5 Die Anwendernorm DIN EN 62061 (VDE 0113-50), in Verbindung mit DIN EN ISO 13849-1

Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme.

5.1 Welche Norm ist anzuwenden: DIN EN ISO 13849-1 oder DIN EN 62061 (VDE 0113-50)?

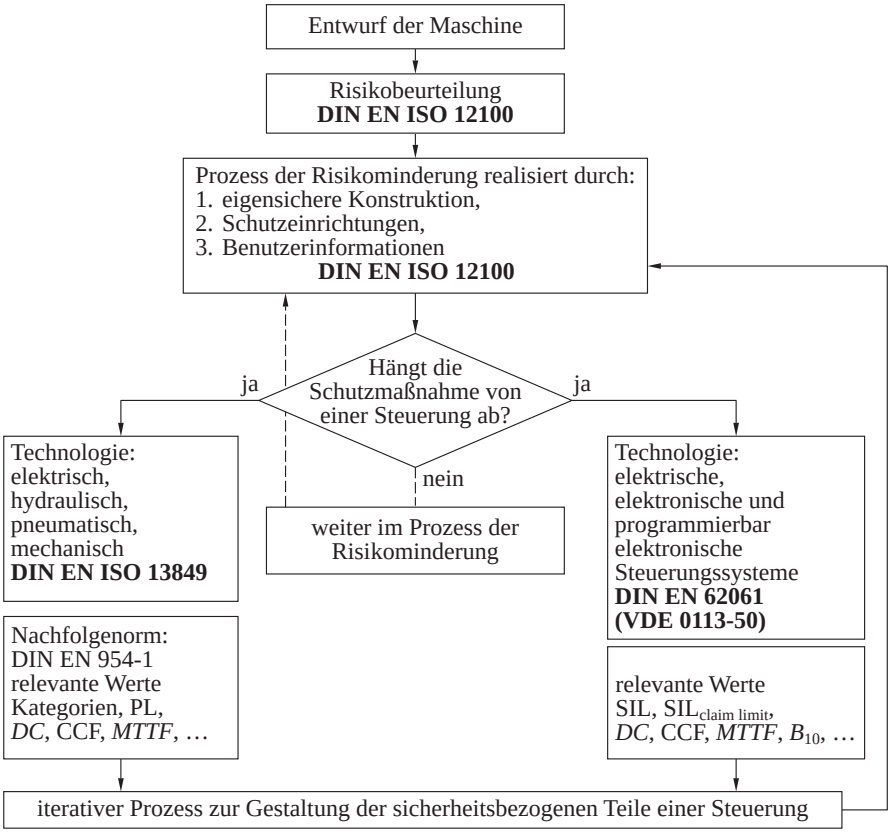

Bild 5.1 Funktionale Sicherheit – zwei Normen

Und? Welche Vorliebe haben Sie? Hört sich seltsam an, aber es ist wirklich so: Wenn ich die Kategorien der DIN EN 954-1 kenne, dann werde ich auch die Nachfolgenorm DIN EN ISO 13849-1 verwenden. Logisch. Wer will schon etwas von Architekturen hören, wenn es Kategorien gibt?

Dass die DIN EN 62061 (**VDE 0113-50**) nichts anderes macht als Kategorien als einkanalige und zweikanalige Architekturen zu umschreiben, ist dem Leser der Norm aufgefallen. Würde man diese dann auch noch mit dem Begriff Kategorie in Verbindung bringen, dann würden sich alle Bedenken in Luft auflösen. Dies geschah leider zu selten und somit lebt der Mythos der Kategorie DIN EN 954-1 weiter.

Einige Menschen haben schon erkannt, dass das kein Kriterium sein darf. Und viele haben erkannt, dass die Grundsätze der Funktionalen Sicherheit der DIN EN 62061 (**VDE 0113-50**) sehr wohl auch für andere Technologien verwendbar sind – der Anwendungsbereich verdeutlicht dies (**Bild 5.2**).

Lassen Sie uns die in **Tabelle 5.1** gezeigte Gegenüberstellung machen und entscheiden Sie selbst wie wichtig der Begriff der „Kategorien“ noch ist.

