Willkommen
bei der

CE-CON GmbH

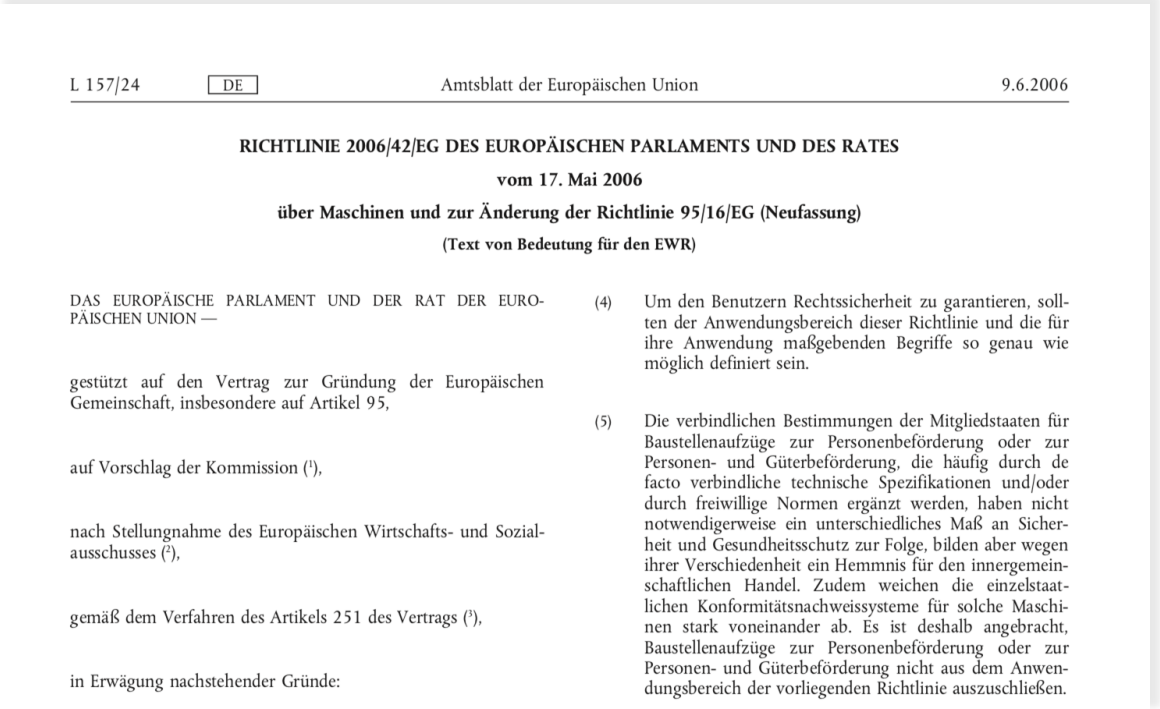
Validierung von Performance Level – Mehr als nur SISTEMA

Gemäß EN ISO 13849-2 müssen sicherheitsbezogenen Teile von Steuerungen an Maschinen validiert werden.
Dies betrifft sowohl die Ausfallwahrscheinlichkeit der Hardware, als auch der Software!
Vielen ist dabei SISTEMA ein Begriff. Was häufig nicht beachtet wird ist, das mittels SISTEMA lediglich die Hardware überprüft werden kann. Die Software-Validierung wird hier gerne einmal vergessen. Zur vollständige Einhaltung der EN ISO 13849-2 ist die Validierung der sicherheitsbezogenen Software jedoch zwingend notwendig, wenn dies zur Anwendung kommt.

Europäisches Recht - Richtlinien

Inhalt von Richtlinien

- Anwendungsbereich der Richtlinie
- Begriffsbestimmungen
- Verfahren zur Konformitätsbewertung
- und diverse Anhänge



L 157/24 DE Amtsblatt der Europäischen Union 9.6.2006

RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. Mai 2006

über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 95,

auf Vorschlag der Kommission (1),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2),

gemäß dem Verfahren des Artikels 251 des Vertrags (3),

in Erwägung nachstehender Gründe:

(4) Um den Benutzern Rechtssicherheit zu garantieren, sollten der Anwendungsbereich dieser Richtlinie und die für ihre Anwendung maßgebenden Begriffe so genau wie möglich definiert sein.

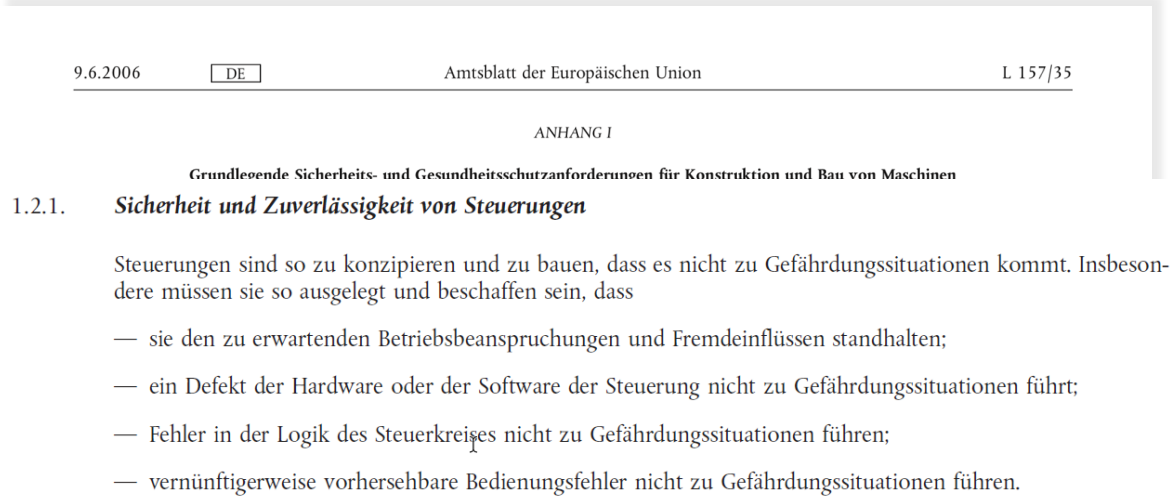
(5) Die verbindlichen Bestimmungen der Mitgliedstaaten für Baustellenaufzüge zur Personenbeförderung oder zur Personen- und Güterbeförderung, die häufig durch de facto verbindliche technische Spezifikationen und/oder durch freiwillige Normen ergänzt werden, haben nicht notwendigerweise ein unterschiedliches Maß an Sicherheit und Gesundheitsschutz zur Folge, bilden aber wegen ihrer Verschiedenheit ein Hemmnis für den innergemeinschaftlichen Handel. Zudem weichen die einzelstaatlichen Konformitätsnachweissysteme für solche Maschinen stark voneinander ab. Es ist deshalb angebracht, Baustellenaufzüge zur Personenbeförderung oder zur Personen- und Güterbeförderung nicht aus dem Anwendungsbereich der vorliegenden Richtlinie auszuschließen.

