Whitepaper

Globale Trends in der Maschinensicherheit
Neue Anforderungen für PL und SIL

Autor:
Carsten Gregorius
Produktmarketing Safety
cgregorius@phoenixcontact.com

AI 04-20.001.L6

Inhaltsverzeichnis

Einleitung

Wer schnell und flexibel auf Kundenanforderungen reagieren möchte, ist auf eine komplexe und dezentrale industrielle Produktion angewiesen. Das Thema funktionale Sicherheit gewinnt dabei an Bedeutung. Der Trend der Dezentralisierung birgt neue Herausforderungen für den Schutz von Mensch, Umwelt und Maschine. Neben den klassischen Sicherheitseinrichtungen, wie z. B. Schutztürverriegelungen, Not-Halt-Einrichtungen oder Sicherheitsschaltern kommen mit steigendem Komplexitätsgrad zunehmend programmierbare oder konfigurierbare Sicherheitssysteme zur Absicherung von Maschinen und Anlagen zum Einsatz. Produktionseinrichtungen sollen nicht mehr als unbedingt notwendig eingeschränkt werden.

Die Sicherheit von Maschinen und Anlagen zum Schutz des Anwenders ist im Wesentlichen von der korrekten Anwendung von Normen und Richtlinien abhängig. Die Basis hierfür bildet in Europa die Maschinenrichtlinie, die Unternehmen durch einheitliche Vorgaben bei der sicherheitsgerichteten Konstruktion von Maschinen unterstützt. Aber auch außerhalb des europäischen Wirtschaftsraums haben viele europäische Sicherheitsnormen aufgrund ihres internationalen Status eine große Bedeutung. Eine wichtige Rolle spielen in diesem Zusammenhang auch die Normen zur funktionalen Sicherheit. Die Anforderungen an Maschinensteuerungen sind festgelegt sowohl in der EN ISO 13849 als auch in der IEC 62061.

Im Jahr 2015 wurde versucht, die beiden Normen **EN ISO 13849** und **IEC 62061** zu vereinen. Heute befinden sich beide Normen getrennt voneinander in der Überarbeitung. Die Veröffentlichung der Änderungen wird im Jahr 2021 erwartet. Bei der EN ISO 13849 ist eine Veröffentlichung im April 2021 eingeplant. Bis zur Verabschiedung der inhaltlichen Anpassungen, voraussichtlich im Herbst 2020, finden noch internationale Abstimmungen statt. Welche Änderungen in Bezug auf PL und SIL zu erwarten sind berichtet Sicherheitsexperte Carsten Gregorius, der für Phoenix Contact in den Normungsgremien vertreten ist: „In einigen Punkten, wie im Bereich der „sicherheitsrelevanten Software“ und dem Thema „Cyber Security“ haben sich beide Normen bereits aneinander angenähert. Viele weitere Anpassungen wurden im Detail aufgenommen, sodass sich insgesamt eine einfachere Durchgängigkeit zwischen den beiden Normen ergibt. Ob sich Auswirkungen auf bisherige Sicherheitsbewertungen ergeben, ist im Einzelfall zu bewerten.“

Lesen Sie im Folgenden, wie die Normänderungen im Detail aussehen können.

Was ändert sich bei PL und SIL?

Neben dem Grundanliegen die Lesbarkeit der Normen zu verbessern, lagen die Arbeitsschwerpunkte bei der EN ISO 13849 u. a. bei der eindeutigen Spezifikation der **Sicherheitsanforderungen (SRS)**. Darüber hinaus wird die Bestimmung des **Risikolevels PLr**, bei dem es detaillierte Festlegungen zur Bestimmung des Parameters P gibt, erweitert. Insbesondere die Anforderungen an **sicherheitsrelevante Software** werden konkretisiert. Weitere Änderungen betreffen bei der EN ISO 13849 Konkretisierungen beim Diagnosedeckungsgrad (DC) sowie bei der Definition von „bewährten Bauteilen“. Der Aspekt der „Fehler gemeinsamer Ursache („Common Cause Failure“) wurde bei der EN ISO 13849 im Hinblick auf den EMV-Einfluss detailliert.

Bei der IEC 62061 hat es aus Konsistenzgründen zur IEC 61508 und anderer Sektornormen eine wichtige Anpassung bei den sicherheitstechnischen Kenngrößen gegeben: Zukünftig wird der Begriff des „SILCL“ (SIL-Claim) ersetzt durch den „SIL“. Darüber hinaus gibt es Detaillierungen zur Bestimmung der Fehlerraten von Bauteilen sowie zum Validierungsprozess.

Bei der Definition von Fehlerraten bei Bauteilen gemäß IEC 62061 wurde ein Bezug zwischen dem verwendeten Begriff λ_D und den in der EN ISO 13849 verwendeten Definitionen $MTTF_D$[1] und $B10_D$[2] hergestellt.

