Grundwissen

Sichere Maschinen

DDOC00626

THE KNOW-HOW FACTORY

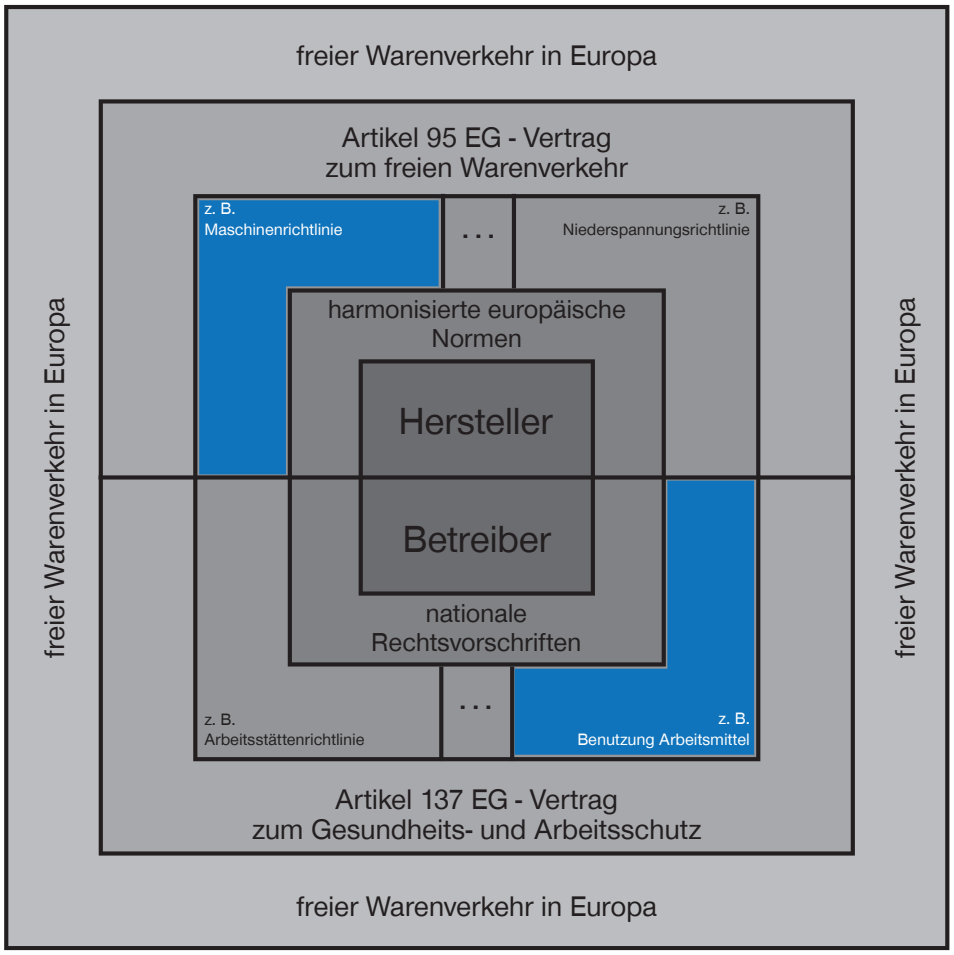
Inhalt

DDOC00626 / a DE / 30.01.2023

Zimmer GmbH · Im Salmenkopf 5 · 77866 Rheinau · +49 7844 9138 0 · +49 7844 9138 80 · www.zimmer-group.com

1. Gesetzliche Grundlagen

Der Maschinenbau ist ein wichtiger technischer Teilsektor und einer der industriellen Kernbereiche der Wirtschaft in der Gemeinschaft. 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 Machinen sachgerecht installiert und gewartet werden.



1.1 Das europäische Regelwerk

Produkte müssen so gebaut werden, dass Mensch, Tier und Umwelt vor Schäden geschützt sind. Darauf ist das europäische Regelwerk ausgelegt.

1.2 Die CE-Kennzeichnung

Mit der CE-Kennzeichnung erklärt der Hersteller, Inverkehrbringer oder EU-Bevollmächtigte gemäß EU-Verordnung, dass das Produkt den geltenden Anforderungen genügt, die in der Rechtsvorschrift der Gemeinschaft über ihre Anbringung festgelegt sind.

Das CE-Kennzeichen ist ein Symbol der Freiverkehrsfähigkeit innerhalb der EU.
Die CE-Kennzeichnung ist rechtlich kein Gütesiegel (Qualitätszeichen), sondern dokumentiert lediglich die Einhaltung der gestzlichen Mindesanforderungen.

