ZVEI:
Die Elektroindustrie

Sicherheit von Maschinen

Information zur Anwendung und Abgrenzung der Normen EN 62061 und EN ISO 13849

Version 1.1

Verband der Elektro- und Digitalindustrie

ZVEI:
Die Elektroindustrie

Sicherheit von Maschinen
Information zur Anwendung und Abgrenzung der Normen EN 62061 und EN ISO 13849
Version 1.1

Herausgeber:
ZVEI e. V.
Fachverband Automation
Lyoner Straße 9
60528 Frankfurt

Dr. Markus Winzenick
Telefon: +49 69 6302-426
E-Mail: winzenick@zvei.org

www.zvei.org

Februar 2022

Inhalt

1 Motivation

Die schnelle und flexible Reaktion auf Kundenanforderungen erfordert eine komplexe und dezentrale industrielle Produktion. Eine Schlüsselfunktion kommt dabei dem Thema „funktionale Sicherheit" zu. Um den Trend zur Digitalisierung und Dezentralisierung zu unterstützen müssen sich die Anforderungen zur Maschinensicherheit und Produktivität gegenseitig ergänzen. Zunehmend kommen mit wachsendem Komplexitätsgrad konfigurierbare bzw. programmierbare Sicherheitssysteme zur Absicherung von Maschinen und Anlagen zum Einsatz.

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 einheitliche Schutzziele bei der Konstruktion von Maschinen unterstützt. Aber auch außerhalb des europäischen Wirtschaftsraums haben viele europäische Normen aufgrund ihres internationalen Status eine große Bedeutung. Eine wichtige Rolle spielen in diesem Zusammenhang auch die Normen zur funktionalen Sicherheit. Die Anforderungen an die sicherheitsrelevanten Teile von Maschinensteuerungen sind festgelegt sowohl in der EN ISO 13849 als auch in der EN 62061.

Die nachfolgenden Erläuterungen beschreiben die wesentlichen Grundzüge beider Normen auf Basis der Ausgabestände IEC 62061:2021 und EN ISO 13849:2015 einschließlich den geplanten Änderungen prEN ISO 13849-1:2021. Daher kann diese Übersicht keinen Anspruch auf Vollständigkeit erheben.

Anm.: Zum Zeitpunkt der Erstellung dieses Dokuments ist der Harmonisierungsvorgang mit den Ausgabeständen 2021 noch nicht abgeschlossen.

2 Gegenüberstellung der wichtigsten Unterschiede

Beide Normen haben sich im Verlauf der Maintenance-Projekte weiter angenähert. Beide Normen sind unter der Maschinenrichtlinie harmonisiert und und können dafür herangezogen werden, um die funktionale Sicherheit von Maschinen zu bewerten.

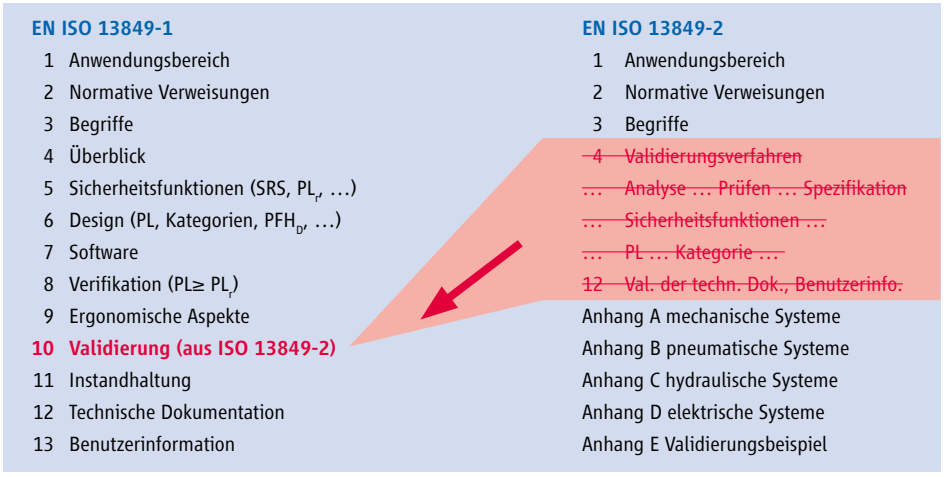
Während die EN 62061 Grundzüge und Terminologie der IEC 61508 übernimmt, wurden die probabilistischen Ansätze bei der EN ISO 13849-1 unter Berücksichtigung der Kategorien betrachtet. Im Detail gibt es Unterschiede bei der Validierung sicherheitsrelevanter Software und bei der Bestimmung der geforderten Risikominderung. Die EN 62061 definiert als Zielgröße den Safety Integrity Level (SIL) dagegen spricht die EN ISO 13849-1 vom Performance Level (PL).

2.1 Was ist neu?

2.1.1 EN ISO 13849

Bei der EN ISO 13849-1 wurden vor allem die folgenden Kapitel neu erstellt bzw. überarbeitet:

- Überblick (Kapitel 4)
- Software (Kapitel 7)
- Validierung (Kapitel 10 wurde übernommen aus der EN ISO 13849-2)
- Die Kombinationen von Subsystemen (Anhang H)
- EMV Anforderungen Anhang L
- Typischen Sicherheitsanforderungen (Anhang M)
- Software Anforderungen (Use-Cases Anhang N)
- Security
- Gerätetypen 1 bis 4 (Anhang O)



2.1.2 EN 62061

Bei der EN 62061 wurden vor allem die folgenden Kapitel neu erstellt bzw. überarbeitet:

- Scope: technologieunabhängig (keine Einschränkung mehr auf E/E/PES)
- Neue Anhänge zu Ausfallraten (Anhang C), Diagnosedeckungsgrad (Anhang E) und Zuverlässigkeitsberechnungen (Anhang K)
- Umbennung von „SILCL“ auf „SIL“
- Neue SW-Level für Anwendungssoftware (Kapitel 8)
- Unabhängigkeitsgrade bei SW-Verifikation und allgemeiner Validierung
- EMV-Anforderungen (Kapitel 6.6)
- SW-basierte Parametrierung klarer gefasst (Kapitel 6.7)
- Ergänzung von Anforderungen zu periodischen Test, z.B. Proof-Test
- Security

3 Was muss ich tun, um eine Maschine richtlinienkonform in Verkehr zu bringen?

Die sozialen Kosten der durch den Umgang mit Maschinen unmittelbar hervorgerufenen zahlreichen Unfälle lassen sich verringern, wenn der Aspekt der Sicherheit in die Konstruktion und den Bau von Maschinen einbezogen wird und wenn Maschinen sachgerecht installiert und gewartet werden.

[2. Erwägungsgrund, Maschinenrichtlinie 2006/42/EG)

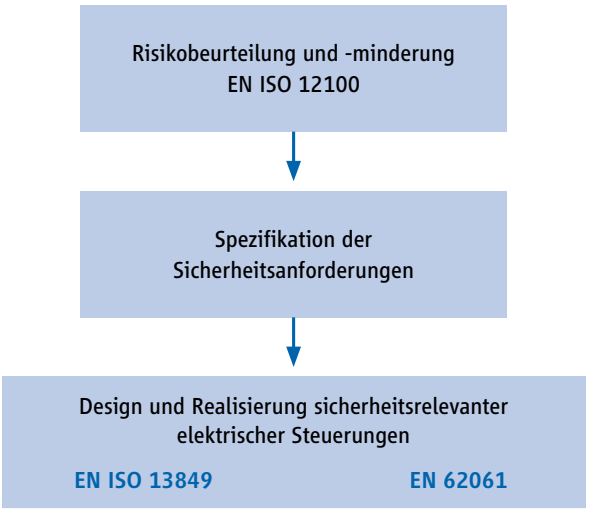
Hierin wird sehr deutlich, dass es eine der zentralen Forderungen der Maschinenrichtlinie ist, dass von Maschinen kein unzulässig hohes Risiko ausgehen darf. Um dies zu erreichen verlangt die Maschinenrichtlinie in Anhang I, dass für jede Maschine, die innerhalb der EU in Verkehr gebracht wird, eine Risikobeurteilung durchgeführt wird und die Maschine unter Berücksichtigung der Ergebnisse der Risikobeurteilung gebaut wird. Wie eine solche Risikobeurteilung durchgeführt werden kann, kann der harmonisierten Norm EN ISO 12100 entnommen werden. Da es ein „Null-Risiko" in der Technik leider nicht gibt, sind alle Anstrengungen zu unternehmen, um ein akzeptables Restrisiko zu erreichen.

