

Die Wahl der richtigen Programmiersprache

Ein weiterer Aspekt ergibt sich im Aufbau und Sprachumfang der zu einem Sicherheitssystem notwendigen Konfigurationssoftware. Die ISO 13849-1 unterscheidet zwischen Programmiersprachen mit eingeschränktem Sprachumfang (LVL „Limited Variability Language“ genannt) und solchen mit uneingeschränktem Sprachumfang (im Folgenden FVL „Full Variability Language“ genannt).

Programmiersprachen mit LVL ermöglichen vordefinierte Bibliotheksfunktionen zu kombinieren, um die Sicherheitsanforderungen im Programm umzusetzen. Als LVL gelten die IEC 61131-3 Programmiersprachen FUP (Funktionsblockdiagramm, Funktionsablaufplan) und KOP (Kontaktplan). Programmiersprachen mit FVL bieten alle Möglichkeiten der Programmierung. Hierzu zählen neben den in der IEC 61131-3 genormten Sprachen AWL (Anweisungslisten) und ST (strukturierter Text) auch die Hochsprachen C, C++ und andere. Der LVL-Anwender wird vor den sonst in der Programmierung üblichen Fehlerquellen geschützt – das Bilden von Schleifen, die Verwendung von Zeigern (Pointer) und globalen Variablen ist verboten. Eine Programmierung in FVL kennt keine Einschränkung und beinhaltet somit auch alle Fehlermöglichkeiten.

Das hat zur Folge, dass für die Implementierung der Anwendungssoftware in FVL ein aufwändigerer Entwicklungsprozess vorgeschrieben ist, als für eine Implementierung in LVL. So fordert die ISO 13849-1 demnach für Implementierungen in LVL einen sehr vereinfachten Software-Entwicklungsprozess. Für die Implementierung einer Anwendungssoftware in FVL hingegen wird auf die Normenreihe IEC 61508 verwiesen, die aus sieben Teilen mit zusammen ca. 430 Seiten besteht und die Installation eines normkonformen Entwicklungsprozesses gemäß IEC 61508 eine hohe Investition darstellt.

Integrated Safety Technology von B&R

B&R hat hier mit seinen Produkten der Integrated Safety Technology neue Maßstäbe in Bezug auf einfache Anwendungen, abgesicherte Wartungsszenarien und durchgängige Skalierbarkeit gesetzt. →



Ab 1. Dezember 2009 muss die Sicherheitstechnik von Maschinen die Anforderungen der ISO 13849-1 bzw. IEC 62061 erfüllen.



Ing. Thomas Müller,
Spezialist Sicherheitstechnik,
Festo Didactic

Der Diagnosedeckungsgrad

Die EN ISO 13849-1 definiert den Diagnosedeckungsgrad (DC) als Maß für die Wirksamkeit der Diagnose – bestimmt wird es als das Verhältnis der erkannten gefährlichen Ausfälle zu den gesamten gefährlichen Ausfällen. Diesem Diagnosedeckungsgrad kommt bei der Wahl der Kategorie (B, 1, 2, 3 oder 4) ab Kategorie 2 entscheidende Bedeutung zu. Für die Kategorien B und 1 ist er nicht relevant.

Zur Abschätzung des DC können beispielsweise die FMEA (Ausfallarten- und Effektanalyse IEC 60812) oder ähnliche Verfahren angewandt werden. Einen vereinfachten Ansatz zur Einschätzung des DC bietet die Norm EN ISO 13849-1 im Anhang E.

Bessere Diagnose erlaubt höhere Gefahren

Angegeben wird der DC in vier Stufen – kein, niedrig, mittel und hoch. Wird der DC durch bessere Diagnosemaßnahmen erhöht, kann bei gleicher Ausführungsarchitektur (Kategorie) ein höherer Performance-Level (zulässiges Gefährdungspotenzial der Maschine) erreicht werden.

Das bedeutet in der Praxis, dass die zusätzliche Überwachung eines Arbeitsventils innerhalb eines einkanaligen Systems – beispielsweise durch einen Druckschalter – maßgeblich zur Erhöhung der Sicherheit einer Maschine beitragen kann. Erkennbar ist das am höheren Performance-Level $PL=c/d$ in Kategorie 2. Ohne die zusätzliche Überwachungsmaßnahme könnte nur ein Performance-Level $PL=b/c$ in Kategorie 1 erreicht werden.

Weniger Aufwand – höherer DC

Setzt man zum Beispiel in einem mehrkanaligen System die von Festo entwickelten stellungsüberwachten Ventile der Baureihe VSVA ein, erlaubt das, bei geringerem Aufwand einen höheren DC-Wert zu erreichen. Denn die Norm sieht bei direkter Überwachung (z. B. elektrische Überwachung der Steuerungsventile) 99 % DC und bei indirekter Überwachung (z. B. durch einen Druckschalter) 90 % bis 99 % DC (abhängig von der Anwendung) vor. Und der höhere DC erlaubt wiederum einen höheren Performance-Level bei sonst identer Ausführung der Maschine. So können kleine Adaptionen große Wirkung zeigen.

Festo Gesellschaft m.b.H.

Linzer Straße 227, A-1140 Wien, Tel. +43 1-91075-0

www.festo.at