IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Unterschiede bei der Verwendung von fertigen Sicherheitsbauteilen und Standardbauteilen für die Realisierung von Sicherheitsfunktionen an Maschinen

Kurzgefasst:

1. Sicherheitsrelevante Steuerungen können grundsätzlich durch den Einsatz von Standardkomponenten realisiert werden, jedoch bieten Sicherheitsbauteile den Vorteil, dass der Maschinenkonstrukteur bei der sicherheitstechnischen Beurteilung und Analyse der verwendeten Bauteile durch den Hersteller von Sicherheitsbauteilen entlastet wird.

2. Zum Erreichen funktionaler Sicherheit ist neben der Verwendung einer geeigneten Architektur (Kategorie), der Realisierung einer erforderlichen Fehlererkennung und der Berücksichtigung von Ausfallraten/-wahrscheinlichkeiten die systematische Eignung von Komponenten zu beachten.

3. Auszuschließen ist im Allgemeinen der Einsatz komplexer Elemente oder Teilsysteme gleichartiger Ausführung (homogene Redundanz), da Fragen nach der systematischen Eignung und der erforderlichen Fehleraufdeckung oft nicht ausreichend beantwortet werden können.

Der Einsatz von Standardkomponenten (Sensoren, Antriebselemente und Steuerelektroniken) in Sicherheitsapplikationen ist nach EN ISO 13849 grundsätzlich möglich. Dies gilt auch, wenn diese Komponenten nicht als Sicherheitsbauteile nach Anhang V der Maschinenrichtlinie 2006/42/EG ausgewiesen sind.

Die aktuellen Normen EN ISO 13849 Teil 1 und 2 (Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze [1], Teil 2: Validierung [2]) beschreiben neben dem bekannten Grundgerüst der Kategorien auch eine probabilistische Bewertung der erreichten funktionalen Sicherheit. Dabei kommt es durchaus zu Missinterpretationen bei der Normenanwendung im Zusammenhang mit dem Einsatz von Standardkomponenten.

Bei der Bewertung der funktionalen Sicherheit wurde die EN ISO 13849-1 gegenüber den Anforderungen der Vorgängernorm EN 954-1 insbesondere um den probabilistischen Aspekt, d. h., um die Verwendung von quantitativen Gerätegrößen erweitert. Das sind vor allem die Größen $MTTF_d$ (mittlere Zeit bis zum gefährlichen Ausfall eines Kanals in Jahren), DC (Diagnosedeckungsgrad in %) und CCF (Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache). Die genannten probabilistischen Aspekte sollen gemeinsam mit der Schaltungsstruktur in Form einer Kategorie bei Verwendung des sog. vereinfachten Ansatzes die neue Zielgröße der EN ISO 13849-1, den Performance Level PL, ergeben. Der Normensetzer hat das entscheidende Element der Vorgängernorm – die Kategorien – nicht grundlegend verändert, jedoch mit den oben genannten zusätzlichen Elementen angereichert. In der Modellierung der Kategorie 2 wurde weiterhin der Aspekt der Testhäufigkeit berücksichtigt.

Anwender der Norm gehen teilweise fälschlicherweise davon aus, dass die probabilistische Beurteilung, also die rechnerische Ermittlung des Performance Levels, für eine sicherheitstechnische Beurteilung ausreichend ist. Sie unterlassen dabei manchmal auch die geforderte Betrachtung

systematischer und umwelttechnischer Einflüsse. Der Performance Level gemäß EN ISO 13849 umfasst neben quantitativen Aussagen auch nicht quantifizierbare, qualitative Aspekte. Lässt sich zwar der rechnerische Nachweis einer ausreichend geringen Ausfallwahrscheinlichkeit/Stunde erbringen, doch fehlt die systematische Eignung, weil z. B. in einer Software noch versteckte Fehler schlummern oder eine Komponente schlichtweg für den Einsatzzweck ungeeignet ist, werden der vorgesehene Performance Level und damit die hinreichende Risikominderung nicht erreicht.