Die Validierung der Sicherheitsfunktionen muss zeigen, dass die Anforderungen an die sicherheitsrelevanten Steuerungsteile in Übereinstimmung mit ihren spezifizierten Eigenschaften realisiert sind. Neu bei der IEC 62061 ist das aus dem Teil 2 der EN ISO 13849 bekannte Flussdiagramm zum Validierungsprozess.

Schlussendlich thematisieren beide Normen den Einfluss von **Cyber Security** auf die „funktionale Sicherheit“.

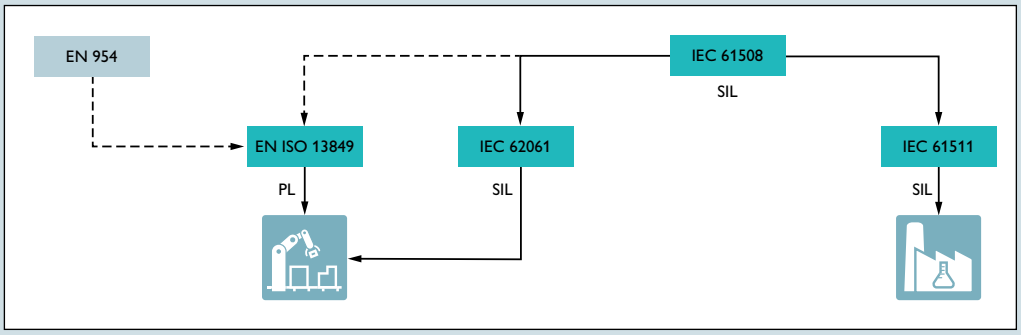
Übersicht der wichtigsten Änderungen bei EN ISO 13849 und IEC 62061

EN ISO 13849	IEC 62061
Erweiterte Festlegungen zur Bestimmung des Parameters P[3] (Risikolevel PLr)	Veränderung der Bezeichnung von „SILCL“ zu „SIL“*
Eindeutige Spezifikation der Sicherheitsanforderungen (SRS)	Berücksichtigung von Low-Demand-Applikationen
Konkrete Definition von „bewährten Bauteilen“	Anpassung Validierungsprozess in Anlehnung an EN ISO 13849*
PFH_D-Ersatzwerte für Ein- und Ausgänge	
Konkrete Anforderungen an sicherheitsrelevante Software	
Einfluss von Cyber Security auf die „funktionale Sicherheit“	
Konkrete Definition von „Diagnosedeckungsgrad“ (DC)*	Beispiele für Fehlerraten ($MTTF_D$), Diagnosedeckungsgrad (DC) in Anlehnung an EN ISO 13849*
Detaillierung des „Fehler gemeinsamer Ursache („Common Cause Failure“) im Hinblick auf EMV-Einfluss*	Beispiele zur Bewertung von Fehlern gemeinsamer Ursache in Anlehnung an EN ISO 13849*

**Neuerungen werden im Whitepaper nicht weiter behandelt*

[1] $MTTF_D$ = mittlere Zeit bis zu einem gefährlichen Ausfall
[2] $B10_D$ = mittlere Schaltspielzahl bis 10 % der Bauteile gefährlich ausgefallen sind
[3] P = Möglichkeit zur Vermeidung einer Gefährdungssituation

