeinheiten oder berührungslos wirkenden Schutzeinrichtungen in Sicherheitssteuerungen (SRP/CS) sowie zur Entwicklung von Teilsystemen unter Verwendung von Sicherheitskomponenten wie Zwei-Hand-Bediengeräten, Verriegelungseinrichtungen, Relais, Schützen, Positionsschaltern oder Zustimmschaltern anwendbar ist.

Die Referenz auf den 2020 zurückgezogenen Technischen Report DIN ISO/TR 23849 bzw. DIN SPEC 33883 [2] zur Anwendung von DIN EN ISO 13849-1 und DIN EN IEC 62061 wurde gestrichen. Die Inhalte sind mittlerweile in den aktuellen Ausgaben beider Normen enthalten. Beide unter der Maschinenrichtlinie harmonisierten Normen können zur Entwicklung und Integration von Sicherheitssteuerungen von Maschinen (einschließlich Software) genutzt werden (siehe auch unten, Abschnitt 6).

Hinsichtlich der Übernahme der Anforderungen zur Validierung aus Teil 2 der Norm in Abschnitt 10 wird für die Übergangszeit bis zum Abschluss der Überarbeitung der DIN EN ISO 13849-2 klargestellt, dass die neueren Anforderungen aus Teil 1 Priorität haben. Gleichzeitig kann davon ausgegangen werden, dass diese erfüllt sind, wenn die Validierungsanforderungen aus Teil 2 umgesetzt sind.

2 Abschnitt 1, Anwendungsbereich

Wie schon in der vorhergehenden Ausgabe wird klargestellt, dass die Norm nur für SRP/CS mit hoher Anforderungsrate oder kontinuierlicher Anforderung gilt. Nach Definition 3.1.44 erfolgt die Anforderung bei dieser Betriebsart häufiger als einmal pro Jahr. Für SRP/CS mit niedriger Anforderungsrate (seltener als einmal pro Jahr), wie sie häufig in der Prozessindustrie zu finden ist, wird nun explizit auf die Normenreihe DIN EN 61508 verwiesen.

IT-Sicherheit wird in der Norm nicht behandelt, aber darauf hingewiesen, dass diese einen Einfluss auf Sicherheitsfunktionen haben kann. Für weitere Informationen wird auf DIN ISO/TR 22100-2 [3] und DIN IEC/TR 63074 [4] verwiesen.

3 Abschnitt 3, Begriffe, Formelzeichen und Abkürzungen

Die überarbeitete Norm enthält eine Vielzahl neuer Definitionen, wohingegen einige alte Definitionen entfallen. Fast alle bestehenden Definitionen haben eine neue Nummerierung.

Besonders hervorzuheben ist, dass die bisherige „Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde“ nun als „mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde“ bezeichnet wird. Deren Abkürzung wird wieder auf PFH[1] (ohne Index „D“) geändert, um eine gleichlautende Benennung wie in den IEC-Normen zur Funktionalen Sicherheit zu erreichen. Technische Änderungen ergeben sich daraus nicht.

4 Abschnitt 4, Überblick

Um dem erklärten Ziel einer besseren Gliederung gerecht zu werden, beginnt dieser Abschnitt zunächst mit Teilen aus dem alten Abschnitt 4 „Gestaltungsaspekte“ zur Einbettung in den iterativen Prozess der Risikobeurteilung und Risikominderung nach DIN EN ISO 12100. Bild 2 der Norm zeigt wie bereits Bild 1, dass die Anwendung der DIN EN ISO 13849-1 als Stufe 2 des Risikominderungsprozesses anzusehen ist, d. h. als Risikominderung durch technische Schutzmaßnahmen. Dann folgt ein kurzer Überblick über die folgenden Abschnitte der Norm, die sich am typischen Ablauf eines Entwicklungsprozesses für SRP/CS orientiert: Auf die Spezifikation von Sicherheitsfunktionen (inklusive deren PL_r) folgt die technische Realisierung und PL-Bestimmung einschließlich Validierung und Dokumentation.

Abschließend werden die grundsätzlichen Möglichkeiten zur Realisierung einer Sicherheitsfunktion aufgezeigt:

- Integration bereits nach einer Norm für Funktionale Sicherheit von Maschinensteuerungen validierter Teilsysteme,
- Eigenentwicklung eines neuen Teilsystems nach DIN EN ISO 13849 selbst oder
- Kombination von Teilsystemen beider vorgenannter Alternativen.

Alle Anforderungen an die Entwicklung von Teilsystemen, einschließlich Hardware und Software, sind nun in den Abschnitt 6 und die darauf folgenden Abschnitte verschoben, da im Entwicklungsablauf zunächst die Sicherheitsfunktionen festzulegen sind.