Die Maßnahmen zur Risikominderung sind vielfältig und sollen dem 3-Stufen-Konzept folgen:

1. Inhärent sichere Konstruktion
2. Technische Schutzmaßnahmen
3. Organisatorische Maßnahmen

Die technischen Schutzmaßnahmen umfassen unter anderem Schutzzäune, konstruktive Anpassungen der Maschine und diverse weitere Maßnahmen. Wenn die Sicherheit von der korrekten Funktion von Steuerungssystemen abhängt (z.B. gefahrbringende Bewegung muss stoppen, wenn eine Schutztür geöffnet wird), müssen diese so konstruiert werden, dass die Wahrscheinlichkeit von sicherheitsrelevanten Fehlern ausreichend gering ist. Dabei ist auch zu prüfen, dass auftretende Fehler nicht zum Verlust der Sicherheitsfunktion führen. Zur Erfüllung dieses Schutzziels ist es sinnvoll, die beiden für diesen Anwendungsfall vorgesehenen harmonisierten Normen – EN ISO 13849 und EN 62061 – zu betrachten, die entsprechend einem Mandat der europäischen Kommission erstellt wurden und im europäischen Amtsblatt veröffentlicht sind (Vermutungswirkung). Nur so kann ein erhöhter Aufwand beim Konformitätsnachweis vermieden werden.

Abb. 1: Funktionale Sicherheit im Risikobeurteilungsprozess



Im Folgenden werden die beiden zentralen Normen zur funktionalen Sicherheit an Maschinen gegenübergestellt und Hilfestellungen für den Anwender gegeben.

4 Anwendungsbereiche der beiden Normen

4.1 EN ISO 13849

Die EN ISO 13849 spezifiziert eine Methodik und bietet eine entsprechende Anleitung für den Entwurf und die Integration von sicherheitsbezogenen Teilen von Steuerungssystemen (SRP/CS), einschließlich des Entwurfs von Software. Sie spezifiziert die Merkmale, die zur Bestimmung des erforderlichen Leistungsniveaus von Sicherheitsfunktionen erforderlich sind. Die EN ISO 13849 gilt für SRP/CS für den High-Demand-Mode einschließlich ihrer Teilsysteme, unabhängig von der Art der Technologie und Energie (z.B. elektrisch, hydraulisch, pneumatisch, mechanisch), für viele Arten von Maschinen. Die Norm gilt nicht für den Low-Demand-Mode.

Die EN ISO 13849 spezifiziert nicht die Sicherheitsfunktionen oder erforderlichen Leistungsstufen, die in bestimmten Anwendungen eingesetzt werden sollen.

Sie enthält keine spezifischen Anforderungen für die Konstruktion von Elementen, die Teil von SRP/CS sind.

4.2 EN 62061

Die internationale Norm spezifiziert Anforderungen und gibt Empfehlungen für den Entwurf, die Integration und die Validierung von sicherheitsbezogenen Steuerungssystemen (SCS) für Maschinen. Sie gilt für Steuerungssysteme, die entweder einzeln oder in Kombination verwendet werden, um Sicherheitsfunktionen an Maschinen zu realisieren, die während der Arbeit nicht von Hand tragbar sind, einschließlich einer Gruppe von Maschinen, die in koordinierter Weise zusammenarbeiten. Der Entwurf komplexer programmierbarer elektronischer Subsysteme oder Subsystemelemente fällt nicht in den Anwendungsbereich dieser Norm. Dies liegt im Anwendungsbereich der IEC 61508 oder damit verbundener Normen. Komplexe (programmierbare) Subsysteme sind beispielsweise Sicherheitssteuerungen, die auf Mikrocontrollertechnologie basieren. Low-Demand- Applikationen werden derzeit bei der EN 62061 nicht berücksichtigt. Es ist jedoch ein „Amendment“ zu diesem Thema geplant.

5 Kurzbeschreibung der Normen

5.1 EN ISO 13849

Die Leistungsfähigkeit einer Sicherheitsfunktion wird durch den Performance Level (PL) beschrieben. Hierbei wird ausgehend von den aus der Risikoanalyse hervorgehenden Sicherheitsfunktionen eine Aufteilung in Teilsysteme vorgenommen. Wesentliches Merkmal der EN ISO 13849 sind die Kategorien, welche die Architektureigenschaften eines SRP/CS definieren. Die EN ISO 13849 betrachtet komplette Sicherheitsfunktionen mit allen an ihrer Ausführung beteiligten Komponenten. Dabei umfasst sie neben elektrischen auch pneumatische, hydraulische und mechanische Systeme.

Mit der EN ISO 13849 erfolgt über einen qualitativen Ansatz (Architektur des Steuerungssystems) hinaus auch eine quantitative Betrachtung der Sicherheitsfunktionen. Aufbauend auf den Kategorien werden hierfür Performance Level (PL) verwendet.
Für SRP/CS sind, abhängig vom Typ, folgende sicherheitstechnischen Kenngrößen definiert:

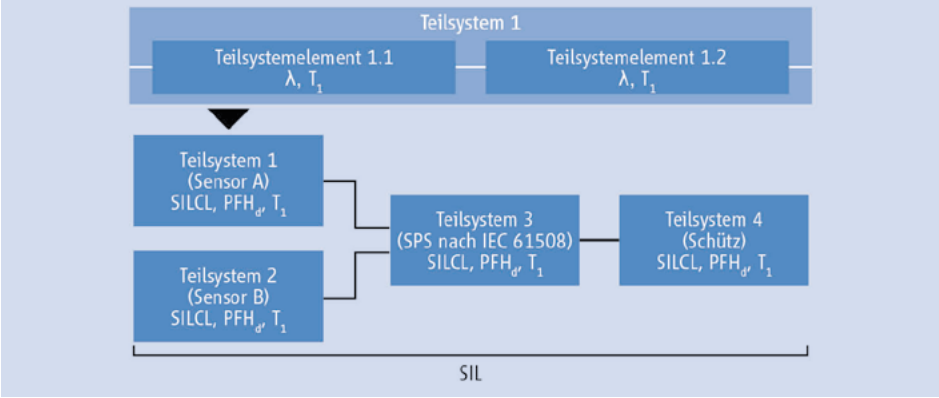
- Kategorie (strukturelle Anforderung)
- PL: Performance Level
- $MTTF_D$: Mittlere Zeit bis zu einem gefährlichen Ausfall
  (en: mean time to dangerous failure)
- B_{10D}: Anzahl von Zyklen bei denen 10% einer Stichprobe der
  betrachteten verschleißbehafteten Komponenten gefährlich ausgefallen sind
- DC: Diagnosedeckungsgrad *(en: diagnostic coverage)*
- CCF: Ausfälle in Folge gemeinsamer Ursache *(en: common cause failure)*
- T_M: Gebrauchsdauer *(en: Mission Time)*

Die Norm beschreibt die Ermittlung des Performance Level (PL) für sicherheitsrelevante Teile von Steuerungen auf Basis vorgesehener Architekturen (designated architectures) für die vorgesehene Gebrauchsdauer T_M.

Bei Abweichungen von den vorgesehenen Strukturen oder einer sehr hohen Komplexität der Systeme verweist die EN ISO 13849 bei elektrisch/elektronischen Systemen auf die IEC 61508. Bei Kombination mehrerer sicherheitsrelevanter Teile zu einem Gesamtsystem macht die Norm Angaben zur Ermittlung des resultierenden PL.

5.2 EN 62061

Die Leistungsfähigkeit einer Sicherheitsfunktion wird durch den Safety Integrity Level (SIL) beschrieben. Hierbei wird ausgehend von den aus der Risikoanalyse hervorgehenden Sicherheitsfunktionen eine Aufteilung in Teilsicherheitsfunktionen und schließlich eine Zuordnung dieser Teilsicherheitsfunktionen auf reale Geräte – Teilsysteme und Teilsystem Elemente genannt – vorgenommen. Ein sicherheitsgerichtetes Steuerungssystem (SCS) besteht aus verschiedenen Teilsystemen. Die Teilsysteme werden durch die Kenngrößen (SIL- und PFHD sowie T1) sicherheitstechnisch beschrieben. Die EN 62061 betrachtet komplette Sicherheitsfunktionen mit allen an ihrer Ausführung beteiligten Komponenten. Dabei umfasst sie in der neuen Fassung - wie bereits die EN ISO 13849 - neben elektrischen auch pneumatische, hydraulische und mechanische Systeme. Die EN 62061 ist seit Dezember 2005 harmonisiert.