Der Inverkehrbringer von einzelnen Sicherheitsbauteilen (Subsystemen), die nach EN ISO 13849-1 und/oder anderen Normen gebaut sind, hat zum Nutzen des Maschinenkonstrukteurs bereits eine Vielzahl von Anforderungen berücksichtigt. Beispielhaft können dies sein:

- Einhaltung von grundlegenden und bewährten Sicherheitsprinzipien,
- Einfehlersicherheit,
- Bestimmung von $MTTF_d$ und DC,
- CCF-Bewertung (Ausfälle infolge gemeinsamer Ursache),
- Beachtung von Einflüssen und Umgebungsbedingungen, die zu systematischen Ausfällen führen können,
- Softwareanforderungen,
- Kategorie- und PL-Bestimmung,
- Anforderungen zur Dokumentation.

Verwendet der Maschinenkonstrukteur dagegen Standardkomponenten für die Realisierung von Sicherheitsfunktionen, muss er die Einhaltung sicherheitsrelevanter Anforderungen selbst beurteilen. Dies kann für ihn – gemessen an den heute gültigen und in Normen niedergelegten Maßstäben – mit einem erheblichen Aufwand verbunden sein oder auch in manchen Fällen praktisch unmöglich sein. Gründe, die ihm eine Beurteilung schwierig machen können, sind zum Beispiel fehlende Herstellerangaben. Zur Beherrschung systematischer Ausfälle ist es wichtig, dass die eingesetzte Komponente (Sensor, Steuerung,…) unter allen zu erwartenden und vorhersehbaren widrigen Einsatz- und Umgebungsbedingungen (Temperatur, Feuchte, Schwingungen, Elektromagnetische Verträglichkeit, optische Störgrößen wie z.B. Umspiegelungen und Fremdlicht…) korrekt arbeitet bzw. bei Ausfall die Maschine in einen sicheren Zustand versetzt wird. Umgebungsbedingungen müssen genauso wie Einsatzgrenzen der Komponente applikationsbezogen berücksichtigt werden. Mitunter kann sich auch die Realisierung und Festlegung eines DC für eine Standardkomponente schwierig gestalten, wenn sich diese nicht durch externe Einrichtungen ausführen lässt.

Generelle Regeln dafür, wann bestimmte Standardkomponenten in Sicherheitsapplikationen einsetzbar sind und wann nicht, können nicht definiert werden. Auszuschließen ist aber im Allgemeinen der Einsatz komplexer Subsysteme (z. B. Standard-SPS) in gleichartiger Ausführung (homogene Redundanz) für die Minderung mittlerer und hoher Risiken, da Fragen nach der systematischen Eignung und der erforderlichen Fehleraufdeckung oft nicht ausreichend beantwortet werden können. In einer Standardsteuerung könnten noch unentdeckte Entwicklungsfehler vorhanden sein. Wird in einer Gefahrensituation eine Sicherheitsfunktion angefordert, dann hilft in einem solchen Fall auch die Verwendung von zwei gleichen Steuerungen nicht, den sicheren Zustand der Maschine zu erreichen. Sicherheits-SPS bieten heute oft auch den Vorteil eines zugehörigen Tools, das den Anwender bei der sicherheitsgerichteten Programmierung und Parametrierung unterstützt (insbesondere in Bezug auf anzunehmende Fehler bei Editierung, Compilierung und Download) und den notwendigen Zugriffschutz sicherstellt.

Der Vorteil der Verwendung der im Blockdiagramm (Bild 1) dargestellten Kategorie 3 nach [1] liegt in der unabhängigen Ausführung der Sicherheitsfunktion durch die einzelnen Kanäle. Einflüsse, die zum gleichzeitigen Ausfall beider Kanäle führen können (sog. systematische Einflüsse) würden den Nutzen der Zweikanaligkeit (Redundanz) zunichte machen.

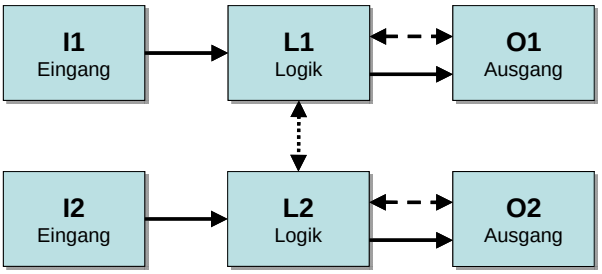

Bild 1: Im Blockdiagramm dargestellte Kategorie 3

Der BGIA-Report 2/2008 zur funktionalen Sicherheit von Maschinensteuerungen [3] beleuchtet im Abschnitt 6.3.10 die Thematik unter dem Aspekt der Anforderungen an die Embedded-Software (SRESW, safety-related embedded software, z. B. Firmware) von Standardkomponenten. Die dort ausgeführten Überlegungen – zum Beispiel die Bewertung von Diversität – können teilweise verallgemeinert werden. Die Tabelle 1 (Tabelle 6.5 aus [3]) gibt eine Übersicht der Empfehlung.

