DGUV Test
Prüf- und Zertifizierungssystem der
Deutschen Gesetzlichen Unfallversicherung

Kann mit einer Standard-SPS PL c erreicht werden?

Sind elektronische Baugruppen als Alternative zu bewährten Bauteilen in Kategorie 1 geeignet?

06
06/2022

Fragestellung

In der Norm DIN EN ISO 13849-1 für sichere Steuerungen an Maschinen werden Steuerungsarchitekturen fünf Kategorien zugeordnet, die einen von fünf Performance Level (PL) erreichen können. Höhere Zuverlässigkeitskennwerte PL erlauben einen Einsatz in Anwendungen mit höherem Risiko.

Einkanalige elektronische Steuerungen ohne Testung und Redundanz erreichen nach aktuellem Stand der Norm nur die niedrigste Kategorie B und maximal PL b. Werden ausschließlich sogenannte bewährte Bauteile eingesetzt, ist die höhere Kategorie 1 und PL c erreichbar.

Die Norm beschränkt diese Möglichkeit allerdings auf bestimmte Technologien: Komplexe elektronische Bauteile, z. B. Speicherprogrammierbare Steuerungen (SPS), Mikroprozessoren und Anwendungsspezifische Integrierte Schaltungen (ASICs), dürfen nicht als bewährte Bauteile betrachtet werden.

Von Seiten der Maschinen-Anwender gab es immer wieder Initiativen, nach über zwei Jahrzehnten Erfahrung mit dem Einsatz elektronischer Komponenten für sicherheitsgerichtete Steuerungen, diese Beschränkung abzuschaffen. Der Verein Deutscher Werkzeugmaschinenfabriken e.V. (VDW) veröffentlichte 2017 eine Studie zur Betriebsbewährtheit von automatischen Multi-Spindel Drehmaschinen, bei denen die Sicherheitsfunktion Werkstückspannung mit einer Standard-SPS angesteuert wird (https://vdw.de/sicherheit-von-standard-sps-steuerung-erneut-belegt-2/).

Auch in Normungsgremien wird dieses Argument diskutiert. Obwohl meist das Beispiel einer Standard-SPS genannt wird, betrifft die grundlegende Fragestellung auch alle anderen Baugruppen mit komplexen elektronischen Steuerungskomponenten, z. B. Mikroprozessoren und integrierte Schaltungen.

Vor diesem Hintergrund und mit Blick auf die kommende Überarbeitung des zweiten Teils der DIN EN ISO 13849, in dem typische bewährte Bauteile für verschiedene Technologien aufgelistet werden, hat sich ein Arbeitskreis aus verschiedenen DGUV Test Prüf- und Zertifizierungsstellen mit dieser Thematik befasst. In diesem Papier wird die gemeinsame Position dargestellt.

Positionierung DGUV Test

Einige Argumente werden immer wieder angeführt, um die **Bewährtheit komplexer elektronischer Komponenten** zu belegen. Diese Begründungen lassen sich wie folgt entkräften:

- Statistische Argumente, die z. B. anhand von Reparaturhistorien geringe Ausfallzahlen nennen, oder die Behauptung, es gäbe kein relevantes Unfallgeschehen

  ► Statistische Erfassungen weisen oft systematische Unzulänglichkeiten auf. Sporadische, nicht-reproduzierbare Ausfälle (z. B. durch Soft-Errors) und Software-Fehler tauchen nicht in Statistiken über ausgetauschte Komponenten auf. Beinahe-Unfälle sind meist nicht oder nicht aussagekräftig dokumentiert.

- Da komplexe Elektronik seit mehreren Jahrzehnten für Funktionale Sicherheit eingesetzt wird, wird behauptet, diese habe mittlerweile eine vergleichbare Zuverlässigkeit wie z. B. Elektromechanik und Fluidtechnik erreicht.

  ► Komplexe Elektronik und ihre Software unterliegen häufig sehr viel kürzeren Innovationszyklen als Elektromechanik und Fluidtechnik. In der Hardware werden z. B. Bauteile auf der Leiterplatte durch modernere Typen ersetzt, Bauteile werden von anderen Lieferanten bezogen, das Design wird modifiziert oder miniaturisiert oder die Fertigungstechnik modernisiert. Die Embedded-Software wird zur Fehlerbehebung oder um neue Funktionalitäten zu ermöglichen regelmäßig aktualisiert. Daher ist Bewährtheit dort trotz hohem Entwicklungsaufwand kaum zu erreichen (siehe z. B. Pentium-Bug: https://de.wikipedia.org/wiki/Pentium-FDIV-Bug).