Für sicherheitsrelevante Steuerungsteile werden abhängig vom Typ folgende Kenngrößen für Teilsysteme definiert:

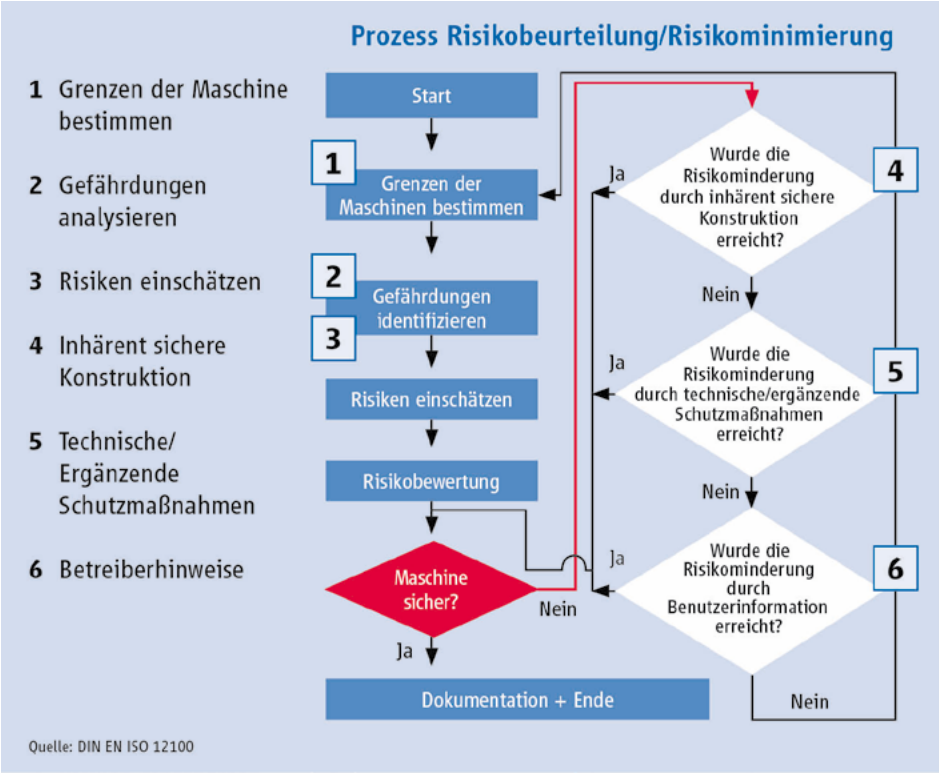
- SIL: Sicherheits-Integritäts-Level *(en: Safety Integrity Level)*
- PFH_D: Wahrscheinlichkeit gefährlicher Ausfalle pro Stunde *(en: probabilityof dangerous failure per hour)*
- T1: Kleinster Wert aus Lebenserwartung oder Prüftest-Intervall *(en: life time or proof test interval)*
- λ: Ausfallrate (en: failure rate); für verschleißbehaftete Elemente (oder ohne konstante Ausfallrate): B_{10D}
- SFF: Anteil sicherer Ausfälle *(en: Safe Failure Fraction)*
- T2: Diagnose-Testintervall *(en: diagnostic test interval)*
- β: Anfälligkeit für Fehler gemeinsamer Ursache *(en: susceptibility to common cause failure)*
- DC: Diagnosedeckungsgrad *(en: diagnostic coverage)*

6 Grundlegende Vorgehensweise

6.1 Risikobeurteilung nach EN ISO 12100

Es wird davon ausgegangen, dass eine an einer Maschine vorhandene Gefährdung früher oder später zu einem Schaden führt, falls keine Schutzmaßnahme(n) durchgeführt wird (werden). Schutzmaßnahmen sind eine Kombination der vom Konstrukteur und der vom Benutzer durchgeführten Maßnahmen. Maßnahmen, die bereits in der Konstruktionsphase getroffen werden können, sind den vom Benutzer durchgeführten Maßnahmen immer vorzuziehen und im Allgemeinen wirksamer als diese.
Unter Berücksichtigung der Erfahrungen von Benutzern ähnlicher Maschinen und des Informationsaustausches mit den potentiellen Benutzern (wann immer dies möglich ist) muss der Konstrukteur in der unten angegebenen Reihenfolge vorgehen:

Abb. 2: Risikobeurteilungsprozess in Anlehnung an EN ISO 12100



Quelle: DIN EN ISO 12100

6.2 Risikominderung durch steuerungstechnische Maßnahmen

Erfolgt die erforderliche Risikominderung mit technischen Schutzmaßnahmen durch sicherheitsrelevante Steuerungsteile, so ist der Entwurf dieser Steuerungsteile ein integraler Teil der gesamten Entwurfsprozedur für die Maschine. Das sicherheitsrelevante Steuerungssystem stellt die Sicherheitsfunktion(en) mit einem SIL oder PL bereit, der die erforderliche Risikominderung erreicht.

6.3 Spezifikation der Sicherheitsanforderungen

Tab. 1

Spezifikation	Hinweis
Auslösendes Ereignis	Durch welches Ereignis wird die Sicherheitsfunktion ausgelöst?
Sicherheitsgerichtete Reaktion	Was ist die sicherheitsgerichtete Reaktion?
Betriebsart	In welcher Betriebsart soll die Sicherheitsfunktion aktiv sein?
PL_r	Mit welchem Performance Level PL_r soll die Sicherheitsfunktion ausgeführt werden?
Häufigkeit der Anforderung	Wie häufig ist mit der Anforderung der Sicherheitsfunktion zu rechnen?
Nachlauf	In welcher Zeit nach Anforderung der Sicherheitsfunktion soll der sichere Zustand erreicht werden?
Verhalten bei Energieausfall	Welche sicherheitsgerichtete Reaktion ist bei Energieausfall erforderlich?
Priorität	Ist die Sicherheitsfunktion vor- oder nachrangig gegenüber anderen Sicherheitsfunktionen?
Ergänzende Sicherheitsfunktion	Setzt der Einsatz der Sicherheitsfunktion weitere aktive Sicherheitsfunktionen voraus?
Zusätzliche Parameter	Welche zusätzlichen Parameter müssen berücksichtigt werden?
Fehlererkennende Maßnahmen	Welche Diagnosemaßnahmen müssen berücksichtigt werden?
Fehlerreaktionsmaßnahmen	Welche Maßnahmen sind bei Fehlererkennung erforderlich?

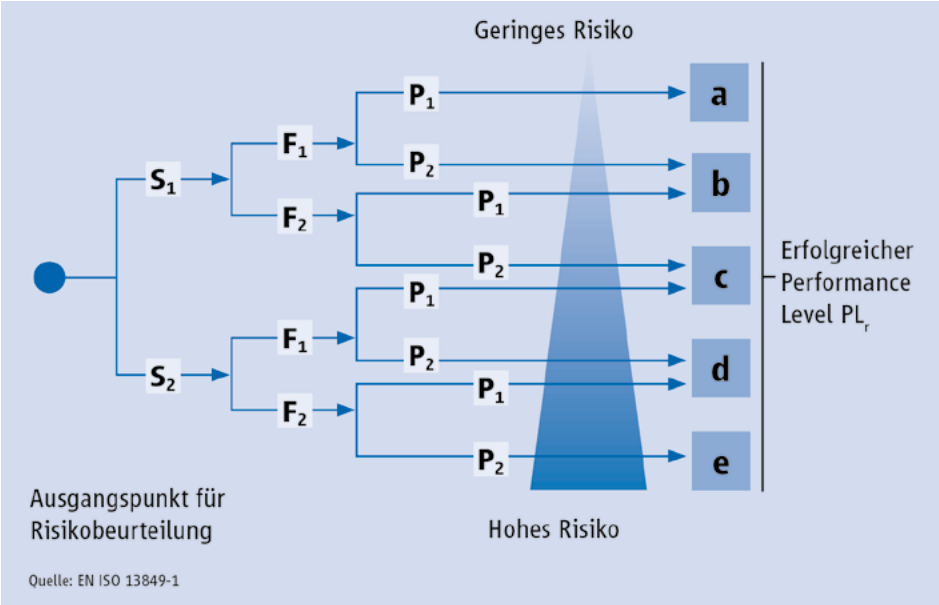
Die Spezifikation der Sicherheitsanforderung ist das wichtigste Dokument (Alpha Dokument). Es beschreibt detailliert die funktionalen Anforderungen jeder einzelnen auszuführenden Sicherheitsfunktion. Die erforderlichen Schnittstellen sowie alle Punkte aus der Tabelle 1 sind wichtige Bestandteile dieses Dokumentes. Jegliche weitere Dokumentation sowie deren Validierung hat ihren Ursprung in diesem Dokument. Fehler in der Spezifikation setzen sich systematisch fort.