„[…]

- *legt keine Anforderungen für die Leistungsfähigkeit von nicht elektrischen (z. B. hydraulischen, pneumatischen) Steuerungselementen für Maschinen fest;*

Anmerkung 4: Obwohl die Anforderungen in dieser Norm spezifisch für elektrische Steuerungssysteme sind, kann der festgelegte Rahmen und die Methodologie für sicherheitsbezogene Teile von Steuerungssystemen anwendbar sein, die andere Technologien verwenden. […]“

Bild 5.2 Anwendungsbereich der DIN EN 62061 (**VDE 0113-50**)

DIN EN ISO 13849-1	**DIN EN 62061 (VDE 0113-50)**			**DIN EN ISO 13849-1**
Kategorie	**Fehlertoleranz der Hardware 0 = einkanalig 1 = zweikanalig**	***SFF* = DC_{avg}**	**Maximal erreichbarer SIL**	**Maximal erreichbarer PL**
1	0	< 60 %	SIL 1	PL c
2	0	60 % … 90 %	SIL 1/2	PL c/d
3	1	< 60 %	SIL 1	PL c
	1	60 % … 90 %	SIL 2	PL d
4	1	> 90 %	SIL 3	PL e

Tabelle 5.1 Vereinfachte sinnvolle Anwendung und Zuordnung von Kategorien zu PL und SIL

Eine Kategorie 2-Anwendung mit einem erreichbaren PL d oder SIL 2 ist mit Vorsicht zu genießen. Kategorie 4 verlangt immer einen Diagnosedeckungsgrad *DC* > 99 % (± 5 %). Da Kategorie 3 bis 90 % (± 5 %) definiert ist, macht die Vereinfachung *DC* > 90 % für Kategorie 4 Sinn.

In der Praxis gibt es aus Anwendersicht nur 60 %, 90 % oder 99 % oder mehr. Die ± 5 %-Aussage wirkt nicht wirklich beruhigend – sie verwirrt den Anwender eher. Aber in der DIN EN ISO 13849-1 ist diese Aussage, unter bestimmten Rahmenbedingungen, sehr wohl nachvollziehbar.

Wie nah beide Normen aber tatsächlich schon heute zu einander stehen, lässt sich wie folgt darstellen und erklären. Im Grunde soll immer eine Sicherheitsfunktion physikalisch abgebildet werden, um dann hinsichtlich ihrer Zuverlässigkeit bewertet werden zu können – das Ursache/Wirkung-Prinzip.

Die Architekturen sind Kategorien

Der Begriff „Fehlertoleranz der Hardware“ in DIN EN 62061 (**VDE 0113-50**) entspricht dem Ansatz der Kategorie der DIN EN ISO 13849-1: Dabei stellt sich die einfache und grundlegende Frage, ob eine einkanalige oder zweikanalige Architektur als technische Realisierung den gewünschten Erfolg bringt. Tabelle 5.1 zeigt vereinfacht die elementaren Zusammenhänge.

Das Teilsystem ist ein SRP/CS

Wenn bei Anwendung der DIN EN ISO 13849-1 eine Sicherheitsfunktion in mehrere SRP/CS unterteilt wird, dann entspricht das genau der Vorgehensweise in DIN EN 62061 (**VDE 0113-50**):

Erfassen (Ursache)	+	Auswerten (Logik)	+	Reagieren (Wirkung)
$\text{Teilsystem}_{\text{Erfassen}}$	+	$\text{Teilsystem}_{\text{Logik}}$	+	$\text{Teilsystem}_{\text{Wirkung}}$
SRP/CS_{I}	+	SRP/CS_{L}	+	SRP/CS_{O}

Dabei stellt sich für jedes einzelne Teilsystem oder SRP/CS die Frage der ausgesuchten Architektur oder Kategorie und der erreichbaren Sicherheitsintegrität. Es verwirrt somit, wenn man von einer Kategorie oder Architektur für eine Sicherheitsfunktion spricht. In der Praxis werden meistens drei Teilsysteme oder SRP/CS verwendet und die Frage der Kategorie oder Architektur bezieht sich dann auf diese einzelnen Teilsysteme oder SRP/CS.