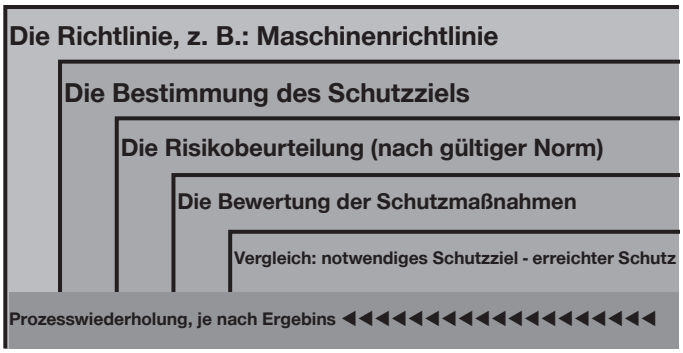
Zimmer GmbH · Im Salmenkopf 5 · 77866 Rheinau · +49 7844 9138 0 · +49 7844 9138 80 · www.zimmer-group.com

2. Der Weg zur sicheren Maschine

⇨ Gefahr erkennen

⇨ Risiko bewerten

⇨ Risiko mindern



Unternehmen, wie die Zimmer Group, die Produkte herstellen, die dem Geltungsbereich der Europäischen Maschinenrichtlinie unterliegen und die ein, nach ISO 9001 zertifiziertes, Qualitätsmanagementsystem nachweisen können, führen ein Konformitätsbewertungsverfahren nach Anhang VIII der Maschinenrichtlinie durch.

Bestandteil dieses entwicklungsbegleitenden Verfahrens ist eine Risikobeurteilung.

Diese Risikobeurteilung analysiert Gefahrenstellen, beurteilt die davon ausgehenden Risiken, bestimmt Maßnahmen zur Risikominimierung und wiederholt die Bewertung so lange, bis eine ausreichende Risikominderung nachgewiesen werden kann.

Risiko = Schwere des möglichen Schadens + Wahrscheinlichkeit des Eintretens

DDOC00626 / a DE / 30.01.2023

Zimmer GmbH · Im Salmenkopf 5 · 77866 Rheinau · +49 7844 9138 0 · +49 7844 9138 80 · www.zimmer-group.com

2.1 Sichere Maschine - relevante Normen (Auszug, nicht vollständig)

EN ISO 12100	Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung
EN 60204-1	Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen
EN 62061	Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronsicher Steuerungssysteme
DIN EN ISO 13849-1/-2	Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen (Teil 1 und 2)

<table>
<tr><td>Konstruktion und Risikobewertung der Maschine</td><td>Elektrische Sicherheitsaspekte</td></tr>
<tr><td>EN ISO 12100

Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung</td><td>EN 60204-1

Sicherheit von Maschinen - Elektrische Aurüstung von Maschinen</td></tr>
<tr><td>⇩</td><td>⇩</td></tr>
<tr><td colspan="2">Entwurf und Realisierung sicherheitsbezogener Steuerungen</td></tr>
<tr><td colspan="2">EN 62061
Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronsicher Steuerungssysteme</td></tr>
<tr><td colspan="2">Beliebige Architektur (Sicherheits-Integritätslevel (SIL))</td></tr>
<tr><td colspan="2">DIN EN ISO 13849-1
Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen (Teil 1)</td></tr>
<tr><td colspan="2">Vorgesehene Architekturen (Steuerungskategorien/Performance Level (PL))</td></tr>
</table>

3. Performance Level, Ausfall, Diagnose und Co.

Der Performance Level (PL) ist eine Funktion von:

- angewendeter Steuerungskategorie (Kat. B bis 4)
- dem Diagnosedeckungsgrad (DC)
- der mittleren Betriebsdauer bis zum Ausfall ($MTTF_d$)
- den Fehlern gemeinsamer Ursache (CCF)

Das bedeutet, dass für ein einzelnes Produkt der PL immer nur im zusammenhang mit der eingesetzten Steuerungsachitektur sowie den anwendungsbezogenen Daten errechnet werden kann!

3.1 $B10_d$-Wert

Der $B10_d$-Wert ist der Zeitpunkt, bei dem statistisch gesehen 10% der Prüflinge ausgefallen sind. In Bezug auf die Maschinensicherheit sind nur die gefährlichen Ausfälle relevant.
Die ISO 13849-1 erlaubt die Annahme, dass jeder zweite Ausfall gefährlich ist. Daher kann angenommen werden:

$$B10_d = 2 \times B_{10}$$

In den Katalogen und den Montage- und Betriebsanleitungen wird daher der $B10_d$-Wert unserer Produkte angegeben. Die Zimmer Group ermittelt diesen Wert in eigenen Testlaboren bzw. in Zusammenarbeit mit benannten Stellen.

