

Effiziente Sicherheit – die Vorteile der DIN EN ISO 13849 nutzen

Thomas Kirschner

Zum Jahresende 2009 sollte zeitgleich mit Einführung der neuen EG-Maschinenrichtlinie 2006/42/EG die DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ die veraltete DIN EN 954-1 ablösen. Die alte Norm hat dann jedoch kurzfristig noch eine Gnadenfrist bis Ende 2011 erhalten. So wird die Einführung der neuen Norm verzögert, obwohl sie für den Maschinenbau viele Vorteile bietet.

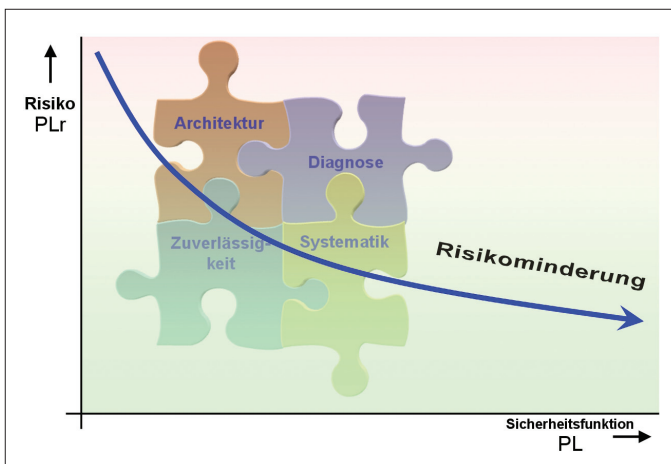


Bild 1. Risikominderung durch Anwendung der DIN EN ISO 13849

Eigentlich hätte die bereits vor Jahren terminierte Ablösung der veralteten DIN EN 954-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ durch die dem Stand der Technik entsprechende DIN EN ISO 13849-1 [1] (mit gleichnamigem Titel) zeitgleich mit Einführung der neuen EG-Maschinenrichtlinie 2006/42/EC zum Jahresende 2009 stattfinden sollen. Aber die DIN EN 954-1 hat – wohl aufgrund des Einspruchs von einflussreichen Verbänden bzw. auf Intervention deren Mitglieder – nochmals eine letzte Gnadenfrist bis Ende 2011 bekommen.

bei den bereits in der Auslaufphase befindlichen Serien Kosten spart.

Risiko für den Hersteller

Allerdings besteht hierin auch ein gewisses Risiko für die Hersteller: Falls es zu einem Unfall kommen sollte, der mit einiger Wahrscheinlichkeit bei Berücksichtigung der DIN EN ISO 13849-1 hätte verhindert werden können, dann bekommen der Hersteller bzw. die dort verantwortlichen Personen ein Problem. Denn ausschlaggebend bei der Klärung der Schuldfrage ist der Stand der Technik – und dieser wird eben nicht mehr durch die auf Deterministik bzw. auf der Auswahl der Steuerungsarchitektur basierende DIN EN 954-1 repräsentiert, sondern durch die weiter gefasste EN 13849 (Bild 1). Diese bezieht darüber hinaus noch

- die Zuverlässigkeit der Bauteile (Verhindern von zufälligen Fehlern durch Bauteilausfälle während der kalkulierten Lebensdauer),
- die Belastung der Bauteile im Betrieb (Schaltzyklen, Strombelastung, Umgebungstemperatur usw.),