Das SRECS (System) ist die Sicherheitsfunktion

Mehrere Teilsysteme oder SRP/CS zusammen bilden die physikalische Abbildung der Sicherheitsfunktion und werden mit dem Begriff SRECS in DIN EN 62061 (**VDE 0113-50**) umschrieben. Die eigentliche Funktion (oder Funktionalität) eines SRECS wird als SRCF in DIN EN 62061 (**VDE 0113-50**) bezeichnet. Diese beiden Begriffe kennt DIN EN ISO 13849-1 nicht, weil ausschließlich immer von der Sicherheitsfunktion gesprochen wird.

DIN EN 62061 (**VDE 0113-50**) legt Wert auf eine funktionale Beschreibung bzw. Aufteilung einer Sicherheitsfunktion (darum auch SRCF), um dann im nächsten Schritt erst die Sicherheitsfunktion physikalisch abbilden zu können. Das Versagen eines Teilsystems führt dazu, dass auch das SRECS (System) versagen wird, und somit auch die Sicherheitsfunktion. Dieser „hierarchische" Ansatz erlaubt eine klare Aufteilung der Sicherheitsfunktion: Von einem System zu einzelnen Teilsystemen, die alle eine entscheidende Rolle spielen.

Diesen Zwischenschritt kennt DIN EN ISO 13849-1 nicht und verwendet deshalb nur den Begriff Sicherheitsfunktion: Es kann sogar ein einzelnes SRP/CS eine Sicherheitsfunktion abbilden. Aber genau diese Möglichkeit verwirrt den Anwender, weil es keine eindeutige Zuordnung mehr zwischen dem auslösenden Ereignis und der eingeleiteten Reaktion gibt, und dadurch die Bewertung der realisierten Lösung schwierig wird.

5.2 Die Zielsetzung

Diese Norm ist eine Anwendungsnorm, die den technologischen Fortschritt nicht einschränken oder gar verhindern möchte. Sie kann nicht alle Anforderungen beinhalten die dem Schutz des Menschen vor Gefahren dienen (z. B. nicht elektrische Verriegelungen, …). Als ein Ergebnis der Automatisierung, der Forderung nach gesteigerter Produktion und reduziertem körperlichen Aufwand des Benutzers, spielen elektrische Steuerungssysteme von Maschinen eine zunehmend wichtige Rolle in der Maschinengesamtsicherheit. Weiterhin verwenden die Steuerungssysteme selbst eine zunehmend komplexe elektronische Technologie.

In der Einleitung der Norm heißt es demnach:

Auszug aus der DIN EN 62061 (VDE 0113-50):2016-05

Es gibt viele Situationen an Maschinen, wo SRECS als Teil der vorgesehenen Sicherheitsmaßnahmen benutzt werden, um eine Minderung des Risikos zu erreichen.

Ein typischer Fall ist die Verwendung einer verriegelten trennenden Schutzeinrichtung, die, wenn geöffnet, um Zugang zum Gefährdungsbereich zu ermöglichen, dem elektrischen Steuerungssystem signalisiert, die gefährliche Maschinenbewegung zu stoppen. Ebenso trägt in der Automatisierung das elektrische Steuerungssystem, das verwendet wird, um den korrekten Betrieb des Maschinenprozesses zu erreichen, oft zur Sicherheit bei, indem es die mit den Gefährdungen, die direkt von Ausfällen des Steuerungssystems herrühren, verbundenen Risiken verringert.

Diese Norm stellt eine Methodologie und Anforderungen bereit, um:

- den erforderlichen Sicherheitsintegritätslevel für jede sicherheitsbezogene Steuerungsfunktion, die vom SRECS auszuführen ist, zu bestimmen;
- den Entwurf des SRECS in Angemessenheit zu der (den) bestimmten sicherheitsbezogenen Steuerungsfunktion(en) zu ermöglichen;
- in Übereinstimmung mit DIN EN ISO 13849-1 entworfene sicherheitsbezogene Teilsysteme zu integrieren;
- das SRECS zu validieren.

[…]

Diese Norm ist zur Verwendung innerhalb des Gesamtrahmens der in DIN EN ISO 12100 beschriebenen systematischen Risikominderung und in Verbindung mit einer Risikobeurteilung gemäß den in DIN EN ISO 12100 beschriebenen Prinzipien vorgesehen. Eine zur Festlegung des Sicherheitsintegritätslevels (SIL) vorgeschlagene Methodologie ist im informativen Anhang A enthalten.