[1] PFH = average frequency of a dangerous failure per hour

5 Abschnitt 5, Spezifikation von Sicherheitsfunktionen, und Anhang M

Die Definition von Sicherheitsfunktionen in der Spezifikation der Sicherheitsanforderungen (SRS[2]) wird nun detaillierter eingefordert. Basis für die Definition jeder Sicherheitsfunktion bleibt der Prozess der Risikobeurteilung und Risikominderung nach DIN EN ISO 12100. Die erforderlichen Angaben für eine genaue und vollständige Definition umfassen für jede Sicherheitsfunktion folgende Punkte:

- eine Kurzbeschreibung bzw. einen Titel (als eindeutige Referenz),
- das auslösende Ereignis, welches die Sicherheitsfunktion anfordert,
- die notwendige Reaktion, welche durch die Sicherheitsfunktion zu erfolgen hat, um den beabsichtigten sicheren Zustand zu erreichen,
- den erforderlichen Performance Level PL_r,
- die erlaubte Ansprechzeit, also die Zeit zwischen Anforderung der Sicherheitsfunktion und Erreichen des sicheren Zustands,
- die Betriebsarten, in denen die Sicherheitsfunktion aktiv sein muss,
- die Schnittstellen der Sicherheitsfunktion mit der Steuerung der Maschine und anderen Sicherheitsfunktionen,
- falls erforderlich, eine Beschreibung der Fehlerreaktion, das heißt, wie die Maschine in einen sicheren Zustand gebracht werden kann, falls in einem Funktionskanal ein Fehler erkannt wird,
- das Verhalten der Maschine bei Energieverlust, z.B. die Forderung nach Rückschlagventilen direkt am Zylinder oder zusätzlichen mechanischen Bremsen (auch die Separation in zwei Sicherheitsfunktionen ist möglich – eine mit verfügbarer Energie oder eine zweite ohne verfügbare Energie),
- die Anforderungsrate der Sicherheitsfunktion,
- die Priorisierung verschiedener Sicherheitsfunktionen, die gleichzeitig aktiv sein können und widersprüchliche Reaktionen auslösen können,
- zusätzliche Sicherheitsanforderungen aus Produktnormen (C-Normen),
- die Bedingungen, die einen Wiederanlauf erlauben, nachdem die Sicherheitsfunktion angefordert wurde.

Weitere Hinweise zu diesem Thema gibt auch das SISTEMA-Kochbuch 6 [5].

Es folgen die bekannten zusätzlichen Anforderungen an besondere Sicherheitsfunktionen, wie sicherheitsbezogene Stoppfunktion, manuelle Rückstellfunktion usw. Hier wird für die manuelle Rückstellung klargestellt, dass zur Vermeidung vorhersehbarer Fehlanwendung ein überwachter Signalwechsel erforderlich ist. In der Praxis bedeutet dies, dass eine fallende oder steigende Signalflanke zur Auslösung der manuellen Rückstellung geeignet ist. Da der Nachlauf nun generell spezifiziert werden soll, entfällt die Ansprechzeit als besonderer Punkt. Neu sind zusätzliche

[2] SRS = safety requirements specification

Anforderungen an die Betriebsartenwahl, um negative Rückwirkungen auf andere Sicherheitsfunktionen zu verhindern. Die Betriebsartenwahl wird als eigene Sicherheitsfunktion betrachtet, wenn dadurch Sicherheitsfunktionen deaktiviert oder aktiviert werden. Auch Hinweise zu Sicherheitsfunktionen für Wartungs- und Instandhaltungsaufgaben sind neu hinzugekommen.

Die bekannten Tabellen mit Verweisen auf internationale Normen zu typischen Sicherheitsfunktionen an Maschinen und einigen ihrer Eigenschaften sind nun aus Abschnitt 5 in einen neuen informativen Anhang M verschoben.

Ein neuer Unterabschnitt 5.2.3 fordert dazu auf, den Manipulationsanreiz zur Umgehung von Sicherheitsfunktionen zu minimieren. Schon bei der Definition der Sicherheitsfunktionen soll deren praktische Umsetzbarkeit bei der Nutzung der Maschine beachtet werden. Ein weiterer neuer Unterabschnitt 5.2.4 schränkt den Fernzugriff normativ insoweit ein, dass gefährliche Situationen durch unbemerkte Anwesenheit von Personen im Gefahrenbereich der Maschine verhindert werden müssen.

Als nächste Schritte zum Abschluss der Spezifikationsphase werden die Bestimmung des PL_r und das Review der Spezifikation der Sicherheitsanforderungen (SRS) beschrieben. Dieses Review ist vor dem Einstieg in die SRP/CS-Entwicklungsphase erforderlich, um Spezifikationsfehler noch frühzeitig korrigieren zu können.

Der letzte Unterabschnitt 5.5 widmet sich der Zerlegung eines SRP/CS in Teilsysteme. Hier zeigt sich deutlich, dass die Norm mit ihrer vierten Ausgabe eine klare Trennung zwischen SRP/CS und Teilsystemen umgesetzt hat. Mit SRP/CS wird der sicherheitsbezogene Teil einer Steuerung beschrieben, der eine komplette Sicherheitsfunktion ausführt – vom auslösenden Ereignis bis zur notwendigen Reaktion, um einen sicheren Zustand zu erreichen oder beizubehalten. Entlang der Hardware-Kette vom Eingang (Sensoren) über die Logik (Verarbeitung) zum Ausgang (Leistungssteuerungselemente) kann dann eine Zerlegung in Teilsysteme erfolgen, die jeweils eine (Sicherheits-)Teilfunktion ausführen. Dabei ist die Zahl der beteiligten Teilsysteme variabel. Wie schon im vorhergehenden Abschnitt erläutert, können bereits validierte Teilsysteme integriert oder Teilsysteme nach DIN EN ISO 13849 aus Teilsystem-Elementen zusammengesetzt werden. Den dafür geltenden Anforderungen an die Entwicklung von Teilsystemen widmet sich der nächste Normabschnitt.

