Im Wandel

Vergleich und Verkettung unterschiedlicher Sicherheitsnormen

Gerhard Plüddemann, Dr. Michael Schäfer, Michael. Hauke*

Safety
Bericht

Aktuelle Produktinformationen sicherheitsrelevanter Komponenten für Maschinensteuerungen zeigen deutlich: Neben der bisherigen Kennzeichnung der funktionalen Sicherheit durch eine Kategorie nach der bewährten Norm EN 954, nach wie vor die einzige harmonisierte Norm für elektrische und nichtelektrische Systeme im Sicherheitsbereich, findet man immer häufiger die Angabe SIL (Safety Integrity Level nach IEC 61508 bzw. IEC 62061) und PL (Performance-Level nach ISO 13849)), meist zusätzlich zu der Angabe einer Kategorie nach EN 954.

Zur IEC 61508 und SIL: Die SIL-Angabe ist vor allem bei komplexen elektronischen Baugruppen, buskompatiblen und softwarebasierten Geräten zu finden, deren Beurteilung durch ein deterministisches Normenwerk wie der EN 954 kaum noch möglich ist. SIL-Level sind nach der Sicherheitsnorm IEC 61508 definiert, die das Beurteilen der Zuverlässigkeit von technischen Sicherheitsfunktionen durch die Anwendung von quantifizierenden Verfahren der Wahrscheinlichkeitsrechnung definiert. Neben diesen rein technisch orientierten Inhalten befasst sich die IEC 61508 auch mit Entwicklungs- und produktionsorientiertem Qualitätsmanagement und dem Lebenszyklusmodell eines Produkts. Als übergreifende Norm für elektrisch basierte Sicherheitstechnik von der Prozesstechnik bis zum Maschinenbau bildet das Werk in 7 Teilen (plus einen Teil 0) schon einen recht repräsentativen Papierstapel. Die Listung in der Maschinenrichtlinie der EU und die damit verbundene Harmonisierung und Gleichstellung mit der EN 954 ist jedoch anderen Normen vorbehalten, so z.B. der IEC 62061, die sich speziell mit Maschinensteuerungen befasst, im Wesentlichen jedoch auf die Mutternorm IEC 61508 verweist.

Weiterentwicklung der EN 954 (ISO 13849)

Doch auch im Bereich der EN 954 ist die Zeit nicht stehen geblieben. Mit der Internationalisierung war die Umbenennung in ISO 13849 verbunden. Besondere Aufmerksamkeit widmete man dabei der Überarbeitung des Teils 1 der EN 954. Hier wurden quantifizierende Methoden zum Beurteilen der funktionalen Sicherheit eingepflegt, viel Wert auf einfache Handhabung und die Ausrichtung auf die für Maschinensteuerungen typischen Merkmale und Architekturen gelegt. Zur Klassifizierung der Risikoreduzierung wurde ein neuer Parameter generiert: Der Performance-Level PL. Die EN 954 wird durch die nach Europäischer Harmonisierung rechtsgültige ISO 13849 ersetzt und umfasst auch nach der Umdeklarierung als ISO 13849 nach wie vor zwei Teile, die beide harmonisiert sind, und damit die Vermutungswirkung zur rechtsverbindlichen Maschinenrichtlinie besitzen.

Es gibt einen ganz grundlegenden Unterschied im Anwendungsbereich der genannten Nomen: Während sich die IEC 61508 elektrotechnisch basierten Baugruppen widmet, kennt die ISO 13849 diese Einschränkung nicht: Sie ist auf alle im Maschinenbau vorkommenden Steuerungsarten anwendbar, sei es in der elektrischen oder der fluidisch orientierten Steuerungstechnik. Doch es lohnt sich, auch einen Blick auf die Gemeinsamkeiten der Normen ISO 13849 und IEC 61508 zu werfen. Obwohl die Betonung der Fehlervermeidung in Entwurf und Entwicklung in beiden Normen stark unterschiedlich ist, knüpfen beide Normen (die ISO 13849 und die IEC 61508 bzw. IEC 62061) die Beurteilung von Sicherheit an die Widerstandsfähigkeit gegenüber zufälligen Hardwarefehlern. Diese wird bestimmt von Ausfallwahrscheinlichkeiten pro Zeiteinheit für gefährliche Fehler, der technischen Architektur der Schaltung (einkanalig/mehrkanalig), der Chance, Fehler zu entdecken, bevor sie zu gefährlichen Ausfällen führen, und die Betrachtung von Fehlern gemeinsamer Ursache, die mehrere Funktionen gleichzeitig „lahm“ legen könnten.