Inhalt der Maschinenrichtlinie 2006/42/EG

Anhang I

Grundlegende Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen

Allgemeingehaltene Forderungen aus Richtlinien werden in Normen konkretisiert!



9.6.2006 DE Amtsblatt der Europäischen Union L 157/35

ANHANG I

Grundlegende Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen

1.2.1. ***Sicherheit und Zuverlässigkeit von Steuerungen***

Steuerungen sind so zu konzipieren und zu bauen, dass es nicht zu Gefährdungssituationen kommt. Insbesondere müssen sie so ausgelegt und beschaffen sein, dass

— sie den zu erwartenden Betriebsbeanspruchungen und Fremdeinflüssen standhalten;

— ein Defekt der Hardware oder der Software der Steuerung nicht zu Gefährdungssituationen führt;

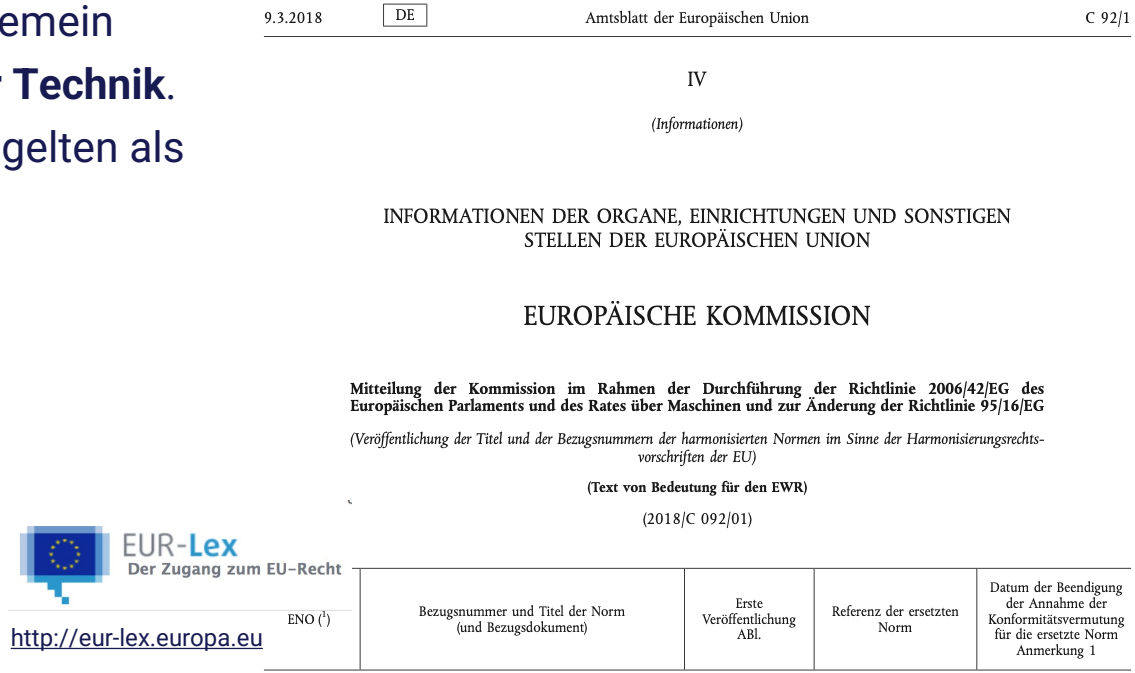
— Fehler in der Logik des Steuerkreises nicht zu Gefährdungssituationen führen;

— vernünftigerweise vorhersehbare Bedienungsfehler nicht zu Gefährdungssituationen führen.

Europäisches Recht - Normen und harmonisierte Normen

Definition Norm

- Normen gelten als allgemein anerkannte **Regeln der Technik**.
- *harmonisierte* Normen gelten als **Stand der Technik**.



9.3.2018 DE Amtsblatt der Europäischen Union C 92/1

IV

(Informationen)

INFORMATIONEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

EUROPÄISCHE KOMMISSION

Mitteilung der Kommission im Rahmen der Durchführung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates über Maschinen und zur Änderung der Richtlinie 95/16/EG

(Veröffentlichung der Titel und der Bezugsnummern der harmonisierten Normen im Sinne der Harmonisierungsrechtsvorschriften der EU)

(Text von Bedeutung für den EWR)

(2018/C 092/01)

EUR-Lex Der Zugang zum EU-Recht

http://eur-lex.europa.eu

ENO [1]	Bezugsnummer und Titel der Norm (und Bezugsdokument)	Erste Veröffentlichung ABl.	Referenz der ersetzten Norm	Datum der Beendigung der Annahme der Konformitätsvermutung für die ersetzte Norm Anmerkung 1

Normen-Typen

Typ-A-Normen ➔ **Grundnormen**

Typ-B-Normen ➔ **Gruppennormen**

Typ-C-Normen ➔ **Fach- und Produktnormen**

Typ-A-Normen

Typ-A-Normen legen grundlegende Begriffe, Terminologie und Gestaltungsleitsätze fest, die für sämtliche Maschinenkategorien anwendbar sind. Die Anwendung derartiger Normen für sich alleine reicht nicht aus, um die Übereinstimmung mit den einschlägigen grundlegenden Sicherheits- und Gesundheitsschutzanforderungen der Richtlinie zu gewährleisten, obwohl sie einen wichtigen Rahmen für die richtige Anwendung der Maschinenrichtlinie bilden und begründet daher keine umfassende Konformitätsvermutung.

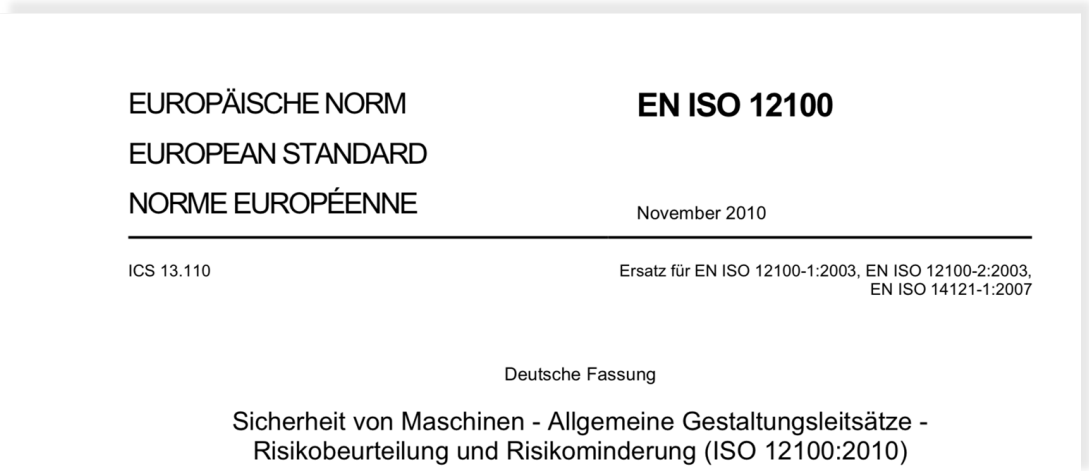
(1)	(2)	(3)	(4)	(5)
CEN	EN ISO 12100:2010 Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung (ISO 12100:2010)	8.4.2011	EN ISO 12100-1:2003 EN ISO 12100-2:2003 EN ISO 14121-1:2007 Anmerkung 2.1	30.11.2013