6 Abschnitt 6, Entwurfsaspekte, und Anhang K

Der neue Abschnitt 6 beschäftigt sich nicht mehr nur mit der Beschreibung der Kategorien und der Kombination von Teilsystemen, sondern mit allen – vorher teilweise in den Unterabschnitten 4.4 und 4.5 genannten – Eigenschaften und Parametern, die in die Bestimmung des erreichten PL eingehen.

Nach einer allgemeinen Einleitung geht es zunächst um die Korrelation zwischen PL und SIL. Die Norm beschränkt die Integration von nach DIN EN 61508 oder DIN EN IEC 62061 entwickelten Teilsystemen auf solche, die für den Einsatz mit hoher Anforderungsrate oder kontinuierlicher Anforderung vorgesehen sind und die nach Route 1_H (siehe DIN EN 61508-2:2011, 7.4.42) entwickelt wurden.

6.1 Unterabschnitt 6.1.3, Kategorien

Bei der Beschreibung der Kategorien haben sich einige wichtige Details geändert oder werden klarer herausgestellt:

- **Kategoriezuordnung auf Teilsystem-Ebene (6.1.3.1)**
  Im Zuge der sauberen Trennung zwischen SRP/CS und Teilsystemen muss jedem nach

DIN EN ISO 13849 entwickelten Teilsystem eine Kategorie zugeordnet werden. Ein SRP/CS darf demnach auch Teilsysteme unterschiedlicher Kategorien oder Teilsysteme mit SIL-Klassifizierung enthalten.

- **Bewährte Bauteile in Kategorie 1 (6.1.3.2.3)**
  Auch wenn sich inhaltlich kaum etwas an den Anforderungen für Kategorie 1 geändert hat, ist die Beschreibung für bewährte Bauteile nun in einen eigenen Unterabschnitt 6.1.11 ausgelagert worden. Dort wird ein direkter Bezug zu den in DIN EN ISO 13849-2 für verschiedene Technologien gelisteten bewährten Bauteilen hergestellt und informativ auch auf das in DIN EN 61508 benutzt Konzept der „Betriebsbewährung“ hingewiesen. Dass komplexe Bauteile nicht als bewährte Bauteile geeignet sind, ist nun normativ und keine Anmerkung mehr.

- **Testung in Kategorie 2 (6.1.3.2.4)**
  Als Hauptmerkmal der Kategorie 2 wird zukünftig die Fehlererkennung im Funktionskanal anstatt der Testung der Sicherheitsfunktion genannt. Damit wird klargestellt, dass nicht unbedingt die Überprüfung der ganzen Teilfunktion eines Kategorie-2-Teilsystems erforderlich ist (was als hundertprozentige Fehleraufdeckung interpretiert werden könnte), sondern eine effektive Fehlererkennung im Funktionskanal gefordert ist – und zwar für jeden Teil des Funktionskanals (Eingabeeinheit, Logik und Ausgabeeinheit) mindestens mit „niedrigem“ Diagnosedeckungsgrad (DC), also 60 % Fehleraufdeckung.
  Zwei bisher nur im Rahmen des vereinfachten Verfahrens zur Abschätzung der quantifizierbaren Aspekte des PL genannte Bedingungen gelten nun allgemein im Rahmen der Kategorie 2:
  Die Testrate muss mindestens 100-mal größer als die Anforderungsrate sein oder die Testung erfolgt bei Anforderung der Sicherheitsfunktion und verhindert die Gefährdung. Die in Anhang K beschriebene Ausnahme einer nur 25-mal größeren Testrate bleibt davon unberührt.
  Außerdem muss die mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) des Testkanals (inklusive OTE – Ausgang der Testeinrichtung) größer als die halbe $MTTF_D$ des gesamten Funktionskanals sein.

- **Fehlerakkumulation in Kategorie 4 (6.1.3.2.6)**
  Mit einer neuen Anmerkung soll ein mögliches Missverständnis bei der Umsetzung einer Kategorie 4 ausgeräumt werden. Im Rahmen einer Failure Mode and Effects Analysis (FMEA) ist es manchmal nicht möglich, 100 % der theoretisch möglichen gefährlichen Ausfälle als erkennbar einzustufen. Daher wird in Kategorie 4 für die PFH-Berechnung „nur“ ein hoher DC von rechnerisch 99 % gefordert. Andererseits darf gemäß der Definition von Kategorie 4 die Anhäufung von (bis zu zwei) unerkannten gefährlichen Ausfällen nicht zum Verlust der Sicherheitsfunktion führen. Gäbe es daher tatsächlich einen unerkannten gefährlichen Ausfall mit praktischer Relevanz, könnte der zweite gefährliche Ausfall zum Versagen einer Kategorie-4-Struktur führen. Hier greift die neue Anmerkung: Unerkannte Ausfälle mit einer sehr niedrigen Wahrscheinlichkeit (theoretisch denkbar, praktisch aber nicht relevant) brauchen für die Fehleranhäufung nicht berücksichtigt zu werden – allerdings nur, wenn diese Fehlerbetrachtung dokumentiert und verifiziert wird.

6.2 Unterabschnitt 6.1.4, $MTTF_D$

Der Liste der möglichen Datenquellen zur Abschätzung eines $MTTF_D$-Wertes wurde eine neue Alternative hinzugefügt: Verlässliche Felddaten für identische Bauteilanwendungen aus vergleichbaren Umgebungen können herangezogen werden, wenn keine Angaben des Herstellers vorliegen und die Methoden aus Anhang C (u. a. Verfahren guter ingenieurmäßiger Praxis) nicht nutzbar sind.

