

Funktionale Sicherheit von Maschinen und Anlagen

Europäische Maschinenrichtlinie – einfach umgesetzt



EN 954-1
EN ISO 13849-1
EN 62061

Safety Integrated

www.siemens.de/safety-integrated

SIEMENS



Neue Normen helfen dem Maschinenbauer

Weltweite Standards, weitreichende Richtlinien

Inhalt

Grundlegende Sicherheitsanforderungen in der Fertigungsindustrie	4
Grundlegende Normen beim Entwurf von Steuerungsfunktionen	5
Schritt für Schritt: Entwurf und Realisierung von sicherheitsbezogenen Steuerungen	6
Schritt 1: Strategie zur Risikominderung	8
Schritt 2: Risikobewertung	9
Schritt 3: Aufbau der Sicherheitsfunktion und Bestimmung der Sicherheitsintegrität	11
Schritt 4: Validierung auf Basis des Sicherheitsplans	17
Durchgängig profitieren: Sicherheit aus einer Hand	18
Anhang: Standard-B10-Werte	18
Glossar	19
Produktportfolio	20

Als Partner in allen Sicherheitsbelangen unterstützen wir nicht nur mit den entsprechenden sicherheitsgerichteten Produkten und Systemen, sondern auch mit stets aktuellem Know-how zu internationalen Normen und Bestimmungen. Maschinenherstellern und Anlagenbetreibern bieten wir ein umfangreiches Angebot an Schulungen sowie Services für den gesamten Lebenszyklus von sicherheitstechnischen Anlagen und Maschinen.



Um beim Bau einer Maschine das Restrisiko unter einem tolerierbaren Maß zu halten, sind Risikobeurteilung und gegebenenfalls -minderung von entscheidender Bedeutung. Die Risikobeurteilung dient einerseits dazu, die Maschine „step by step“ sicherheitstechnisch zu optimieren, andererseits als „Beweismittel“ im Schadensfall. Die Dokumentation beschreibt den Weg der Beurteilung und die erreichten Ergebnisse zur Gefahrenminimierung. Sie ist die Basis für einen sicheren Gebrauch der Maschine – wobei der Arbeitsschutz verlangt, dass der Betreiber seine Mitarbeiter dahingehend umfassend schult. Führt der Betreiber bestehende Maschinen zu einer Anlage zusammen oder nimmt er bestimmte Änderungen oder Erweiterungen an der Maschine vor, wird er selbst zum Maschinenbauer.

Die Einhaltung der Maschinenrichtlinie kann auf unterschiedliche Weise gewährleistet werden: in Form einer Maschinenabnahme durch eine Prüfstelle, durch Erfüllung der harmonisierten Normen – oder durch den alleinigen Sicherheitsnachweis mit erhöhtem Prüf- und Dokumentationsaufwand. In jedem Fall ist die CE-Kennzeichnung mit entsprechendem Sicherheitsnachweis der sichtbare Beweis für die Erfüllung der Maschinenrichtlinie. Laut EU-Rahmenrichtlinie für Arbeitsschutz ist sie verbindlich vorgeschrieben.

Unfälle vermeiden, Folgen verhindern

Verglichen mit den physischen oder psychischen Folgen, die ein Mensch durch Maschinen- oder Anlagenunfälle erleiden kann, sind Schäden an der Technik eher tolerierbar – auch wenn ein eventueller Maschinenausfall oder Produktionsstillstand finanziell enorm ins Gewicht fallen kann. Kommt es aber tatsächlich zum „Worst-Case-Szenario“, muss die Schuldfrage in einer Untersuchung geklärt werden. Stellt sich heraus, dass nicht alle relevanten Richtlinien eingehalten wurden, kann das zu erheblichen Schadenersatz-Forderungen führen. Zudem kann auch das Unternehmens-Image darunter leiden – mit weitreichenden Konsequenzen. Werden jedoch alle relevanten Normen erfüllt, kann davon ausgegangen werden, dass die Anforderungen der entsprechenden Richtlinien ebenfalls bedient werden (Vermutungswirkung).

Im Folgenden zeigen wir Ihnen Schritt für Schritt, wie Sie mit Ihrer Maschine jederzeit auf der sicheren Seite sind.

Das Safety Evaluation Tool

Das Safety Evaluation Tool für die Normen IEC 62061 und ISO 13849-1 bringt Sie auf direktem Weg ans Ziel. Denn dieses TÜV-geprüfte Online-Tool aus dem Safety Integrated Programm von Siemens hilft Ihnen schnell und sicher bei der Bewertung von Sicherheitsfunktionen Ihrer Maschine.

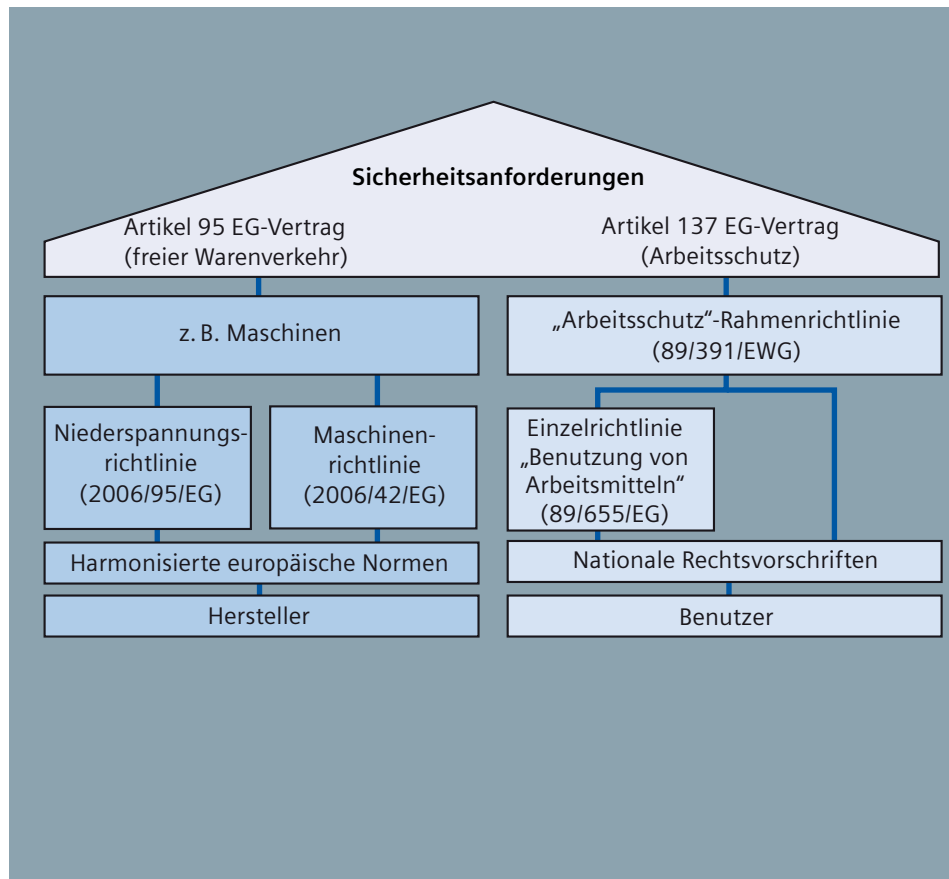
Als Ergebnis erhalten Sie einen normenkonformen Bericht, der als Sicherheitsnachweis in die Dokumentation integriert werden kann.

www.siemens.de/safety-evaluation-tool

Grundlegende Sicherheitsanforderungen in der Fertigungsindustrie

Ziel:
Schutz von Mensch, Maschine und Umwelt

Ergebnis:
CE-Kennzeichnung zum Nachweis einer „sicheren Maschine“



Mit der Einführung des einheitlichen europäischen Binnenmarktes wurden die nationalen Normen und Vorschriften, welche die technische Realisierung von Maschinen betreffen, durchgängig harmonisiert:

- Dabei wurden grundlegende Sicherheitsanforderungen festgelegt, die sich zum einen – für den freien Warenverkehr bestimmt (Artikel 95) – an den Hersteller richten und zum anderen – für den Arbeitsschutz (Artikel 137) – an den Benutzer (Betreiber).
- Dies hatte zur Folge, dass die Maschinenrichtlinie als eine Binnenmarkt-richtlinie – auf Basis der EG-Verträge – von den einzelnen Mitgliedsstaaten inhaltlich in nationales Recht umgesetzt werden musste. In Deutschland wurde diese z. B. im Gerätesicherheitsgesetz GSG verankert.

Damit die Konformität mit einer Richtlinie sichergestellt ist, empfiehlt es sich, die entsprechend harmonisierten europäischen Normen anzuwenden. Dies löst die so genannte „Vermutungswirkung“ aus und gibt Hersteller und Betreiber Rechtssicherheit bezüglich der Erfüllung nationaler Vorschriften wie auch der EG-Richtlinie.