Typ-B-Normen

Typ-B-Normen befassen sich mit bestimmten Aspekten der Maschinensicherheit oder bestimmten Arten von Schutzeinrichtungen, die über eine große Bandbreite von Maschinenkategorien verwendet werden können. Die Anwendung der Spezifikationen von Typ-B-Normen begründet eine Konformitätsvermutung mit den hierdurch abgedeckten grundlegenden Anforderungen der Maschinenrichtlinie, wenn aus einer Typ-C-Norm oder der Risikobeurteilung des Herstellers hervorgeht, dass eine durch die Typ-B-Norm festgelegte technische Lösung für die betreffende Kategorie oder für das entsprechende Modell der Maschine angemessen ist. Die Anwendung von Typ-B-Normen, die Spezifikationen für gesondert in Verkehr gebrachte Sicherheitsbauteile enthalten, ergibt eine Konformitätsvermutung für die betreffenden Sicherheitsbauteile hinsichtlich der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen, die durch die Normen abgedeckt werden.

Typ-A-Normen

- Festlegung grundlegender Begriffe, Terminologie und Gestaltungsleitsätze
- Anwendbar auf alle Maschinenkategorien
- Alleinige Anwendung reicht nicht (...) für eine umfassende Konformitätsvermutung



EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN ISO 12100

November 2010

ICS 13.110

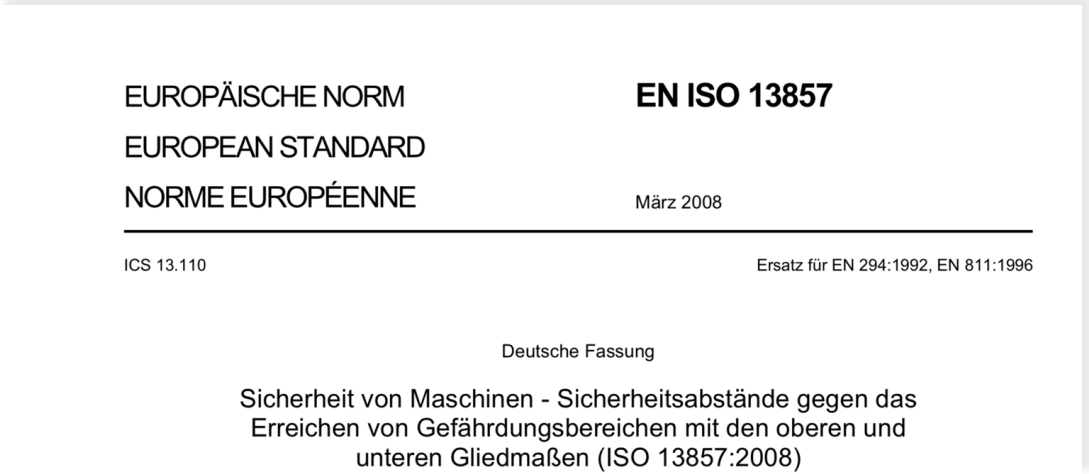
Ersatz für EN ISO 12100-1:2003, EN ISO 12100-2:2003, EN ISO 14121-1:2007

Deutsche Fassung

Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung (ISO 12100:2010)

Typ-B-Normen

- Bestimmte Aspekte der Maschinensicherheit
- Bestimmte Arten von Schutzeinrichtungen
- Begründet Konformitätsvermutung



EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN ISO 13857

März 2008

ICS 13.110

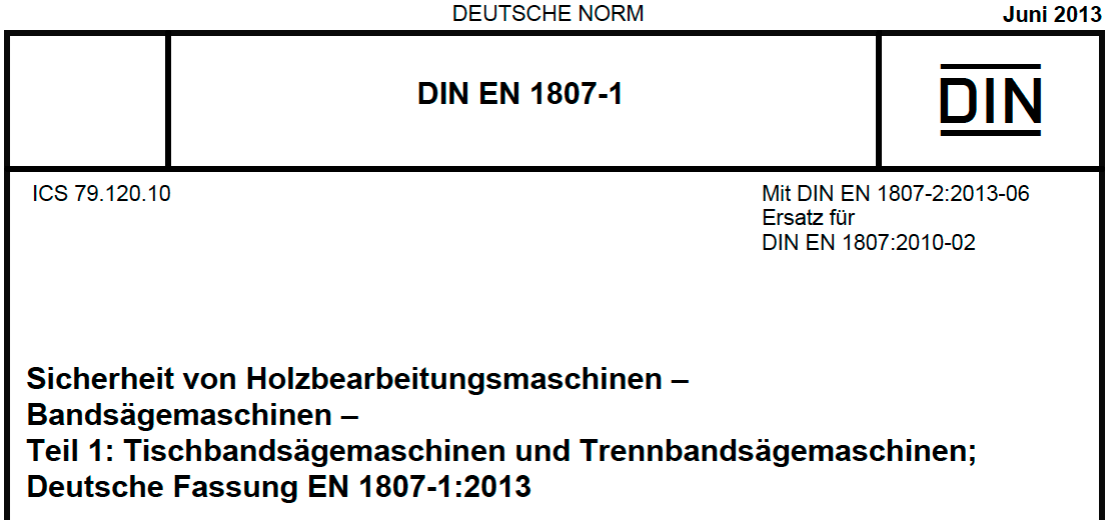
Ersatz für EN 294:1992, EN 811:1996

Deutsche Fassung

Sicherheit von Maschinen - Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen (ISO 13857:2008)

Typ-C-Normen

- Spezifikationen für eine bestimmte Maschinenkategorie
- Können Verweise auf Typ-A- oder Typ-B-Normen enthalten
- Können von den Spezifikationen der Typ-A und -B-Normen abweichen. Typ-C-Norm hat dann Vorrang.