6.3 Unterabschnitt 6.1.6, CCF

Die Anforderung zur Vermeidung von Ausfällen infolge einer gemeinsamen Ursache ist nun in einem eigenen Unterabschnitt 6.1.6 genannt, der für eine Anleitung zur praktischen Umsetzung auf den bekannten Anhang F verweist.

6.4 Unterabschnitt 6.1.7, Systematische Ausfälle

Auch die Forderung zur Vermeidung und Beherrschung systematischer Fehler hat nun einen eigenen Unterabschnitt 6.1.7 erhalten. Neu ist die ausdrückliche Forderung nach einem Plan der funktionalen Sicherheit, der das Management der funktionalen Sicherheit definiert, um vor systematischen Fehlern in Spezifikation, Umsetzung und Modifikation zu schützen. Details dazu wurden im Anhang G ergänzt (siehe Abschnitt 15 dieses Beitrags).

6.5 Unterabschnitt 6.1.8, vereinfachtes Verfahren, Säulendiagramm und Anhang K

Das vereinfachte Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL einschließlich des Säulendiagramms (in der Norm jetzt Bild 12) befindet sich nun im Unterabschnitt 6.1.9. Hier gibt es nur zwei nennenswerte Änderungen: Die Anforderungen an die Testrate und Zuverlässigkeit des Testkanals gelten nun allgemein für Kategorie 2, wie schon oben genannt. Außerdem wurde Tabelle 6 aus der dritten Ausgabe der Norm, die das Säulendiagramm in vereinfachter tabellarischer Form darstellte, gelöscht.

6.6 Unterabschnitt 6.1.9, alternatives Verfahren zur Bestimmung von PL und PFH ohne $MTTF_D$

Das in der letzten Ausgabe der Norm eingeführte alternative Verfahren für den Ausgangsteil eines SRP/CS wurde verändert und auf den Eingangs- und Logikteil erweitert. Gleichzeitig ist seine Anwendbarkeit nun eingeschränkt: Es gilt nach wie vor für Teilsysteme, die mechanische, (elektro-) hydraulische oder (elektro-)pneumatische Bauteile enthalten, für die keine Zuverlässigkeitsdaten (z.B. als $MTTF_D$-Angaben) verfügbar sind – aber neuerdings nur, wenn auch das Verfahren guter ingenieurmäßiger Praxis aus Anhang C.2 der Norm nicht anwendbar ist.

Das bekannte Verfahren für den Ausgangsteil (Energieübertragungselemente) ist nun auch auf den Eingangsteil anwendbar. Als zusätzliche Anforderung gilt in Kategorie 2, 3 und 4 allerdings, dass wie in Kategorie 1 nur bewährte Bauteile eingesetzt werden. Die alternative Nutzung betriebsbewährter Bauteile ist entfallen.

Für den Logikteil wurde ein neuer Ansatz hinzugefügt: Teilsysteme der Kategorie B, 2 oder 3 können einen geschätzten Wert von zehn Jahren für die $MTTF_D$ jedes Kanals nutzen. In Kategorie 1 ist dieser Schätzwert auf 30 Jahre erhöht, da bewährte Bauteile verwendet werden müssen. Für Logik-Teilsysteme in Kategorie 4 ist diese Methode ausgeschlossen. Maximal ist PL c erreichbar.

6.7 Unterabschnitt 6.1.10, Fehlerbetrachtung und Fehlerausschluss

Der bisherige Abschnitt 7 der Norm zu Fehlerbetrachtungen und Fehlerausschlüssen ist nun im Unterabschnitt 6.1.10 angesiedelt und hat eine ausführlichere Einleitung erhalten. Zusätzlich wird eine Einschränkung genannt, die bisher nur aus DIN ISO/TR 23849 [2] bekannt war: Ein PL e für Teilsysteme darf nicht allein auf Fehlerausschlüssen beruhen.

6.8 Unterabschnitt 6.2, Kombination von Teilsystemen

Neben der klaren begrifflichen Trennung zwischen Teilsystemen und SRP/CS (als Kombination von Teilsystemen) wurde das bevorzugte Verfahren der Addition bekannter PFH-Werte deutlicher vom alternativen, tabellenbasierten Verfahren für Teilsysteme ohne PFH getrennt.

6.9 Unterabschnitt 6.3, softwarebasierende manuelle Parametrierung

Die Anforderungen an softwarebasierte Parametrierung sicherheitsbezogener Parameter sind nun bewusst vom übrigen Softwareteil der Norm gelöst. Außerdem wird betont, dass es dabei nur um manuelle, softwarebasierte Parametrierung durch autorisierte Personen geht. Darunter fällt etwa Parametrierung durch speziell qualifizierte Parametrierwerkzeuge, aber keine Parametrierung auf Basis von DIP-Schaltern (DIP: Dual In-Line Package) sowie keine automatisierte Parametrierung oder direkte Steuerung einer Maschine durch eine Bedienperson, z. B. die Geschwindigkeitsregelung eines Gabelstaplers. Neu sind zusätzliche Informationen zu möglichen Einflüssen, die zu einer fehlerhaften Parametrierung führen können, und ausführlichere Anforderungen an die Dokumentation von Parametrierungsvorgängen.