- die Diagnosefähigkeit der Steuerung (Fehlererkennung, um eine Anhäufung von unentdeckten Fehlern und somit eine schleichende Degeneration der Sicherheitsfunktion zu verhindern),
 - die Fehler mit einer gemeinsamer Ursache (systematische Fehler, zum Beispiel durch Versäumnisse in der Entwicklungs- und Konstruktionsphase)
 - sowie Bewertungsmaßstäbe für den Einsatz von programmierbaren Steuerungen und elektronischen Baugruppen in Sicherheitsfunktionen
- in die Betrachtung und Bewertung mit ein. Sofern Maschinenhersteller die Verlängerung der Vermutungswirkung der DIN EN 954-1 trotzdem in Anspruch nehmen, so müssen sie beachten, dass die meisten Sicherheitsproduktnormen bereits die DIN EN ISO 13849-1 referenzieren oder in Kürze entsprechend umgestellt werden. Falls also eine solche Produktnorm für die zu bewertende Maschine existiert, dann wird oder wurde die sogenannte „Verlängerung der Vermutungswirkung“ der DIN EN 954-1 entsprechend abgekürzt.

Diskussion um die Sicherheitsbewertung

Die Diskussion um die Sicherheitsbewertung nach der DIN EN ISO 13849-1 wird in den einschlägigen Publikationen meist aus Sicht von Fachleuten der Sicherheitstechnikanbieter oder der Verbände geführt, was wahrscheinlich an der – auf den ersten Blick – für die Maschinen- und Anlagenhersteller bürokratisch und komplex erscheinenden Norm liegt. Wenn man sich aber etwas näher mit der DIN EN ISO 13849-1 beschäftigt, dann erscheint deren Umsetzung bald nicht mehr so aufwendig und man erkennt schnell den Nutzen, der mit dem tatsächlich überschaubaren Zusatzaufwand einhergeht:

- Die DIN EN ISO 13849-1 bietet gegenüber der DIN EN 954-1 mehr Flexibilität bei der Wahl der steuerungstechnischen Lösung. Zum Beispiel kann eine Standard-SPS oder -Software innerhalb der Sicherheitsfunktion nach festgelegten Kriterien eingesetzt und bewertet werden. Elektronische Geräte werden den elektromechanischen (verschleißbehafteten) sogar als teilweise überlegen eingestuft.

Thomas Kirschner ist Bereichsleiter Elektrik bei der IST Metz GmbH in Nürtingen.

E-Mail: thomas.kirschner@ist-uv.com



- Die Berechenbarkeit der gewählten Lösung verschafft dem Hersteller Gewissheit, dass das erforderliche Sicherheitsniveau erreicht wird. Dies dient auch der persönlichen Absicherung des Konstrukteurs bei Schadensfällen.
- Über die Möglichkeit des Vergleichs von Varianten derselben Sicherheitsfunktion erhält man die für die jeweilige Anwendung kostengünstigste Lösung, da zum Beispiel ohnehin für die Prozesssteuerung oder -überwachung vorgesehene Steuerungsfunktionen zusätzlich für Diagnoseaufgaben oder als zweiter Kanal mit einbezogen werden können. Oder weil man auf alternativen Wegen, zum Beispiel mit unterschiedlichen Kombinationen aus Zuverlässigkeits- und Diagnosewerten, zu gleichwertigen Ergebnissen gelangt.
- Der Vergleich von unterschiedlichen Bauteilen innerhalb einer Sicherheitsfunktion ermöglicht eine Kostenoptimierung durch bessere Ausgewogenheit aller Komponenten hinsichtlich einheitlicher Zuverlässigkeit und Lebensdauer.
- Durch die Einbeziehung der berechneten Zeit bis zum gefährlichen Ausfall bzw. die errechnete Gebrauchsdauer der Komponenten kann das Sicherheitsniveau über die vorgesehene Lebensdauer der Anlage aufrecht erhalten werden. Falls einzelne Komponenten vorzeitig unsicher werden (statistisch gesehen), erhält der Betreiber konkrete Vorgaben, wann diese Komponenten vorsorglich zu tauschen sind.

Praktische Umsetzung

Bei der praktischen Umsetzung der DIN EN ISO 13849-1 ist zu beachten, dass nennenswerte Einspareffekte nur dann erzielt werden, wenn Gefährdungsanalyse, Risikobeurteilung und Sicherheitsbewertung vor oder spätestens begleitend zur Entwicklung und Konstruktion der Maschine oder Anlage erfolgen. Andernfalls entstehen zwangsläufig „Schleifen“ im Design-Prozess, die zu teuren Nachbesserungen führen können.