3.2 $MTTF_d$-Wert

mittlere Betriebsdauer bis zum Ausfall (mean time to failure)
Der Wert der $MTTF_d$ jedes Kanals wird in drei Stufen angegeben (siehe Tabelle „5“) und muss für jeden Kanal individuell berücksichtigt werden (z. B. einzelner Kanal oder jeder Kanal eines redundanten Systems).

Für alle Produkte, die in sicherheitsbezogene Teile, Maschinen oder Anlagen von Steuerungen eingebaut werden und die direkt an der Sicherheitsfunktion mitwirken, muss dieser Wert nach folgender Formel berechnet werden:

$$MTTF_d = \frac{B10_d}{0{,}1 \times n_{op}}$$

Dabei lässt die Variable n_{op} erkennen, dass dieser Wert unmittelbar mit den Betriebsbedingungen beim Anwender zusammenhängt.
n_{op} = mittlere Anzahl jährlicher Betätigungen
d_{op} = Betriebstage/Jahr
h_{op} = Betriebsstunden/Tag
t_{cycle} = Zykluszeit in [s]

$MTTF_d$-Wert für unterschiedliche Kanäle, Symmetrisierung der $MTTF_d$ für jeden Kanal:

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} + MTTF_{dCn} \ldots - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}} + \frac{1}{MTTF_{dCn}} \ldots}\right]$$

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{cycle}}$$

DDOC00626 / a DE / 30.01.2023

Zimmer GmbH · Im Salmenkopf 5 · 77866 Rheinau · +49 7844 9138 0 · +49 7844 9138 80 · www.zimmer-group.com

Folgend ist ein Auzug der Tabelle „5“ „mittlere Zeit jedes Kanals bis zum gefahrbringenden Ausfall“ (MTTF) aus der EN ISO 13849-1.

$MTTF_d$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_d$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_d$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_d$ < 100 Jahre

3.3 DC-Wert

Diagnosedeckungsgrad = Maß für die Wirksamkeit der Diagnise des Prozesses.
Dabei werden die erkannten gefährlichen Ausfälle zu den gesamten gefährlichen Ausfällen ins Verhältnis gsetzt.

$$DC = \frac{\sum (\text{erkannte gefährliche Fehler}}{\sum (\text{erkannte gefährliche Fehler}}$$

Der gesamte Diagnosedeckungsgrad kann sich dabei aus der Summe der Werte der Einzelelemente (1 ... n) einer Steuerungsachitektur zusammensetzen.

$$DC = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dn}}}$$

Dem Diagnosedeckungsgrad kommt bei der Wahl der notwendigen Steuerungskategorie entscheidende Bedeutung zu. Für die Kategorie B und 1 ist dieser Wert nicht relevant.

Zur Abschätzung des DC können beispielsweise die Ausfallarten- und Effektanalysen (FMEA) nach ISO 60812 angewendet werden.

Ein vereinfachter Ansatz zur Einschätzung des DCs bietet die EN ISO 13849-1 im Anhang E.

Angegeben wird der DC in vier Stufen: kein, niedrig, mittel, hoch

Wird der DC durch bessere Diagnosemaßnahmen erhöht, kann bei gleicher Steuerungsarchitektur ein höherer PL erreicht werden.

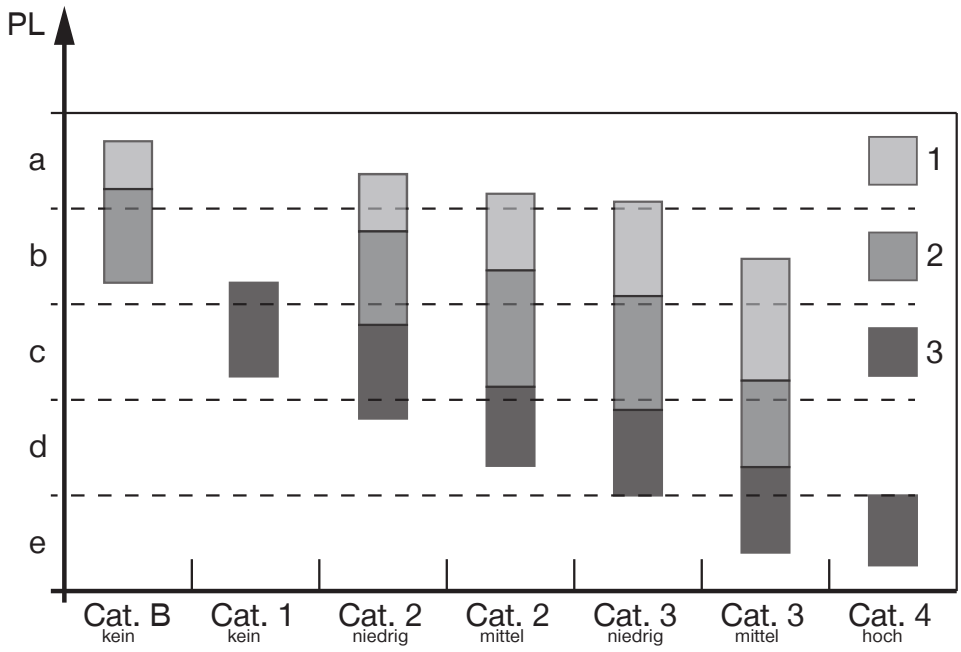
3.4 Diagnosedekungsgrad / Sicherheitsarchitektur

