EN 13849-1 Performance Level PL bestimmen

Der Beitrag der Schaltung zur Risikoreduzierung, hier eben Performance Level PL genannt, lässt sich anhand folgender Tabelle aus Ihren Werten für die Zuverlässigkeit (MTTFd) und dem Diagnosedeckungsgrad DC ermitteln:

(die Spalte Kategorie erklären wir gleich; es handelt sich um EN 954-1 ähnliche Kategorien)

Tab. 1: Beziehung zwischen DC, MTTFd und erreichtem PL

Kategorie	B	1	2	2	3	3	4
DC avg	kein	kein	niedrig	mittel	niedrig	mittel	hoch
MTTFd niedrig	A	nicht abgedeckt	a	b	b	c	nicht abgedeckt
MTTFd mittel	B	nicht abgedeckt	b	c	c	d	nicht abgedeckt
MTTFd hoch	nicht abgedeckt	c	c	d	d	d	e

In der Norm ist ein Bild dazu enthalten, das aber schnell missverständlich werden kann – deshalb haben wir uns für die Darstellung in einer Tabelle entschieden. Das Bild lässt mehr Grenzbereiche zu, also anstelle b dann c etc.

Wichtig und immer zu beachten ist der Begriff Kategorie, der schon bei der Vorgängernorm ganz wesentlich die Struktur vorgab!

Der Begriff Kategorie in EN 13849-1

Ganz ähnlich der Vorgängernorm EN 954-1 werden Kategorien wie folgt definiert:

B – Die Basiskategorie für das Sicherheitsverhalten

Grundlegende Sicherheitsprinzipien müssen verwendet werden. SRP/CS müssen in Übereinstimmung mit den zutreffenden Normen ausgewählt, gestaltet, gebaut und kombiniert werden, dass diese den zu erwartenden Betriebsbeanspruchungen standhalten.

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.

Prinzip zum Erreichen der Sicherheit ist durch die Auswahl von Bauteilen charakterisiert.

Der MTTFd jeden Kanals ist niedrig bis mittel.

DC avg ist nicht bestimmt (keine).

CCF ist nicht relevant.

Kategorie 1

Die Anforderungen von Kategorie B müssen erfüllt sein, zusätzlich gelten erhöhte Anforderungen an die Bauteilzuverlässigkeit. Bewährte Bauteile und Sicherheitsprinzipien müssen angewendet werden.

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.

Prinzip zum Erreichen der Sicherheit ist durch die Auswahl von Bauteilen charakterisiert.

Der MTTFd jeden Kanals ist hoch.

DC avg ist nicht bestimmt (keine).

CCF ist nicht relevant.

Kategorie 2

Die Anforderungen von Kategorie B und die Verwendung bewährter Sicherheitsprinzipien usw. müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung getestet werden.

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, der durch den Test erkannt wird.

Prinzip zum Erreichen der Sicherheit ist durch die Struktur charakterisiert.

Der MTTFd jeden Kanals ist niedrig bis hoch.

DC avg ist niedrig bis mittel.

CCF ist anzuwenden.

Kategorie 3

Die Anforderungen von Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Ein einzelner Fehler darf nicht zum Verlust der Sicherheitsfunktion führen, wann immer in angemessener Weise durchführbar, soll der Fehler erkannt werden. Eine Anhäufung von Fehlern kann zum Verlust der Sicherheitsfunktion führen.

Das Auftreten eines einzelnen Fehlers führt nicht zum Verlust der Sicherheitsfunktion. Es werden aber nicht alle Fehler erkannt. Erst eine Häufung von Fehlern kann zum Verlust der Sicherheitsfunktion führen.

Prinzip zum Erreichen der Sicherheit ist durch die Struktur charakterisiert.

Der MTTFd jeden Kanals ist niedrig bis hoch.

DC avg ist niedrig bis mittel.

CCF ist anzuwenden.