[…]

Zu erwartende Änderung in der VDE 0113-50

Zielgruppe Maschinenbauer, als Hersteller oder Integrator

Diese internationale Norm ist für die Verwendung durch Maschinenkonstrukteure, Steuerungshersteller und Integratoren, sowie andere Personen bestimmt, die an der Spezifikation, dem Entwurf und der Validierung eines SCS beteiligt sind. Sie legt einen Ansatz fest und enthält Anforderungen zur Erreichung der erforderlichen Leistungsfähigkeit und erleichtert die Spezifikation der Sicherheitsfunktionen, mit denen die Risikominderung erreicht werden soll.

Dieses Dokument bietet einen Maschinensektor spezifischen Rahmen für die funktionale Sicherheit eines SCS von Maschinen. Es deckt nur die Aspekte des Sicherheitslebenszyklus ab, die sich auf die Zuordnung von Sicherheitsanforderungen bis hin zur Validierung der Sicherheit beziehen. Es werden Anforderungen an Informationen für

den sicheren Einsatz von SCS von Maschinen gestellt, die auch für spätere Phasen des Lebenszyklus eines SCS relevant sein können.

This international Standard is intended for use by machinery designers, control system manufacturers and integrators, and others involved in the specification, design and validation of an SCS. It sets out an approach and provides requirements to achieve the necessary performance and facilitates the specification of the safety functions intended to achieve the risk reduction.

This document provides a machine sector specific framework for functional safety of an SCS of machines. It only covers those aspects of the safety lifecycle that are related to safety requirements allocation through to safety validation. Requirements are provided for information for safe use of SCS of machines that can also be relevant to later phases of the lifecycle of an SCS.

Sektornorm der IEC 61508 und harmonisiert unter der Maschinenrichtlinie

Die IEC 61508 ist nicht unter der Maschinenrichtlinie gelistet. Das ist und war auch nicht ihr Anspruch. Sie ist eine „safety publication".

Aber die IEC 61508 hat die Philosophie der EN 954-1:1996 (die im Jahr 1999 in die ISO 13849.1:1999 umbenannt wurde) grundsätzlich im Sinne

1. von Vorgehensweise und Architekturbewertungen zur Realisierung von Sicherheitsfunktionen,
2. als Basis für eine neue deterministische und systematische Betrachtungsweise,
3. für komplexe elektronische Komponenten

übernommen.

Die IEC 62061 ihrerseits hat die Methodik von der IEC 61508 (oft spricht man von ihrer Mutternorm) übernommen, und den Bedürfnissen der Maschinensicherheit angepasst: sie ist also eine Sektornorm.

Da die IEC 62061 eine internationale Norm ist – die EN IEC 62061 stellt die europäische Fassung durch CENELEC dar, die zur Harmonisierung unter der Maschinenrichtlinie herangezogen wird –, findet sich keine Aussage zu diesem Thema Harmonisierung.

In Europa genießt sie aber den Status einer harmonisierten Norm als DIN EN 62061.

Mit ihr kann also im Rahmen der Anwendung der DIN EN ISO 12100 eine Vermutungswirkung zur Erfüllung der grundlegenden Anforderungen hinsichtlich „Entwurf von Sicherheitsfunktion mit einem Steuerungssystem" der Maschinenrichtlinie ausgesprochen werden. Dies findet sich in der deutschen Fassung der VDE 0113-50 in dem Vorwort A1 und dem europäischen Vorwort A2 wieder.

Die Zielsetzung der DIN EN ISO 13849-1 ist grundsätzlich dieselbe:

Auszug aus der DIN EN ISO 13849-1:2016-06

Als Teil einer Gesamtrisikominderung an einer Maschine wird ein Konstrukteur oft Maßnahmen durch die Anwendung von Schutzeinrichtungen zur Risikoreduzierung ergreifen, die eine oder mehrere Sicherheitsfunktionen verwenden.

Teile einer Maschinensteuerung, die Sicherheitsfunktionen liefern sollen, werden sicherheitsbezogene Teile einer Steuerung (SRP/CS) genannt, und diese Teile können entweder aus Hardware und Software bestehen und separater oder integraler Bestandteil der Maschinensteuerung sein. Zusätzlich zur Bereitstellung von Sicherheitsfunktionen kann ein SRP/CS auch Betriebsfunktionen liefern (z. B. eine Zweihandsteuerung zum Start eines Prozesses).