Mit der CE-Kennzeichnung dokumentiert der Hersteller einer Maschine die Einhaltung aller zutreffenden Richtlinien und Vorschriften im freien Warenverkehr. Da die europäischen Richtlinien weltweit anerkannt sind, hilft deren Anwendung auch beim Export in EWR-Länder.

Alle nachfolgenden Erläuterungen richten sich an den Hersteller einer Maschine oder dessen Betreiber, sofern dieser sicherheitsrelevante Änderungen an der Maschine vornimmt oder vornehmen lässt.

Grundlegende Normen beim Entwurf von Steuerungsfunktionen

Ziel:

Erfüllen aller zutreffenden Sicherheitsanforderungen durch ausreichende Risikominderung – mit dem Ziel, haftungssicher und „exportfähig“ zu sein.

Ergebnis:

Realisierung von risikomindernden Schutzmaßnahmen durch Anwendung harmonisierter Normen – dadurch Konformität mit den Sicherheitsanforderungen der Maschinenrichtlinie auf Basis der „Vermutungswirkung“.

Konstruktion und Risikobewertung der Maschine

EN ISO 12100	Sicherheit von Maschinen	Grundbegriffe, allgemeine Gestaltungsleitsätze
EN ISO 14121-1	Sicherheit von Maschinen	Risikobeurteilung, Teil 1: Leitsätze

Funktionale und sicherheitsrelevante Anforderungen für sicherheitsbezogene Steuerungen

Entwurf und Realisierung sicherheitsbezogener Steuerungen

EN 62061:2005
Sicherheit von Maschinen
 Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

EN ISO 13849-1:2006
Sicherheit von Maschinen
 Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze
Nachfolgenorm der EN 954-1:1996, Übergangsfrist bis Ende 2011

Beliebige Architekturen
Sicherheits-Integritätslevel (SIL)
 SIL 1, SIL 2, SIL 3

Vorgesehene Architekturen (Kategorien)
Performance Level (PL)
 PL a, PL b, PL c, PL d, PL e

Elektrische Sicherheitsaspekte

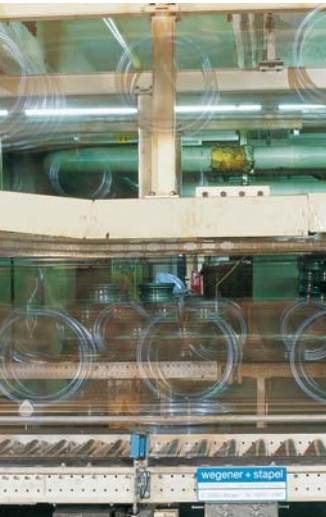
EN 60204-1	Sicherheit von Maschinen:	Elektrische Ausrüstung von Maschinen, Teil 1: Allgemeine Anforderungen
------------	---------------------------	--

Sicherheit erfordert Schutz vor vielfältigen Gefährdungen. Diese können wie folgt beherrscht werden:

- Konstruktion gemäß risikomindernder Gestaltungsleitsätze – und Risikobewertung der Maschine (EN ISO 12100-1, EN ISO 14121-1)
- Technische Schutzmaßnahmen, ggf. durch Verwendung sicherheitsbezogener Steuerungen (funktionale Sicherheit nach EN 62061 oder EN ISO 13849-1)
- Elektrische Sicherheit (EN 60204-1)

Im Folgenden wird die **funktionale Sicherheit** behandelt. Dabei handelt es sich um den Teil der Sicherheit einer Maschine oder Anlage, der von der korrekten Funktion ihrer Steuerungs- oder Schutzeinrichtungen abhängt. Dem Anwender stehen dabei zwei Normen zur Verfügung:

- EN 62061:2005 – als europäische Sektornorm der Basisnorm IEC 61508.
- EN ISO 13849-2006 – als revidierte Nachfolgenorm der EN 954-1, da diese in Bezug auf die Kategorien nicht mehr ausreicht.



Schritt für Schritt

Entwurf und Realisierung von sicherheitsbezogenen Steuerungen

Die Norm EN 62061

Die Norm EN 62061 „Sicherheit von Maschinen – funktionale Sicherheit von elektrischen, elektronischen und programmierbaren Steuerungen von Maschinen“ definiert umfangreiche Anforderungen. Außerdem gibt sie Empfehlungen für Entwurf, Integration und Validierung von sicherheitsbezogenen elektrischen, elektronischen sowie programmierbaren elektronischen Steuerungssystemen (SRECS) für Maschinen. Die Norm betrachtet erstmalig die gesamte Sicherheitskette vom Sensor bis zum Aktor. Um einen Sicherheitsintegritäts-Level wie etwa SIL 3 zu erreichen, genügt es nicht mehr, dass die Einzelkomponenten entsprechend zertifiziert sind. Vielmehr muss die gesamte Sicherheitsfunktion den definierten Anforderungen gerecht werden.

Anforderungen an die Leistungsfähigkeit von nicht elektrischen – z. B. hydraulischen, pneumatischen oder elektromechanischen – sicherheitsbezogenen Steuerungselementen für Maschinen werden von der Norm nicht festgelegt.

Anmerkung:

Werden nicht elektrische sicherheitsbezogene Steuerungselemente über eine passende elektrische Rückleseinformation überwacht, so können diese Elemente für die Sicherheitsbetrachtung bei Erfüllung der Anforderung vernachlässigt werden.

Die Norm EN ISO 13849-1

Die EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze“ setzt auf den bekannten Kategorien der EN 954-1, Ausgabe 1996 auf. Sie betrachtet die kompletten Sicherheitsfunktionen mit allen Geräten, die an ihrer Ausführung beteiligt sind.

Mit der EN ISO 13849-1 erfolgt – über den qualitativen Ansatz der EN 954-1 hinaus – auch eine quantitative Betrachtung der Sicherheitsfunktionen. Aufbauend auf den Kategorien werden hierfür Performance Level (PL) verwendet. Die Norm beschreibt die Ermittlung des PL für sicherheitsrelevante Teile von Steuerungen auf Basis vorgesehener Architekturen (designated architectures) für die vorgesehene Gebrauchsdauer. Bei Abweichungen hiervon verweist EN ISO 13849-1 auf IEC 61508. Bei Kombination mehrerer sicherheitsrelevanter Teile zu einem Gesamtsystem macht die Norm Angaben zur Ermittlung des resultierenden PL.

Dabei darf sie auf sicherheitsbezogene Teile von Steuerungen (SRP/CS) und alle Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie, elektrisch, hydraulisch, pneumatisch, mechanisch usw. angewendet werden.

Die Übergangsfrist von EN 954-1 zu EN ISO 13849-1 endet 2011. In dieser Zeit dürfen beide Normen alternativ angewendet werden.



Sicherheitsplan nach EN 62061 – Leitfaden bei der Realisierung einer sicheren Maschine

Durch ein systematisches Vorgehen über den gesamten Produkt-Lebenszyklus lassen sich alle sicherheitsrelevanten Aspekte und Regelungen für die Konstruktion und den Betrieb einer sicheren Maschine bestimmen und umsetzen. Der Sicherheitsplan (Safety Plan) begleitet Anwender in allen Phasen – bis hin zu Modernisierung und Upgrade. Aufbau und Umsetzungspflicht des Sicherheitsplans sind in EN 62061 definiert.

Die Norm fordert in diesem Rahmen eine systematische Vorgehensweise bei der Realisierung eines Sicherheitssystems (SRECS). Dazu gehört, dass alle Aktivitäten im Sicherheitsplan dokumentiert werden: von der Gefährdungsanalyse und Risikobeurteilung der Maschine über den Entwurf und die Realisierung des SRECS – bis hin zur Validierung. Dabei muss der Sicherheitsplan immer synchron mit der Realisierung des SRECS aktualisiert werden.

Folgende Themen und Aktivitäten werden im Sicherheitsplan dokumentiert:

- **Planung und Vorgehensweise aller – für die Realisierung eines SRECS erforderlichen – Aktivitäten.**

Zum Beispiel:

- Entwickeln der Spezifikation der sicherheitsbezogenen Steuerungsfunktion (SRCF)
- Entwurf und Integration des SRECS
- Validierung des SRECS
- Erstellen der Benutzerdokumentation zum SRECS
- Dokumentation aller relevanten Informationen zur Realisierung des SRECS (Projektdokumentation)

- **Strategie zur Erreichung der funktionalen Sicherheit**

- **Verantwortlichkeiten bezüglich Ausführung und Überprüfung aller Aktivitäten**

Die hier beschriebenen Tätigkeiten sind in der EN ISO 13849-1:2006 nicht explizit beschrieben – jedoch für die korrekte Umsetzung der Maschinenrichtlinie notwendig.

Schritt 1: Strategie zur Risikominderung nach EN ISO 12100-1, Abschnitt 1

Ziel:
Risikominderung

Ergebnis:
Schutzmaßnahmen definieren
und bestimmen

Die primäre Aufgabe einer Risikominderung ist es, Gefährdungen zu erkennen, zu bewerten – und mit Hilfe von Schutzmaßnahmen zu beherrschen, so dass kein Schaden von ihnen ausgehen kann.

