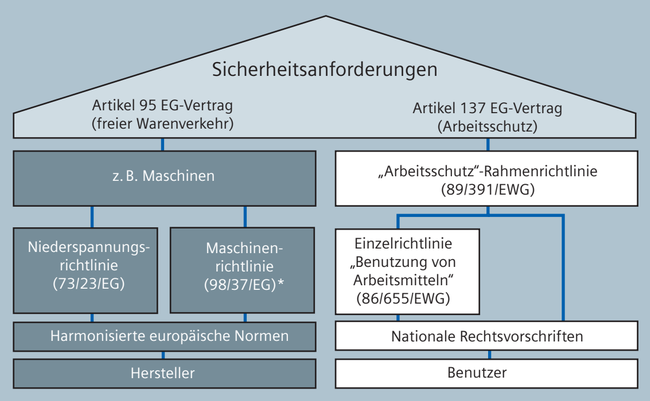
Funktionale Sicherheit in Maschinen und Anlagen –

Europäische Maschinenrichtlinie einfach umgesetzt

Grundlegende Sicherheitsanforderungen in der Fertigungsindustrie



** Die Maschinenrichtlinie 98/37/EG ist derzeit verbindlich. Spätestens ab Ende 2009 wird sie durch die neue Maschinenrichtlinie 2006/42/EG ersetzt.*

Harmonisierte Normen (Vermutungswirkung)

Grundlegende Normen für sicherheitsbezogene Steuerungsfunktionen

Konstruktion und Risikobewertung der Maschine

EN ISO 12100	Sicherheit von Maschinen	Grundbegriffe, allgemeine Gestaltungsleitsätze
EN 1050 (prEN 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 voraussichtlich 2009*
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

Entwurf und Realisierung von sicherheitsbezogenen Steuerungen

Strategie zur Risikominderung nach EN ISO 12100-1

Festlegen von risikomindernden Maßnahmen durch einen iterativen Prozess:

1. Festlegen der Grenzen der Maschine
2. Identifizierung der Gefährdungen, Risikoeinschätzung, Risikobewertung
3. Einschätzen des Risikos für jede identifizierte Gefährdung und Gefährdungssituation
4. Bewerten des Risikos und Treffen von Entscheidungen zur Risikominderung
5. Beseitigen der Gefährdung oder Verminderung des mit der Gefährdung verbundenen Risikos durch Maßnahmen (3-Schritt-Methode: inhärent sichere Konstruktion, technische Schutzmaßnahmen, Benutzerinformation)

EN 1050 (prEN ISO 14121) enthält detaillierte Informationen zu den Schritten 1–4

Anwendbar bei sicherheitsbezogenen elektrischen, elektronischen und programmierbaren elektronischen Steuerungssystemen (SRECS) für Maschinen

EN 62061: 2005 (Sektornorm innerhalb des Rahmens der IEC 61508)

Anwendbar bei sicherheitsbezogenen Teilen von Steuerungen und allen Arten von Maschinen, ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch usw.)

EN ISO 13849-1:2006 (Nachfolgenorm der EN 954-1: 1996, Übergangsfrist bis voraussichtlich 2009)

Sicherheitsplan

Strategie zur Realisierung der Sicherheitsfunktion, Zuständigkeiten, Wartung ...

Risikobewertung

Risiko bezogen auf die identifizierte Gefährdung = Schwere des Schadens **S** und

Frequenz und Dauer der Aussetzung	**F**
Eintrittswahrscheinlichkeit	**W**
Möglichkeit der Vermeidung	**P**

Bestimmung des erforderlichen SIL

(durch SIL-Zuordnung)

Häufigkeit und/oder Aufenthaltsdauer **F**		Eintrittswahrscheinlichkeit des Gefährdungsereignisses **W**		Möglichkeit zur 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 1	SIL 2	SIL 3
Reversibel, medizinische Behandlung	2				SIL 1	SIL 2
Reversibel, Erste Hilfe	1					SIL 1

Vorgehensweise

1. Schadensausmaß S festlegen
2. Punkte für Häufigkeit F, Wahrscheinlichkeit W und Vermeidung P bestimmen
3. Summe der Punkte F + W + P = Klasse K
4. Schnittpunkt Zeile Schadensausmaß S und Spalte K = geforderter SIL

Bestimmung des erforderlichen PL

(durch Risikograf)