DEUTSCHE NORM Juni 2013

DIN EN 1807-1

DIN

ICS 79.120.10

Mit DIN EN 1807-2:2013-06
Ersatz für
DIN EN 1807:2010-02

**Sicherheit von Holzbearbeitungsmaschinen –
Bandsägemaschinen –
Teil 1: Tischbandsägemaschinen und Trennbandsägemaschinen;
Deutsche Fassung EN 1807-1:2013**

Harmonisierte Normen für Steuerungen

Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015);
Deutsche Fassung EN ISO 13849-1:2015

Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen

Teil 2: Validierung

(ISO 13849-2:2012)

EN ISO 13849-1

1 Anwendungsbereich

Dieser Teil der ISO 13849 stellt Sicherheitsanforderungen und einen Leitfaden für die Prinzipien der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen (SRP/CS) bereit, einschließlich der Entwicklung von Software. Für diese Teile der SRP/CS werden Eigenschaften, einschließlich des Performance Levels, festgelegt, die zur Ausführung der entsprechenden Sicherheitsfunktionen erforderlich sind. Er ist anzuwenden auf SRP/CS aller Arten von Maschinen mit Betriebsart mit hoher Anforderungsrate und Betriebsart mit kontinuierlicher Anforderung, ungeachtet der verwendeten Technologie und Energie (elektrisch, hydraulisch, pneumatisch, mechanisch, usw.).

Er legt nicht fest, welche Sicherheitsfunktionen oder Performance Level für einen speziellen Fall verwendet werden.

Dieser Teil der ISO 13849 stellt spezielle Anforderungen für SRP/CS mit programmierbar elektronischem(n) System(en) bereit.

Er stellt keine speziellen Anforderungen an den Entwurf von Produkten, die Teile von SRP/CS sind. Trotzdem können die angegebenen Prinzipien, wie Kategorien oder Performance Level, verwendet werden.

EN ISO 13849-2

1 Anwendungsbereich

Dieser Teil von ISO 13849 legt die Vorgehensweisen und Bedingungen fest, die bei der Validierung durch Analyse und Prüfung zu befolgen sind, für

— die festgelegten Sicherheitsfunktionen;

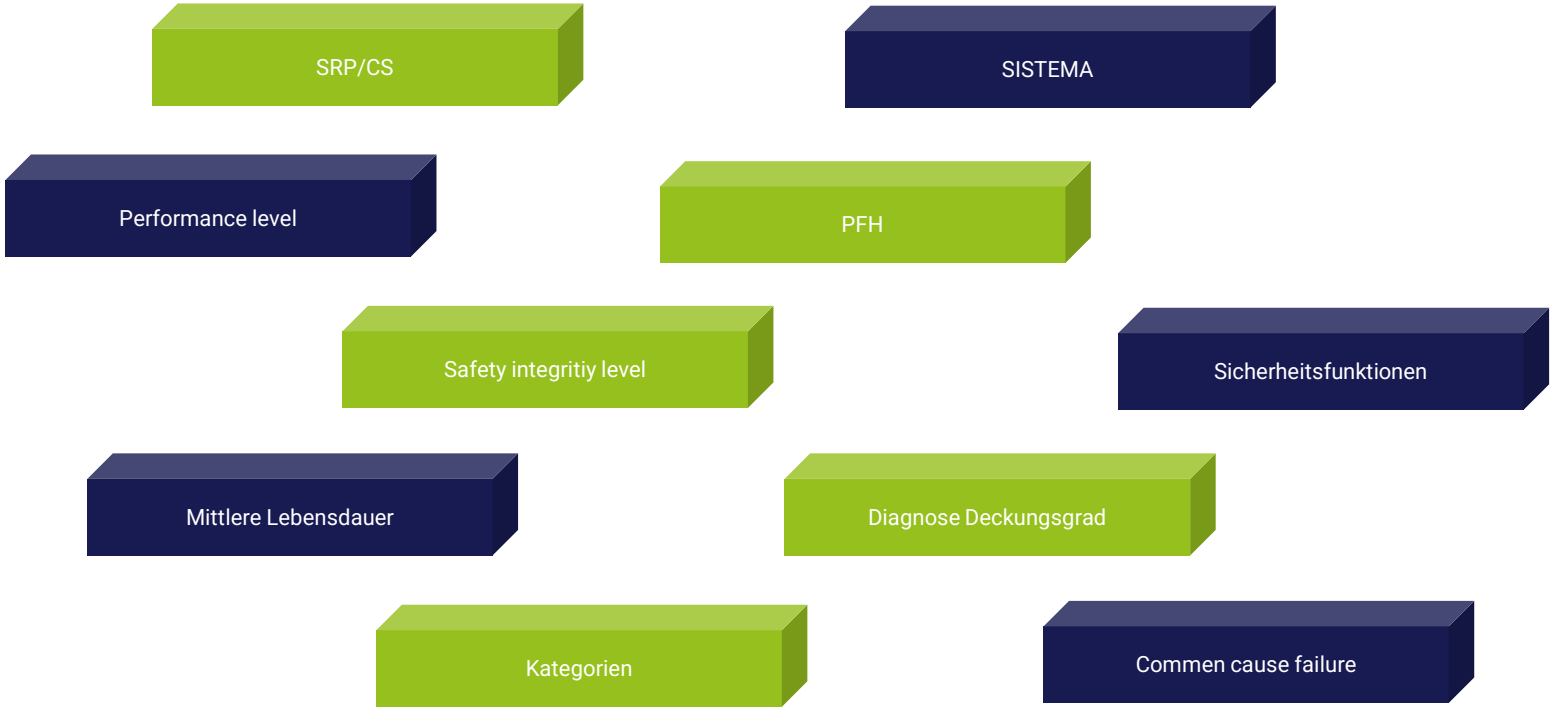
— die erreichten Kategorien, sowie

— den erreichten Performance Level

der sicherheitsbezogenen Teile der Steuerung (SRP/CS), die in Übereinstimmung mit ISO 13849-1 entwickelt wurden.

Funktionale Sicherheit

Was ist funktionale Sicherheit?