6.4. Überlagernde Gefährdungen

Treten Kombination von Gefährdungen immer gleichzeitig auf, dann sollten sie bei der Risikoabschätzung kombiniert betrachtet werden. Ein kontinuierlich arbeitender Schweißroboter erzeugt beispielsweise verschiedene Gefahrensituationen gleichzeitig. So kann es zum Beispiel gleichzeitig zur Quetschung durch Bewegung als auch zur Verbrennung durch den Schweißprozess kommen. In diesem Fall würden die relevanten Teilsysteme kombiniert in einer Sicherheitsfunktion betrachtet werden in dem die jeweiligen PFH_D-Werte addiert werden.

6.4.1 Bestimmung des erforderlichen Performance Level nach der EN ISO 13849-1

Abb. 3: Bestimmung des PL_r



Der informative Anhang A der EN ISO 13849-1 bietet eine Abschätzung der erforderlichen Risikoreduzierung und ist als Anleitung für den Konstrukteur und Normungssetzer bei der Bestimmung des PL_r gedacht.

Schweregrad der Verletzung S1 und S2
S1 = leichte reversibel Verletzungen
S2 = schwere irreversibel Verletzungen sowie der Tod

Häufigkeit und/oder Expositionszeiten gegenüber der Gefährdung, F1 und F2
Ein allgemein gültiger Zeitraum kann für den Parameter F1 oder F2 nicht angegeben werden. F2 sollte gewählt werden, wenn eine Person häufig oder ständig der Gefährdung ausgesetzt ist. F1 wenn die kumulierte Expositionszeit nicht mehr als 1/20 der Gesamtbetriebszeit beträgt und die Frequenz nicht höher als einmal pro 15 min ist.

Möglichkeit, den Schaden zu vermeiden P1 und P2
P1: möglich unter bestimmten Bedingungen
P2: nicht möglich

Bei einem gefährlichen Ereignis sollte P1 nur dann gewählt werden, wenn es eine realistische Chance gibt die Gefährdung zu vermeiden. Andernfalls sollte P2 gewählt werden. Die folgenden zwei Tabellen sind in der Fassung von 2021 neu aufgenommen worden und sollen helfen den Parameter P zu bestimmen.

Bestimmung des Parameters P auf der Grundlage von fünf Faktoren

Faktor	C	B	A
1. Nutzung der Maschine durch		Ungelernte Person	Befähigte Person (Fachmann)
2. Geschwindigkeit des Teils der Maschine, der ein gefährliches Ereignis auslösen kann (abhängig von der spezifischen Maschine)	Ereignis bei hoher Geschwindigkeit Keine Möglichkeit zu entkommen (z.B. über 1 000 mm/s, Zeit bis zur Gefährdung < 1 s)	Ereignis bei mittlerer Geschwindigkeit Begrenzte Möglichkeit zu entkommen (z.B. 251 mm/s bis 1 000 mm/s, Zeit bis zur Gefährdung < 3 s)	Ereignis bei niedriger oder sehr niedriger Geschwindigkeit Ausreichende Möglichkeit zu entkommen (z.B. max. 250 mm/s, Zeit bis zur Gefährdung ≥ 3 s)
3. Möglichkeit die Gefährdung zu vermeiden	Nicht möglich	In weniger als 50 % der Fälle möglich	In mehr oder gleich 50 % der Fälle möglich
4. Möglichkeit der Wahrnehmung der Gefährdung	Nicht möglich (z.B. Instrumentierung notwendig, der menschliche Sinn ist nicht in der Lage, die Gefahr wahrzunehmen, Umweltbedingungen verdecken die Wahrnehmung)	In weniger als 50 % der Fälle möglich	In mehr oder gleich 50 % der Fälle möglich
5. Komplexität der Operationen (menschliche Interaktion im Hinblick auf die Anzahl der Operationen und/ oder die für diese Operationen verfügbare Zeit)		Hohe Komplexität (z.B. Fehlerbehebung) oder Mittlere Komplexität (z.B. Verwendung der Hold-To-Run-Steuerung zum Einrichten eines Teils der Maschine)	Geringe Komplexität (z.B. Einstellen der Werkstückspanner) oder Sehr geringe Komplexität / oder keine Interaktion (z.B. ein Werkstück in die Maschine einlegen)

Quelle: ZVEI in Anlehnung an prEN ISO 13849-1:2021

Auswahl des Parameters P1 oder P2

Gesamtpunktzahl		Parameter „P“
ein oder mehrere „C“	■ □ □ □ □	P2
kein „C“, drei oder mehr „B“	■ ■ ■ □ □	P2
kein „C“, zwei „B“, der Rest „A“	■ ■ □ □ □	P1 oder P2 je nach Spezifikation der Maschine
kein „C“, ein oder kein „B“, der Rest „A“.	■ □ □ □ □ □ □ □ □ □	P1

Quelle: ZVEI in Anlehnung an prEN ISO 13849-1:2021

Überlappende Gefährdungen

Treten Kombination von Gefährdungen immer gleichzeitig auf, dann sollten sie bei der Risikoabschätzung kombiniert betrachtet werden. Ein kontinuierlich arbeitender Schweißroboter erzeugt beispielsweise verschiedene Gefahrensituationen gleichzeitig. So kann es zum Beispiel gleichzeitig zur Quetschung durch Bewegung als auch zur Verbrennung durch den Schweißprozess kommen. In diesem Fall würden die relevanten Teilsysteme kombiniert in einer Sicherheitsfunktion betrachtet.

6.4.2 Bestimmung der erforderlichen Leistungsfähigkeit Safety Integrity Level nach der EN 62061

Abb 4: Bestimmung des erforderlichen SIL

Risikoabschätzung und Festlegung des erforderlichen Safety Integrity Levels (SIL)

Auswirkung und Schwere	Se	Häufigkeit und Dauer	Fr	Wahrscheinlichkeit des gef. Ereignisses	Pr	Vermeidung	Av	Klasse K				
								3-4	5-7	8-10	11-13	14-15
Tod, Verlust eines Auges oder Armes	4	≤ 1/Stunde	5	Häufig	5			SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, Verlust von Fingern	3	> 1/Stunde - ≤1/Tag	5	Wahrscheinlich	4				AM	SIL1	SIL2	SIL3
Reversibel, medizinische Behandlung	2	> 1/Tag - ≤2/Woche	4	Möglich	3	unmöglich	5			AM	SIL1	SIL2
Reversibel, Erste Hilfe	1	2/Woche - ≤1/Jahr	3	Selten	2	Möglich	3				AM	SIL1
		> 1/Jahr	2	Vernachlässigbar	1	Wahrscheinlich	1					

AM = Andere Maßnahmen empfohlen

Quelle: EN 62061

Klasse K = Fr + Pr + Av

Der informative Anhang A der EN 62061 enthält Methoden für einen qualitativen Ansatz zur Risikoabschätzung und SIL Zuweisung, die auf SCS für Maschinen angewendet werden können, um den erforderlichen SIL zu bestimmen.
Erfahrungen im erfolgreichen Umgang mit ähnlichen Maschinen/Gefahren sollten bei der Abschätzung des erforderlichen SIL berücksichtigt werden.
Weitere SIL-Zuweisungsmethoden sind in IEC 61508-5 und IEC 61511-3 verfügbar.

Abschätzung des Risikos

Die Risikoeinschätzung sollte für jede Gefahr durchgeführt werden, indem die Risikoparameter bestimmt werden:

- Schwere des Schadens
- Wahrscheinlichkeit des Auftretens dieses Schadens
- Häufigkeit und Dauer der Exposition von Personen gegenüber der Gefährdung
- der Wahrscheinlichkeit des Auftretens eines gefährlichen Ereignisses
- Möglichkeiten zur Vermeidung oder Begrenzung des Schadens

Schweregrad (Se)-Klassifizierung

Konsequenzen	Schweregrad (Se)
Irreversibel: Tod, Verlust eines Auges oder Arms	4
Irreversibel: gebrochene Extremität(en), Verlust eines Fingers (von Fingern)	3
Reversibel: erfordert die Behandlung durch einen Arzt	2
Reversibel: Erste Hilfe erforderlich	1

Klassifizierung der Häufigkeit und Dauer der Exposition (Fr)

Häufigkeit der Exposition	Häufigkeit, Fr	
	Dauer der Exposition ≥ 10 min	Dauer der Exposition < 10 min
≥ 1 pro h	5	5
< 1 pro h an ≥ 1 pro Tag	5	4
< 1 pro Tag an ≥ 1 pro 2 Wochen	4	3
< 1 pro 2 Wochen an ≥ 1 pro Jahr	3	2
< 1 pro Jahr	2	1