Dazu wird in EN ISO 12100-1 folgender iterativer Prozess vorgeschlagen:

1. Festlegen der physikalischen und zeitlichen Grenzen der Maschine
2. Identifizierung der Gefährdungen, Risikoeinschätzung und -bewertung
3. Einschätzen des Risikos für jede identifizierte Gefährdung und Gefährdungssituation
4. Bewerten des Risikos und Festlegen von Entscheidungen zur Risikominderung
5. Beseitigen der Gefährdung oder Vermindern des mit der Gefährdung verbundenen Risikos durch die „3-Schritt-Methode“ – inhärent sichere Konstruktion, technische Schutzmaßnahmen sowie Benutzerinformation

Die Norm EN ISO 14121-1 enthält detaillierte Informationen zu den Schritten 1 bis 4.

Aus den ermittelten Risiken ergeben sich die Sicherheitsanforderungen, die erfüllt werden müssen. Dabei unterstützt EN 62061 mit dem Sicherheitsplan ein strukturiertes Vorgehen: Für jede erkannte Gefährdung muss eine Sicherheitsfunktion spezifiziert werden. Hierzu gehört auch die Testspezifikation – siehe „Validierung“.

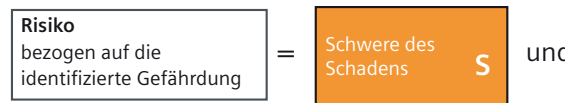


Schritt 2: Risikobewertung

Ziel:
Risikoelemente für eine Sicherheitsfunktion bestimmen und bewerten

Ergebnis:
Geforderte Sicherheitsintegrität festlegen

Die Risikoelemente (S, F, W und P) dienen als Eingangsgröße für beide Normen. Die Bewertung dieser Risikoelemente erfolgt auf unterschiedliche Art und Weise. Nach EN 62061 wird ein geforderter Sicherheitsintegritäts-Level (SIL) bestimmt, nach EN ISO 13849-1 ein Performance Level (PL).



Frequenz und Dauer der Aussetzung	F
Eintrittswahrscheinlichkeit	W
Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens	P

Anhand des Beispiels „Eine rotierende Spindel muss beim Öffnen einer Schutzhaube sicher stillgesetzt werden“ soll das Risiko unter Anwendung beider Normen bewertet werden.

Bestimmung des erforderlichen SIL (durch SIL-Zuordnung)

Häufigkeit und/oder Aufenthaltsdauer F		Eintrittswahrscheinlichkeit des Gefährdungsereignisses W		Möglichkeit der Vermeidung P	
≤ 1 Std.	5	häufig	5		
> 1 Std. bis ≤ 1 Tag	5	wahrscheinlich	4		
> 1 Tag bis ≤ 2 Wo.	4	möglich	3	unmöglich	5
> 2 Wo. bis ≤ 1 Jahr	3	selten	2	möglich	3
> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Auswirkungen	Schadensausmaß S	Klasse K = F + W + P				
		3-4	5-7	8-10	11-13	14-15
Tod, Verlust von Auge oder Arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, Verlust von Fingern	3	andere Maßnahmen			SIL 2	SIL 3
Reversibel, medizinische Behandlung	2	andere Maßnahmen			SIL 1	SIL 2
Reversibel, Erste Hilfe	1	andere Maßnahmen				SIL 1

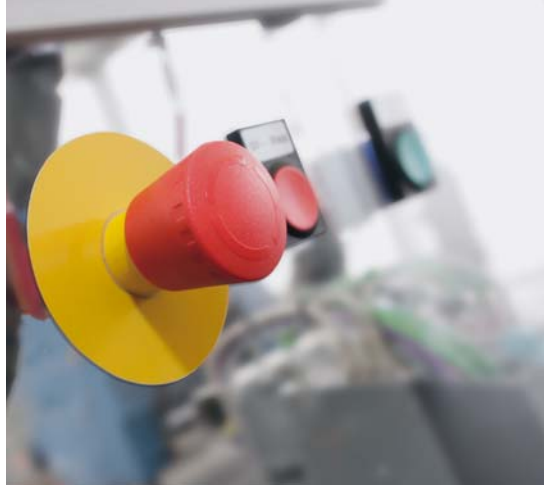
Beispiel

Gefährdung	S	F	W	P	=	K	Sicherheitsmaßnahmen	Sicher
Rotierende Spindel	3	5	4	3		12	Überwachung Schutzhaube mit einem geforderten SIL 2	Ja, mit SIL 2

Vorgehensweise

- Schadensausmaß S festlegen: Permanent, Verlust von Fingern, S = 3
- Punkte für Häufigkeit F, Wahrscheinlichkeit W und Vermeidung P bestimmen:
 - Aufenthalt im Gefahrenbereich: einmal pro Tag, F = 5
 - Eintrittswahrscheinlichkeit: wahrscheinlich, W = 4
 - Möglichkeit zur Vermeidung: möglich, P = 3
- Summe der Punkte F + W + P = Klasse K: K = 5 + 4 + 3 = 12
- Schnittpunkt Zeile Schadensausmaß S und Spalte K = geforderter SIL: SIL 2

Der geforderte SIL ist somit SIL 2



Bestimmung des erforderlichen PL (durch Risikograf)

Die Einschätzung des Risikos erfolgt anhand der gleichen Risikoparameter:

Risikoparameter

S = Schwere der Verletzung

- S1 = leichte (üblicherweise reversible) Verletzung
- S2 = schwere (üblicherweise irreversible) Verletzung, einschließlich Tod

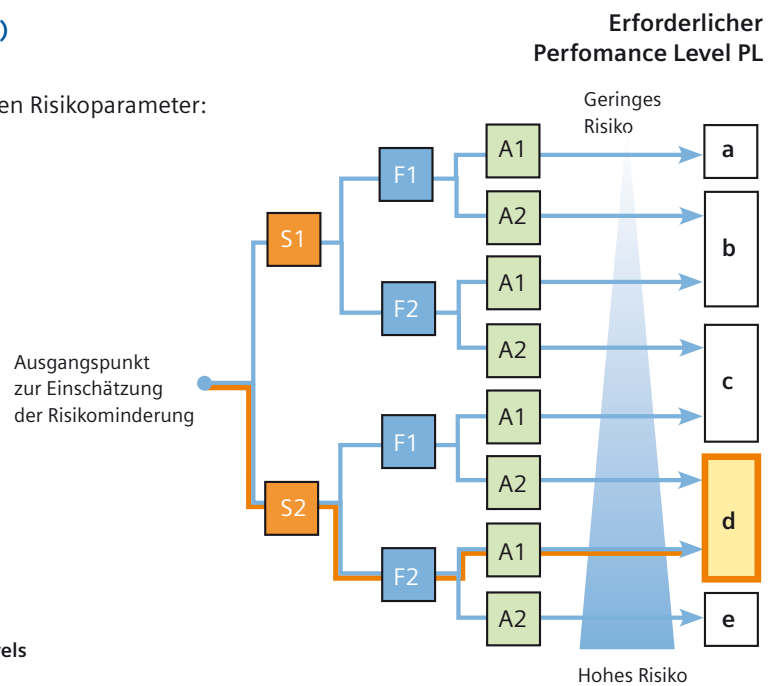
F = Häufigkeit und/oder Aufenthaltsdauer der Gefährdungsaussetzung

- F1 = selten bis öfter und/oder Zeit der Gefährdungsaussetzung ist kurz
- F2 = häufig bis dauernd und/oder Zeit der Gefährdungsaussetzung ist lang

P = Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens

- P1 = möglich unter bestimmten Bedingungen
- P2 = kaum möglich

a, b, c, d, e = Ziele des sicherheitsgerichteten Performance Levels



Vorgehensweise

1. Schadensausmaß S festlegen:

S2 = schwere (üblicherweise irreversible) Verletzung, einschließlich Tod

2. Häufigkeit und/oder Aufenthaltsdauer der Gefährdungsaussetzung F festlegen:

F2 = häufig bis dauernd und/oder Zeit der Gefährdungsaussetzung ist lang

3. Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens P festlegen:

P1 = möglich unter bestimmten Bedingungen

Der geforderte Performance Level ist somit PL d.

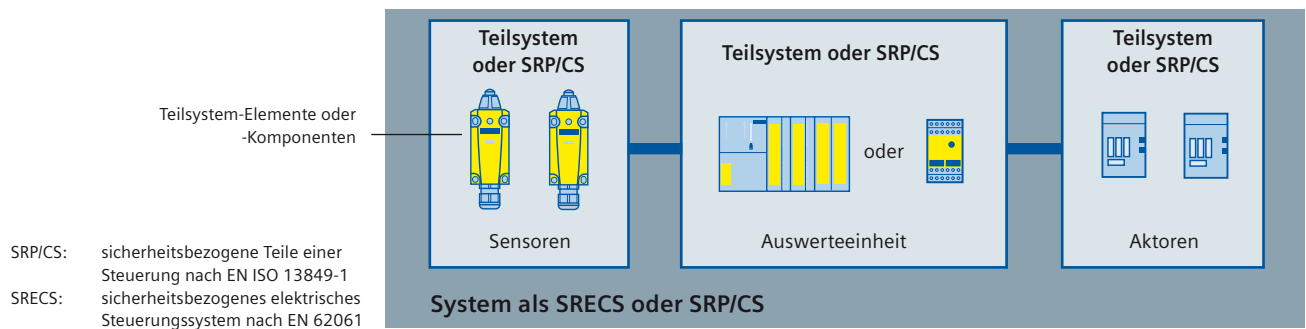
Schritt 3:**Aufbau der Sicherheitsfunktion und Bestimmung der Sicherheitsintegrität****Ziel:**

Steuerungsfunktion und Bestimmung der Sicherheitsintegrität

Ergebnis:

Güte der ausgewählten Steuerungsfunktion

Innerhalb beider Normen wird zwar eine unterschiedliche Methodik zur Bewertung einer Sicherheitsfunktion angewendet, die Ergebnisse lassen sich dennoch ineinander überführen. Beide Normen verwenden ähnliche Begriffe und Definitionen. Die Betrachtung der gesamten Sicherheitskette beider Normen ist vergleichbar: Eine Sicherheitsfunktion wird als System bezeichnet.

Aufbau einer Sicherheitsfunktion**Beispiel:**

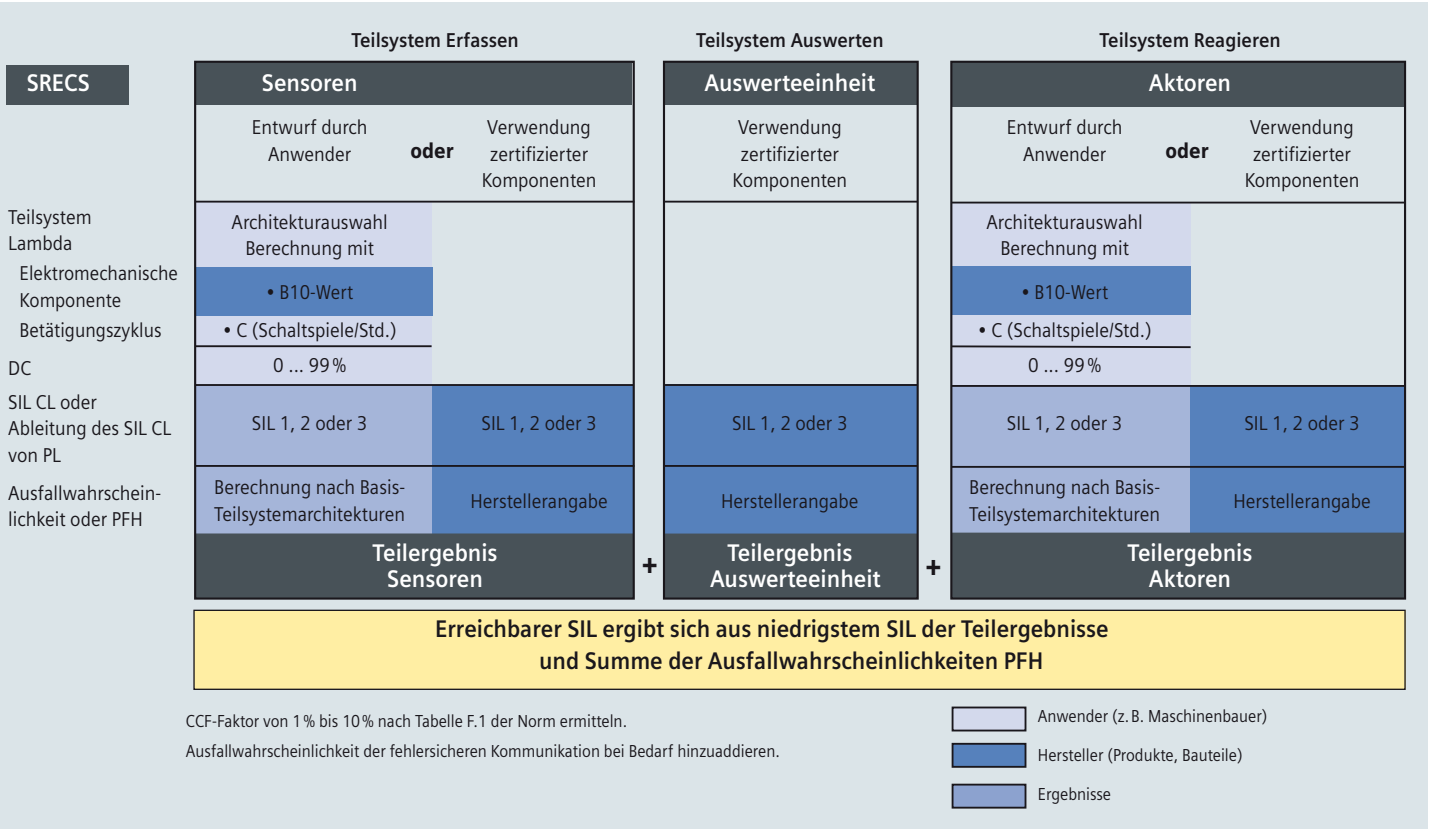
- Anforderung: Eine rotierende Spindel muss beim Öffnen einer Schutzhaube sicher stillgesetzt werden.
- Lösung: Die Schutzhauben-Überwachung wird mit zwei Positionsschaltern (Sensoren) realisiert. Das Abschalten der rotierenden Spindel erfolgt mit zwei Lastschützen (Aktoren). Die Auswerteeinheit kann eine fehlersichere Steuerung (CPU, F-DI, F-DO) oder ein Sicherheitsschaltgerät sein.

Die Verbindungstechnik zwischen den Teilsystemen ist in die Betrachtungen einzubeziehen.

Gemeinsame und vereinfachte Vorgehensweise:

1. Jedes Teilsystem bzw. SRP/CS bewerten und „Teilergebnisse“ erhalten. Hierzu gibt es zwei Möglichkeiten:
 - a. Verwendung zertifizierter Komponenten mit Herstellerangaben (z. B. SIL CL, PFH oder PL).
 - b. Auf Basis der ausgewählten Architektur (ein- oder zweikanalig) erfolgt die Berechnung der Ausfallraten der Teilsystem-Elemente oder -Komponenten. Anschließend erfolgt die Berechnung der Ausfallwahrscheinlichkeit des Teilsystems oder der SRP/CS.
2. Die Teilergebnisse bzgl. der strukturellen Anforderungen (SIL CL bzw. PL) beurteilen und die Ausfallwahrscheinlichkeiten/PFH addieren.

Methodik nach EN 62061



- Anmerkungen:**
- Eine genaue Vorgehensweise zur Bestimmung der Sicherheitsintegrität finden Sie im Funktionsbeispiel zur EN 62061. Siehe hierzu auch: <http://support.automation.siemens.com/WW/view/de/2399647>
 - Auf Seite 19 der vorliegenden Broschüre finden Sie Erklärungen zu den Abkürzungen.

Teilsystem „Erfassen“ – Sensoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte (SIL CL und PFH). Bei Verwendung von elektromechanischen Komponenten im Anwenderentwurf können SIL CL und PFH-Wert wie folgt ermittelt werden.

Bestimmung des SIL CL

Für das Beispiel kann SIL CL 3 angenommen werden, da die verwendete Architektur der Kategorie 4 nach EN 954-1 entspricht und entsprechende Diagnose vorhanden ist.

Berechnung der Ausfallraten λ der Teilsystem-Elemente „Positionsschalter“

Mit dem B10-Wert und den Schaltspielen C kann mit einer Formel gemäß EN 62061 Abschnitt 6.7.8.2.1 die gesamte Ausfallrate λ einer elektromechanischen Komponente berechnet werden:

$$\lambda = (0,1 * C) / B10 = (0,1 * 1) / 10.000.000 = 10^{-8}$$

C = Anwenderangabe der Betätigungszyklen pro Stunde (duty cycle)
 B10-Wert = Herstellerangabe (siehe Anhang Seite 18 – Tabelle B10-Werte)

Die Ausfallrate λ setzt sich aus ungefährlichen (λ_S) und gefahrbringenden (λ_D) Anteilen zusammen:

$$\lambda = \lambda_S + \lambda_D$$

$$\lambda_D = \lambda * \text{Anteil gefahrbringender Ausfälle in \%}$$

$$= 10^{-8} * 0,2 = 2 * 10^{-9}$$

(siehe Anhang Seite 18 – Tabelle B10-Werte)

Berechnung der gefahrbringenden Ausfallwahrscheinlichkeit PFH_D nach verwendeter Architektur

Die EN 62061 definiert vier Architekturen für Teilsysteme (Basis-Teilsystemarchitektur A bis D). Für die Ermittlung der Ausfallwahrscheinlichkeit PFH_D stellt die Norm für jede Architektur Berechnungsformeln zur Verfügung.