Tabelle 1: Anforderungen an die SRESW von Standardkomponenten

Nr.	**PL**	**Kategorie, Redundanz**	**SRESW**
1	a b	Kategorie B/2/3	Es gelten die Basismaßnahmen für PL a bis b. Zwei Alternativen: a) Bestätigung durch Hersteller b) abgedeckt durch qualitätssichernde Entwicklung nach relevanten Produktstandards, dann ist keine Herstellerbestätigung über die Einhaltung der Anforderungen nach DIN EN ISO 13849-1 erforderlich
2	c d	Zwei Komponenten für zwei Kanäle in Kategorie 2/3 diversitäre SRESW oder diversitäre Technologie	Bonus durch die Diversität der SRESW oder der Technologien. Es gelten die Basismaßnahmen für PL a bis b. Zwei Alternativen: a) Bestätigung durch Hersteller b) abgedeckt durch qualitätssichernde Entwicklung nach relevanten Produktstandards, dann ist keine Herstellerbestätigung über die Einhaltung der Anforderungen nach DIN EN ISO 13849-1 erforderlich
3	c d	Zwei Komponenten für zwei Kanäle in Kategorie 2/3 SRESW homogen	Kein Bonus durch Diversität. Es gelten die Basismaßnahmen für PL a bis b und zusätzliche Maßnahmen für PL c bzw. d. Eine Herstellerbestätigung über die Einhaltung aller Anforderungen nach DIN EN ISO 13849-1 ist erforderlich.

Die Realisierung von Sicherheitsfunktionen durch Integration von Sicherheitsbauteilen vereinfacht auch die probabilistische Betrachtung z. B. im Rahmen der Bestimmung eines Performance Level nach [1]. Das unten gezeigte Beispiel in Anlehnung an das Beispiel im Bild H.1 der Norm verdeutlicht, dass die Quantifizierung im günstigsten Fall aus der einfachen Addition von drei Zahlenwerten bestehen kann.

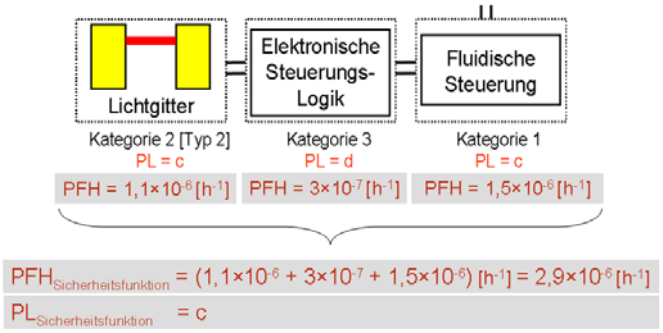

Bild 2: Lineare Kombination von SRP/CS (mit PFH-Werten) für die Sicherheitsfunktion „Bei Unterbrechung des Lichtgitters stoppt der Antrieb“.

Existiert für eine Anwendung oder ein Produkt eine Norm, so müssen selbstverständlich auch deren Anforderungen zur Beherrschung und Vermeidung von Ausfällen berücksichtigt werden. Handelt es sich beispielsweise um einen optischen Sensor, sind die Anforderungen der Normenreihe DIN EN 61496 relevant.

Literatur:

[1] DIN EN ISO 13849-1 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (12.08). Beuth, Berlin 2008

[2] DIN EN ISO 13849-2 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen Teil 2: Validierung (09.08). Beuth, Berlin 2008

[3] Funktionale Sicherheit von Maschinensteuerungen. BGIA-Report 2/2008. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2008
Download unter http://www.dguv.de/ifa/13849

Autoren: Dipl.-Ing. Thomas Bömer, Dr. Michael Schaefer
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin