Martin Lange

Leben und Leiden mit der ISO 13849

Die ISO 13849 ist – insbesondere in Europa – die meist angewandte Norm, wenn es um die Entwicklung von sicheren Steuerungskomponenten für Maschinen geht. In der täglichen Arbeit mit der Norm zeigen sich jedoch immer wieder Stolpersteine: Anforderungen sind nicht eindeutig, widersprechen einander oder sind schlicht nicht zu erfüllen. Was also tun?

Die International Electrotechnical Commission (IEC) hat im Jahr 1998 eine Lawine losgetreten, deren Auswirkungen noch heute die Automatisierungsbranche und den Maschinenbau prägen: Mit der Veröffentlichung der neuen Norm IEC 61508 zur ‚Funktionalen Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme' gab es plötzlich einen einheitlichen Standard für eine unabsehbare Vielzahl von Steuerungssystemen in unterschiedlichsten Anwendungen, die bisher nur durch einzelne nationale oder branchenspezifische Vorgaben reglementiert worden waren.

Jedoch – es gab noch eine Schonfrist: Die IEC 61508 als Basisnorm hatte (und hat) nicht selbstbindende Wirkung für den Entwickler/Anwender sicherheitsrelevanter Maschinen- und Anlagensteuerungen, sondern ihr Hauptziel ist, „für ein bestimmtes Anwendungsgebiet die Entwicklung einer entsprechenden Internationalen Norm durch das jeweils verantwortliche Komitee zu ermöglichen."

Parallel begannen nun sowohl die IEC als auch die International Organization for Standardization (ISO) auf Basis der IEC 61508 neue Normen für die Sicherheit von Maschinen zu formulieren: die IEC 62061 und die ISO 13849.

Die beiden Ansätze hätten jedoch unterschiedlicher kaum sein können: Während die IEC sich sehr eng an die IEC 61508 anlehnte (so sehr, dass man sich manchmal fragt, ob der eine Satz „die Vorgaben der IEC 61508 sind einzuhalten" nicht gereicht hätte), ging die ISO einen ganz eigenen Weg: Es existierte im europäischen Raum mit der EN 954 bereits eine Norm für Maschinensteuerungen, die bei Erscheinen der IEC 61508 gerade mal zwei Jahre alt war und deren Konzepte man nicht sofort wieder über den Haufen werfen wollte. So versuchte die ISO den Spagat, die Konzepte beider Normen miteinander zu verheiraten: auf der einen Seite die EN 954, die vor allem die Architektur von sicherheitsbezogenen Maschinensteuerungen im Blick hatte; auf der anderen Seite die IEC 61508 mit ihrem neuen probabilistischen Ansatz sowie mit dem neuen Fokus auf Prozesse, der sich nicht nur durch die Entwicklung, sondern durch den gesamten Lebenszyklus sicherheitsbezogener Systeme zieht.

Heute hat sich der Ansatz der ISO durchgesetzt: Viele Anwendungsnormen beziehen sich auf die ISO 13849, zum Beispiel die Normen für Robotik

(Bild: Computer&AUTOMATION / Quellen: Schuler; Fotolia_pathdoc)

(ISO 10218), für Kräne (EN 13000) und viele andere. Und doch tauchen immer wieder Schwierigkeiten auf, wenn man als Entwickler von Steuerungskomponenten mit der ISO 13849 arbeitet. Teile scheinen sich zu widersprechen, sind nicht eindeutig. Und so stellt sich die Frage, wie mit solchen Schwierigkeiten umgegangen werden kann.

Die Kategorien

Wie erwähnt, haben die Kategorien der ISO 13849 schon eine ältere Tradition. In aufsteigender Reihenfolge werden hier grundlegende Methoden der Sicherheitstechnik beschrieben und gefordert:

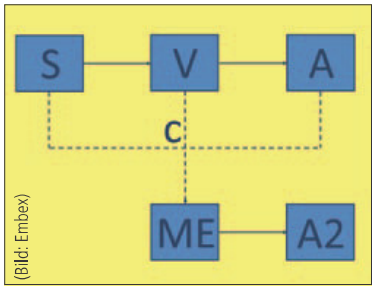
- Kategorie B: grundlegende Sicherheitsprinzipien wie das Prinzip der Energietrennung;
- Kategorie 1: bewährte Sicherheitsprinzipien und -bauteile, zum Beispiel Relais mit zwangsgeführten Kontakten;
- Kategorie 2: Diagnose von Ausfällen der Sicherheitsfunktion;
- Kategorie 3: Zweikanaligkeit;
- Kategorie 4: Kombination von Diagnose und Zweikanaligkeit.