Während die IEC 13849 mit einer Auswahl vorberechneter Strukturen arbeitet und maschinenbautypische Risiken abdeckt, ist die IEC 62061 nicht auf feste Strukturen festgelegt und in der Lage, bei komplexen Schaltungen höhere Risiken abzudecken. Mit der IEC 62061 liegt eine auf den Maschinenbau orientierte Norm vor, die SIL – bezogen ist und, ebenso wie die ISO 13849, von Sicherheitsfunktionen mit hoher Anforderungsrate ausgeht. Durch die derzeitige Koexistenz mehrerer Normenwerke (EN 954, ISO 13849, IEC 62061) ist es naheliegend, dass in der Praxis Komponenten gleicher oder unterschiedlicher Sicherheitsdefinitionen miteinander linear verkettet werden. So lassen sich die Verkettungen bewerten: Zur li-

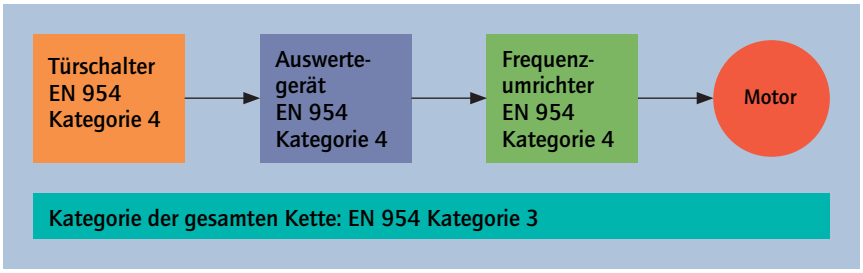

Bild 1: Lineare Verkettung von sicherheitsrelevanten Funktionsblöcken nach EN 954

*Dipl.-Ing. Gerhard Plüddemann, Ingenieurbüro Plüddemann, Viernheim, Dr. Michael Schäfer, BGIA St. Augustin, Michael Hauke, BGIA St. Augustin.

nearen Verkettung sicherheitsrelevanter Komponenten nach EN 954: Eine Sicherheitsfunktion (z.B. Sicherer Halt eines Antriebs) besteht oft aus mehreren verketteten Komponenten, z.B. einem Sicherheitsschalter an einer Schutztür, einem Sicherheitsbaustein zur Auswertung der Schaltersignale und einem Frequenzumrichter mit Motor (Bild 1). Die Beurteilung der Gesamtkette ist eine einfache Sache aus Sicht der EN 954. Hier ist die geringste in der Kette vorkommende Sicherheitskategorie (z.B. Kategorie 3) für die gesamte Kette maßgebend, unabhängig von der Anzahl der verketteten Systeme. Zur linearen Verkettung sicherheitsrelevanter Komponenten nach ISO 13849: Ein etwas längerer Blick ist notwendig bei der Verkettung von Komponenten mit PL nach ISO 13849. Doch auch hier ist die Lösung in den meisten Fällen schnell durch Anwendung einer Kombinationstabelle für die Reihenschaltung von Systemen gefunden. Das geringste PL und dessen Anzahl bestimmen das PL der gesamten Kombination (siehe Beispiel: Bild 2 und Tabelle 1).

Bezug mechanischer Schalter auf SIL

Zur linearen Verkettung sicherheitsrelevanter Komponenten nach IEC 61508 bzw. IEC 62061: Beim Verketten von Systemen, die mit einem SIL-Level nach IEC 61508 ausgestattet sind, basiert die Gesamtbeurteilung in erster Linie auf der Addition der Zuverlässigkeitswerte der Einzelsysteme. Es ist also notwendig, sich vom SIL-Begriff zu lösen und stattdessen die PFH-Werte (Probability of dangerous failure per hour) zu addieren, die dem SIL-Level zugrunde lagen. Sollten diese Werte nicht bekannt sein, so sind sie beim Hersteller zu erfragen. Über das Gesamt-PFH kann dann der SIL der Funktion bestimmt werden. Die Betrachtung weiterer Rahmenbedingen ist notwendig (Hardware-Fehlertoleranz, Proof-Test Interval, Safe Failure Fraction).