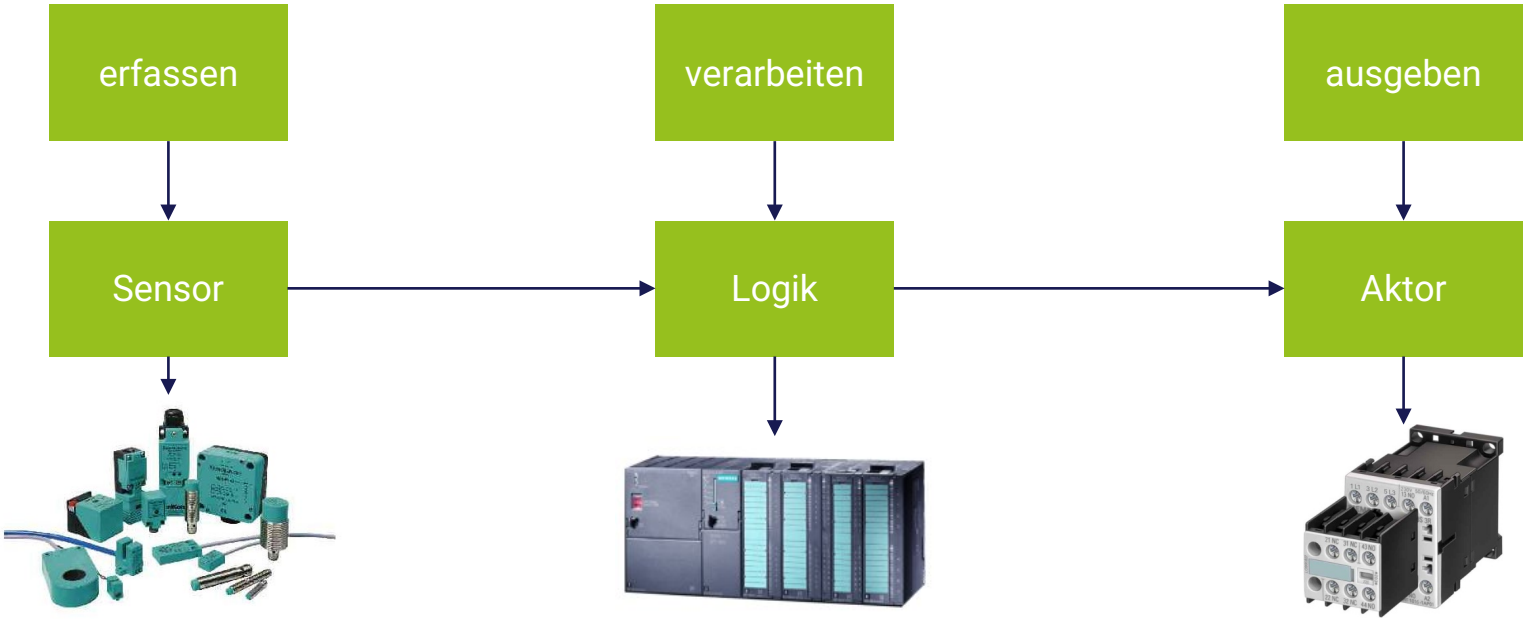
Design von SRP/CS

Was bedeutet SRP / CS?

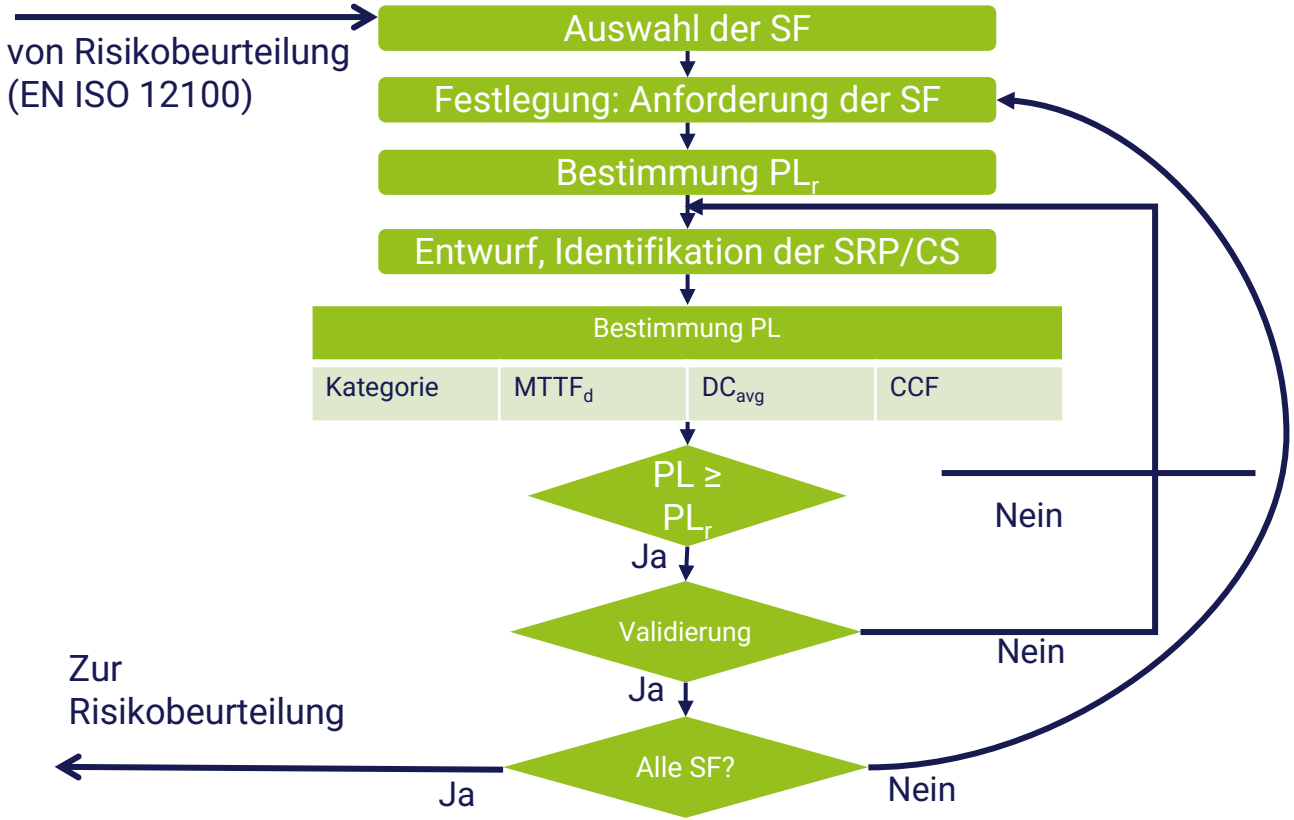
Safety- related part of a control system (Sicherheitsbezogene Teile von Steuerungen)

Sicherheitsfunktionen und Steuerung

- Sicherheitsfunktionen dienen zur Reduzierung des Risikos
- Sicherheitsfunktionen werden von sicherheitsbezogenen Teilen eines Steuerungssystems (SRP/CS) ausgeführt