Die Grundlagen, Fachbegriffe und Vorgehensweise werden in den Normen und der Fachliteratur [2, 3, 4] bereits erschöpfend behandelt, weshalb hier lediglich einige Hinweise und Praxistipps zu typischen Schwierigkeiten gegeben werden sollen.

Gefährdungen analysieren und Risiken bewerten

Im ersten Schritt sollte zunächst nur die „nackte“ Gefährdung – also ohne Berücksichtigung der bereits bekannten oder

schon umgesetzten konstruktiven und technischen Maßnahmen – beschrieben werden. Danach soll jede einzelne Maßnahme zur Risikominderung separat dargestellt und bewertet werden. Es sind solange weitere Schritte erforderlich, bis das Restrisiko niedrig genug geworden ist.

Die Markt- und Wettbewerbsbeobachtung ist eine der Pflichten des Maschinenherstellers: Gibt es bei eigenen oder bei fremden Maschinen evtl. Vorfälle oder Rückrufe, die auf Probleme, Sicherheitslücken, missbräuchliche Verwendung, Manipulation von Sicherheitseinrichtungen, nicht berücksichtigte Gefährdungen usw. hinweisen? Zum Beispiel kann die regelmäßige Auswertung der Wartungs- und Serviceberichte von in Betrieb befindlichen Maschinen dem Konstrukteur wertvolle Informationen liefern.

Es müssen alle Lebensphasen der Maschine berücksichtigt werden, nicht nur die eigentliche Betriebsphase. Also auch Aufstellung, Montage und Inbetriebnahme gemäß der Auflistung in der DIN EN ISO 14121-1 [5]. Beispielsweise kann von Vorrichtungen, die nur für Transport oder Aufstellung der Maschine benötigt werden, eine besondere Gefährdung ausgehen.

Der Risikograph aus der DIN EN ISO 13849-1 erlaubt nur eine relativ grobe Einstufung des Risikos. Empfehlenswert für die Praxis ist deshalb zum Beispiel die Anlehnung an die DIN EN 62061 (VDE 0113-50) [6] oder eine Kombination mit der Kinney-Methode, um feinere Abstufungen vorzunehmen. Durch diese Vorgehensweise werden zudem die subjektiven Beurteilungen leichter nachvollziehbar und lassen sich besser dokumentieren. Die Berechnung und Dokumentation kann mittels einer Excel-Datei realisiert werden, in die weitere Funktionalitäten integriert werden. Oder man verwendet eine Software, wie den Safexpert von Sick [7].

Aufgrund subjektiver Einschätzungen können die Ergebnisse verschiedener Bewerter etwas voneinander abweichen. Deshalb ist eine regelmäßige Abstimmung aller betroffenen Mitarbeiter untereinander für möglichst einheitliche Maßstäbe bei der Bewertung erforderlich.

Falls eine Sicherheitsproduktnorm für den zu bewertenden Maschinentyp vorhanden ist, muss daraus die konkrete Vorgabe des erforderlichen Performance Level (PL_r, Sollwert) für die Sicherheitsfunktion entnommen werden. Diese Vorgabe entbindet den Hersteller aber nicht vollständig von einer eigenen Bewer-

tung, denn das in seiner Maschine vorhandene Risiko könnte aufgrund von Besonderheiten größer sein, als in der Produktnorm angenommen.