Auch wenn diese Prinzipien zunächst einleuchten und sich nicht zuletzt seit ihrer Einführung tausendfach bewährt haben, so treten bei der Arbeit mit den konkret formulierten Anforderungen doch immer wieder Probleme auf, die im Folgenden anhand einiger Beispiele betrachtet werden sollen. Eine Anmerkung in diesem Zusammenhang: Wie die meisten Normen der funktionalen Sicherheit hat auch die ISO 13849 eine eigene Bezeichnung für die Systeme ‚erfunden', die sie behandelt. In diesem Fall lautet dieser Name: ‚safety-related part of a control system' (SRP/CS). Auf Deutsch: ‚sicherheitsbezogenes Teil einer Steuerung', was nicht zu verwechseln ist mit dem ‚sicherheitsbezogenen elektrischen Steuerungssystem' (SRE/CS) der IEC 2061.

Testen oder prüfen – ein folgenschwerer Übersetzungsfehler

Die Kategorie 2 fordert in der deutschen Übersetzung: „SRP/CS (…) müssen so gestaltet werden, dass ihre Funktionen in angemessenen Zeitabständen durch die Maschinensteuerung getestet werden."

Es ist allseits bekannt, wie man eine Funktion testet. Man stimuliert das zu testendes System (man fordert die Sicherheitsfunktion an) und beobachtet, ob die geforderte Funktion ausgeführt wird. Konkret: Der Anwender lässt den Zweihandschalter los und die Maschinensteuerung überwacht, dass die



(Bild: Embex)

Kategorie 2 nach ISO 13849 mit Sensor (S), Verarbeitungseinheit (V), Aktor (A), Überwachungeinheit (ME) und zweitem Abschaltpfad (A2). Die gestrichelten Linien stellen den ‚Check' der Sicherheitsfunktionen durch die Überwachungseinheit dar.

Maschine tatsächlich stehen bleibt. Die Kategorie 2 fordert für diesen Test einen mittleren Diagnosedeckungsgrad (DC_{avg}) von mindestens 60 %.

Wenn nun an der Sicherheitsfunktion auch ein Mikroprozessor beteiligt ist, so herrscht ein breiter Konsens darüber, dass die Unversehrtheit (Freiheit von internen Hardware-Fehlern) eines Mikroprozessors nicht durch die Testung einer einzigen Funktion nachweisbar ist – nicht einmal zu 60 %. Dazu wären die üblichen Prozessor-Selbsttests erforderlich (Speichertests, CPU-Tests etc.), die aber im eigentlichen Sinne keinen ‚Test', sondern eine ‚Prüfung' bedeuten. Tatsächlich wird immer wieder von Prüfstellen in Frage gestellt, ob sich die Forderung nach einem ‚Test' der Funktion mit einem Mikroprozessorsystem vereinbaren lässt.

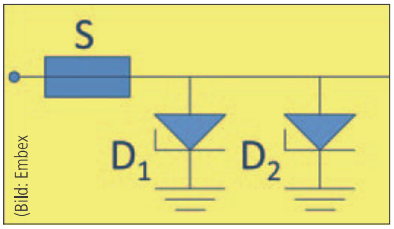
Wirft man jedoch einen Blick in das englische Original der Norm, so ist dort nicht etwa von ‚test' die Rede, sondern von ‚check' – also von einer Prüfung, als welche auch ein zyklischer Prozessor-Selbsttest ohne Weiteres anzusehen ist.

Der ‚kategorische Imperativ' und die Probabilistik

Natürlich hat sich Immanuel Kant nicht in die ISO 13849 verirrt, aber sie beinhaltet – in den Kategorien 3 und 4 – eine Forderung, die in ihrer Unbedingtheit durchaus als ‚kategorisch' zu bezeichnen ist:

„SRP/CS der Kategorie 3/4 müssen so gestaltet werden, dass ein einzelner Fehler (…) nicht zum Verlust der Sicherheitsfunktion führt."