Was aber, wenn Systeme verkettet werden, die nach unterschiedlichen Normensystemen spezifiziert sind? Da umfassende Konvertierungstabellen nicht verfügbar sind, müssen auf den Einzelfall bezogene Überlegungen angestellt werden.

Soll z.B. ein mechanischer Sicherheitsschalter in eine Kette eingereiht werden, die eine SIL-Definition verlangt, so kann z.B. mittels in der ISO 13849 genannter Methoden der PFH-Wert des Schalters anhand von Herstellerdaten (B10d-Wert) und der Nutzungsrate errechnet werden und dann mit den PFH-Werten der anderen Systeme in der Kette addiert werden. Die Betrachtung weiterer Rahmenbedingen ist notwendig (Hardware-Fehlertoleranz, Proof-Test Interval, Safe Failure Fraction).

Konvertierung von PL und Kat. nach SIL

Schwieriger wird es, Systeme, die nach ISO 13849 mit PL definiert sind, nach SIL gem. IEC 61508 zu konvertieren. Ein rein technischer Vergleich ist durch die Anwendung einer Zuordnungstabelle PL zu SIL über den Parameter PFH möglich (Tabelle 2). Ein weiterer wichtiger Vergleichsparameter ist die Systemarchitektur (1- oder 2-Kanaligkeit bzw. HFT= Hardware-Fehlertoleranz Hardware Failure Tolerance). Die Bewertung des Diagnosedeckungsgrads und die Behandlung von Fehlern gemeinsamer Ursache (CCF) sollten bei konsequenter Anwendung der Normen in beiden Normenwelten vergleichbar abgedeckt sein. Da jedoch die IEC 61508 über die rein technischen Anforderungen hinaus auch Anforderungen des Qualitätsmanagements und des Produktlebenszyklus abdeckt, stärker betont, kann aus einem PL nicht automatisch ein SIL werden, ohne diese Aspekte zu berücksichtigen. Weil die praxisrelevanten Aspekte der Vermeidung systematischer Fehler in der ISO 13849 aber ebenfalls berücksichtigt werden müssen, wird Vergleichbarkeit wohl meist gegeben sein. Umgekehrt ist der Vergleich über die Zuordnung von PFH (Tabelle 2) ▶

geringster PL	Anzahl der Elemente mit dem geringsten PL	Gesamt-PL
a	größer 3	keiner, nicht erlaubt
	bis 3	a
b	größer 2	a
	bis 2	b
c	größer 2	b
	bis 2	c
d	größer 3	c
	bis 3	d
e	größer 3	d

Tabelle 1: Bestimmung des verketteten Performance Level (PL) der Kombination aus Bild 1. Quelle: BGIA/prEN ISO 13849.

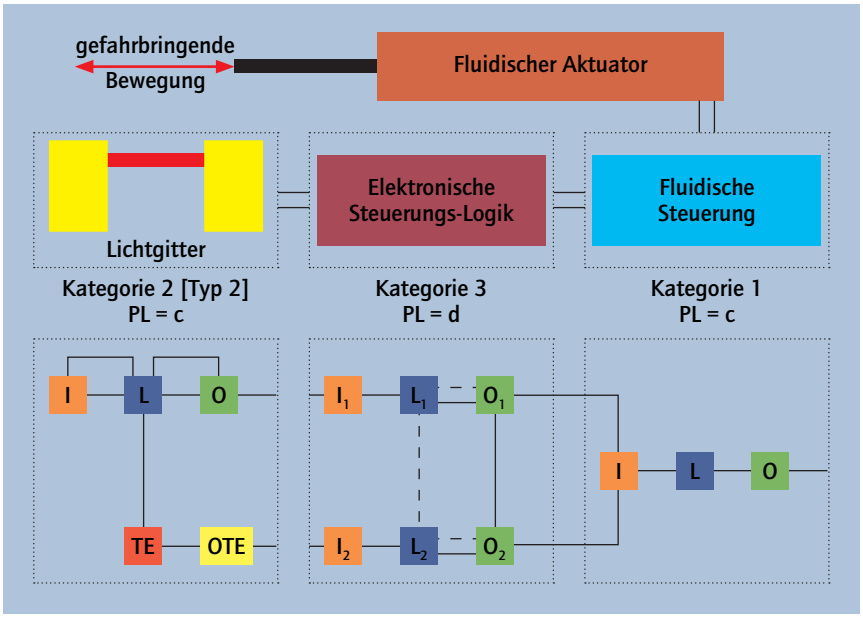

Bild 2: Lineare Verkettung von sicherheitsrelevanten Funktionsblöcken nach ISO 13849.