Risiken reduzieren

Zufällige und systematische Fehler werden durch eine oder mehrere der folgenden Maßnahmen verhindert. Zum Beispiel mit Konstruktionen für die inhärente Sicherheit (Vermeidung von Quetsch- und Schergeräten durch Einhaltung der Sicherheitsabstände oder Gestaltung der Form, Begrenzung von Energie, Geschwindigkeit, Hub sowie Verlagerung beweglicher Teile in ein Gehäuse) oder die Realisierung von Sicherheitsfunktionen (Schutzeinrichtungen). Der Konstrukteur macht dabei zunächst einen Entwurf aus seiner Erfahrung heraus für die steuerungstechnische Umsetzung. Die Annäherung an die passende Lösung erfolgt dann in einem iterativen Prozess:

- Auswahl der Kategorie bzw. Steuerungsarchitektur: der erforderliche PL_r schränkt die Auswahl bereits ein,
- Auswahl von Steuerungskomponenten, unter Berücksichtigung der Belastung im Betrieb in Relation zu den Herstellerangaben (falls die statistische Zeitdauer bis zum gefährlichen Ausfall (MTTF_d) kleiner als 20 Jahre ist, so muss in der Bedienungsanleitung auf den Zeitpunkt für den vorbeugenden Austausch hingewiesen werden),
- Einbau von Diagnosefunktionen: Diese Maßnahme ist in der Regel nicht sehr kostenintensiv (zum Beispiel Software und Digitaleingänge im vorhandenen Steuerungsrechner), sie kann aber die Zuverlässigkeit der Sicherheitsfunktion steigern, weil eine Anhäufung von unentdeckten Fehlern dann weniger wahrscheinlich ist,
- Durchführung von Zusatzmaßnahmen (zum Beispiel Mitarbeiterschulungen, Untersuchung von Umgebungseinflüssen), um systematische Fehler zu vermeiden.

Weitere Maßnahmen sind Warnschilder an den Gefahrenstellen und Warnhinweise in der Bedienungsanleitung. Dies ist jedoch nur ergänzend zulässig, wenn alle anderen technischen Maßnahmen zur Risikominderung bereits ausgeschöpft sind.

Sicherheitsbewertung und Validierung

Falls der erreichte Performance Level (PL, Istwert) deutlich über den Anforderungen (PL_r, Sollwert) liegt, so darf die Sicherheitsfunktion vereinfacht und so-



mit kostengünstiger gestaltet werden.

Der Stromlaufplan und/oder das Pneumatik-/Hydraulikschema ist in ein sicherheitsgerichtetes Blockdiagramm umzusetzen. Dieses dient nicht nur zur Unterstützung bei der Berechnung, sondern auch der späteren Dokumentation, zum Beispiel für Zertifizierungen durch akkreditierte Stellen (GS-Zeichen der Berufsgenossenschaften usw.).

Folgende Zuverlässigkeitswerte sind von den Komponentenherstellern zu beschaffen:

- Ausfallraten für elektronische Komponenten als λ (Einheit FIT bzw. $10^{-9}/h$),
- Ausfallraten für elektromechanische Bauteile als B10/B10d (Schaltzyklenzahl bis zum Ausfall von 10% der Teile),
- Ausfallraten als MTTF/MTTF_d (durchschnittliche Zeit bis zum Ausfall) sowie für Sicherheitsbauteile als PL (Performance Level) mit Angabe des PFH-Werts (Wahrscheinlichkeit des gefährlichen Ausfalls je Stunden).

Die Berechnung des erreichten PL für jede Sicherheitsfunktion kann mittels eines der größtenteils kostenfrei angebotenen Software-Pakete, zum Beispiel Sistema [8] des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung oder einer vergleichbaren Software eines Sicherheitstechnik-Anbieters, wie Pascal von Pilz [9], erfolgen. Dies ermöglicht den Aufbau einer firmeninternen Datenbank oder einer Art Baukasten, wodurch der Aufwand für Sicherheitsbewertungen mit der Zeit immer weiter reduziert wird.