Iterativer Entwurfs- und Entwicklungsprozess

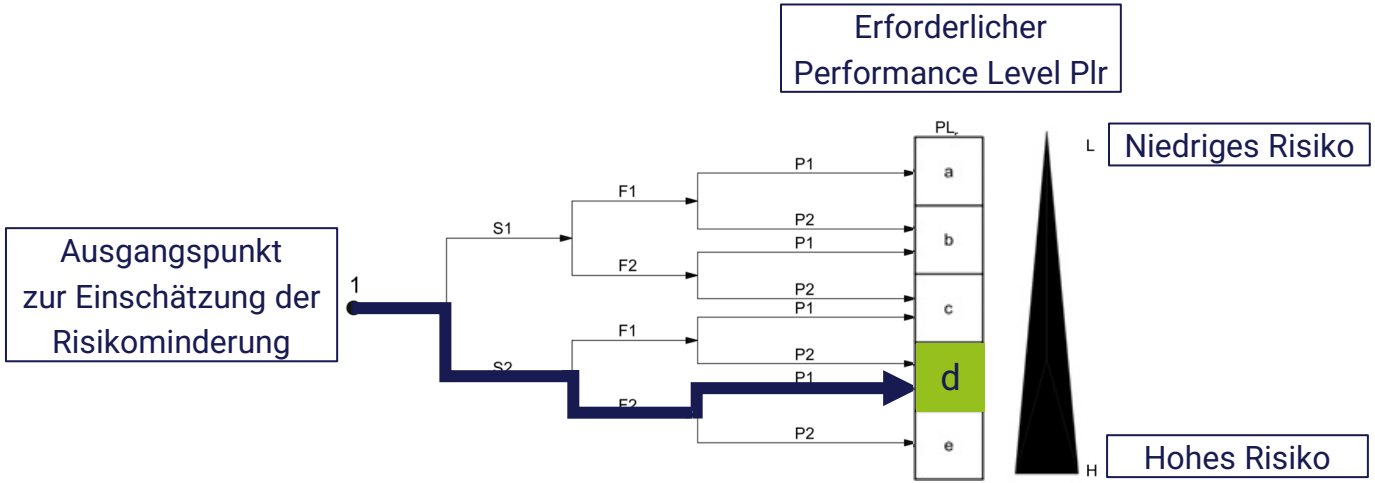


Design von SRP/CS

Performance level (PL)
Diskreter Level, der verwendet wird, um die Fähigkeit von sicherheitsbezogenen Teilen von Steuerungssystemen zu spezifizieren, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen.

„Indikator für die Zuverlässigkeit von Steuerungssystemen.“

Wie wird der Performance Level ermittelt?



S	Schwere der Verletzung	Reversibel S1
		irreversible oder Tod S2
F	Häufigkeit und/oder Dauer der Gefährdungsexposition	selten oder kurz F1
		häufig oder von langer Aufenthalt F2
P	Möglichkeit zur Vermeidung oder Begrenzung	möglich P1
		kaum möglich P2

Kategorien

Vorgesehene Architektur nach Kategorien:

- B: Ein Fehler kann zum Verlust der Sicherheitsfunktion führen
- 1: Wiederstand gegen Fehler wird durch Auswahl von bewährten Bauteilen erreicht
- 2: Zusätzlich zu 1 werden durch eine weiter Testeinrichtung Fehler detektiert
- 3: Ein einzelner Fehler darf nicht zum Verlust der Sicherheitsfunktion führen, Redundante Ausführung (2-Kanaligkeit)
- 4: Zusätzlich zu 3 muss eine höhere Widerstandsfähigkeit gegen Fehleranhäufung gewährleistet sein.

$MTTF_d$

Mean time to dangerous failure eines jeden Kanals($MTTF_d$)

Der MTTFd-Wert gibt die mittlere Ausfall Wahrscheinlichkeit von Bauteilen innerhalb eines Kanals an. Diese Werte werden in Abhängigkeit der Herstellerdaten der einzelnen Bauteile ermittelt.

$MTTF_D$ für jeden Kanal	
Bezeichnung	**Bereich**
Nicht angemessen	0 Jahre ≤ $MTTF_D$ < 3 Jahre
Niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
Mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
Hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre
nur in Kategorie 4 zulässig	100 Jahre < $MTTF_D$ ≤ 2 500 Jahre

DC

Diagnostic coverage (DC)

Der Diagnose Deckungsgrad ist das Maß für die Wirksamkeit der Diagnose.
Dieser Wert ist das Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und der Ausfallrate der gesamten gefährlichen Ausfälle.

➔ **Für einen vereinfachten Ansatz zur Schätzung von DC siehe Anhang E der EN ISO 13849-1.**

Diagnosedeckungsgrad (*DC*)	
Bezeichnung	**Bereich**
kein	$DC < 60\,\%$
niedrig	$60\,\% \leq DC < 90\,\%$
mittel	$90\,\% \leq DC < 99\,\%$
hoch	$99\,\% \leq DC$

Ausfallwahrscheinlichkeit von Steuerungen

- Bremslicht redundante ausgeführt
- Die Funktion einer Leuchte allein genügt
- Lebensdauer der Leuchte ca. 1 Jahr

Ausfallwahrscheinlichkeit von Steuerungen

- Situation nach ca. 1 Jahr
- Wie kann der Nutzer reagieren?
- Was wäre sinnvoll zur Aufrechterhaltung der Funktion?

Ausfallwahrscheinlichkeit von Steuerungen

- Situation nach einem guten Jahr ohne Leuchtenwechsel
- Warum hat die Zweifach-Redundanz nicht geholfen?

CCF

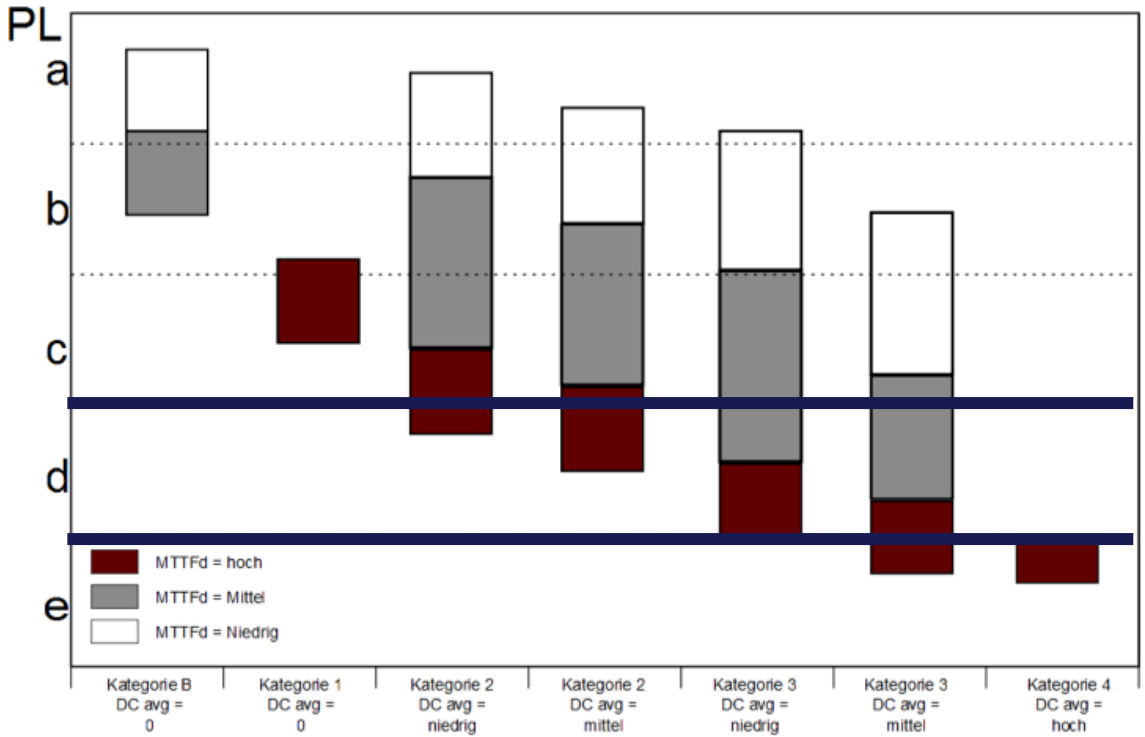
Comon Cause Failure (CCF)

Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle nicht auf gegenseitiger Ursache beruhen.