Für ein zweikanaliges Teilsystem mit Diagnose (Basis-Teilsystemarchitektur D) sowie mit gleichen Elementen errechnet sich für jedes Teilsystem folgende gefahrbringende Ausfallrate λ_D :

$$\lambda_D = (1 - \beta)^2 * \{[\lambda_{De}^2 * DC * T2] + [\lambda_{De}^2 * (1 - DC) * T1]\} + \beta * \lambda_{De}, \approx 2 * 10^{-10}$$

$$PFH_D = \lambda_D * 1 \text{ Std.} \approx 2 * 10^{-10}$$

$$\lambda_{De} = \text{ gefahrbringende Ausfallrate für ein Teilsystem-Element}$$

Für die Berechnung des Beispiels wurden folgende Annahmen getroffen:

$\beta = 0,1$	konservative Annahme, da Maximalwert aus der Norm
$DC = 0,99$	durch Diskrepanz- und Kurzschlussüberwachung
$T2 = 1/C$	durch Auswertung im Sicherheitsprogramm
$T1 = 87.600 \text{ Std.}$ (10 Jahre)	Gebrauchsdauer der Komponente

Teilsystem „Auswerten“ – Auswerteeinheit:

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte.

Beispielwerte:
SIL CL = SIL 3
PFH_D = < 10⁻⁹

Teilsystem „Reagieren“ – Aktoren:

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte:

Beispielwerte:
SIL CL = SIL 2
PFH_D = 1,29 * 10⁻⁷

Bei Entwurf durch Anwender für Teilsystem „Reagieren“ wird mit der gleichen Vorgehensweise gearbeitet wie beim Teilsystem „Erfassen“.

Bestimmung der Sicherheitsintegrität der Sicherheitsfunktion

Es muss die kleinste SIL-Anspruchsgrenze (SIL CL) aller Teilsysteme der sicherheitsbezogenen Steuerungsfunktion (SRFC) bestimmt werden:

$$SIL \text{ CL Min} = \text{Minimum (SIL CL (Teilsystem 1))SIL CL (Teilsystem n)}$$

$$= SIL \text{ CL 2}$$

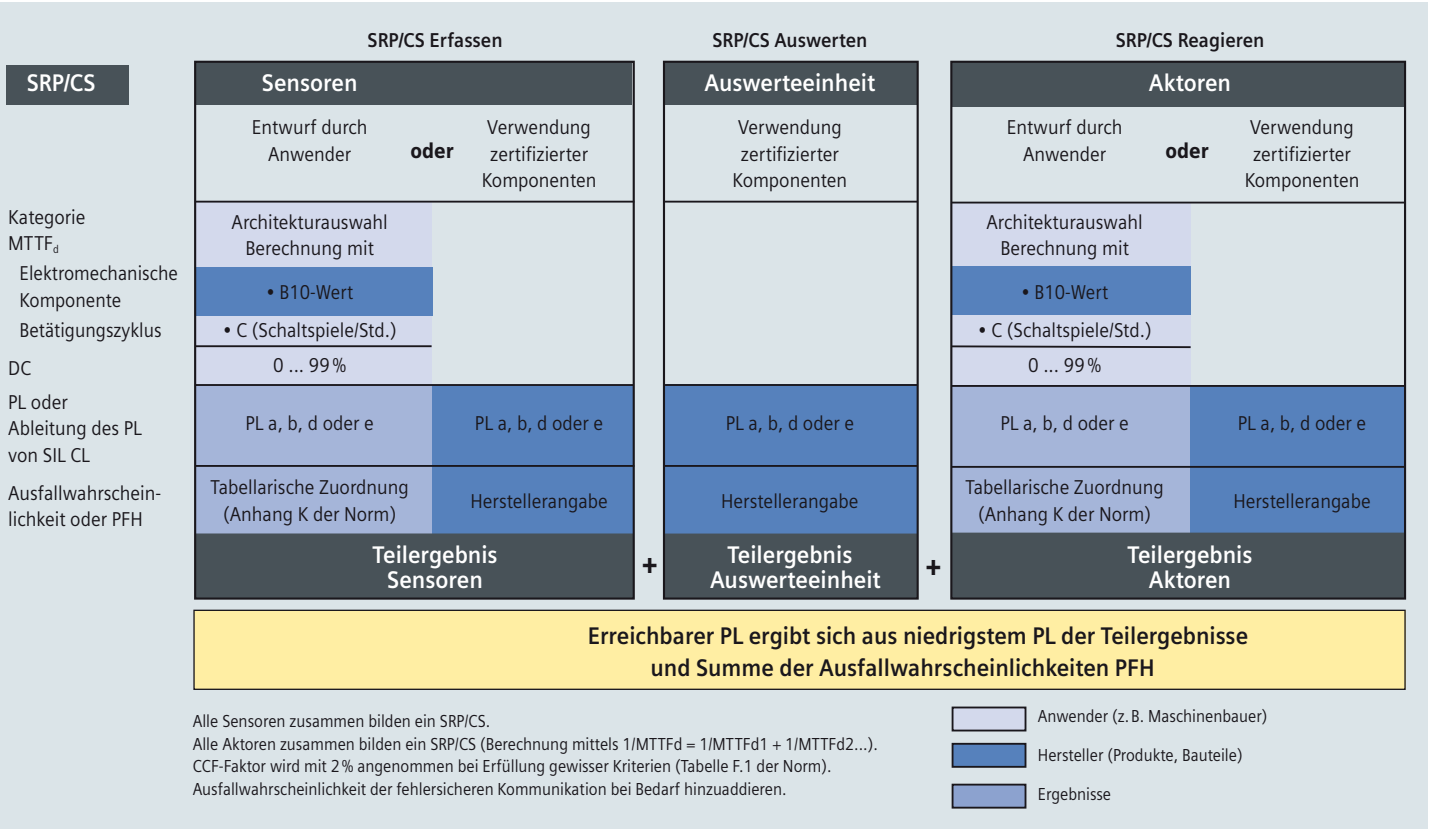
Summe der gefahrbringenden Ausfallwahrscheinlichkeiten (PFH_D) der Teilsysteme

$$PFH_D = PFH_D (\text{Teilsystem 1}) + \dots + PFH_D (\text{Teilsysteme n}) = 1,30 * 10^{-7}$$

$$= < 10^{-6} \text{ entspricht SIL 2}$$

Ergebnis: Die Sicherheitsfunktion erfüllt die Anforderung für SIL 2

Methodik nach EN ISO 13849-1



SRP/CS „Erfassen“ – Sensoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte (PL, SIL, CL oder PFH_D). Der SIL, CL und der PL können auf Basis der Ausfallwahrscheinlichkeiten ineinander überführt werden, siehe Punkt Umsetzung von SIL und PL.

Bei Verwendung von elektromechanischen Komponenten im Anwenderentwurf können PL und PFH_D-Wert wie folgt ermittelt werden.

Berechnung der Ausfallraten der SRP/CS-Elemente „Positionsschalter“

Mit dem B10-Wert und dem Schaltspiel n_{op} kann der Anwender die Ausfallrate $MTTF_d$ der elektromechanischen Komponente berechnen:

$$MTTF_d = B10_d / 0,1 * n_{op} = 0,2 * 10^8 \text{ Stunden} = 2.300 \text{ Jahre entspricht } MTTF_d = \text{hoch}$$

mit n_{op} = Betätigungen pro Jahr (number of operations: Angabe des Anwenders)

$$n_{op} = (d_{op} * h_{op} * 3.600 \text{ s/h}) / t_{zyklus}$$

mit folgenden Annahmen, die in Bezug zur Anwendung des Bauteils getroffen worden sind:

- h_{op} ist die mittlere Betriebszeit in Stunden je Tag;
- d_{op} ist die mittlere Betriebszeit in Tagen je Jahr;
- t_{zyklus} ist die mittlere Zeit zwischen dem Beginn zweier aufeinander folgender Zyklen des Bauteils (z. B. Schalten eines Ventils) in Sekunden je Zyklus.

Für die Bewertung des Beispiels wurden folgende Annahmen getroffen:

DC „hoch“ durch Diskrepanz- und Kurzschlussüberwachung
Kategorie 4

Ergebnis: Es wird Performance Level PL e mit einer Ausfallwahrscheinlichkeit von $2,47 \cdot 10^{-8}$ erreicht

(aus Anhang K der Norm EN ISO 13849-1: 2006)

SRP/CS „Auswerten“ – Auswerteeinheit

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte.

Beispielwerte:
SIL CL = SIL 3, entspricht PL e
 $PFH_D = < 10^{-9}$

SRP/CS „Reagieren“ – Aktoren

Bei zertifizierten Komponenten liefert der Hersteller die notwendigen Werte:

Beispielwerte:
SIL CL = SIL 2, entspricht PL d
 $PFH_D = 1,29 \cdot 10^{-7}$

Bei Entwurf durch Anwender für SRP/CS „Reagieren“ wird mit der gleichen Vorgehensweise gearbeitet wie beim SRP/CS „Erfassen“.