Wahrscheinlichkeits (Pr)-Klassifikation

Wahrscheinlichkeit der Schadensvermeidung oder -begrenzung (Av)	
Unmöglich	5
Selten	3
Wahrscheinlich	1

7 Entwurf der Steuerungsarchitektur

7.1 EN ISO 13849

Für jede gewählte SRP/CS und/oder der Kombination von SRP/CS die eine Sicherheitsfunktion ausführt, muss eine Abschätzung des erreichten
PL durchgeführt werden.
Der PL der SRP/CS muss bestimmt werden durch
die Abschätzung folgender Parameter:

- des $MTTF_D$ oder B_{10D} Wertes einzelner Komponenten;
- der DC;
- der CCF;
- der Struktur,
- des Verhaltens im Fehlerfall;
- sicherheitsbezogener Software
- systematischer Ausfälle
- der Fähigkeit eine Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen.
- Anwendung bewährter Sicherheitsprinzipien

Performance level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]
a	$10^{-5} \leq PFH_D < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH_D < 10^{-5}$
c	$10^{-6} \leq PFH_D < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH_D < 10^{-6}$
e	$PFH_D < 10^{-7}$

7.2 EN 62061

Die Auswahl oder der Entwurf der SRECS muss prinzipiell mindestens die folgenden Anforderungen erfüllen:
Anforderungen zur Sicherheitsintegrität der Hardware bestehend aus:

- den strukturellen Einschränkungen zur Sicherheitsintegrität der Hardware
- den Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle
- sowie den Anforderungen zur systematischen Sicherheitsintegrität bestehend aus
- den Anforderungen zur Vermeidung von Ausfällen und
- den Anforderungen zur Beherrschung systematischer Fehler.

Die EN 62061 beschreibt auch Anforderungen an die Realisierung von Applikations-Programmen.

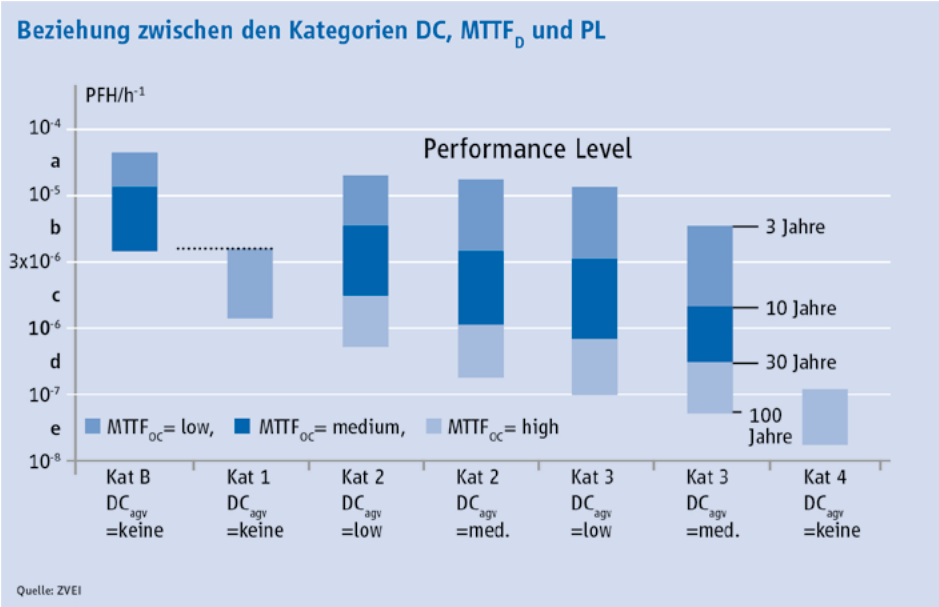
Sicherheitstechnische Kenngrößen für Teilsysteme:

- SIL: SIL-Eignung
- PFH_D: Wahrscheinlichkeit gefährlicher Ausfälle pro Stunde
- T1: Proof Test Intervall

SIL (IEC 61508)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

7.3 EN ISO 13849-1

Abb 4: Beziehung zwischen Kategorien, DC, $MTTF_D$ und PL



Anmerkung:
Die PFH_D-Werte stellen eine notwendige Voraussetzung zur Ermittlung des Performance Levels dar. Darüber hinaus müssen noch zur vollständigen Ermittlung des PL auch Maßnahmen zur Fehlervermeidung wie CCF, Kategorie sowie der DC herangezogen werden.
Bei Kategorie 4 kann die $MTTF_D$ = high auf bis zu 2.500 Jahre erhöht werden.

7.4 EN 62061

Sicherheitstechnische Kenngrößen für Teilsystemelemente (Geräte):

- λ: Ausfallrate;
- $B10_D$-Wert: für verschleißbehaftete Bauteile (ohne konstante Ausfallrate)
- T1: Lebensdauererwartung
- T2: Diagnose-Testintervall
- β: Empfindlichkeit für Ausfälle gemeinsamer
- Ursache
- DC: Diagnosedeckungsgrad
- SFF: Anteil sicherer Ausfälle (en: Safe failure Fraction)
- HFT: Hardware-Fehler-Toleranz

SFF	HFT 0	HFT 1	HFT 2
< 60%	Nicht zulässig	SIL 1	SIL 2
≥ 60% bis < 90%	SIL 1	SIL 2	SIL 3
≥ 90% bis < 99%	SIL 2	SIL 3	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

Quelle: ZVEI in Anlehnung an EN 62061

Performance level (PL)	Safety Integrity Level (SIL)
a	-
b	-
c	1
d	2
e	3

Quelle: ZVEI in Anlehnung an EN 62061

Anmerkung:
Die obige Tabelle beschreibt die Beziehung zwischen den beiden Konzepten der Normen (PL und SIL). Sofern nicht von C-Normen eine spezifische Kategorie gefordert wird, kann beispielsweise ein Teilsystem gemäß SIL 3 (EN 62061) innerhalb einer Sicherheitsfunktion gemäß EN ISO 13849 bis PL e eingesetzt werden.

8 Software

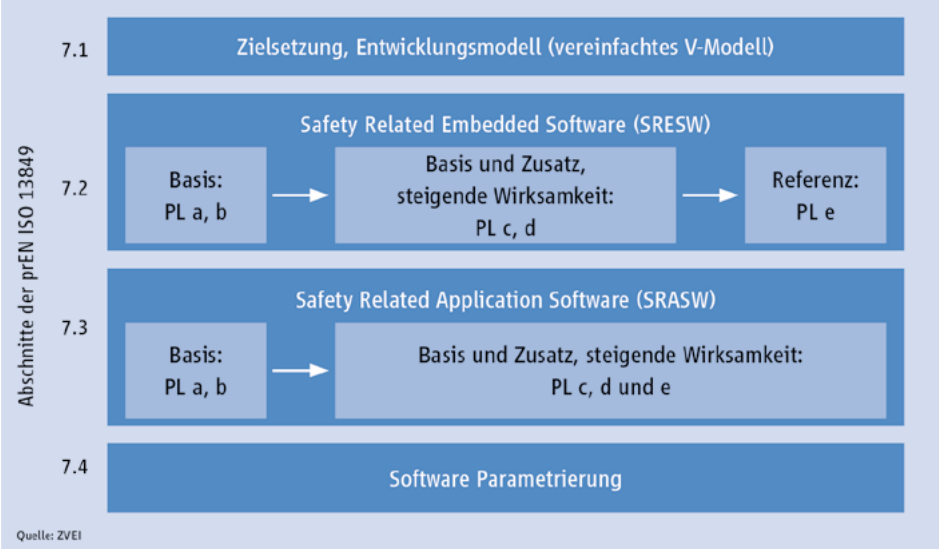
Wie keine zweite Technologie übernimmt Software heute eine höhere Verantwortung als je zuvor und das trifft damit auch auf die Programmierenden zu. Die EN ISO 13849 verweist genauso wie die EN 62061 auf die Teile der IEC 61508. Die sicherheitsrelevante Software muss lesbar, verständlich, testbar und wartbar sein. Aus diesem Grund müssen Fehler schon in der Entwicklungsphase erkannt werden

8.1 EN ISO 13849

In der EN ISO 13849 wurden für programmierbare Steuerungen die Anforderungen an die Software an den heutigen Stand der Technik angepasst. Die im Abschnitt 7 der beschriebenen Maßnahmen ermöglichen es, sicherheitsbezogene Anwendungssoftware für Maschinensteuerungen bis zum Performance Level PLr e zu entwickeln.