Bedeutung der EN ISO 13849 und IEC 62061

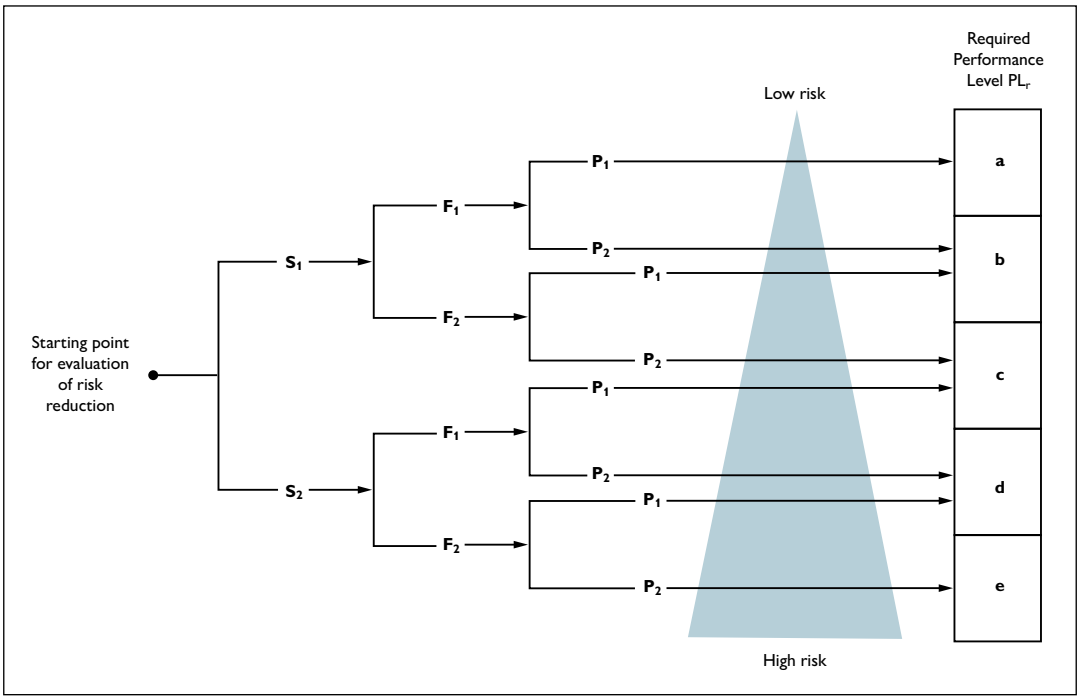


Die Anforderungen an Maschinensteuerungen sind sowohl in der EN ISO 13849 als auch in der IEC 62061 festgelegt. Viele C-Normen verweisen bei der sicheren Gestaltung von Maschinen auf mindestens eine der beiden Normen. Beide Normen berücksichtigen Aspekte der Grundnorm IEC 61508. Die EN ISO 13849 ist vor ca. 20 Jahren aus der damaligen EN 954 entstanden, die IEC 62061 wurde dagegen als Sektornorm für „Maschinen“ entwickelt. Parallel dazu existiert die IEC 61511 als Sektornorm für die Prozessindustrie, die hier jedoch nicht weiter betrachtet wird.

1. Festlegung des erforderlichen PLr gemäß EN ISO 13849

Eine zentrale Bedeutung im Risikominderungsprozess kommt dem „erforderlichen Performance Level (PLr)“ zu. Je nach Risikohöhe wird eine der fünf Stufen „a“ bis „e“ anhand der folgenden Parameter gewählt: S (Schadensausmaß), F (Häufigkeit der Gefährdungsexposition) oder P (Möglichkeit der Vermeidung).

In der Vergangenheit ergab sich insbesondere beim Parameter P die Frage, wann P1 (möglich, unter bestimmten Bedingungen) oder P2 (unmöglich) zu wählen ist.



Bestimmung des PLr

Zur Bestimmung des Parameters P1 bzw. P2 wird zukünftig eine Auswahlhilfe bereitgestellt, die die Aspekte Qualifikation, Ausbreitungsgeschwindigkeit der Gefährdung sowie Komplexität bewertet.

Beschreibung	A	B	C
Training	Geschultes Personal	Nicht geschultes Personal	–
Geschwindigkeit der gefährlichen Bewegung	Gering: < 250 mm/s, Zeit bis zum Erreichen der Gefährdung > 3 s	Mittel: 251 mm/s –1000 mm/s, Zeit bis zum Erreichen der Gefährdung < 3s	Hoch: <1000 mm/s, Zeit bis zum Erreichen der Gefährdung < 1s
Räumliche Möglichkeit sich der Gefährdung zu entziehen	> = 50 % der Fälle	< 50 % der Fälle	Nicht möglich
Möglichkeit der Erkennung	> = 50 % der Fälle	< 50 % der Fälle	Nicht möglich
Komplexität (Anzahl/ Zeit der Bedienereingriffe)	Geringer Komplexitätsgrad (z. B. Justage von Spannzangen, Einlegen von Werkstücken)	Hoher oder mittlerer Komplexitätsgrad (Fehlersuche, Einrichten im Tippbetrieb)	–

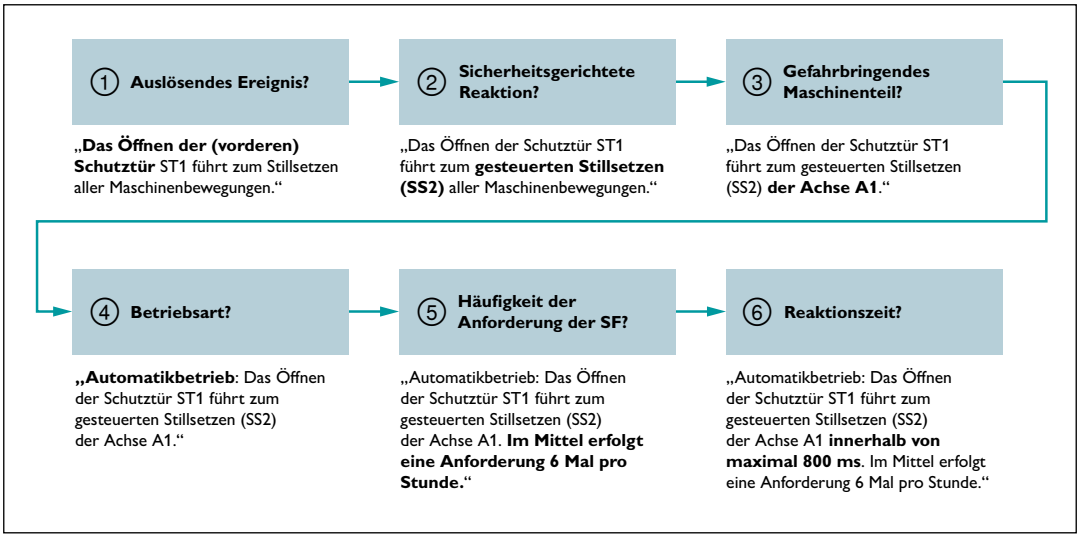
Je nach Anzahl der resultierenden Einstufungen A, B oder C lässt sich dann der Paramater P1 bzw. P2 festlegen. Ist im Bewertungsprozess mindestens 1 x C oder 3 x B festgelegt, so führt dies unmittelbar zu einer P2-Einstufung.