Bestimmung der Sicherheitsintegrität der Sicherheitsfunktion

Es muss der kleinste PL aller SRP/CS der sicherheitsbezogenen Steuerungsfunktion (SRCF) bestimmt werden:

$PL_{Mn} = \text{Minimum} (PL (SRP/CS 1)) \dots PL (SRP/CS n) = PL d$

Summe der gefahrbringenden Ausfallwahrscheinlichkeiten (PFH_D) der SRP/CS
 $PFH_D = PFH_D (SRP/CS 1) + \dots + PFH_D (SRP/CS n) = 1,74 \cdot 10^{-7} = < 10^{-6}$ entspricht PL d

Ergebnis: Die Sicherheitsfunktion erfüllt die Anforderung für PL d



Bestimmung des Performance Levels aus Kategorie, DC und MTTFd

Innerhalb beider Normen wird zwar eine unterschiedliche Methodik zur Bewertung einer Sicherheitsfunktion angewendet, die Ergebnisse lassen sich aber ineinander überführen. Vereinfachtes Verfahren zur Bewertung des durch ein SPR/CS erreichten PL:

Kategorie	B	1	2	2	3	3	4
DC _{avg}	kein	kein	niedrig	mittel	niedrig	mittel	hoch
MTTF _d jedes Kanals							
niedrig	a	nicht abgedeckt	a	b	b	c	nicht abgedeckt
mittel	b	nicht abgedeckt	b	c	c	d	nicht abgedeckt
hoch	nicht abgedeckt	c	c	d	d	d	e

Umsetzung von SIL und PL

Die Bewertung der Sicherheitsfunktion kann wie zuvor gezeigt nach zwei unterschiedlichen Methoden erfolgen. Der SIL und der PL können auf Basis der gefahrbringenden Ausfallwahrscheinlichkeiten miteinander verglichen werden, siehe nachfolgende Tabelle.

SIL und PL sind aufeinander abbildbar

Sicherheits-Integritätslevel SIL	Wahrscheinlichkeit gefahrbringender Ausfälle pro Stunde (1/h)	Performance Level PL
–	$\geq 10^{-5}$ bis $< 10^{-4}$	a
SIL 1	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$	b
SIL 1	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$	c
SIL 2	$\geq 10^{-7}$ bis $< 10^{-6}$	d
SIL 3	$\geq 10^{-8}$ bis $< 10^{-7}$	e

Schritt 4: Validierung auf Basis des Safety Plans

Ziel:

Überprüfung der Umsetzung der spezifizierten Sicherheitsanforderungen

Ergebnis:

Dokumentierter Nachweis in Bezug auf die Erfüllung der Sicherheitsanforderungen

Bei der Validierung wird überprüft, ob das Sicherheitssystem (SRECS) die in der „Spezifikation der SRCF“ beschriebenen Anforderungen erfüllt. Grundlage ist dabei der Sicherheitsplan. Folgende Vorgehensweise wird bei der Validierung gefordert:

- Die Verantwortlichkeiten sind zu definieren und zu dokumentieren.
- Auch alle Tests müssen dokumentiert werden.
- Jede SRCF muss durch Test und/oder Analyse validiert werden.
- Die systematische Sicherheitsintegrität des SRECS muss ebenfalls validiert werden.

Planen

Der Sicherheitsplan ist zu erstellen. Die Validierung wird anhand dieses Dokumentes durchgeführt.

Testen/Prüfen

Es müssen alle Sicherheitsfunktionen gemäß der Spezifikation – wie in Schritt 1 beschrieben – geprüft werden.

Dokumentation

Die Dokumentation ist ein wesentlicher Bestandteil der Begutachtung im Schadensfall. Der Inhalt der Dokumentationsliste ist durch die Maschinenrichtlinie vorgegeben. Im Wesentlichen gehören hierzu:

- Gefährdungsanalyse
- Gefährdungsbewertung
- Spezifikation der Sicherheitsfunktionen
- Hardwarekomponenten, Zertifikate etc.
- Schaltpläne
- Testergebnisse
- Software-Dokumentation inklusive Signaturen, Zertifikaten etc.
- Informationen zum Gebrauch inklusive Sicherheitshinweisen und Einschränkungen für den Betreiber

Nach erfolgreicher Validierung kann die EG-Konformitätserklärung bezüglich der risikomindernden Schutzmaßnahme erstellt werden.



Durchgängig profitieren: Sicherheit aus einer Hand

Ob Erfassen, Auswerten oder Reagieren: Mit unserem Safety Integrated Produktportfolio decken wir alle Sicherheitsaufgaben in der Fertigungsindustrie ab.

Lückenlose Sicherheitstechnik aus einer Hand, die im Sinne von Totally Integrated Automation integriert und durchgängig ist. Das heißt für Sie: sicherer, zuverlässiger und wirtschaftlicher Betrieb.

Sicherheitstechnik integrieren, Kosten sparen

Safety Integrated ist die konsequente Umsetzung von Sicherheitstechnik im Sinne von Totally Integrated Automation – unserem einzigartig umfassenden und durchgängigen Produkt- und Systempektrum zur Realisierung von Automatisierungslösungen. D.h., sicherheitstechnische Funktionen werden konsequent in die Standardautomatisierung integriert, sodass ein durchgängiges Gesamtsystem entsteht. Der Vorteil für Maschinenhersteller wie Anlagenbetreiber: deutliche Kosteneinsparungen über den gesamten Lebenszyklus hinweg.

Mit unseren Produkten und Systemen für die Standard- und Sicherheitstechnik sowie entsprechenden Services und Training aus einer Hand können Sie sicher sein: Safety Integrated bietet immer eine schnelle und vor allem wirtschaftliche Lösung.

Unabhängig davon:

- ob Sie sich für eine konventionelle, busbasierte oder steuerungs- bzw. antriebsbasierte Lösung entscheiden (**Maß an Flexibilität**) und/oder
- ob es sich um eine einfache NOT-HALT-Funktion, eine einfache Verkettung von Sicherheitskreisen oder um hochdynamische Vorgänge handelt (**Maß an Komplexität**).



SIRIUS – Standard-B10-Werte elektromechanischer Komponenten

In Anlehnung an die ISO 13849-2 (Anhang D), die ISO/FDIS 13849-1:2005 (Anhang C) und die DIN EN 62061 (Anhang D, Ausfallarten elektrischer/elektronischer Bauteile) sind in der folgenden Tabelle die SIRIUS Standard-B10-Werte und der Anteil gefahrbringender Ausfälle aufgelistet. In der Siemens-Norm SN 31920 finden Sie detaillierte Erläuterungen.

Siemens SIRIUS Produktgruppe (elektromechanische Komponenten)	B10-Wert (Schaltspiele)	Anteil gefahrbringender Ausfälle
NOT-HALT-Befehlsgeräte (mit zwangsöffnenden Kontakten)		
• zugentriegelt	30.000	20%
• drehentriegelt (auch mit Schloss)	100.000	20%
Seilzugschalter für NOT-AUS/NOT-HALT-Funktion (mit zwangsöffnenden Kontakten)	1.000.000	20 %
Standard-Positionsschalter (mit zwangsöffnenden Kontakten)	10.000.000	20 %
Positionsschalter mit getrenntem Betätiger (mit zwangsöffnenden Kontakten)	1.000.000	20 %
Positionsschalter mit Zuhaltung (mit zwangsöffnenden Kontakten)	1.000.000	20 %
Scharnierschalter (mit zwangsöffnenden Kontakten)	1.000.000	20 %
Positionsschalter mit getrenntem Betätiger (mit zwangsöffnenden Kontakten)	1.000.000	20 %
Drucktaster (nicht verrastend, mit zwangsöffnenden Kontakten)	10.000.000	20 %
Schütze/Motorstarter (mit zwangsgeführten Kontakten bei 3RH/3TH bzw. Spiegelkontakten bei 3RT/3TF)	1.000.000	75 %

Begriffe zur funktionalen Sicherheit

Ausfall (failure)

Die Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen.

β, Beta

Faktor des Ausfalls in Folge gemeinsamer Ursache
CCF-Faktor: common cause failure factor β
(0,1 – 0,05 – 0,02 – 0,01)

B10

Der B10-Wert für verschleißbehaftete Komponenten wird in Anzahl Schaltspiele ausgedrückt: dies ist die Anzahl der Schaltspiele, bei der im Laufe eines Lebensdauerversuchs 10% der Prüflinge ausgefallen sind. Mit dem B10-Wert und dem Betätigungszyklus kann die Ausfallrate für elektro-mechanische Komponenten errechnet werden.

B10d

$B10d = B10 / \text{Anteil gefahrbringender Ausfälle}$

CCF (common cause failure)

Ausfall in Folge gemeinsamer Ursache (z. B. Kurzschluss). Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle nicht auf gegenseitiger Ursache beruhen.

DC (diagnostic coverage),

Diagnosedeckungsgrad

Abnahme der Wahrscheinlichkeit gefahrbringender Hardwareausfälle, die aus der Ausführung der automatischen Diagnostik resultiert.