7 Abschnitt 7 zu Software-Anforderungen und Anhänge J und N

Die Anforderungen an die Entwicklung sicherheitsgerichteter Software sind nun in einem eigenen Abschnitt 7 zusammengefasst. In der Einleitung wird darauf hingewiesen, dass hier keine spezifischen Anforderungen an Software, die künstliche Intelligenz nutzt, enthalten sind.

Im V-Modell des Software-Sicherheitslebenszyklus werden die Verifikationsschritte (Reviews und Tests) und die Ergebnisse der Phasen genauer benannt. Auch die auf dem absteigenden Ast entstehenden Dokumentationen, die mit jeder Spezifikationsphase immer feinteiliger werden, sind nun mit dargestellt. Neu ist eine vereinfachte zweistufige Variante des V-Modells für Programmiersprachen mit eingeschränktem Sprachumfang (LVL[3]), die validierte Funktionsblöcke verwenden und als Anwendungsprogramm (SRASW[4]) auf geprüfter Hardware laufen. Da hier die Programmierung typischerweise nur einfache logische Verknüpfungen von Eingangs- und Ausgangsblöcken realisiert, kann die sicherheitsbezogene Software-Spezifikation direkt in die Kodierungsphase übergehen.

Sicherheitsbezogene Embedded-Software (SRESW[5]) erfordert in der Regel eine Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL[6]), während SRASW auch in LVL geschrieben werden kann. Eine neue Entscheidungshilfe zur Einordnung der verwendeten Programmiersprache in LVL oder FVL ergänzt nun den Software-Abschnitt. Programmiersprachen in Übereinstimmung mit DIN EN 61131-3 [6] – Kontaktplan, Funktionsbaustein-Sprache, Ablaufsprache und boolesche Algebra – gelten als LVL. Zusätzlich können durch Programmierrichtlinien, Compiler und Entwicklungswerkzeuge realisierte Beschränkungen, die einen definierten Programmfluss sicherstellen, zur Einordnung als LVL führen.

Da die Anforderungen für SRESW bisher nur sehr knapp beschrieben waren, enthält die neue Normausgabe nun für alle Basismaßnahmen und zusätzlichen Maßnahmen vertiefende beispielhafte Hinweise. Weiterführende Erläuterungen dazu enthält der IFA Report 1/2020 [7].

[3] LVL = limited variability language
[4] SRASW = safety related application software
[5] SRESW = safety related embedded software
[6] FVL = full variability language

Die Randbedingungen für die Möglichkeit, Bauteile mit nicht zugänglicher Embedded-Software einzusetzen, sind angepasst: Die für PL c und d bestehende Forderung nach Diversität kann nicht nur durch verschiedenartige Technologien, sondern nun auch durch verschiedenartige Konstruktion erfüllt werden. Klargestellt ist, dass die zugehörige Hardware und vorhandene SRASW den Anforderungen der Norm genügen müssen.

Die je nach PL_r und vorhandener Diversität abgestuften Softwaremaßnahmen sind im konkreten Anwendungsfall nicht immer direkt eindeutig zuordenbar. Hier soll der erste Teil des neuen informativen Anhangs N helfen: Zunächst kann aus der Anwendung heraus einer von vier Einsatzfällen bestimmt werden, die auf dem PL_r (a/b, c, d oder e) basieren, aber je nachdem, wo die Software eingesetzt wird, um eine Stufe herabgesetzt werden können. Diese Abstufung ist möglich für Software im Testkanal von Kategorie 2 oder in diversitären Funktionskanälen von Kategorie 3 oder 4. Dann können mit dem zutreffenden Einsatzfall in zwei Tabellen die verbindlichen und empfohlenen Einzelmaßnahmen abgelesen werden.

Der zweite Teil des neuen Anhangs N demonstriert die Softwarevalidierung durch Analyse und Tests am Beispiel einer SRASW, die auf validierte Funktionsblöcke zurückgreift.

Das Beispiel für die Realisierung von SRESW im informativen Anhang J wurde an das aktuelle V-Modell des Software-Sicherheitslebenszyklus angepasst.

Die bisherigen Unterabschnitte zur Verifikation des erreichten Performance Levels und zu ergonomischen Aspekten der Gestaltung wurden ohne nennenswerte Änderungen zu den Abschnitten 8 und 9.

8 Abschnitt 10, Validierung

Der neue Abschnitt 10 zur Validierung wurde komplett aus den Abschnitten 4 bis 12 der DIN EN ISO 13849-2 übernommen. Trotz einiger Umstellungen sind die Inhalte und Anforderungen grundsätzlich gleich geblieben. Sie widmen sich in bekannter Weise den Validierungsprinzipien einschließlich Validierungsplan, Validierungsprotokoll und der Validierung durch Analyse und Tests. Inhalte der Validierung sind hauptsächlich die Spezifikation der Sicherheitsanforderungen, die Sicherheitsfunktionen, die Sicherheitsintegrität (Wirksamkeit von Sicherheitsfunktionen) einschließlich Kategorien, Hardware und Software, die Umgebungsanforderungen und die Benutzerinformation. Im Überblick über den Validierungsprozess wird deutlich gemacht, dass unabhängig von der Kategorie neben der Analyse zumindest ein Funktionstest der Sicherheitsfunktionen erforderlich ist.