2. Spezifikation der Sicherheitsfunktion gemäß EN ISO 13849

Kritische Vorfälle an sicherheitsrelevanten Steuerungen sind häufig auf eine unzureichende Spezifikation zurückzuführen. Dies kann dazu führen, dass trotz aller weiteren korrekt durchgeführten Verifikationsschritte am Ende nur eine unzureichende Risikominderung erreicht wird. Aus diesem Grund haben die Normensetzer der EN ISO 13849 einen Schwerpunkt gelegt auf die detaillierte Beschreibung der sogenannten SRS (Safety Requirements Specification).

Folgende Fragestellungen sollen den Validierungsprozess unterstützen:

1. Was ist das auslösende Ereignis?
2. Was ist die sicherheitsgerichtete Reaktion?
3. Welches sind die gefahrbringenden Maschinenteile?
4. In welcher Betriebsart wirkt die Sicherheitsfunktion?
5. Wie häufig wird die Sicherheitsfunktion angefordert?
6. Innerhalb welcher Reaktionszeit wird der sichere Zustand erreicht?



Beispiel für die Spezifikation einer Sicherheitsfunktion

Das Beispiel zeigt exemplarisch die einzelnen Schritte, die für eine detaillierte „Spezifikation der Sicherheitsanforderungen“ erforderlich sind. Bei dieser Vorgehensweise wird die Nutzung weit verbreiteter Tools ermöglicht, die ebenfalls diese Herangehensweise unterstützen (z. B. SISTEMA[4]).

3. Bewährte Bauteile gemäß EN ISO 13849

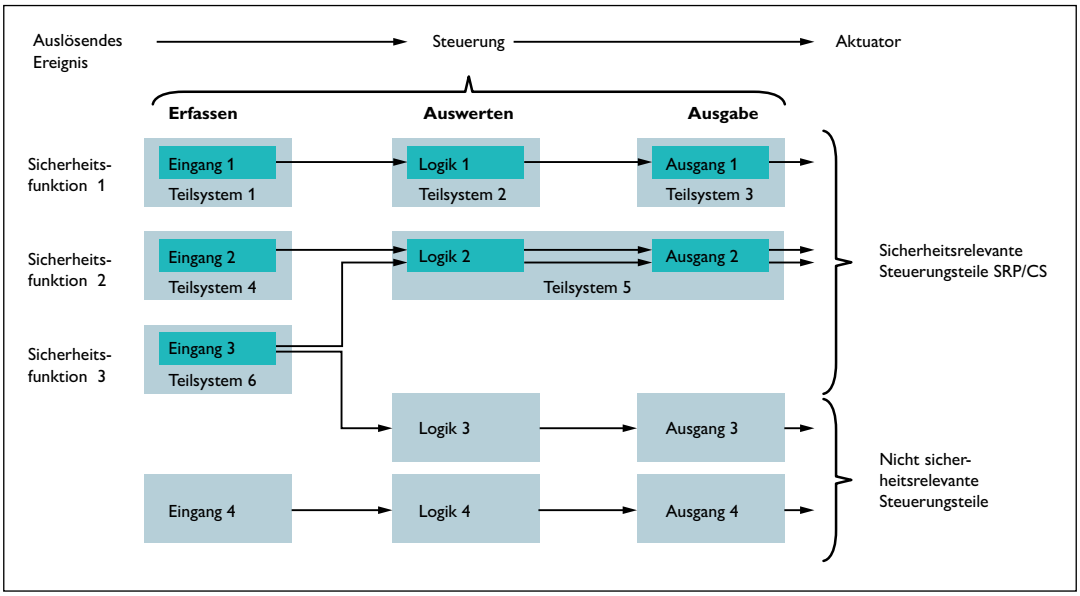
Der Begriff der „bewährten Bauteile“ ist insbesondere bei Auslegung gemäß Kategorie 1 der EN ISO 13849 relevant. Als „bewährt“ angesehen werden Bauteile, die in der Vergangenheit bereits in ähnlichen Anwendungen erfolgreich eingesetzt und dokumentiert wurden. Alternativ gelten solche Bauteile als bewährt, die hinsichtlich ihrer Eignung und Zuverlässigkeit für sicherheitsrelevante Anwendungen hergestellt und verifiziert sind.