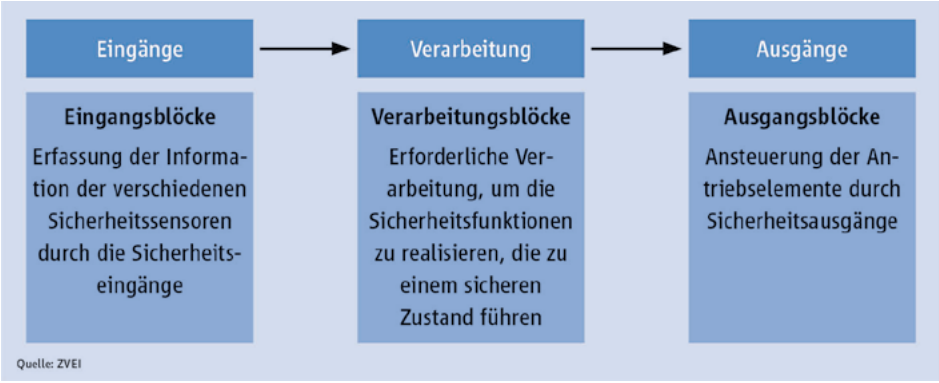
Fehler in der Software entstehen nicht durch zufällige Bauteilausfälle, sondern haben systematische Ursachen. Bei der Entwicklung von sicherheitsbezogener Software, muss alles Mögliche getan werden, um Fehler zu vermeiden.

Abb. 6: SW-Anforderungen



Die EN ISO 13849 beschreibt das Risiko und definiert Fehlervermeidende Maßnahmen in Abhängigkeit der Arten und Sprachtypen der Software und des geforderten Performance Levels.

Abb. 7: Entwurf eines SW-Beispiels auf Funktionsblockebene



An die Software gelten die gleichen Anforderungen, um den Performance Level zu erfüllen (z. B. Struktur, Zuverlässigkeit, Validierbarkeit usw.).

Abb. 8: V-Modell

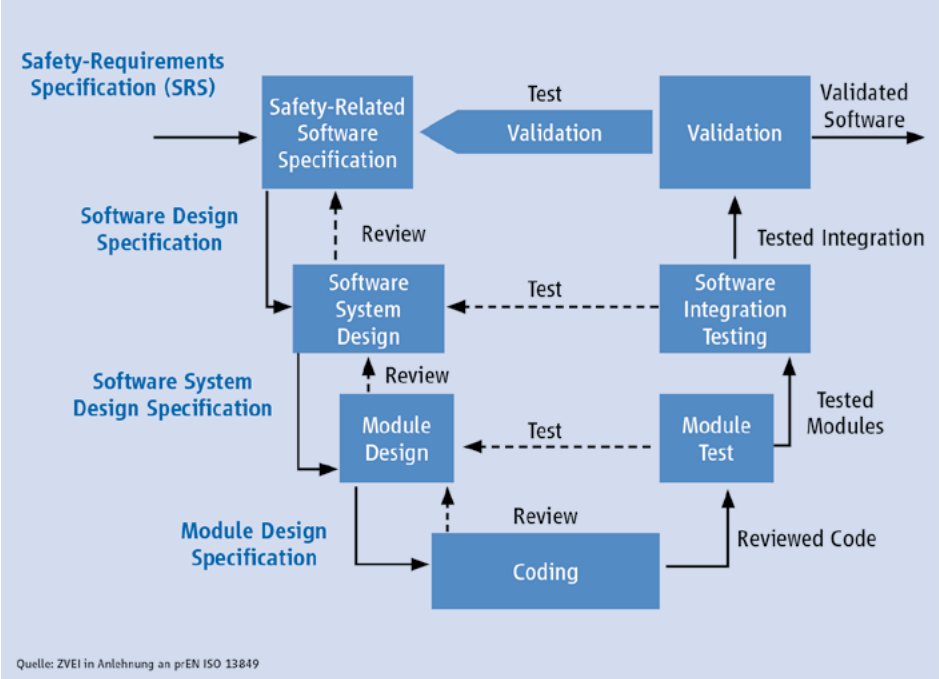
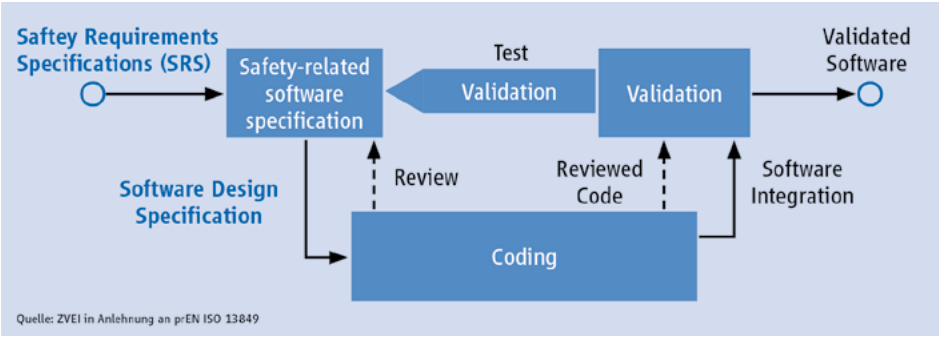


Abb. 9: Vereinfachtes V-Modell



V-Modell für Software, wenn vorbewertete sicherheitsrelevante Hardware und Software Module in Kombination mit LVL verwendet werden.

Full variability language (FVL)
Diese Art von Sprache ist für Programmierer gedacht und bietet die Möglichkeit eine Vielzahl von Funktionen und Anwendungen zu implementieren.

FVL-typische Beispiele: Ada, C, Pascal, Anweisungsliste, Assemblersprachen, C++, Java, Mathlab, Simulink und SQL (ohne Nutzungseinschränkungen und volle Vielfalt an Anweisungen).

Limited variability language (LVL)
Software-Programmiersprache, deren Notation textuell oder grafisch ist oder Merkmale von beiden aufweist.
LVL sollte so gestaltet werden, dass sie für den Softwareentwickler einfach verständlich und zu implementierenden ist. Anmerkung: Im Anhang J der ISO EN 13849 wird ein Softwarebeispiel beschrieben.

8.2 EN 62061

Die EN62061 führt den Begriff des SW-Level „neu" ein: Je nach Komplexitätsgrad wird ein PES in eine der nachfolgenden SW-Level 1-3 einsortiert:

Einteilung in Software Level (SW)

SW-Level	Wesentliches Prinzip	Grundlage	Beispiel
1	Plattform (Kombination aus Hardware und Software), die gemäß IEC 61508 oder anderen mit IEC 61508 verknüpften Normen zur funktionalen Sicherheit, z. B. IEC 61131-6, bereits entworfen und geprüft wurde. Anwendungssoftware, die eine Sprache mit begrenzter Variabilität (LVL) verwendet.	Anwendungssoftware, die mit diesem Dokument übereinstimmt.	Sicherheits-SPS mit LVL oder programmierbares Sicherheitsrelais
2	Plattform (Kombination aus Hardware und Software), die gemäß IEC 61508 oder anderen mit IEC 61508 verknüpften Normen zur funktionalen Sicherheit, z. B. IEC 61131-6, bereits entworfen und geprüft wurde. Anwendungssoftware, die eine Sprache mit begrenzter Variabilität (LVL) verwendet.	Anwendungssoftware, die mit diesem Dokument übereinstimmt.	Sicherheits-SPS mit FVL (FVL, die diesem Dokument entspricht.)
3		Anwendungssoftware, die der IEC 61508-3 entspricht.	Sicherheits-SPS mit LVL oder FVL (FVL gemäß IEC 61508)

Quelle: ZVEI in Anlehnung an EN 62061

In Abhängigkeit des SW-Level (1-3) sowie des zu erreichenden SIL (1-3) ergeben sich unterschiedliche Anforderungen an

a) Minimale Unabhängigkeitsgrade für V&V (Verifikation und Validierung)
b) Umfang der V&V-Tätigkeiten (V-Modell)

Unabhängigkeitsgrade Verifikation und Validierung

Für Verifikationstätigkeiten gelten die nachfolgenden Unabhängigkeitsgrade in Abhängigkeit des zu erreichenden SIL.