- In manchen Anwendungen (z. B. Werkzeugmaschinen oder Erdbaumaschinen) wird einkanalige komplexe Elektronik (Standard-SPS oder Standard-Sensoren) in Kategorie B für PL b bereits schon länger für Sicherheitsfunktionen eingesetzt, die im Fehlerfall bei Versagen der Sicherheitsfunktion zu schweren (tödlichen oder irreversiblen) Verletzungen führen können. Wendet man zur Bestimmung des erforderlichen Performance Levels (PL_r) den Risikograph der DIN EN ISO 13849-1 an, wäre im Fall schwerer Verletzungen im Vergleich dazu ein PL_r von c oder höher das Ergebnis. Lösungen zum Erreichen von PL c oder höher (einkanalig getestet oder zweikanalig) seien jedoch technisch zu aufwändig, die Kosten dafür zu hoch oder die Leistungsfähigkeit nicht ausreichend.

  ► Produktnormen können die Anforderungen in ihrem Anwendungsbereich individuell festlegen und können dabei von den in Sicherheitsfachgrundnormen wie DIN EN ISO 13849-1 genannten Grundsätzen abweichen, um anwendungsspezifische Besonderheiten, den Stand der Technik und das Unfallgeschehen (z. B. wenn nur leichte, reversible Verletzungen vorkommen) angemessen zu berücksichtigen. Dabei können als unangemessen hoch bewertete Anforderungen an die Zuverlässigkeit der Maschinensteuerung im begründeten Einzelfall auch heruntergestuft und durch ausrüstungstechnische oder organisatorische Anforderungen ergänzt werden, solange eine vergleichbare Sicherheit auf anderem Wege erreicht wird. Weiterhin gibt es seit der dritten Ausgabe der Norm von 2016 grundsätzlich die Möglichkeit, durch die Berücksichtigung einer niedrigen Eintrittswahr-

scheinlichkeit eines Gefährdungsereignisses bei der Risikobewertung den PL_r um ein Level zu verringern. Die Festlegung möglichst konkreter, praktikabler und wirksamer Anforderungen ist sowohl im Interesse der Anwender als auch des Arbeitsschutzes.

Um die Bewährtheit komplexer Elektronik, speziell programmierbarer Komponenten wie z. B. einer Standard-SPS, zu beurteilen, erfordern **folgende bekannte Fehlerquellen und Schwachstellen** besondere Aufmerksamkeit:

- Unfalluntersuchungen zeigen Ausfälle komplexer Elektronik als Ursachen für Steuerungsversagen. Beispiele sind u. a. das Durchlegieren von Ausgangskarten, welches zu Stuck-At-Fehlern (statische Signale, Kurzschluss oder Unterbrechung) führt, oder das Nicht-Zurücknehmen eines Interrupts. Es wurde auch beobachtet, dass die Spannungsversorgung nicht komplett zurückgenommen wurde und ein niedriger Spannungspegel von 5 V reichte, um Ausgangsschaltelemente (z. B. Schütze, Relais, elektromechanisch angesteuerte Ventile) im gehaltenen Zustand zu belassen.

  ► Können hier geeignete Maßnahmen zur Fehlererkennung und Fehlerreaktion getroffen werden, die beim Auftreten eines gefährlichen Fehlers zum Erreichen eines sicheren Zustands führen?

- Schwankungen in der Energieversorgung (speziell Überspannungen), Alterung von Bauteilen, Signaldrift, elektromagnetische Störungen und andere Umwelteinflüsse (z. B. Temperatur, Luftfeuchte, anwendungsspezifische Besonderheiten) können zu undefinierten und gefährlichen Zuständen führen.