ISO 13849 Performance LevelPL	Wahrscheinlichkeit gefährlicher Fehler pro Stunde, PFH (1/h)	IEC 61508 Safety Integrity Level SIL
a	≥ 10-5 bis < 10-4	nicht definiert
b	≥ 3*10-6 bis < 10-5	1
c	≥ 10-6 bis < 3*10-6	1
d	≥ 10-7 bis < 10-6	2
e	≥ 10-8 bis < 10-7	3
nicht definiert	≥ 10-9 bis < 10-8	4

Tabelle 2: Der Vergleich über die Zuordnung von PFH gilt als einfach, weil die über SIL abgedeckten organisatorischen Anforderungen nicht aufwändig dokumentiert werden müssen.

STANDPUNKT

Gerhard Plüddemann, Ingenieurbüro Plüddemann:

„Der Umgang mit den verschiedenen Normen, die alle das gemeinsame Ziel haben, Unfälle zu vermeiden und Menschen zu schützen, ist etwas verwirrend und stellt Anwender ebenso wie Sachverständige vor manch neue Frage. Etwas mehr ‚Homogenität' wäre wünschenswert. Um dem Rechnung zu tragen, sind in den Normengremien neue Ideen bereits im Brutkasten. Ziel: Eine Norm, die die Inhalte der ISO 13849 und die der IEC 62061 zukünftig in einem Werk zusammenführt. Aus heutiger Sicht stellt die Definition elektrischer Systeme nach SIL den deutlich aufwändigeren, aber auch, nicht zuletzt durch die gute Konvertierbarkeit nach PL, den universelleren Weg dar, wobei jedoch die ISO 13849 durch die Abdeckung elektrischer, fluidischer und mechanischer Systeme ein breiteres Anwendungsfeld aufweist."

▶etwas einfacher, da die über SIL abgedeckten organisatorischen Anforderungen verglichen mit dem Profil von PL und Kat. nicht in entsprechend aufwändigem Maße dokumentiert werden müssen. Beim Konvertieren von SIL zu PL und Kat. gilt allerdings die Einschränkung, dass ein SIL 3 – System nur dann ein PL e nach ISO 13849 bekommen kann, wenn es mehrkanalig aufgebaut ist, auch wenn die Rate der sicheren Ausfälle (SFF) nach IEC 61508 größer oder gleich 99% ist.

Konvertierung von SIL nach PL und Kat.

Die Konvertierung von SIL in Kat. ist allerdings recht heikel, weil die Kategorien über typische Strukturmerkmale genau definiert sind, die sich aus einer reinen Ausfallwahrscheinlichkeit nicht mehr nachträglich herauslesen lassen. Hier sind zwar Analogieschlüsse möglich, aber im Einzelfall zählt doch der genaue Blick bzw. die Rückfrage beim Hersteller. Der Einsatz eines Bussystems präsentiert sich durch einen weiteren Block in einer linearen Systemkette. Die Sicherheit des Busaufbaus gründet sich neben den zugehörigen Hardwarekomponenten vor allem auf den Aufbau des Busprotokolls. Auch hier ist eine Quantifizierung durch Ermittlung eines PFH-Wertes möglich und in der Fachliteratur beschrieben. (siehe „Sichere Bussysteme für die Automation", Hüthig-Verlag, ISBN 3-7785-2797-5). Ist allerdings die ausreichende Unwahrscheinlichkeit von Fehlern in der Datenübertragung nachgewiesen, so braucht der rechnerische Ausfallwert in der Systemkette nicht mehr berücksichtigt werden. Ohne Fehlerausschlüsse geht es nicht. Auf die Zuverlässigkeit einer Schaltschrankverdrahtung z. B. muss man sich verlassen können. Hier werden auch von Anwendern der IEC 61508 die Angaben der ISO 13849-2 herangezogen. (Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Teil 2: Validierung). *(klu)*

Ing.-Büro Plüddemann
Tel. +49(0)6204 608249

www.elektrotechnik.de
Homepage Plüddemann

InfoClick 194355