Minimale Unabhängigkeits-grad für Verifika-tionstätigkeiten	Erf. SIL für die Sicherheitsfunktion		
	SIL 1	SIL 2	SIL 3
Gleiche Person	nicht ausreichend	nicht ausreichend	nicht ausreichend
Andere Person	nicht ausreichend *	nicht ausreichend *	nicht ausreichend
Unabhängige Person**	ausreichend	ausreichend	ausreichend

Quelle: ZVEI in Anlehnung an EN 62061

** Für die Softwarelevel 1, bei der nur Kombinationen von vorgefertigten Softwaremodulen verwendet werden, ist eine „andere Person" ausreichend. Software Level 2 ist für SIL 3 nicht anwendbar.*

*** Abhängig von der Unternehmensorganisation und den Fachkenntnissen innerhalb des Unternehmens kann die Forderung nach einer „unabhängigen Person" durch den Einsatz einer externen Organisation erfüllt werden müssen. Umgekehrt können Unternehmen, die über interne Organisationen verfügen, die in der Risikobeurteilung und der Anwendung sicherheitsbezogener Systeme qualifiziert sind, die von den für die Hauptentwicklung verantwortlichen Personen unabhängig und (durch Management- und andere Ressourcen) getrennt sind, in der Lage sein, ihre eigenen Ressourcen einzusetzen, um die Anforderungen an eine unabhängige Organisation zu erfüllen.*

Für Validierungstätigkeiten gelten die nachfolgenden Unabhängigkeitsgrade in Abhängigkeit des zu erreichenden SIL

Minimale Unabhängigkeits-grad für Validie-rungstätigkeiten	Erf. SIL für die Sicherheitsfunktion		
	SIL 1	SIL 2	SIL 3
Gleiche Person	nicht ausreichend	nicht ausreichend	nicht ausreichend
Andere Person	nicht ausreichend	nicht ausreichend	nicht ausreichend
Unabhängige Person**	ausreichend	ausreichend	ausreichend

Quelle: ZVEI in Anlehnung an EN 62061

Für SW-Level 1 kann das vereinfachte V-Modell angewandt werden.

Abb. 10: vereinfachtes V-Modell für SW-Level 1

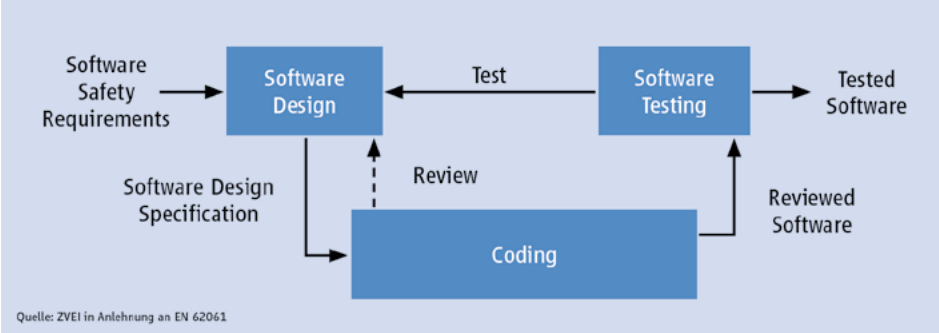
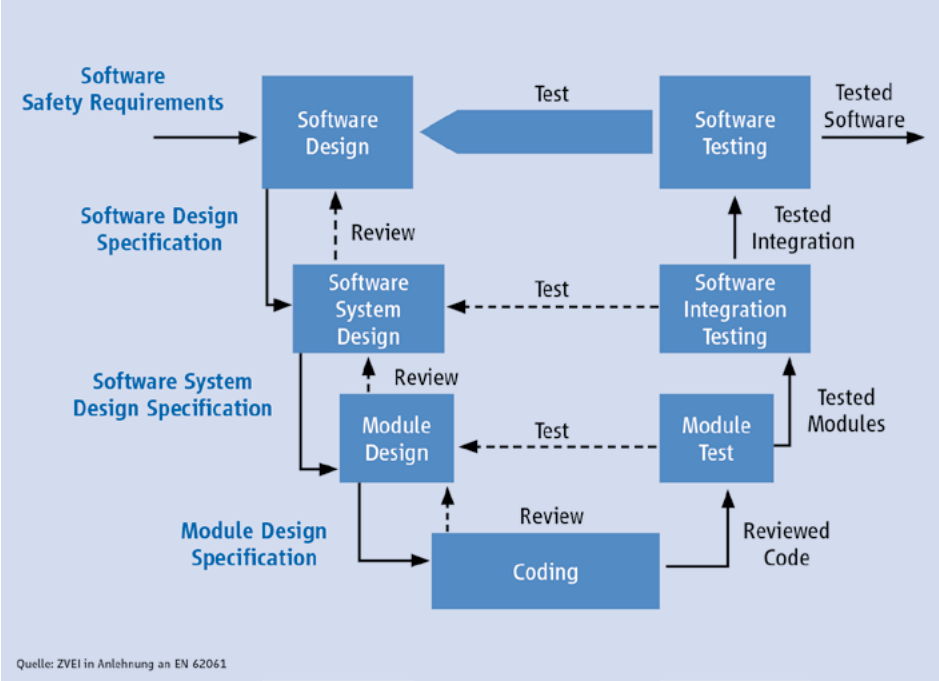


Abb. 11: V-Modell für SW-Level 2



Für SW-Level 3 siehe IEC 61508-3.

9 Security

Hat die Security Einfluss auf die funktionale Sicherheit müssen Maßnahmen getroffen werden. Securityaspekte mit Einfluss auf die funktionale Sicherheit sind zu berücksichtigen. Es werden jedoch keine spezifischen Anforderungen beschrieben. Stattdessen wird auf IEC TR 63074, die ISO TR 22100-4, und die IEC 62443 verwiesen.

10 Verifikation

Für jede einzelne Sicherheitsfunktion muss der PL der zugehörigen SRP/CS(en) dem „Erforderlichen Performance Level", entsprechen. Die PLs verschiedener SRP/CS, die Teil einer Sicherheitsfunktion sind, müssen größer oder gleich dem erforderlichen Performance Level dieser Funktion sein.

Bei der Zusammenschaltung mehrerer SRP/CS kann der endgültige PL mit Hilfe der Tabelle 9 aus der EN ISO 13849 bestimmt werden. Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls jeder SRCF (Safety related control function) als Folge gefahrbringender zufälliger Hardwareausfälle muss gleich oder kleiner als der in der Spezifikation der Sicherheitsanforderungen festgelegte Ausfallgrenzwert sein.

Der SIL, der durch das SRECS auf Grund der strukturellen Einschränkungen erreicht wird, ist geringer als oder gleich der niedrigsten SIL irgendeines Teilsystems, das an der Ausführung der Sicherheitsfunktion beteiligt ist.

11 Validierung

Die Gestaltung einer sicherheitsbezogenen Steuerungsfunktion muss validiert werden. Es wird die Eignung der sicherheitsbezogenen Steuerungsfunktion für die Anwendung überprüft. Die Validierung kann durch Analyse oder Prüfung erfolgen (z. B. durch gezielte Simulation von Einzel- oder Mehrfachfehlern). Die EN ISO 13849 hat die Abschnitte 4-9 aus der ISO EN 13849-2 im Kapitel 10 Validierung übernommen.

12 Was bedeuten die Änderungen für den Anwender?

Beide Normen haben sich nach den zu erwartenden Änderungen weiter angenähert. In der Praxis bedeutet dies, dass Teilsysteme, die nach einer der beiden Normen entwickelt wurden, einfacher in die andere Norm überführt werden können. Die Anpassungen bei der Risikoeinstufung sollten im Rückblick auf bestehende Konzepte neu bewertet werden. In einigen Fällen ergibt sich eine höhere Flexibilität hinsichtlich der anzunehmenden Risiko-Parameter. Neu zu berücksichtigen ist insbesondere der Einfluss von Cyber-Security im Hinblick auf die funktionale Sicherheit. Hier bieten spezifische IEC- und ISO-Regelwerke weitere Hilfestellungen die relevanten Schutzziele aus der Norm EN 62443 (IT-Sicherheit für industrielle Automatisierungssysteme) umzusetzen. Im Hinblick auf programmierbare bzw. konfigurierbare Systeme, die nach IEC 61508 entwickelt und zertifiziert Systeme wurden, sind hinsichtlich der Verifikation und Validierung von Anwendersoftware deutliche Vereinfachungen zu erwarten.

Derzeit ist jedoch noch offen, ob und welche Übergangszeiten für die Publizierung der Normen im Amtsblatt vorgesehen sind. Es besteht aber eine berechtigte Hoffnung, dass es eine Übergangsfrist von ca. 2-3 Jahren geben wird.