  ► Kann eine ausreichende Widerstandsfähigkeit sichergestellt werden, z. B. orientiert an SIL-1-Umweltanforderungen in Tabelle A.16 und B.5 der DIN EN 61508-2, an den Umgebungsanforderungen in Abschnitt 4.3 der DIN EN IEC 61496-1 und an den erhöhten Anforderungen hinsichtlich Widerstandsfähigkeit gegenüber elektromagnetischen Störungen in Abschnitt 12.5 der DIN EN 61131-6 (funktionale Sicherheit), die über die Anforderungen in Abschnitt 8.3 DIN EN 61131-2 (Betriebsmittelanforderungen und Prüfungen) hinausgehen? Die DGUV Test Information 15 und ein neuer Anhang L in der kommenden vierten Ausgabe der DIN EN ISO 13849-1 geben weitere Hinweise zur praktischen Umsetzung der Anforderungen an eine ausreichende elektromagnetische Verträglichkeit.

- Im Gegensatz zur Anwendungs-Software ist bei programmierbaren Standard-Komponenten die Embedded-Software (Betriebssystem) für den Integrator oder Anwender nicht zugänglich. Sie wurde weder vom Hersteller für Sicherheitsanforderungen ausgelegt, noch kann dies vom Anwender auf einfache Weise nachgeholt werden. Auch ein Nachweis der Betriebsbewährung für die Embedded-Software kann in der Praxis wegen systematischer Schwierigkeiten in der statistischen Erfassung nicht begründet werden (s. o. „statistische Argumente“).

  ► Diese Problematik wird in DIN EN ISO 13849-1 aufgegriffen, indem dieser Fall für PL a und b bei Umsetzung mit Kategorie B, 2 oder 3 toleriert wird. Für PL c und d mit Kategorie 2 oder 3 wird alternativ die Verwendung diversitärer Technologien gefordert. Eine einkanalige Realisierung (Kategorie B oder 1) in PL c ist wegen des Ausschlusses komplexer Elektronik als bewährtes Bauteil für Kategorie 1 nicht vorgesehen.

Die bisher genannten Argumente, Fehlerquellen und Schwachstellen führen zusammengefasst auf folgende **Argumente, die den Ausschluss komplexer elektronischer Komponenten aus der Liste bewährter Bauteile nach wie vor rechtfertigen**:

- Standard-SPSen und andere komplexe elektronische Komponenten, z. B. Sensoren, sind in einer unüberschaubaren Vielzahl (z. B. Kompaktsteuerung, Laptop, Mikrokontrollersysteme) mit kurzen Innovationszyklen und dadurch sehr preiswert erhältlich.

- Komplexe elektronische Bauteile zeigen ein vielfältiges, teilweise unvorhersehbares Ausfallverhalten, z. B. ausgelöst durch elektromagnetische Störungen. Software-Fehler oder Soft-Errors sind praktisch nicht mehr vollständig beherrschbar. Folgerichtig dürfen diese grundsätzlich nicht als „Black Box“ mit einfachem, definiertem Ausfallverhalten betrachtet werden.

- Die Änderungsrate komplexer elektronischer Bauteile (Modifikation von Hardware und Software) ist deutlich höher als bei Elektromechanik und Fluidtechnik, daher besteht eine zusätzlich erhöhte Wahrscheinlichkeit für systematische Ausfälle. Diese ergeben sich aus Fehlern im Entwicklungs- und Fertigungsprozess.

- Für Kategorie 1 und PL c fordert die Norm neben den grundlegenden Sicherheitsprinzipien auch die Umsetzung der bewährten Sicherheitsprinzipien. Ein belastbarer Nachweis über die Erfüllung insbesondere folgender Anforderungen ist somit erforderlich: Überdimensionierung, Gleichgewicht zwischen Komplexität und Vereinfachung, Trennung sicherheitsbezogener von anderen Funktionen, sowie für Software: Integrität und Zuverlässigkeit, Vermeidung undefinierter Zustände. Dieser Nachweis ist nach den geltenden Anforderungen für einkanalige komplexe Elektronik nicht umsetzbar.

Positionierung DGUV Test

Unter Berücksichtigung der hier genannten Argumente, Fehlerquellen und Schwachstellen ist der bestehende Ausschluss komplexer elektronischer Komponenten aus der Liste bewährter Bauteile nach wie vor richtig.