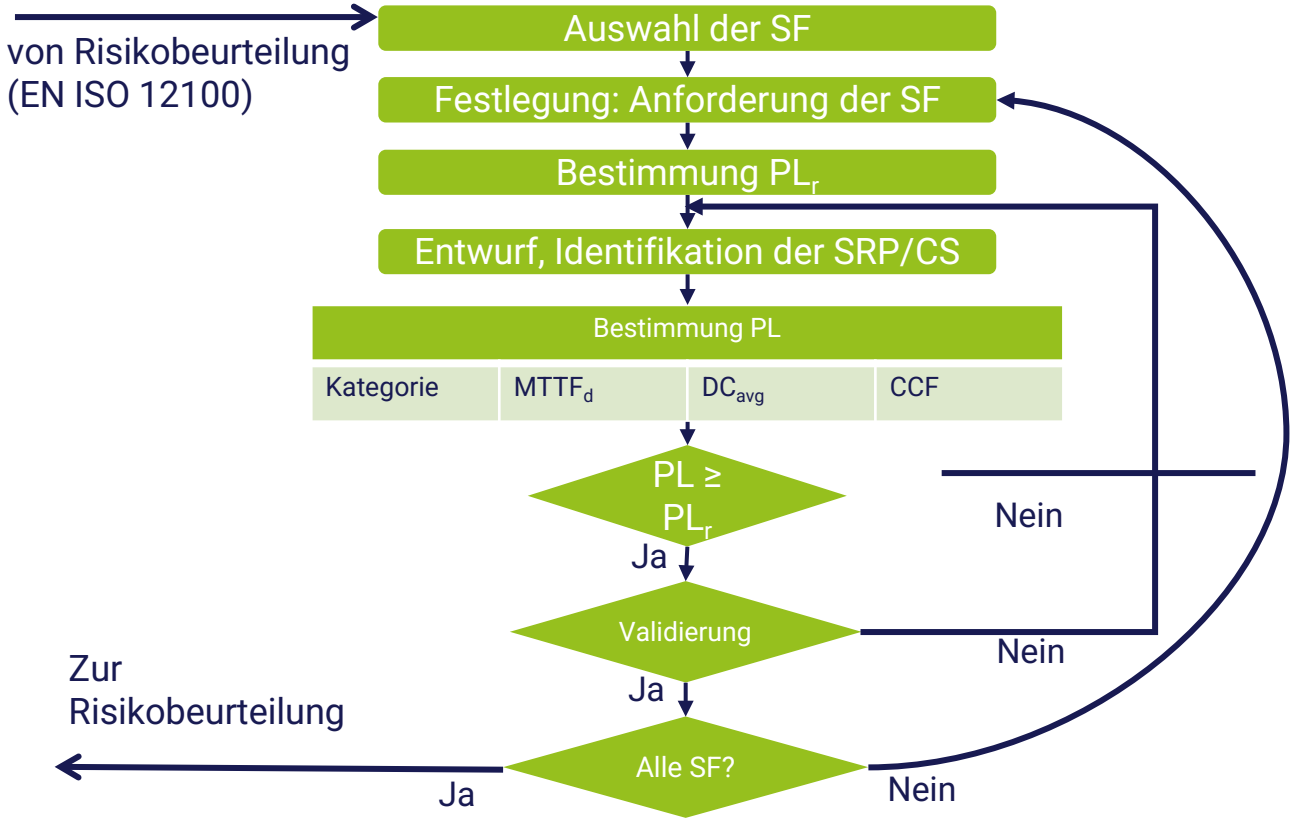
Physikalische Maßnahmen zum verhindern von Fehlern.
Wie z.B.
- Umgebungsbedingungen (Temperatur, Feuchtigkeit etc.)
- Kompetenz (Ausbildung des Konstrukteurs)
- Gestaltung (Überspannungsschutz)

und vieles mehr.

SRP/CS – Performance Level



Iterativer Entwurfs- und Entwicklungsprozess



Angabe der Ausfallwahrscheinlichkeit

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde

PFH

In h^{-1}

Average **p**robability of a dangerous **f**ailure per **h**our

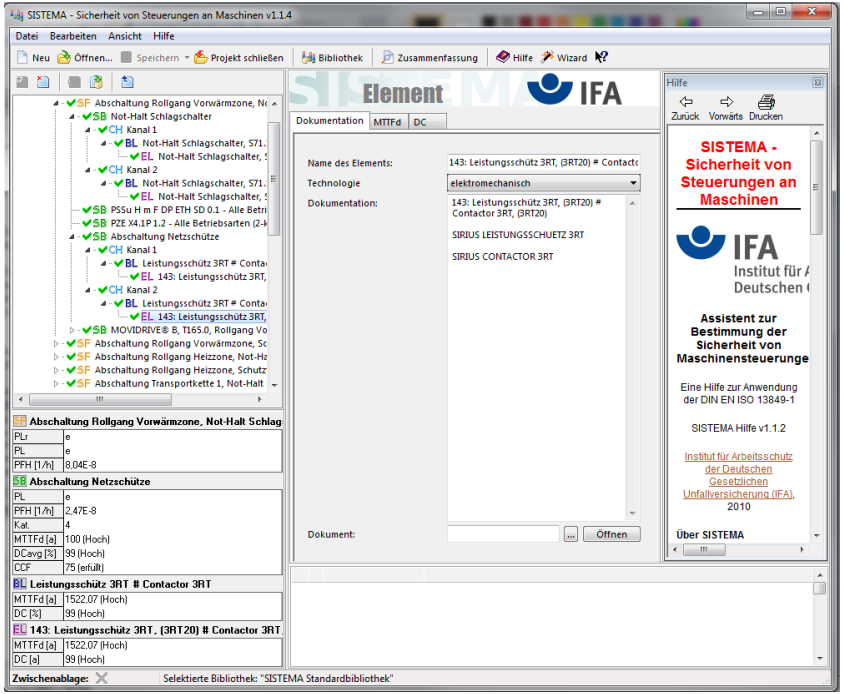
SRP/CS – Performance Level

Performance Level

- Schaltungs-Design
- Bauteildaten
- Fehlererkennung
- PLr = PL?