Die Fähigkeit sicherheitsbezogener Teile von Steuerungen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, wird einer von fünf Stufen zugeordnet, den sogenannten Performance Level (PL). Diese Performance Level werden definiert in Form der Wahrscheinlichkeit eines Gefahr bringenden Ausfalls je Stunde.

Die Wahrscheinlichkeit eines Gefahr bringenden Ausfalls der Sicherheitsfunktion hängt von mehreren Faktoren ab, einschließlich der Hardware- und Softwarestruktur, dem Umfang der Fehler-Detektionsmechanismen [Diagnosedeckungsgrad (*DC*)], der Zuverlässigkeit von Bauteilen [mittlere Zeit bis zum Gefahr bringenden Ausfall ($MTTF_D$), den Ausfällen infolge gemeinsamer Ursache (CCF)], dem Gestaltungsprozess, der Belastung im Betrieb, den Umgebungsbedingungen und den betrieblichen Einsatzbedingungen.

Um den Konstrukteur zu unterstützen und als Hilfe zur Bestimmung des erreichten PL, stellt diese Norm eine Methode auf Basis einer Kategorisierung von Strukturen nach speziellen Entwurfskriterien und spezifiziertem Verhalten bei Fehlerbedingungen bereit. Diese Kategorien werden einer von fünf Stufen zugeordnet, genannt Kategorien B, 1, 2, 3 und 4.

Die Performance Level und Kategorien können angewendet werden für sicherheitsbezogene Teile von Steuerungen, wie:

- nicht trennende Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen), berührungslos wirkende Schutzeinrichtungen (z. B. Lichtschranken), druckempfindliche Schutzeinrichtungen,
- Steuerungsbaugruppen (z. B. die Logik für Steuerungsfunktionen, Datenverarbeitung, Überwachung usw.) und
- Leistungsschaltelemente (z. B. Relais, Ventile usw.)

als auch Sicherheitsfunktionen ausführende Steuerungen in allen Arten von Maschinen – von einfachen (z. B. einer kleinen Küchenmaschine oder automatischen Türen und Toren) bis zu einer Fertigungsanlage (z. B. Verpackungsmaschinen, Druckmaschinen, Pressen).

[…]

Wenn beide Normen die gleiche Zielsetzung verfolgen, warum gibt es dann beide Normen?

Das europäische Projekt STSARCES ist der Grund (siehe Kapitel 1). Komplexe Elektronik war nicht mehr bewertbar mit der DIN EN 954-1. Mit der Normenreihe IEC 61508 (Erstellung 1999) wurde ein Hilfsmittel geschaffen, das eine Bewertung erstmals erlaubte.

Die Anwendungsnorm DIN EN 62061 (**VDE 0113-50**) war die logische Konsequenz für den Anwender (Maschinenhersteller). Da die IEC-Normen Anforderungen an elektrotechnische Aspekte stellt, ist die Formulierung der Zielsetzung in DIN EN 62061 (**VDE 0113-50**) nachvollziehbar – quasi als Geschäftsauftrag. Im Grunde dürfte DIN EN ISO 13849-1 diese elektrotechnischen Aspekte nicht betrachten, weil das die Hoheitsaufgabe der IEC ist. Nun gab es aber die DIN EN 954-1:1997-03 und ein potenzieller Konflikt war damit vorprogrammiert. Dies findet sich im Anwendungsbereich beider Normen wieder.

5.3 Der Anwendungsbereich

Diese Norm dient der praktischen Anwendung der Funktionalen Sicherheit. Sie soll also dem Anwender helfen den technologischen Fortschritt zu nutzen:

Auszug aus der DIN EN 62061 (VDE 0113-50):2016-05

Diese Norm ist eine Anwendungsnorm und ist nicht dazu gedacht, den technologischen Fortschritt zu begrenzen oder zu behindern. Sie umfasst nicht alle Anforderungen (z. B. Verwendung von Schutzeinrichtungen, nicht elektrische Verriegelung oder nicht elektrische Steuerung), die notwendig sind oder durch andere Normen oder Vorschriften gefordert werden, um Personen vor Gefährdungen zu schützen. Jede Art von Maschine besitzt eigene Anforderungen, die erfüllt werden müssen, um für ausreichende Sicherheit zu sorgen.