Alternative Möglichkeiten, PL ≥ c unter Verwendung einer Standard-SPS zu realisieren

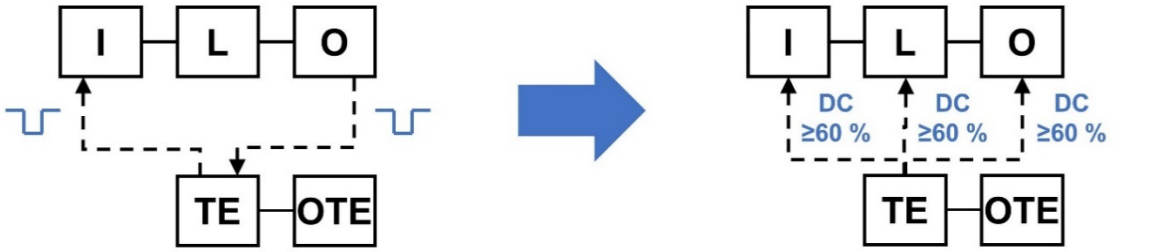
Nach DIN EN ISO 13849-1 kann ein PL c statt mit einkanaligen Steuerungen unter Verwendung bewährter Bauteile (Kategorie 1) auch mit einkanaligen getesteten Steuerungen (Kategorie 2) oder zweikanaligen getesteten Steuerungen (Kategorie 3) erreicht werden. Diese beiden alternativen Möglichkeiten können je nach Steuerungsaufgabe schon mit einem überschaubaren zusätzlichen Aufwand umgesetzt werden.

Allerdings sind wie in Kategorie 1 auch in Kategorie 2 und 3 zusätzlich zu den grundlegenden Sicherheitsprinzipien bewährte Sicherheitsprinzipien umzusetzen und alle normativen Anforderungen an die entsprechende Kategorie zu erfüllen. Besonderes Augenmerk erfordert hier die effektive Testhäufigkeit und die Widerstandsfähigkeit gegen Ausfälle gemeinsamer Ursache, die eine ausreichende Unabhängigkeit von Testeinrichtung und Funktionskanal einschließt.

Realisierung in Kategorie 2

- Bei Steuerungen gemäß Kategorie 2 wird es mit der kommenden vierten Ausgabe der DIN EN ISO 13849-1 nicht mehr erforderlich sein, die fehlerfreie Ausführung der gesamten Sicherheitsfunktion in geeigneten Zeitabständen zu testen. Dann reicht eine Testung des Funktionskanals mit mindestens niedrigem Diagnosedeckungsgrad (DC), d. h. 60 % der gefährlichen Fehler müssen erkannt werden. Diese Mindestanforderung an die Testabdeckung muss allerdings für jeden der Blöcke Input (I), Logik (L) und Output (O) im Funktionskanal einzeln erfüllt werden. Da somit nicht mehr der Ausfall der Sicherheitsfunktion, sondern – speziell für PL c – nur ein Großteil der gefährlichen Fehler durch Tests erkannt werden muss, lohnt sich eine Prüfung der Umsetzbarkeit als Kategorie 2 im Einklang mit den Anforderungen der Norm.

Abb. 1: Beispielhafte Realisierung einer Steuerung gemäß Kategorie 2 in der kommenden vierten Ausgabe der DIN EN ISO 13849-1, Quelle DGUV Test



DIN EN ISO 13849-1:2016
(dritte Ausgabe)

Test der Sicherheitsfunktion
in angemessenen Zeitabständen
durch die Maschinensteuerung

vierte Ausgabe der DIN EN ISO 13849-1
(voraussichtlich 2022/2023)