Kategorie 4

Die Anforderungen von Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Ein einzelner Fehler darf nicht zu einem Verlust der Sicherheitsfunktion führen und der Fehler muss, wenn irgendwie möglich, bei oder vor der nächsten Anforderung erkannt werden. Eine Anhäufung von Fehlern darf nicht zum Verlust der Sicherheitsfunktion führen.

Prinzip zum Erreichen der Sicherheit ist durch die Struktur charakterisiert.

Der MTTFd jeden Kanals ist hoch.

DC avg ist hoch einschließlich Fehlerhäufung.

CCF ist anzuwenden.

Umsetzung in die Praxis

Dabei ist zu beachten, dass, wenn z.B. an einer Maschine fünf Not-Halt-Geräte enthalten sind und diese auf eine zentrale Logik auflaufen, nur ein Not-Halt-Gerät in die nachfolgende Rechnung aufgenommen wird. Es sind aber, wenn z.B. an einer Maschine vier Motoren abgeschaltet werden müssen, um einen sicheren Zustand zu erzeugen, alle vier Motoren mit in die Rechnung einzubeziehen.

In vielen Fällen ist es sinnvoll, den Wartungsbetrieb mit seinen anderen Zugangsmöglichkeiten (weitere Zugänge) getrennt zu bestimmen. Normalerweise sind hier deutlich niedrigere PLr gefordert.

An dieser Stelle wichtig und meist recht einfach durchzuführen ist die nochmalige Überlegung und Überprüfung, ob wirklich die wichtigen Gefahrenstellen so abgesichert sind.

Wer Schaltschränke in diese Überlegungen mit einbezieht, sieht einen weit übertriebenen Schutz vor – ein Schaltschrank lässt sich durch einen Schlüsselschalter gegen unbefugten Zutritt absichern; deshalb ist hier unter normalen Umständen keine Überwachung notwendig. Dies wird durch CCF nicht wirklich berücksichtigt bzw. gefordert! Nur Schaltkästen an Maschinen sind manchmal sinnvoll abzusichern – aber das sind wirklich Ausnahmen! Normalerweise gilt auch, dass alle Abdeckungen von Maschinen, die mit Werkzeug abmontiert werden müssten, um irgendwie Zugang zu innen liegenden Teilen zu ermöglichen, nicht überwacht werden müssen – Ausnahmen davon zeigen ein generelles Problem an.

Allgemeines zum PL

Die Norm beschreibt die Berechnung des Performance Level (PL) für sicherheitsrelevante Teile von Steuerungen auf Basis vorgesehener Architekturen. Bei Abweichungen hiervon verweist die EN ISO 13849-1 auf die IEC 61508. Der PL muss für die sicherheitsrelevanten Teile eines Systems bestimmt werden, die die Sicherheitsfunktionen ausführen. Die Norm beschreibt das Verfahren zur Einschätzung des PL bzw. des SIL.

Je höher die Minderung des Risikos in Abhängigkeit von der SRP/CS ist, desto höher ist der erforderliche PL bzw. SIL. Der Beitrag an Zuverlässigkeit und der Struktur kann mit der verwendeten Technologie variieren.

Den Zusammenhang der EN ISO 13849-1 und der IEC 62061 über die Wahrscheinlichkeit eines gefahrbringenden Ausfalls (PFHD) zeigt diese Tabelle:

Tab. 2: Zusammenhang zwischen IEC 62061 und EN ISO 13849-1

PL	Wahrscheinlichkeit	SIL nach IEC 61508
a	$10^{-5} \leq PFH_D < 10^{-4}$	keine Entsprechung
b	$3 \cdot 10^{-6} \leq PFH_D < 10^{-5}$	SIL 1
c	$10^{-6} \leq PFH_D < 3 \cdot 10^{-6}$	SIL 2
d	$10^{-7} \leq PFH_D < 10^{-6}$	SIL 3
e	$10^{-8} \leq PFH_D < 10^{-7}$	SIL 4