Das Rezept der ISO 13849 zur Umsetzung dieser Anforderung ist klar: Zweikanaligkeit. Immer wieder stellt sich aber die Frage, ob sich dieser ‚kategorische Imperativ' auch mit einer



Kategorie-4-konforme Schutzschaltung gegen eine definierte Überspannung mit einer Schmelzsicherung (S) und zwei Schutzdioden (D1 und D2).

Nein, der Philosoph Immanuel Kant hat sich nicht in die Welt der Maschinensicherheit verirrt. Aber die ISO 13849 stellt für Maschinensteuerungen ab einem bestimmten Gefährdungsrisiko eine Forderung auf, die ähnlich ‚kategorisch' ist wie Kants berühmter Imperativ.

einkanaligen Struktur mit einer entsprechend wirksamen (und der Zweifehlersicherheit wegen getesteten) Diagnose erfüllen lässt. Dabei steht man dann sofort vor dem Problem, dass die ISO 13849 für jegliche Diagnose nur eine maximale Wirksamkeit (DC) von 99 % kennt (Tabelle E.1). In einem Prozent der Fälle wird also ein Fehler auch durch die beste Diagnose nicht aufgedeckt. Kurzum: Der ‚kategorische Imperativ' ist nicht erfüllt. Ende der Diskussion? Vielleicht nicht ganz!

Etwas versteckt räumt die ISO 13849 nämlich sehr wohl selbst ein, dass auch in Kategorie-3/4-Systemen ein kleiner Anteil – und zwar 2 % – der möglichen Fehler zum Verlust der Sicherheitsfunktion führen: die Fehler gemeinsamer Ursache (common cause failures – CFF). Da nun aber die 100-%ige Erfüllung des ‚kategorischen Imperativs' sowieso nicht erreichbar ist, erscheint es als ein sinnvoller Ansatz, auch einkanalige Kategorie-3/4-Systeme zuzulassen, sofern die Diagnose einen DC von >99 % erreicht und ihrerseits mit der von der Kategorie geforderten Wirksamkeit getestet oder überwacht wird.

Das kleine Wörtchen ‚kann'

Die Kategorie 4 fordert, dass „ein einzelner Fehler (…) nicht zum Verlust der Sicherheitsfunktion führt". Darüber hinaus „darf die Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen". Das bedeutet, es müssten theoretisch in komplexen Systemen Verkettungen von Tausenden einzelner Fehler betrachtet und daraufhin analysiert werden, ob nicht irgendwann doch die Sicherheitsfunktion verloren geht. Soviel zur Theorie.

Zum Glück steht ganz am Ende noch ein kleiner Satz: „In der Praxis kann die Betrachtung einer Fehlerkombination für zwei Fehler ausreichend sein." Zunächst einmal schafft dieser Satz Entlastung. Nur: Wann ‚kann' die Betrachtung tatsächlich auf zwei Fehler reduziert werden? Hierzu schweigt die Norm. Im Zweifelsfall heißt das: Wenn man diesen Satz in Anspruch nimmt, füllt man viel Papier, um darzulegen, warum man das im Einzelfall tun darf. Oder man betreibt ein wenig Normengeschichte. Die alte EN 954-1 war an diesem Punkt nämlich ganz klar:

„Diese Fehlerbetrachtung darf auf zwei Fehler beschränkt werden, wenn

- die Fehlerraten der Bauteile niedrig sind
- und die kombinierten Fehler überwiegend unabhängig voneinander auftreten
- und die Sicherheitsfunktion unterbrochen wird, wenn die Fehler nur in einer ganz bestimmten Reihenfolge auftreten."

In der Praxis hat es sich bewährt, diese eigentlich nicht mehr gültigen Bedingungen weiterhin anzuwenden. Wenn zum Beispiel in einer Schaltung eine Sicherung als Überspannungsschutz verwendet werden soll, beantwortet sich damit die Frage, wie viele Schutzdioden gegen Masse hinter der Sicherung nötig sind, ganz einfach mit „zwei".

Von der Kategorie zum Performance Level

In der Welt der EN 954-1 war die Arbeit erledigt, wenn das System/Gerät designt und einer bestimmten Kategorie zugeordnet war. In der ‚neuen Welt' ist nun aber aus der Kategorie, dem DC_{avg} und der mittleren Zeit bis zum gefährlichen Fehler (mean time to dangerous failure – $MTTF_d$) der erreichte Performance Level (PL) zu bestimmen. Und auch auf diesem Weg ist noch das ein oder andere Schlagloch zu umkurven. Zwei davon sollen hier beispielhaft erläutert werden. Es reicht nicht, einfach

intuitiv Diagnosemechanismen in der Hardware und der Software zu verteilen. Zur Bestimmung des PLs muss die Wirksamkeit der einzelnen Maßnahme nachgewiesen werden.