Hilfsmittel:

- **SISTEMA**



Validierung sicherheitsbezogener Software

Wenn Software für die Sicherheitsfunktion(en) maßgeblich ist, muss die Software-Dokumentation Folgendes enthalten:

- eine Spezifikation, die klar und eindeutig ist, und die die sicherheitstechnische Leistungsfähigkeit, die die Software erreichen muss, angibt,
- den Nachweis, dass die Software so gestaltet ist, dass sie den erforderlichen Performance Level erreicht und
- Einzelheiten über Prüfungen (insbesondere Prüfberichte), die durchgeführt wurden, um nachzuweisen, dass die geforderte sicherheitstechnische Leistungsfähigkeit erreicht wurde.

Validierung sicherheitsbezogener Software

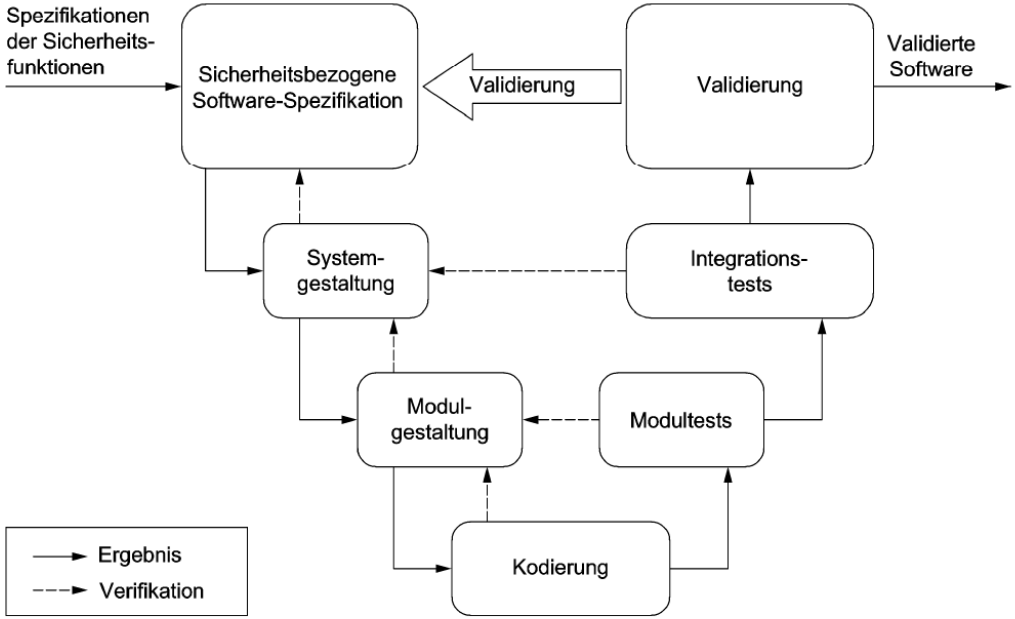
Wann ist dies Maßgebend?

Wenn menschliche Fehler in der Programmierung entstehen können.

Insbesondere bei:
- Verwendung einer speicherprogrammierbaren Sicherheitssteuerung (F-CPU, sichere Kleinsteuerungen, etc.)

Jedoch nicht bei:
- Bei vorprogrammierten Sicherheitssteuerung (Sicherheitsschaltgeräte)

Generelles Vorgehen



ANMERKUNG Anhang J zeigt detailliertere Empfehlungen für Tätigkeiten des Lebenszyklus.

Bild: EN ISO 13849-1

Abschaltmatrix

Erstellung:

1. Auflistung aller sicherheitsrelevanten Hardware Ein- und Ausgängen inkl. BMK und Softwareadresse

2. Eintragung der Abschaltungen nach Vorgabe des Sicherheitskonzeptes bzw. der Risikobeurteilung

3. Ggf. Eintragung weiterer Vorgaben wie z.B. Stopp-Kategorie, Energieart usw.

Abschaltmatrix

Validierung / Verifizierung an der Maschine:

1. IO-Check -> Test aller Ein- und Ausgänge an der Maschine
2. Überprüfung **aller** Abschaltungen gemäß der Abschaltmatrix (nicht nur punktuell)
3. Verifikation der relevanten Anforderungen aus der Risikobeurteilung / des Sicherheitskonzeptes
    - Sind die Herstellervorgaben der eingesetzten Steuerung erfüllt?
    - Ist der Sicherheitsausdruck vorhanden?
    - Wurde ein Passwortschutz vergeben?
    - Wurden Reaktionszeiten der Steuerung berücksichtigt?
    - Wurden bei der Programmierung die vorgegebenen, zertifizierten Bibliotheksbausteine des Herstellers verwendet?
    - Existiert ein sinnvolles Quittierungs-Konzept?
    - Stimmten die Produkt- / Projektinformationen überein (passt die Abschaltmatrix zum Schaltplan und zur Risikobeurteilung)?

Verifikation / Validierung

Sicherheitssoftware

- Aufbau
- Funktionsweise
- Fehlererkennung

Bild: IFA

Technische Dokumentation

F-Signatur der Soft- und Hardware nach erfolgter Validierung / Verifizierung des Auslieferungszustandes dokumentieren
-> Schützt vor Haftungsansprüchen

Notwendig um nachträgliche Manipulation oder Eingriffe in die Sicherheitssteuerung nachweisen zu können!

Teil der internen Dokumentation

Verifikation / Validierung

Was muss geprüft werden?

- Produktdaten
- Anwendbare Richtlinien
- Angewandte Normen
- Risikobeurteilung
- Performance Level
- Software
- Betriebsanleitung
- Piktogramme
- Konformitätserklärung

Hilfsmittel

Dokumentenablage

- **Software**
- **Checklisten**
- **Strukturierte Datenablage**
  - Fileserver
  - Dokument Management System
- **Zugriffsrechte vergeben**

Vielen Dank
für Ihre Aufmerksamkeit!

Ihre Ansprechpartner in

Bremen
Lloydstr. 4-6
28217 Bremen
T 0421 944 067 – 40

Augsburg
Am Alten Schlachthof 1
86153 Augsburg
T 0821 567 280 – 0

Besuchen Sie uns online!

www.ce-con.de

www.facebook.com/CECONTeam

www.xing.com/companies/ce-congmbh

www.linkedin.com/company/ce-con

Weitere Schulungsangebote

CE-Beauftragter

In 3 Tagen zum
CE-Experte

Functional Safety Engineer

Praktische Umsetzung
von Schutzmaßnahmen

Certified LoTo Expert

In 3 Tagen zum
LoTo-Experte