Ob eine bestimmte Komponente als “bewährt” akzeptiert wird, hängt von der Anwendung ab, z. B. aufgrund der Umwelteinflüsse. Komplexe elektronische Komponenten (z. B. SPS, Mikroprozessor, anwendungsspezifische integrierte Schaltung) gelten nicht als gleichwertig.

[4] SISTEMA: Sicherheit von Steuerungen an Maschinen
(Hrsg. IFA = Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung)

4. Was, wenn die Kennwerte fehlen? Ersatzwerte gemäß EN ISO 13849

Nach der Definition der Sicherheitsfunktion (SRS) und der Bestimmung des PLr gemäß EN ISO 13849 werden zunächst die sicherheitsrelevanten Steuerungsteile identifiziert und anschließend die Sicherheitsfunktion in „Teilsysteme“ zerlegt. Hierbei können Teilsysteme verschiedenen Sicherheitsfunktionen zugeordnet werden.



Sicherheitsfunktionen und Zuordnung zu Teilsystemen

Je Teilsystem werden im weiteren Verlauf die sicherheitstechnischen Kennwerte (PFH_D, Gebrauchsdauer etc.) bestimmt. Im einfachsten Fall bedient sich der Anwender der Werte, die der Hersteller der Komponente (z. B. Sicherheits-SPS) zur Verfügung stellt. Jedoch sind bei einigen Anwendungen Standardbauteile im Einsatz für die diese Kennwerte nicht verfügbar sind. Bisher konnte man mit einer Annahme von einer $MTTF_D$ = 10 Jahre ausgehen, die aber in vielen Fällen zu „konservativ“ ist. Zukünftig besteht die Möglichkeit bei Teilsystemen aus diskreten Bauteilen mit den PFH_D-Ersatzwerten der nachstehenden Tabelle zu arbeiten, sofern keine Herstellerangaben verfügbar sind.

	PFH_D [1H]	Kategorie B	Kategorie 1	Kategorie 2	Kategorie 3	Kategorie 4
PL b	$5*10^{-6}$	X	O	O	O	O
PL c	$1,7*10^{-6}$	–	X*	X*	O	O
PL d	$2,9*10^{-7}$	–			X*	O
PL e	$4,7*10^{-8}$	–	–	–	–	X*

PFH_D-Ersatzwerte für Ein- und Ausgänge

X angewandte Kategorie ist empfohlen

O angewandte Kategorie ist optional

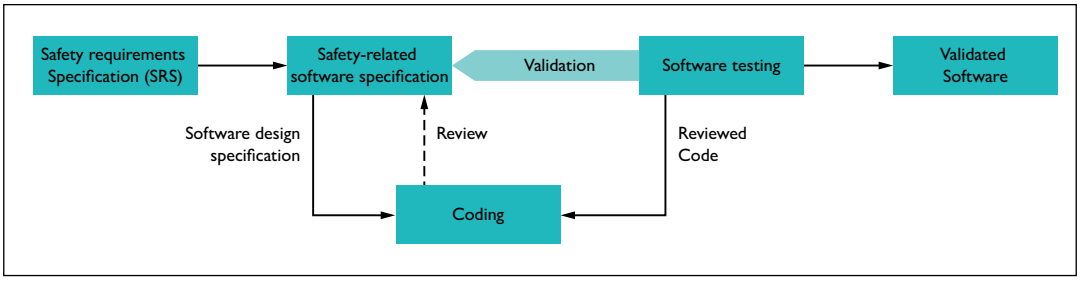
* *bewährte Bauteile und sicherheitstechnisch bewährte Prinzipien müssen verwendet werden*