Fehlertoleranz

Fähigkeit eines SRECS (sicherheitsbezogenes elektrisches Steuerungssystem), eines Teilsystems oder Teilsystem-Elements, eine geforderte Funktion beim Vorhandensein von Fehlern oder Ausfällen weiter auszuführen (Widerstandsfähigkeit gegenüber Fehlern).

Funktionale Sicherheit

Teil der Gesamtsicherheit, bezogen auf die Maschine und das Maschinen-Steuerungssystem, die von der korrekten Funktion des SRECS (sicherheitsbezogenes elektrisches Steuerungssystem), sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt.

Gefahrbringender Ausfall (dangerous failure)

Jede Fehlfunktion in der Maschine oder in deren Energieversorgung, die das Risiko erhöht.

Kategorien B, 1, 2, 3 oder 4

(vorgesehene Architekturen)

Die Kategorien beinhalten neben qualitativen auch quantifizierbare Aspekte (wie z. B. MTTFd, DC und CCF). Mit einem vereinfachten Verfahren, auf Basis der Kategorien als „vorgesehene Architekturen“, kann der erreichte PL (Performance Level) beurteilt werden.

λ , Lambda

Statistische Ausfallrate, die sich aus der Rate sicherer Ausfälle (λ_s) und der Rate gefahrbringender Ausfälle (λ_b) zusammensetzt. Die Einheit von Lambda ist FIT (Failure In Time).

MTTF / MTTF_d

(Mean Time To Failure/Mean Time To Failure dangerous)

Mittlere Zeit bis zu einem Ausfall bzw. gefährlichem Ausfall. Die MTTF kann für Bauelemente durch die Analyse von Felddaten oder mittels Vorhersagen durchgeführt werden. Bei einer konstanten Ausfallrate ist der Mittelwert der ausfallfreien Arbeitszeit $MTTF = 1 / \lambda$, wobei Lambda λ die Ausfallrate des Gerätes ist. (Statistisch gesehen kann angenommen werden, dass nach Ablauf der MTTF 63,2% der betreffenden Komponenten ausgefallen sind.)

PL (Performance Level)

Diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen: von PL „a“ (höchste Ausfallwahrscheinlichkeit) bis PL „e“ (niedrigste Ausfallwahrscheinlichkeit).

PFH_b (Probability of dangerous failure per hour)

Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde.

Proof-Test-Intervall oder Gebrauchsdauer (T1)

Wiederkehrende Prüfung, die Fehler oder eine Verschlechterung in einem SRECS und seinen Teilsystemen erkennen kann, sodass, falls notwendig, das SRECS und seine Teilsysteme in einen „Wie-neu-Zustand“ oder so nah wie praktisch möglich diesem Zustand entsprechend wiederhergestellt werden können.

SFF (safe failure fraction)

Anteil sicherer Ausfälle an der Gesamtausfallrate eines Teilsystems, der nicht zu einem gefahrbringenden Ausfall führt.

SIL (Safety Integrity Level) Sicherheits-Integritätslevel

Diskrete Stufe (eine von drei möglichen) zur Festlegung der Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen Steuerungsfunktionen, die dem SRECS zugeordnet wird, wobei der Sicherheits-Integritätslevel 3 den höchsten und der Sicherheits-Integritätslevel 1 den niedrigsten Sicherheits-Integritätslevel darstellt.

SIL CL (Claim Limit), SIL-Anspruchsgrenze

Maximaler SIL, der für ein SRECS-Teilsystem in Bezug auf strukturelle Einschränkungen und systematische Sicherheitsintegrität beansprucht werden kann.

Sicherheitsfunktion

Funktion einer Maschine, wobei ein Ausfall dieser Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann.

SRCF (Safety-Related Control Function), Steuerungsfunktion

Vom SRECS ausgeführte sicherheitsbezogene Steuerungsfunktion mit einem festgelegten Integritätslevel, die dazu vorgesehen ist, den sicheren Zustand der Maschine aufrechtzuerhalten oder einen unmittelbaren Anstieg von Risiken zu verhindern.

SRECS (Safety-Related Electrical Control System)

Sicherheitsbezogenes elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung von Risiken führt.

SRP/CS (Safety-Related Parts of Control System)

Sicherheitsbezogenes Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt.

Teilsystem

Einheit des Architekturentwurfs des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Teilsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt.

Teilsystem-Element

Teil eines Teilsystems, das ein einzelnes Bauteil oder irgendeine Gruppe von Bauteilen umfasst.

Erfassen







Produkte	SIRIUS Positionsschalter, Scharnierschalter, Kurzhubschalter, Magnetschalter (berührungslos)	SIRIUS Befehls- und Meldegeräte, NOT-HALT, Seilzugschalter, Zweihand-Bedienpult, Fußschalter, Signalsäulen und Einbauleuchten	DP/AS-i F-Link (ASIsafe Solution PROFIsafe)	Mobile Panel SIMATIC 277F IWLAN
Zulassung (max.)				
IEC 62061 (IEC 61508)	Bis SIL 3	Bis SIL 3	Bis SIL 3	Bis SIL 3
ISO 13849-1	Bis PL 3	Bis PL e	Bis PL e	Bis PL e
EN 954-1 bzw. IEC/EN 61496	Bis Kat. 4	Bis Kat. 4	Bis Kat. 4	Bis Kat. 4
Weitere			NFPA 79, NRTL-gelistet	
Anwendung/ Sicherheitsfunktionen	Zur mechanischen Überwachung an Schutzeinrichtungen und Schutztürverriegelung	NOT-HALT-Anwendungen in der Fertigungs- und Prozessindustrie; Zustandssignalisierung an Maschinen und Anlagen	Sicheres Gateway zur Übergabe der ASIsafe-Signale ins PROFIsafe Telegramm für Sicherheitsanwendungen in der Fertigungsautomatisierung	Maschinennahes Bedienen und Beobachten von Produktionsanlagen mit sicherheitskritischen Applikationen, Durchführung von sicherheitsrelevanten Aufgaben, wie z. B. Fehlerbehebung an laufenden Anlagen Sicherheitsfunktionen: <ul style="list-style-type: none"> • NOT-HALT-Taster • Zwei Zustimmtaster (rechts/links) • Transponder-Identifikation und Distanzmessung zur sicheren Anmeldung und Bedienung
Möglichkeiten fehlersicherer Kommunikation	AS-Interface (ASIsafe)	AS-Interface (ASIsafe)	AS-Interface (ASIsafe) und PROFIBUS mit PROFIsafe Profil	PROFINET mit PROFIsafe Profil, IWLAN mit PROFIsafe

Auswerten



Sicherheitschaltgeräte SIRIUS 3TK28	ASIsafe 1) Sichere Eingangsmodule 2) Sicherheitsmonitor (ASIsafe Solution local) 3) Sichere AS-i Ausgänge	Modulares Sicherheitssystem SIRIUS 3RK3	SIMATIC Controller	SIMATIC Peripherie
Bis SIL 3	Bis SIL 3	Bis SIL 3	Bis SIL 3	Bis SIL 3
Bis PL e	Bis PL e	Bis PL e	Bis PL e	Bis PL e
Bis Kat. 4	Bis Kat. 4	Bis Kat. 4	Bis Kat. 4	Bis Kat. 4
NFPA 79, NRTL-gelistet	NFPA 79, NRTL-gelistet		NFPA 79, NFPA 85, NRTL-gelistet, IEC 61511	NFPA 79, NFPA 85, NRTL-gelistet, IEC 61511
<ul style="list-style-type: none"> • Überwachung von Schutz- einrichtungen wie z. B. NOT-HALT-Befehlsgeräte, Positionsschalter und berührungslos wirkende Sensoren • Sichere Stillstands- überwachung: geberlose Überwachung des Stillstands von Motoren • Sichere Drehzahl- überwachung: – Drei parametrierbare Grenzwerte für Stillstand, Einrichtdrehzahl und Automatdrehzahl – Anschluss verschiedener Sensoren und Encoder möglich – Schutztürüberwachung integriert 	<ol style="list-style-type: none"> 1) Sichere Anbindung bzw. Vernetzung von Sicherheitsschaltern und elektronischen Sicherheits- sensoren 2) Alle Sicherheitsanwen- dungen in der Fertigungs- automatisierung: <ul style="list-style-type: none"> • Überwachen und Aus- werten von sicheren Signalen über AS-Interface inkl. Abschalten auf 1–2 Freigabekreisen • Möglichkeit der Ansteuerung sicherer AS-i Ausgänge zur Abschaltung von Motoren oder Ansteuerung z.B. sicherer Ventile • Sichere Kopplung von ASIsafe Netzen 	<p>Modulares, parametrier- bares Sicherheitssystem für alle Sicherheitsanwen- dungen in der Fertigungs- automatisierung</p> <ul style="list-style-type: none"> • Sicheres Auswerten von mechanischen und be- rührungslos wirkenden Schutzeinrichtungen • Integrierte Diagnose- funktion • Integrierte Signaltest- und Diskrepanzzeit- Überwachung 	<p>Skalierbare, fehlersichere Controller</p> <ul style="list-style-type: none"> • Modulare Controller: CPU 315F/317F/319F CPU 414F/416F ET 200F-CPU für ET 200S und ET 200pro • Technologie-Controller mit Motion Control: CPU 317TF-2DP • PC-based Automation: Software-Controller, Embedded Controller, IPC <p>Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> • Integrierte Diagnose • Koexistenz von Standard- und fehlersicheren Programmen in einer CPU • Software: S7 Distributed Safety mit F-FUP und F-KOP sowie integrierter Bibliothek mit TÜV-zertifizierten Sicherheitsbausteinen. Optional: Bibliothek mit Funktionsbausteinen für Pressen und Brenner. 	<p>Skalierbare und redundante Peripheriesysteme</p> <ul style="list-style-type: none"> • ET 200eco • ET 200M • ET 200iSP • ET 200S • ET 200pro <p>Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> • Integrierte Signaltest- und Diskrepanzzeit- Überwachung • Ein dezentrales Peripherie- system mit Standard- und fehlersicheren Ein- und Ausgabebaugruppen • Konfiguration von Signal- test- und Diskrepanzzeit- Visualisierung mit STEP 7
	<ol style="list-style-type: none"> 1) AS-Interface (ASIsafe) 2) AS-Interface (ASIsafe Solution local) 	Diagnose über PROFIBUS	<ul style="list-style-type: none"> • PROFINET mit PROFIsafe, IWLAN mit PROFIsafe 	<ul style="list-style-type: none"> • PROFIBUS mit PROFIsafe Profil: alle Systeme • PROFINET mit PROFIsafe Profil: ET 200S, ET200M, ET 200pro (IWLAN Interface-Modul verfügbar)