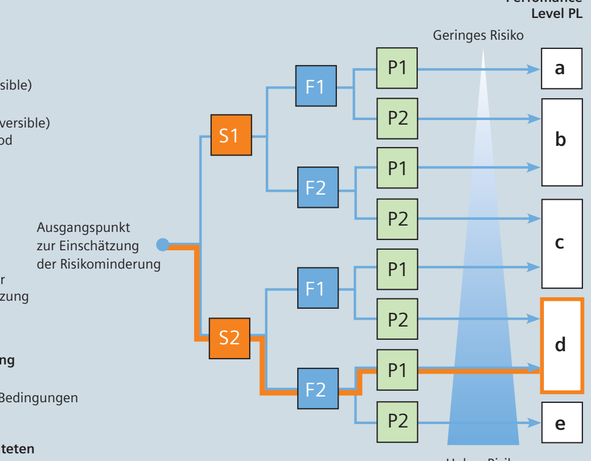
Risiko-Parameter

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

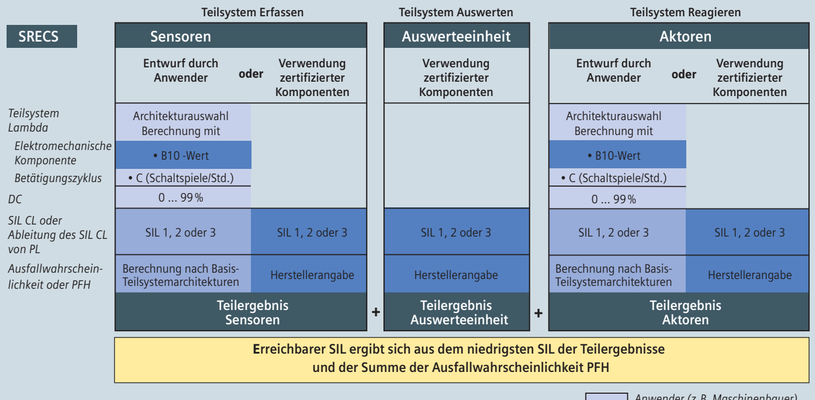
F = Häufigkeit und/oder Aufenthaltsdauer (der Gefährdungsaussetzung)
- F1 = selten bis öfter und/oder Zeit der Gefährdungsaussetzung ist kurz
- F2 = häufig bis dauernd und/oder Zeit der Gefährdungsaussetzung ist lang

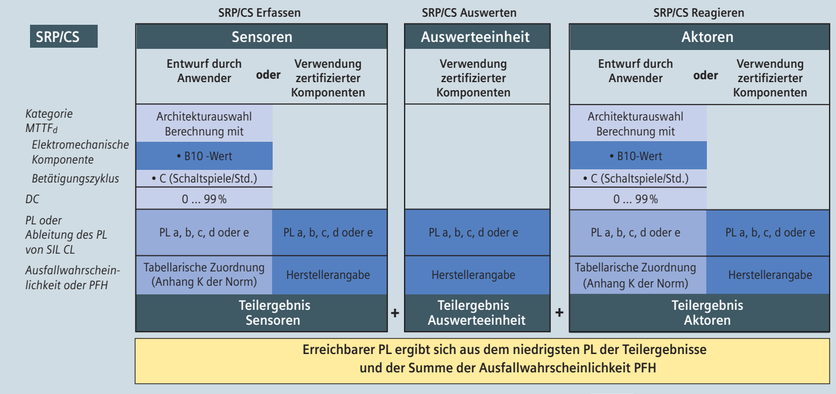
P = Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
- P1 = möglich unter bestimmten Bedingungen
- P2 = kaum möglich

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



Aufbau der Sicherheitsfunktion und Bestimmung der erreichten Sicherheitsintegrität





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

Validierung auf Basis des Validierungsplans

Überprüfung der Umsetzung der spezifizierten Sicherheitsanforderungen		
Planen	Testen/Prüfen	Dokumentieren

CE-Kennzeichung (Konformitätserklärung)

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 elektromechanische Komponenten errechnet werden.

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 Diagnosetests 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. $MTTF_d$, DC und CCF). Mit einem vereinfachten Verfahren, auf Basis der Kategorien als „vorgesehene Architekturen", kann der erreichte PL (Performance Level) beurteilt werden.

λ, **Lambda**
Ausfallrate, die sich aus der Rate sicherer Ausfälle (λ_s) und der Rate gefahrbringender Ausfälle (λ_D) zusammensetzt.

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 / λ, 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_D (Probability of dangerous failure per hour)
Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde.

Proof-Test, Wiederholungsprüfung
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.

Safety Integrated

Answers for industry.

SIEMENS