Durch die Übernahme der Validierungsanforderungen aus dem weniger bekannten Teil 2 der Norm soll die Validierung als wichtige Maßnahme gegen Spezifikations-, Entwicklungs- und Umsetzungsfehler betont und ihre praktische Umsetzung bestärkt werden. Langfristig soll nach einer Überarbeitung von Teil 2 der Norm, der sich dann nur noch auf die Tabellen und das Validierungsbeispiel in den Anhängen beschränkt, ein kompletter Übergang des Teils 2 in den Teil 1 der Norm erfolgen. Bis dahin sind die Validierungsanforderungen in beiden Teilen der Norm kompatibel und es entsteht dadurch kein Widerspruch.

9 Abschnitt 11, Wartungsfreundlichkeit

Der bisherige Abschnitt zur Instandhaltung ist um den Aspekt der Wartbarkeit erweitert worden, damit Zugänglichkeit, einfache Handhabung, Sichtbarkeit, Vereinfachung und automatisch generierte Wartungshinweise berücksichtigt werden.

10 Abschnitte 12 und 13, Technische Dokumentation und Benutzerinformation

Die bisherigen Anforderungen an die (herstellerinternen) technischen Dokumente wurden geringfügig ergänzt und die Anforderungen an die Benutzerinformation in zwei Unterabschnitte aufgeteilt: Der erste wendet sich mit einer detaillierten Liste technischer Kenndaten an SRP/CS-Integratoren und der zweite mit Angaben zur Bedienung, Anzeigen, Reinigung, Wartung usw. an Nutzer der Maschine.

11 Anhang A, PL_r-Bestimmung

Im informativen Anhang A zur PL_r-Bestimmung gibt es zwei nennenswerte Änderungen.

Die Parameter „Möglichkeit zur Vermeidung oder Begrenzung des Schadens“ (Parameter P) und „Eintrittswahrscheinlichkeit eines Gefährdungsereignisses“ sind nicht länger vermischt. Die „Eintrittswahrscheinlichkeit eines Gefährdungsereignisses“ wird jetzt nur noch am Rande erwähnt und in der Regel zur sicheren Seite als hoch (100 %) abgeschätzt. In Fällen, in denen eine Abschätzung als niedrig möglich ist, kann der mit dem Risikographen bestimmte PL_r um eine Stufe herabgestuft werden. Neu ist, dass diese Entscheidung gerechtfertigt und dokumentiert werden soll. Da in der vierten Normausgabe keine Beschreibung mehr vorhanden ist, wie die „Eintrittswahrscheinlichkeit eines Gefährdungsereignisses“ bestimmt werden soll, kann hier zu Informationszwecken nur auf die dritte Normfassung zurückgegriffen werden, da auch die DIN EN ISO 12100 wenig Hinweise zu diesem Risikoelement liefert.

Für den Parameter P wird demgegenüber nun eine detailliertere Hilfestellung zur Ermittlung anhand von fünf Faktoren angeboten. Drei dieser Faktoren, nämlich die Geschwindigkeit, mit der die Gefährdungssituation auftritt, die räumliche Möglichkeit, der Gefährdung auszuweichen, und die Wahrnehmbarkeit der Gefährdung können bei ungünstiger Ausprägung schon jeweils allein die Wahl von P2 (Vermeidung oder Begrenzung des Schadens kaum möglich) begründen. Zwei weitere Faktoren begründen nur in Verbindung mit weiteren ungünstigen Faktoren die Wahl von P2: Zum einen, ob die Nutzung der Maschine durch fachkundiges Personal erfolgt und zum anderen die Komplexität der Bedienung,

12 Anhänge C und D, $MTTF_D$-Werte

Gibt der Hersteller eines Bauteils mit mechanischem Verschleiß, z. B. eines pneumatischen oder elektromechanischen Bauteils, statt eines B_{10D}-Werts (Anzahl der Zyklen, bis 10 % der Bauteile gefährlich ausgefallen sind) nur einen B_{10}-Wert an, so kann für die Umrechnung nun – soweit bekannt – der Anteil der gefahrbringenden Ausfälle RDF[7] genutzt werden, gemäß der Beziehung $B_{10D} = B_{10}/RDF$. Bisher gab es hier nur den Hinweis, als Abschätzung 50 % gefährliche Ausfälle anzunehmen, also $B_{10D} = 2 \cdot B_{10}$. Auch in der neuen Normausgabe gilt aber die Zusatzbedingung, dass bei RDF kleiner als 50 % der T_{10D}-Wert auf maximal $2 \cdot T_{10}$ beschränkt wird. Dadurch vergrößert sich bei einem kleinen Anteil gefahrbringender Ausfälle zwar der B_{10D}-Wert (und der daraus ermittelte $MTTF_D$-Wert), nicht aber der T_{10D}-Wert, also die Zeit, nach der ein Bauteil mit mechanischem Verschleiß ausgetauscht werden muss, um den ermittelten PL aufrechtzuerhalten.