Reagieren

			
Motorstarter für <ul style="list-style-type: none"> • ET 200S (IP20) • ET 200pro (IP65) 	Frequenzumrichter für <ul style="list-style-type: none"> • ET 200S • ET 200pro FC 	Frequenzumrichter <ol style="list-style-type: none"> 1) SINAMICS G120 2) SINAMICS G120D 	Frequenzumrichter <ul style="list-style-type: none"> SINAMICS G130 SINAMICS G150
Bis SIL 3	Bis SIL 2	Bis SIL 2	Bis SIL 2
	Bis PL d	Bis PL d	Bis PL d
Bis Kat. 4	Bis Kat. 3	Bis Kat. 3	Bis Kat. 3
NFPA 79, NRTL-gelistet			
<p>Alle Sicherheitsanwendungen in der Fertigungs-automatisierung und dezentrale Antriebsaufgaben wie in der Fördertechnik oder bei Hubantrieben</p> <ul style="list-style-type: none"> • Starten und sicheres Abschalten mit konventioneller und elektronischer Schalttechnik • Integrierter Motorschutz • Sicheres selektives Abschalten (ET 200S) • Alle Vorteile der Systeme SIMATIC ET 200S und SIMATIC ET 200pro <p>Integrierte, autarke Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> • Sicher abgeschaltetes Moment 	<p>Systemintegrierter, dezentraler Antrieb (Frequenzumrichter) an geberlosen Normasynchronmotoren</p> <p>Integrierte, autarke Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> • Sicher abgeschaltetes Moment • Sicherer Stopp 1 • Sicher begrenzte Geschwindigkeit 	<ol style="list-style-type: none"> 1) Modularer, zentraler, sicherer Frequenzumrichter für Anwendungen von 0,37 bis 250 kW 2) Dezentraler Frequenzumrichter ohne Geber an Normasynchronmotoren <p>Integrierte Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> • Sicher abgeschaltetes Moment • Sicherer Stopp 1 • Sicher begrenzte Geschwindigkeit • G120: Sichere Drehrichtung (i.V.) • G120: Sichere Bremsen-ansteuerung 	<p>Frequenzumrichter für drehzahlvariable Einzelantriebe von 75 bis 1500 kW, z. B. Pumpen, Lüfter, Ventilatoren, Kompressoren, Förderbänder, Extruder, Mischer, Mühlen</p> <p>Integrierte Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> • Sicher abgeschaltetes Moment • Sicherer Stopp 1
<ul style="list-style-type: none"> • Solution PROFIsafe: PROFIBUS/PROFINET mit PROFIsafe Profil • Solution Local: Vor-Ort-Sicherheitsapplikation 	PROFIBUS/PROFINET mit PROFIsafe Profil	PROFIBUS/PROFINET mit PROFIsafe Profil	PROFIBUS/PROFINET mit PROFIsafe Profil

Reagieren


**Positionierantrieb
SINAMICS S110**
**1) Antriebssystem
SINAMICS S120
2) Schrankgerät
SINAMICS S150**
**Werkzeugmaschinensteuerung
SINUMERIK 840D sl**
**Werkzeugmaschinensteuerung
SINUMERIK 828D**

Bis SIL 2

Bis SIL 2

Bis SIL 2

Bis SIL 2

Bis PL d

Bis PL d

Bis PL d

Bis PL d

Bis Kat. 3

Bis Kat. 3

Bis Kat. 3

Bis Kat. 3

NFPA 79, NRTL-gelistet *

NFPA 79, NRTL-gelistet

NFPA 79, NRTL-gelistet

Einachs-Servoantrieb für einfache Positionieranwendungen mit Synchron-/Asynchronmotoren mit Leistungen von 0,12 bis 90 kW

Integrierte Sicherheitsfunktionen:

- Sicher abgeschaltetes Moment
- Sicherer Stopp 1*** und 2
- Sicherer Betriebshalt
- Sicher begrenzte Geschwindigkeit***
- Sichere Drehrichtung (i.V.)
- Sichere Geschwindigkeitsüberwachung
- Sichere Bremsenansteuerung

1) Antriebssystem für hochperformante Regelungsaufgaben mit Leistungen von 0,12 bis 4500 kW im Maschinen- und Anlagenbau, z. B. für Verpackungs- oder Kunststoffmaschinen, Handlingsgeräte, Walzwerke oder Papiermaschinen

2) Anspruchsvolle, drehzahlveränderbare Einzelantriebe mit großer Leistung (75 bis 1200 kW) wie Prüfstände, Zuckerzentrifugen, Querschneider, Kabelwinden oder Förderbänder

Integrierte Sicherheitsfunktionen:

- Sicher abgeschaltetes Moment
- Sicherer Stopp 1*** und 2
- Sicherer Betriebshalt
- Sicher begrenzte Geschwindigkeit***
- S120: Booksize/Blocksize: Sichere Drehrichtung (i.V.)
- Sichere Geschwindigkeitsüberwachung
- Sichere Bremsenansteuerung **

Numerische Steuerung mit integrierter Sicherheitstechnik in Steuerung und Antrieb für Werkzeugmaschinen (Drehen, Fräsen, Schleifen, Nibbeln ...)

Integrierte Sicherheitsfunktionen:

- Sicher abgeschaltetes Moment
- Sicherer Stopp 1 und 2
- Sichere Überwachung auf Beschleunigung
- Sicherer Betriebshalt
- Sicher begrenzte Geschwindigkeit
- Sichere begrenzte Lage
- Sicheres Bremsenmanagement
- Sichere Bremsenansteuerung
- Sicherer Bremsentest
- Sichere Softwarenocken
- Sicherheitsgerichtete Ein-/Ausgänge
- Sichere programmierbare Logik
- Integrierter Abnahmetest

Numerische Steuerung für Dreh- und Fräsmaschinen mit integrierter Sicherheitstechnik im Antrieb

Die SINUMERIK 828D ist eine panel-basierte CNC-Steuerung für anspruchsvolle Anwendungen auf Dreh- und Fräsmaschinen, wie sie typischerweise in der Werkstatt eingesetzt werden.

Integrierte Sicherheitsfunktionen:

- Sicher abgeschaltetes Moment
- Sicherer Stopp 1 und 2
- Sicherer Betriebshalt
- Sicher begrenzte Geschwindigkeit
- Sichere Drehrichtung (i.V.)
- Sichere Geschwindigkeitsüberwachung
- Sichere Bremsenansteuerung

PROFIBUS/PROFINET mit PROFIsafe Profil

PROFIBUS/PROFINET mit PROFIsafe Profil

PROFIBUS mit PROFIsafe Profil

PROFIBUS mit PROFIsafe Profil

Siemens AG
Industry Automation
and Drive Technologies
Postfach 23 55
90713 FÜRTH
DEUTSCHLAND

www.siemens.de/safety-integrated

Änderungen vorbehalten 11/10
Bestell-Nr.: E20001-A230-M103-V4
Dispostelle 27610
WÜ/29757 XX03.52.1.05 PA 11102.0
Gedruckt in Deutschland
© Siemens AG 2010

Die Informationen in dieser Broschüre enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Erzeugnisbezeichnungen können Marken oder Erzeugnisnamen der Siemens AG oder anderer, zuliefernder Unternehmen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.