Der Diagnosedeckungsgrad – Kochrezept oder Berechnung?

Die ISO 13849-1 stellt dafür eine Art Kochrezept zur Verfügung. In ihrer Tabelle E.1 sind typische Diagnosemechanismen mit dem im Normengremium beschlossenen DC aufgeführt. Doch was, wenn ein Hersteller nachweisen kann, dass eine Diagnose, die in dieser Tabelle beschrieben und in seinem Gerät realisiert ist, wirksamer ist, als Tabelle E.1 behauptet?

Ein Beispiel: Betrachten wir (digitale) Eingangssignale. Laut Tabelle E.1 hat die Verwendung ‚zyklischer Testimpulse' einen DC von 90 %. Trotzdem kann es gut sein, dass eine detaillierte Analyse (eine so genannte Failure Modes, Effects and Diagnosis Analysis – FMEDA) ergibt, dass mit dieser Maßnahme mehr als 99 % aller anzunehmenden Bauteil-Fehler aufgedeckt werden. Gilt dann die Berechnung oder die Norm?

Die Antwort gibt die Norm selbst. Tabelle E.1 steht unter der Überschrift ‚Abschätzungen des Diagnosedeckungsgrades'. Und kaum jemand wird bezweifeln, dass eine detaillierte Berechnung immer einer Abschätzung überlegen ist. So ist Tabelle E.1 als eine Vereinfachung zu verstehen – eben als Kochrezept für denjenigen, dem die Detail-Kenntnisse oder die Mittel für eine detaillierte Analyse fehlen. Liegt eine solche Analyse dagegen vor, so wird Tabelle E.1 damit obsolet.

Das vereinfachte Verfahren

Es liegt ein großes Mysterium in der ISO 13849: Wie steht sie zur IEC 62061? Gleich am Anfang (Tabelle 1) erklärt sie, wann die Anwendung welcher der beiden Normen ‚empfohlen' ist. Wann die Anwendung zwar möglich, aber eben nicht ‚empfohlen' ist, erfährt der Leser hingegen nicht. Später wurde von der ISO noch ein eigener ‚Technical Report' (ISO/TR 23849) zur Kompatibilität beider Normen herausgegeben, der den Eindruck hinterlässt, dass ein Performance Level (PL) nach ISO 13849 weniger wert sei als ein Safety Integrity Level (SIL) nach IEC 62061.

In Kapitel 4.5 wird dann der Zusammenhang zwischen SIL und PL dargestellt, der den Eindruck erweckt, beide seien mehr oder weniger gleichwertig. Zuvor aber ist zum ersten Mal vom ‚vereinfachten Verfahren' zur Bestimmung des PL die Rede. Eben jenes, das auf den Kategorien $MTTF_d$ und DC_{avg} beruht. Und damit fragt man sich: Gibt es noch ein anderes, vielleicht komplizierteres, aber allgemeineres Verfahren zur Bestimmung des PLs eines Geräts/Systems? Dazu schweigt die Norm.

Der Anhang K vermittelt den Eindruck, als ginge es am Ende nur darum, die von der IEC 62061 geforderte Ausfallwahrscheinlichkeit (probability of dangerous failure – PFHD) zu erzielen. Kann ich also den entsprechenden PL in Anspruch nehmen, wenn ich mit meinem System die entsprechende PFHD erziele (und die Anforderungen an die Software nach Kap. 4.6 und bezüglich Common-Cause-Fehlern nach Anhang F erfülle)? Die Antwort darauf ist ein Mysterium. Und so bleibt nur die Hoffnung, dass in diesen Punkten die zukünftige ISO 17305 Licht in das Dunkel bringt. An dieser Norm, welche die ISO 13849 und die IEC 62061 zusammenführen soll, wird derzeit im Rahmen der ISO gearbeitet. Wünschenswert wäre, dass dabei in dem ein oder anderen genannten Detail der Norm in Zukunft etwas mehr Klarheit geschaffen würde. *gh*

Martin Lange

ist bei der Firma Embex für das Thema Funktionale Sicherheit verantwortlich.