– *Kategorie ist nicht zulässig*

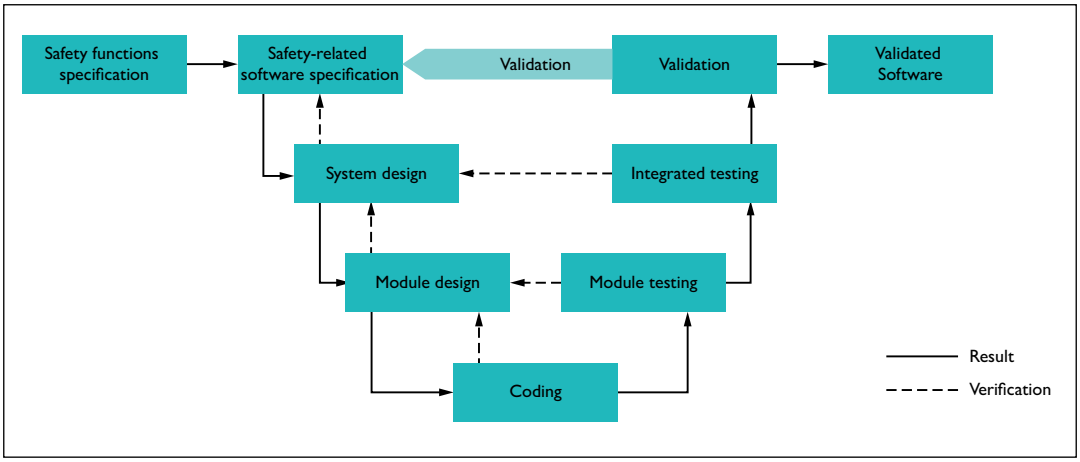
5. Anforderungen an sicherheitsrelevante Software gemäß EN ISO 13849 / IEC 62061

Zunehmend kommen bei Maschinensteuerungen konfigurierbare oder programmierbare Systeme zum Einsatz, die bereits gemäß IEC 61508 zertifiziert sind.

Insbesondere für die zuvor genannten Systeme sowie bei Systemen die LVL[5]-Sprachen verwenden, sind zukünftig wesentliche Vereinfachungen bei der Verifikation und der Validierung von Sicherheitsfunktionen zu erwarten. So wird das bestehende V-Modell in der EN ISO 13849 für diesen Anwendungsfall vereinfacht, sodass neben der Software-SRS lediglich die Schritte „Codierung“ und „Software-Testing“ verbleiben.



Vereinfachtes V-Modell



V-Modell für FVL[6]-Sprachen

[5] LVL: Limited Variability Languages = Programmiersprachen mit begrenztem Sprachumfang
[6] FVL: Full Variability Languages = Programmiersprachen mit vollem Sprachumfang

Werden jedoch FVL[6]-Sprachen wie Ada, C, Assembler etc. verwendet, so bleibt das bisherige V-Modell in der Anwendung verbindlich.

Bei der IEC 62061 sind analog dazu sogenannte „Software-Level“ definiert. In der Norm werden drei Stufen beschrieben: In der ersten Stufe sind die vorgefertigten Systeme („pre-designed“) mit LVL-Sprachen beschrieben, für die ein vereinfachtes Validierungsverfahren möglich wird (analog zur EN ISO 13849). Beim Einsatz von sogenannten FVL-Sprachen sieht der Verifikations- und Validierungsprozess umfangreicher aus.

Software-Level	**Plattform** (Kombination aus Hard- und Software)	**Beispiel**
1	„pre-designed“ nach IEC 61508 (Anwendungs-Software, die LVL verwendet)	Sicherheits-SPS mit LVL oder programmierbares Sicherheitsschaltgerät
2	„pre-designed“ nach IEC 61508 (Anwendungs-Software, die keine LVL verwendet)	Sicherheits-SPS mit FVL nach IEC 61508
3	„pre-designed“ nach IEC 61508 (Anwendungs-Software, die keine LVL verwendet)	Sicherheits-SPS mit FVL nach IEC 62061

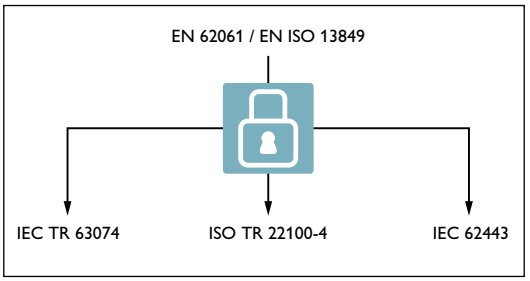
Die nachstehende Tabelle zeigt die daraus resultierenden, minimal erforderlichen Unabhängigkeitsgrade für **Software-Level 1**. Zusätzlich darf der Anwender das vereinfachte V-Modell (siehe EN ISO 13849) anwenden.

Minimaler Unabhängigkeits-grad	**Erforderlicher SIL für die Sicherheitsfunktion**		
	1	**2**	**3**
Gleiche Person	Nicht ausreichend	Nicht ausreichend	Nicht ausreichend
Andere Person	Nur wenn vorzertifizierte Software-Module verwendet werden	Nur wenn vorzertifizierte Software-Module verwendet werden	Nicht ausreichend
Unabhängige Person	ausreichend	ausreichend	ausreichend
Unabhängige Abteilung	Nicht erforderlich	Nicht erforderlich	Nicht erforderlich
Unabhängige Organisation	Nicht erforderlich	Nicht erforderlich	Nicht erforderlich

Zusammenfassend lässt sich sagen, dass beim Einsatz von vorzertifizierten Systemen und Software-Bausteinen eine deutliche Vereinfachung beim Verifikations- und Validierungsprozess zu erwarten ist.