[7] RDF = ratio of dangerous failures

13 Anhang E, Diagnosedeckungsgrad

In der Tabelle E.1 mit Beispielmaßnahmen zur Fehlererkennung gibt es nun zusätzliche Anmerkungen für die geschätzten DC, bei denen bisher eine Spanne erreichbarer DC-Werte angegeben war:

- Grundsätzlich sollte eine FMEA (Ausfalleffektanalyse) die Basis für die Bestimmung des DC in der konkreten Anwendung sein.
- Bei der Überwachung von Ausgängen und beim Kreuzvergleich von Eingangs- oder Ausgangssignalen ohne dynamischen Test kann die Testrate, die sich aus der jeweiligen Anwendung ergibt, als begrenzender Faktor für den DC wirken, z. B. indem nur Tests, die mindestens einmal pro Monat erfolgen, überhaupt einen DC von 99 % erreichen können, und Tests, die seltener als einmal pro Jahr erfolgen, mit einem DC von 0 % abgeschätzt werden.
- Für die Fehlererkennung durch den Prozess kann das Verhältnis von Prozessdiagnoserate (Testrate) und Anforderungsrate der Sicherheitsfunktion für eine Begrenzung des erreichbaren effektiven DC-Werts bis hinab zu einem Wert von 60 % genutzt werden.
- Mehrere DC-Maßnahmen, die auf ein Bauteil wirken, können kombiniert werden, um einen höheren DC zu erreichen. Auch die Einschränkung, dass Fehlererkennung durch den Prozess als alleinige Maßnahme für PL_r e nicht ausreichend ist, kann durch eine solche Kombination mit weiteren DC-Maßnahmen überwunden werden.

14 Anhänge F und I, CCF und Beispiele zur vereinfachten PL-Bestimmung

Die Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) werden nun in Tabelle F.1 nur stichpunktartig genannt, dafür aber im neuen Unterabschnitt F.3 detaillierter beschrieben als vorher. Ein neuer Hinweis betont, dass für SRP/CS, die auf Bauteilebene nicht ausreichend gegen Überspannungen oder andere Umwelteinflüsse geschützt sind, der erforderliche Schutz auch auf Systemebene erreicht werden kann, z. B. durch die Verwendung von externen Schutzkomponenten, Filtern oder Abschirmung. Die Bewertung der Maßnahmen gegen CCF erfolgt üblicherweise auf der Teilsystemebene, da sich die Maßnahmen je nach Teilsystem unterscheiden können. Bei der Bewertung sollte die erwartete Anwendung einschließlich vorhersehbarer Fehler und vernünftigerweise vorhersehbarer Fehlanwendung zugrunde gelegt werden. Eine ingenieurmäßige Beurteilung dient dazu, typische Ursachen für CCF weitestgehend zu eliminieren oder die Auswirkungen der Ursachen zu reduzieren. Diese Beurteilung sollte auch dokumentiert werden.

Dementsprechend werden im zweiten Beispiel in Anhang I, das der Illustration des vereinfachten Verfahrens zur Abschätzung des PL von Teilsystemen dient, die angewendeten Maßnahmen gegen CCF nun auch genau benannt.

15 Anhang G, Systematische Fehler, Plan der funktionalen Sicherheit

Der Hinweis auf Anhang F der DIN EN 61508-2 zu fehlervermeidenden Maßnahmen bei der Entwicklung von ASICs, FPGAs und PLDs wurde zwar gelöscht, gilt aber implizit weiterhin.

Ein neuer Unterabschnitt G.5 beschreibt, wie durch Maßnahmen für das Management der funktionalen Sicherheit die normativen Anforderungen aus Abschnitt 6.1.7 umgesetzt werden können. Ziel ist es, durch ein systematisches Vorgehen bei der Entwicklung und Umsetzung von SRP/CS, eine fehlerhafte Spezifikation, Umsetzung oder Modifikation zu verhindern. Kernstück ist der Plan der funktionalen Sicherheit, der alle diesbezüglichen Aktivitäten dokumentiert. Seine Form und sein Umfang richten sich z. B. nach der Projektgröße, der Komplexität oder der Neuartigkeit. Er soll alle relevanten Aktivitäten im gesamten Entwicklungsprozess von der Spezifikation bis zur Validierung und

Modifikation identifizieren sowie Verantwortlichkeiten, Ressourcen und Verfahren beschreiben.

16 Anhang L, Elektromagnetische Störfestigkeit

Seit der dritten Normausgabe wurde eine neue Fachgrundnorm DIN EN 61000-6-7 [8] zu Störfestigkeitsanforderungen für sicherheitsbezogene Systeme der funktionalen Sicherheit etabliert. Um deren Umsetzung zu erleichtern, stellt nun ein neuer informativer Anhang L Leitlinien zur Umsetzung der erforderlichen Maßnahmen für die elektromagnetische Störfestigkeit dar. Dabei werden je nach Anwendung vier alternative Pfade zur Auswahl gestellt:

A. Störfestigkeitsanforderungen aus einer zutreffenden Produktnorm besitzen die oberste Priorität (unabhängig vom zu erreichenden PL) und ersetzen die allgemeinen Anforderungen der Fachgrundnorm.

B. Für PL a und PL b wird die Einhaltung der niedrigeren Störfestigkeitsanforderungen aus DIN EN IEC 61000-6-2 [9] für Industriebereiche, die nicht für funktionale Sicherheit ausgelegt sind, als ausreichend angesehen.