13 Glossar

Abkürzung	Englischer Begriff	Deutsche Erklärung
B_{10D}		Anzahl von Zyklen, bis 10% Komponenten gefahrbringend ausfallen
λ	Failure Rate	Ausfallrate
λ_S	Failure Rate, Safe	Ausfallrate bei ungefährlichen Fehlern
λ_D	Failure Rate, Dangerous	Ausfallrate bei gefahrbringenden Fehlern
CCF	Common Cause Failure	Ausfall in Folge gemeinsamer Ursache
DC	Diagnostic Coverage	Diagnosedeckungsgrad
DCavg	Average Diagnostic Coverage	Fehleraufdeckungsrate im Durchschnitt
	Designated Architecture	Vorausberechnete Struktur eines SRP/CS
HFT	Hardware Fault Tolerance	Hardware Fehlertoleranz
MTBF	Mean Time Between Failures	Mittlere Ausfallzeit, die im normalen Betrieb vergeht, bevor ein Fehler auftritt.
MTTF	Mean Time To Failure	Mittlere Zeit bis zum Ausfall
$MTTF_D$	Mean Time To Dangerous Failure	Mittlere Zeit bis zum gefahrbringenden Ausfall
MTTR	Mean Time To Repair	Mittlere Reparaturzeit (immer deutlich kleiner als die MTTF)
PFH	Probability Of Failure Per Hour	Wahrscheinlichkeit eines Ausfalls pro Stunde
PFH_D	Probability Of Dangerous Failure Per Hour	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde
PL	Performance Level	Fähigkeit von sicherheitsbezogenen Teilen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen, um die erwartete Risikoreduzierung zu erfüllen.
PL_r	Performance Level required	Erforderlicher Performance Level
SIL	Safety Integrity Level	Sicherheits-Integritätslevel
SRCF	Safety Related Control Function	Sicherheitsbezogene Steuerungsfunktion

Abkürzung	Englischer Begriff	Deutsche Erklärung
SRP/CS	Safety Related Parts of a Control System	Sicherheitsbezogener Teil einer Steuerung
SRECS	Safety Related Electrical Control Systems	Sicherheitsbezogenes elektrisches Steuerungssystem
T_1	Proof test intervall	Lebenserwartung oder Wiederholungs-prüfung des Sicherheitssystems
T_2	Diagnostic Test Interval	Diagnose Testintervall
T_M	Mission Time	Gebrauchsdauer
β	Common Cause Failure	Ausfälle gemeinsamer Ursache
C	Duty Cycle	Betätigungszyklus (pro Stunde) eines elektromechanischen Bauteils
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle
Security		IT-Sicherheit
Safety		Sammelbegriff u.a. für funktionale Sicherheit und Maschinensicherheit
Maschinen-sicherheit		Nach erfolgter Gefährdungsanalyse durch Maßnahmen erreichte Risiko-minimierung auf akzeptiertes Restrisiko
Funktionale Sicherheit		Teil der Gesamtsicherheit, bezogen auf die Maschine und das Maschinen-Steuerungs-system, der von der korrekten Funktion des SRECS, sicherheitsbezogenen Systemen anderer Technologie und externen Ein-richtungen zur Risiko-minderung abhängt

14 FAQ

Die nachfolgende Ansammlung gibt Antworten auf häufig gestellte Fragen im Kontext zur funktionalen Sicherheit.

F: Gibt es für Magnetventile / Schütze vom Hersteller eine SIL oder PL-Angabe?
A: Sind diese Bauteile „nur" elektromechanische Bauteile, so gibt es i.d.R. nur einen $B10_D$ Wert. Basierend auf dem $B10_D$ Wert, den Einsatzbedingungen (u.a. der Schalthäufigkeit, Lastfall,…) und den in der Sicherheitsfunktion realisierten Diagnosemaßnahmen kann dann für die Sicherheitsfunktion ein SIL bzw., PL ermittelt werden.

F: Welchen Diagnosedeckungsgrad kann ich bei Relais und Schützen mit zwangsgeführten Kontakten in Anspruch nehmen?
A: Das „reine" Schütz / Relais hat keinen Diagnosedeckungsgrad. Durch Auswertung der zwangsgeführten Kontakte durch eine übergeordnete Instanz kann ein DC von 99% erreicht werden. Voraussetzung hierfür ist eine entsprechende Fehlerreaktion.

F: Kann ich mit einem einzelnen mechanischen Schutztürschalter die Hardware-Fehlertoleranz von 1 erreichen?
A: Nein, in der Regel führt bereits ein Fehler zum Versagen. Für magnetisch betätigte oder RFID – basierte Systeme ist eine Bestätigung einer Hardware-Fehlertoleranz von 1 durch die Hersteller möglich.

F: Was bedeutet der Index „D" bei $MTTF_D$?
A: Der Index „D" steht für „dangerous". Die $MTTF_D$ beschreibt den Erwartungswert der Zeit bis zum ersten gefahrbringenden Fehler.

F: Darf ich bei der Integration komplexer programmierbarer Elektronik die EN ISO 13849 anwenden?
A: Ja. Die Neuausgabe der EN ISO 13849 beschreibt Anforderungen an komplexe Systeme einschließlich Software bis PLe.

F: Was mache ich, wenn ich vom Hersteller meiner Komponenten keine Kennwerte bekomme?
A: Die EN ISO 13849 bzw. EN 62061 bietet im Anhang ersatzweise Referenzwerte für häufig verwendete Komponenten. Vorzugsweise sollten jedoch immer die Originalwerte des Herstellers verwendet werden.

F: Kann ich bei Prozessventilen/Armaturen in Sicherheitsfunktionen, die seltener als einmal pro Jahr angefordert / geschaltet werden (Low-Demand-Mode), für die Berechnung der $MTTF_D$ die EN ISO 13849 anwenden?
A: Nein, die EN ISO 13849 beschreibt nur den High-Demand-Mode. Daher lässt sich eine MTTF-Bewertung nur mit zusätzlichen Maßnahmen wie „Zwangsdynamisierung" vornehmen, welche sicherstellt, dass eine Anforderung mindestens einmal pro Jahr stattfindet.

F: Kann ich bei Low-Demand-Komponenten , die seltener als einmal pro Jahr geschaltet werden für die Berechnung der Ausfallrate die EN 62061 anwenden?
A: Es ist geplant, dass die EN 62061 zukünftig die Möglichkeit bietet Low-Demand-Applikationen zu bewerten. Dies soll im Rahmen eines „Amendments" zur EN 62061 umgesetzt werden.

F: Muss Applikations-Software zertifiziert werden? Wenn „Ja“ nach welcher Norm?

A: Nein. Eine Zertifizierungspflicht auf Basis der beiden Normen besteht nicht separat für die Software, sondern orientiert sich an Umfang und Komplexität des Gesamtprojektes. Im Rahmen der Verifikation und Validierung von Sicherheitsfunktionen kann eine Softwareprüfung erforderlich sein. Hinweise hierzu finden sich in EN ISO 13849 und EN 62061 sowie in EN 61508-3 und, bei Verwendung einer Sicherheits-SPS oder einer vergleichbaren Komponente, in der Dokumentation der Sicherheits-SPS. Jedoch ist geplant, dass es Anpassungen im Rahmen der Überarbeitung bei der Maschinenrichtlinie geben soll.

F: Kann man Standard-Komponenten für die z.B. nur ein MTTF-Wert angegeben ist für die Sicherheitstechnik verwenden?

A: Sicherheitsrelevante Steuerungen können grundsätzlich durch den Einsatz von Standardkomponenten realisiert werden, jedoch bieten Sicherheitsbauteile den Vorteil, dass der Maschinenkonstrukteur bei der sicherheitstechnischen Beurteilung und Analyse der verwendeten Bauteile durch den Hersteller von Sicherheitsbauteilen entlastet wird. Zum Erreichen funktionaler Sicherheit ist neben der Verwendung einer geeigneten Architektur (Kategorie), der Realisierung einer erforderlichen Fehlererkennung und der Berücksichtigung von Ausfallraten/-wahrscheinlichkeiten die systematische Eignung von Komponenten zu beachten. Auszuschließen ist im Allgemeinen der Einsatz komplexer Elemente oder Teilsysteme gleichartiger Ausführung (homogene Redundanz), da Fragen nach der systematischen Eignung und der erforderlichen Fehleraufdeckung oft nicht ausreichend beantwortet werden können.

15 Redaktion

Carsten Gregorius – Phoenix Contact

Michael Niehaus - Lenze

Thomas Schulz-Basten – Berufsgenossenschaft Holz und Metall

Klaus Stark - Pilz

Weiterführende Informationen zum Thema **„funktionale Sicherheit“ finden Sie auf www.zvei.org, Fachverband Automation „Schaltanlagen, Schaltgeräte & Industriesteuerungen“** sowie im Internet der beteiligten Mitgliedsfirmen des ZVEI.

ZVEI e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telephone: +49 69 6302-0
Fax: +49 69 6302-317
E-mail: zvei@zvei.org
www.zvei.org