6. Einfluss von Cyber Security auf die funktionale Sicherheit gemäß EN ISO 13849 / IEC 62061

Im Gegensatz zur funktionalen Sicherheit schützt die Cyber Security Güter vor einer nachteiligen Beeinträchtigung durch beabsichtigte oder versehentliche Attacken auf die Verfügbarkeit, Integrität und Vertraulichkeit der Daten. Dazu werden vorbeugende, technische sowie organisatorische Maßnahmen verwendet.



Normative Situation:
Cyber Security bei funktionaler Sicherheit

Durch die zunehmende Vernetzung der Automatisierungssysteme mit der IT-Welt können Szenarien auftreten, die insbesondere von Safety-Anwendungen eine neue Herangehensweise erfordern. Ein wichtiges Einfallstor für Hacker stellen die Netzwerkübergänge zwischen der Office-IT und dem Produktionsnetz dar. Dieses Gefährdungspotential spiegelt sich auch in beiden Normungsprojekten wider und muss zukünftig berücksichtigt werden, z. B. indem eine IT-Risikobeurteilung in Anlehnung an die Norm IEC 62443 durchgeführt wird.

7. Low-Demand-Systeme für Maschinen gemäß IEC 62061

Der Anwendungsbereich der Maschinenrichtlinie ist in der praktischen Anwendung einerseits sehr weit gefasst. So fallen z. T. neben klassischen Arbeitsmaschinen auch Anlagen wie Gas- und Dampfturbinen, Kompressoren, Generatoren oder Pumpen unter die Richtlinie. Auf der anderen Seite haben die beiden harmonisierten Normen zur funktionalen Sicherheit – EN ISO 13849 und IEC 62061 – „Low-Demand-Applikationen“ [7] bisher nicht berücksichtigt. In der Folge entstand aufgrund der fehlenden Konformitätsvermutung eine Rechtsunsicherheit bei den Herstellern solcher Systeme. Zumindest die IEC 62061 greift nun diesen Ansatz auf, indem es in Anlehnung an die IEC 61508 jetzt PFD[8]-Ausfallgrenzwerte definiert.

Bei korrekter Anwendung der IEC 62061 können daher nun auch Low-Demand-Applikationen unter Inanspruchnahme der „Konformitätsvermutung“ im Anwendungsbereich der Maschinenrichtlinie bewertet werden.

SIL	PFDavg-Grenzwerte bei Low-Demand
1	$<10^{-1}$
2	$<10^{-2}$
3	$<10^{-3}$

[7] Betriebsart, bei der die Häufigkeit der Anforderungen an eine Sicherheitsfunktion nicht mehr als 1 pro Jahr und nicht mehr als das Doppelte der Frequenz der Proof-Tests beträgt
[8] Probability of dangerous failure on demand

Exkurs: Arbeiten im Normungsgremium

Carsten Gregorius

Die Experten von Phoenix Contact sind in allen wichtigen Normungsgremien vertreten. Für den Kunden steht dieses Know-how entweder über unsere Vertriebskanäle im Netz aber auch durch unsere Präsenz vor Ort zur Verfügung.

Carsten Gregorius ist als Sicherheitsexperte für Phoenix Contact in den nationalen Normungsgremien zur EN ISO 13849 und IEC 62061 vertreten.

Wie sieht die Arbeit in einem Normengremium aus?

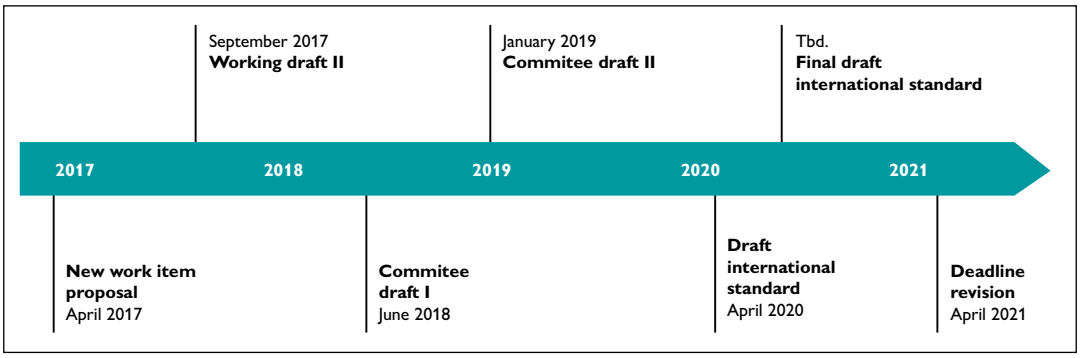
Bevor ein neues Normungsvorhaben auf internationaler Ebene startet, muss zunächst ein Vorschlag (NWIP = New work Item Proposal) quasi als „Steckbrief“ erarbeitet werden. Ist dieser Prozess positiv durchlaufen, beginnt das Projekt mit der Aufsetzung einer internationalen Expertengruppe. In diesem internationalen Gremium laufen die eigentlichen inhaltlichen Ausarbeitungen. Aus der internationalen Arbeitsgruppe werden dann Normentwürfe, so genannte „commitee drafts“ oder „FDIS“ erarbeitet. Diese werden dann den nationalen Normungsgremien, auch „Spiegelgremien“ genannt, zur Kommentierung bereitgestellt. In Deutschland übernimmt der DIN häufig die Federführung in den Spiegelgremien.