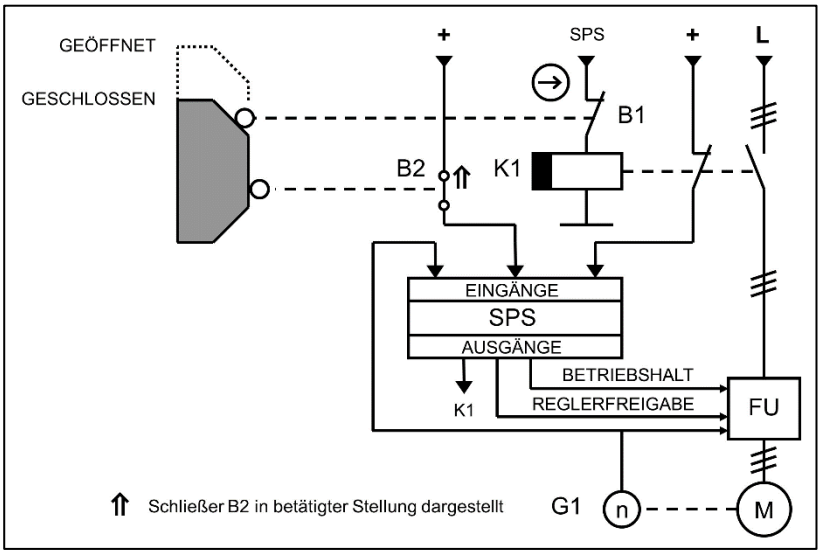
Testung des Funktionskanals (I, L, O)
in angemessenen Zeitabständen;
der DC aller Teile des Funktionskanals
(I, L, O) muss mindestens niedrig sein

Realisierung in Kategorie 3

- Das Hinzufügen eines zweiten Funktionskanals, der sich mit wenigen Bauteilen auf die reine Ausführung der Sicherheitsfunktion beschränkt, erweitert die Steuerung auf eine Kategorie 3. Da mit der Standard-SPS bereits eine (programmierbar) elektronische Komponente vorhanden ist, lässt sich oft auch der mindestens erforderliche niedrige Diagnosedeckungsgrad mit begrenztem Aufwand nachrüsten.

  Steuerungsbeispiel B in Anhang I der DIN EN ISO 13849-1 zeigt eine solche Umsetzung, mit der unter gewissen Voraussetzungen sogar PL d erreicht werden kann, wenn alle normativen Anforderungen eingehalten werden. Dort wird der bestehende Funktionskanal aus Positionsschalter B2, Standard-SPS und Frequenzumrichter FU um einen zweiten elektromechanischen Funktionskanal erweitert, der mit einem weiteren Positionsschalter B1 und einem Hilfsschütz K1 auskommt. Die notwendige Fehlererkennung wird hauptsächlich in der bestehenden Standard-SPS implementiert:

  Abb. 2: Beispielhafte Realisierung einer Steuerung gemäß Kategorie 3 basierend auf Abschnitt I.4 der DIN EN ISO 13849-1, Quelle DGUV Test



B1	Positionsschalter (Öffner mit zwangsöffnenden Kontakten)
B2	Positionsschalter (Schließer, in betätigter Stellung dargestellt)
K1	Hilfsschütz (abfallverzögerte Kontakte)
SPS	Speicherprogrammierbare Steuerung ohne integrierte Sicherheit
FU	Frequenzumrichter
G1	Drehgeber
M	Motor

Weiterführende Informationen

- DIN EN ISO 13849-1:2016-06, Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015)
  Die überarbeitete vierte Ausgabe der DIN EN ISO 13849-1 soll in der ISO-Fassung Ende 2022 erscheinen und in der DIN-Fassung 2023.

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

- Sichere Maschinensteuerungen nach DIN EN ISO 13849: www.dguv.de/ifa/13849

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

- DIN EN IEC 61496-1:2021-06, Sicherheit von Maschinen - Berührungslos wirkende Schutzeinrichtungen - Teil 1: Allgemeine Anforderungen und Prüfungen (IEC 61496-1:2020)

- DIN EN 61131-2:2015-06, Speicherprogrammierbare Steuerungen - Teil 2: Betriebsmittelanforderungen und Prüfungen (IEC 65B/957/CD:2014)

- DIN EN 61131-6:2013-10, Speicherprogrammierbare Steuerungen - Teil 6: Funktionale Sicherheit (IEC 61131-6:2012)

- EMV und Funktionale Sicherheit im Maschinenbereich, Erhöhte Störfestigkeit im Kontext der DIN EN ISO 13849-1 bei der Integration von SRP/CS, DGUV Test Information 15 (12/2016), www.dguv.de/dguv-test Webcode: m819745

Geschäftsstelle DGUV Test
Alte Heerstraße 111
53757 Sankt Augustin
Telefon: +49 30 13001-4566
Fax: +49 30 13001-864566
E-Mail: dguv-test@dguv.de