C. Bis PL d (und bei Erfüllen der Anforderungen für Kategorie 4 sogar bis PL e) kann die geforderte Störfestigkeit statt durch Störfestigkeitstests auch durch Schutzmaßnahmen auf Systemebene, also etwa Abschirmung, Filter, störunempfindliche Verkabelung, Trennung, Fehlererkennung oder Risikoanalyse, erreicht werden. Diese alternative Nachweisstrategie wird explizit auch in DIN EN 61000-6-7, 4.1, Anmerkung 1 genannt. Tabelle L.1 der Norm stellt dazu eine Liste von 23 verschiedenen Maßnahmen zur Verfügung, deren Einhaltung 10 bis 30 Punkte liefert. Ab einer Gesamtpunktzahl von 280 für zweikanalige Systeme (Kategorie 2, 3 und 4) oder 230 für einkanalige Systeme (Kategorie B und 1) gelten die Störfestigkeitsanforderungen als erfüllt. Fünf Maßnahmen sind für einkanalige Teilsysteme nicht anwendbar. Acht der genannten Maßnahmen sind als dringend empfohlen markiert: Sind diese anwendbar, aber nicht umgesetzt, so muss ausführlich begründet werden, wie die Störfestigkeit auf gleichwertige Weise erreicht wird.

D. Bis PL e kann die Einhaltung der erhöhten Störfestigkeitspegel durch Anwendung der DIN EN 61000-6-7 oder anderer allgemeiner EMV-Normen für funktionale Sicherheit wie DIN EN 61326-3-1 nachgewiesen werden.

17 Anhang O, Gerätetypen

Ein neuer Anhang O definiert vier Gerätetypen und zugehörige charakteristische Kennwerte, die z. B. im Datenblatt des Herstellers angegeben werden sollten. Während Teilsysteme (Gerätetyp 1 oder 4) in der Regel durch PL (oder SIL), PFH, Kategorie (oder Hardware-Fehlertoleranz) und Gebrauchsdauer spezifiziert werden, sind Teilsystemelemente in der Regel durch $MTTF_D$ oder λ_D (Gerätetyp 2) oder B_{10D} (Gerätetyp 3) in Verbindung mit einer Gebrauchsdauer beschrieben. Weiterführende Informationen liefert das VDMA-Einheitsblatt 66413 (universelle Datenbasis) [10].

18 Fazit

Die vierte Ausgabe der DIN EN ISO 13849-1 ist das Ergebnis einer grundsätzlichen Überarbeitung der Norm. Dabei wurden auf Basis der bewährten Konzepte eine klarere Struktur etabliert und weitere Anwendungshilfen hinzugefügt. Auch wenn im Ergebnis der Seitenumfang deutlich gewachsen ist – die Anwendungsfreundlichkeit ist es auch.

Die bekannten Anwendungshilfen des IFA zur DIN EN ISO 13849 werden sukzessive an die Änderung der Norm angepasst und unter www.dguv.de/ifa/13849 verfügbar gemacht. Der Software-Assistent SISTEMA wird in einer zukünftigen Version 3.0 alle Änderungen enthalten und auch die IFA Reports 2/2017 und 4/2018 inklusive der Schaltungsbeispiele werden nach und nach an den neuen Stand der Norm angepasst werden.

19 Literatur

[1] ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (04.23). Beuth, Berlin 2023

[2] DIN ISO/TR 23849; DIN SPEC 33883: Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen (12.14). Beuth, Berlin 2014

[3] DIN ISO/TR 22100-2: Sicherheit von Maschinen - Beziehung zu ISO 12100 - Teil 2: Wie ISO 12100 und ISO 13849-1 zusammenhängen (09/14). Beuth, Berlin 2014

[4] DIN IEC/TR 63074: Maschinensicherheit - Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen (05/21). Beuth, Berlin 2021
(aktuellere englische Fassung: PD IEC/TS 63074: Safety of machinery – Security aspects related to functional safety of safety-related control systems (02/23). Beuth, Berlin 2023)

[5] Apfeld, R.; Hauke, M.; Otto, S.: Das SISTEMA-Kochbuch - Teil 6: Definition von Sicherheitsfunktionen - Was ist wichtig? - Version 1.0 (DE). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015
http://www.dguv.de/webcode/d109240

[6] DIN EN 61131-3: Speicherprogrammierbare Steuerungen - Teil 3: Programmiersprachen (06/14). Beuth, Berlin 2014

[7] Bömer, T.; Büllesbach, K.-H.; Hauke, M.; Otto, S.; Werner, C.: Praxisgerechte Umsetzung der Anforderungen für sicherheitsbezogene Embedded-Software nach DIN EN ISO 13849-1 (IFA Report 1/2020). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2020.
http://www.dguv.de/webcode/d1182706

[8] DIN EN 61000-6-7: 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 (12.15). Beuth, Berlin 2015

[9] DIN EN IEC 61000-6-2: Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen – Störfestigkeitsanforderungen für Industriebereiche (11.19). Beuth, Berlin 2019

[10] VDMA 66413: Funktionale Sicherheit – Universelle Datenbasis für sicherheitsbezogene Kennwerte von Komponenten oder Teilen von Steuerungen (10.12). VDMA-Einheitsblatt, Verband Deutscher Maschinen- und Anlagenbau e.V., Frankfurt/Main 2012. Beuth, Berlin 2012

Verfasst von: Michael Hauke, Thomas Bömer, Karl-Heinz Büllesbach
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin

Herausgeber

Deutsche Gesetzliche
Unfallversicherung e.V. (DGUV)

Glinkastraße 40
10117 Berlin
Telefon: 030 13001-0 (Zentrale)
Fax: 030 13001-9876
E-Mail: info@dguv.de
Internet: www.dguv.de
Webcode: p022401