Was passiert dann weiter?

Prinzipiell kann jeder seine Anmerkungen oder Änderungswünsche an einem Normentwurf über die nationalen Normungsgremien einspeisen. Daher umfassen die Kommentare je nach Normungsvorhaben und Mitgliedsland nicht selten hunderte von Einzelkommentaren, die alle bearbeitet werden müssen. Da aber gerade kleinen und mittelständischen Unternehmen häufig die Zeit fehlt überall in den verschiedenen Normungsgremien mitzuwirken, übernehmen Interessenverbände wie VDMA oder ZVEI einen Teil dieser Aufgaben.

Und wie entsteht dann eine Neufassung einer Norm?

Nachdem alle Kommentare von den nationalen Spiegelgremien zurück an die internationale Normungsgruppe gespielt worden sind, werden diese in einem neuen Entwurf berücksichtigt. Dieser wird dann schlussendlich als FDIS[9] zur finalen Abstimmung den einzelnen Ländern mit Stimmberechtigung bereitgestellt. Ein FDIS wird dann im Mehrheitsprinzip angenommen oder abgelehnt. Bei einem positiven Ergebnis entsteht im weiteren Verlauf z. B. die Neufassung der EN ISO 13849.



Zeitlicher Fahrplan für die Überarbeitung der EN ISO 13849

[9] FDIS: Final draft International Standard

Welche Projekte folgen als Nächstes?

Nach Abschluss der Überarbeitung der EN ISO 13849 (Teil 1) soll in einem nächsten Überarbeitungsschritt der technische Report EN ISO/TR 23849 mit Berechnungsmodellen zur Bestimmung des PFHD ergänzt werden. In einem weiteren Projekt erfolgt dann die Überarbeitung von Teil 2 der EN ISO 13849 (Validierung) bevor anschließend die beiden Teile 1 und 2 zusammengeführt werden.

Glossar

Ausfall gemeinsamer Ursache

Darunter versteht man den Betriebsausfall von verschiedenen Elementen, die aus gemeinsamen Einzelereignissen hervorgehen und nicht voneinander begünstigt wurden.

Diagnosedeckungsgrad

Ein Maß für die Wirksamkeit der Diagnose, das als Verhältnis zwischen der Ausfallrate, der entdeckten Fehlerraten und der Rate der Totalausfälle dargestellt wird. Der diagnostische Umfang kann entweder auf das gesamte System oder bestimmte Komponenten bezogen sein, wie z. B. für Sensoren, logische Systeme oder finale Elemente.

Performance Level

Der Performance Level (PL) ist eine qualitative Einstufung der einzelnen SRP/CS (sicherheitsbezogene Teile von Steuerungssystemen) in Bezug auf das Leistungsvermögen der einzelnen Sicherheitsfunktionen bei unvorhersehbaren Situationen.

Gefahrbringender Ausfall je Stunde

Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde. PFH_D bedeutet probability of dangerous failure per hour.

Harmonisierte Norm

Harmonisierte Normen sind europäische Normen für Produkte, die im Amtsblatt unter einer europäischen Richtline gelistet sind. Sie gehören zu dem „New Approach“ (neues Konzept) der Europäischen Kommission, indem grundlegende Anforderungen an Produkte durch die Organisationen CEN und CENELEC erarbeitet werden. Die harmonisierten Normen werden im Amtsblatt der EU veröffentlicht. Nur Waren und Dienstleistungen, die den grundlegenden Anforderungen der Richtlinien entsprechen, dürfen in den Verkehr gebracht werden. Man erkennt sie anhand von Bescheinigungen oder CE-Kennzeichnungen.

Weiterführende Literatur und weiterführende Links

Safety meets Security – gemeinsame Strategie erforderlich

Besuchen Sie uns auf phoe.co/safety-meets-security

Funktionale Sicherheit von Maschinen –

Praktische Anwendung der DIN EN ISO 13849-1
(Beuth-Verlag: ISBN 978-3-410-25249-8)

Ihren lokalen Partner fi nden Sie auf

phoenixcontact.com

PHOENIX CONTACT