Probleme bei der Datenbeschaffung

Bei Sicherheitsbauteilen enthalten die Datenblätter bereits alle nötigen Angaben. Aber bei Standardbauteilen, die

durchaus in Sicherheitsfunktionen eingesetzt werden (dürfen), gibt es großen Nachholbedarf. Manche Komponentenhersteller schicken auf Anfrage Einzelwerte oder sogar eine vollständige Liste mit den Daten ihrer Produkte oder haben diese schon im Internet zur Verfügung gestellt. Andere Hersteller müssen zuvor über Sinn und Zweck aufgeklärt werden („unser Produkt ist doch kein Sicherheitsbauteil, also können wir Ihnen dafür keine Zuverlässigkeitswerte zur Verfügung stellen“) oder sie müssen die erforderlichen Werte erst noch in Dauerversuchen ermitteln.

Das Sammeln der zur PL-Berechnung erforderlichen Zuverlässigkeitsangaben beansprucht einen hohen Anteil des Validierungsprozesses, deshalb wäre ein einfacherer Zugang zu den benötigten Herstellerdaten hilfreich.

Manche Hersteller befürchten vielleicht auch, sensible Daten über die Zuverlässigkeit ihrer Produkte herauszugeben. Für die Anwender sind diese Informationen von großem Interesse, denn sie erlauben unter anderem Vergleiche zwischen verschiedenen Anbietern hinsichtlich der Qualität und Langlebigkeit der Produkte – sofern die Herstellerangaben belastbar sind bzw. realistisch ermittelt wurden.

Fazit

Die Anwendung der DIN EN ISO 13849-1 ermöglicht eine strukturiertere Vorgehensweise bei der Entwicklung und Konstruktion von Maschinen und Anlagen. Wer sie konsequent nutzt, vermeidet gleichermaßen Unsicherheiten wie auch Überdimensionierung bei der sicherheitstechnischen Auslegung. Der firmeninterne Standardisierungsgrad für Maschinensteuerungen wird sich durch das ebenfalls standardisierte Bewertungsverfahren zwangsläufig erhöhen. Die Me-

thodik der Norm bietet darüber hinaus noch weitere Möglichkeiten, zum Beispiel die Berechnung von Zuverlässigkeit bzw. Verfügbarkeit für normale, nicht sicherheitsrelevante Steuerungsfunktionen, um damit die Erfüllung des eigenen Qualitätsanspruches zu prüfen oder Schwachstellen im Steuerungssystem zu finden. Dafür kann Berechnungs-Software „zweckentfremdet“ werden, wenn man als Eingabewerte nicht nur die gefahrbringenden, sondern alle Ausfälle von Bauteilen verwendet und als Ergebnis die PFH-Werte der gesamten Steuerungsfunktion erhält.

Literatur

- [1] DIN EN ISO 13849-1:2008-12 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze. Berlin: Beuth
- [2] BG-Broschüre „Sicheres Konstruieren von Druck- und Papierverarbeitungsmaschinen – Mechanik“ (Best.nr .220.1), Papierausgabe oder Download: http://www.bgdp.de/pages/medien/auswahl_nach_art/broschueren.htm
- [3] BG-Broschüre „Sicheres Konstruieren von Druck- und Papierverarbeitungsmaschinen – Elektrische Ausrüstung und Steuerung“, (Best.nr 220.2), Papierausgabe oder Download: http://www.bgdp.de/pages/medien/auswahl_nach_art/broschueren.htm
- [4] BGIA-Report 2/2008 „Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849“, Papierausgabe oder Download: <http://www.dguv.de/ifa/de/pub/rep/rep07/bgia0208/index.jsp>
- [5] DIN EN ISO 14121-1:2007-12 Sicherheit von Maschinen – Risikobeurteilung – Teil 1: Leitsätze. Berlin: Beuth
- [6] DIN EN 62061 (VDE 0113-50):2005-10 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme. Berlin · Offenbach: VDE VERLAG
- [7] Sick AG, Waldkirch: www.sick.com
- [8] Software Sistema: kostenfreier Download (nach Registrierung) von <http://www.dguv.de/ifa/de/pra/softwa/sistema/index.jsp>
- [9] Pilz GmbH & Co. KG, Ostfildern: www.pilz.com