Der Diagnosedeckungsgrad (DC) gibt an, mit welcher Wahrscheinlichkeit die Fehler durch einen Test übermittelt werden. Die Sicherheitssysteme (Testkanäle) können einkanalig, zweikanalig oder mehrkanalig aufgebaut sein.
Während einkanalige Sicherheitssysteme in der Regel nur auf Fehler mit einem Versagen reagieren, so prüfen sich zwei- oder mehrkanalige Sicherheitssysteme gegenseitig und erkennen eventuelle Fehler.

Die Einordnung des Diagnosedekungsgrads geschieht in den Stufen „klein“, „niedrig“, „mittel“ und „hoch“.
Einzelne Diagnosedeckungsgrade sind aus der Tabelle E1 der EN ISO 13849 abzulesen.
Folgend ist ein Auzug der Tabelle 6 des Diagnosedeckungsgrads aus der EN ISO 13849.

Diagnosedeckungsgrad (DC)	
Bezeichnung	**Bereich**
klein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Beziehung zwischen den Kategorien DC, MTTFd jedes Kanals und PL:



PL	Performance Level
1	$MTTF_d$ jedes Kanals = niedrig
2	$MTTF_d$ jedes Kanals = mittel
3	$MTTF_d$ jedes Kanals = hoch

Die Abbildung oben zeigt die unterschiedlichen möglichen Kombinationen zur Abschätzung der Kategorie mit DC (horizontal Achse) und $MTTF_d$ jedes Kanals (Balken). Die Balken im Diagramm zeigen die drei $MTTF_d$-Bereiche jedes Kanals (niedrig, mittel, hoch), die gewählt werden können, um den erforderlichen PL zu erreichen.

4. Beispiele für Steuerungskategorien

Die hier gezeigten Steuerungsbeispiele sind nicht zu 100% auf die kundenspezifischen Anforderung übertragbar. Sie sind lediglich eine beispielhafte Darstellung zum Erreichen des benötigten PL nach EN ISO 13849-1.
Für die Realisierung der Sicherheitsfunktion ist die Verwendung „bewährter Bauteile“, wie sie im Kapitel 6.2.4 der EN ISO 13849-1 beschrieben werden, ausreichend.

⇨ Wird ein Ventil zur Ansteuerung eines Produkts in einer einkanaligen Steuerungsachitektur mit einem Druckschalter überwacht, kann das maßgeblich zur Erhöhung der Maschinensicherheit beitragen.
⇨ Beispielhaft ist das an der Tabelle Kapitel 4.5.4 in EN ISO 13849-1 erkennbar. Hier erkennbar am erhöhten PL d in der Kategorie 2.
⇨ Ohne die beschriebene Überwachungsmaßnahme (also kein DC) wäre nur PL b/c in der Steuerungskategorie 1 erreichbar.

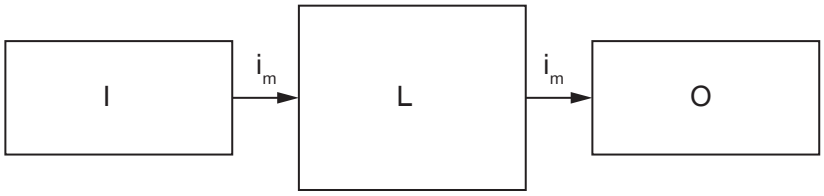
4.1 Steuerungskategorie B

In Sicherheitssystemen der Steuerungskategorie „B“ gibt es keinen DC (DC_{avg} = kein) und die $MTTF_d$ jedes Kanals kann „niedrig“ bis „mittel“ sein. In solchen Sicherheitssystemen (üblicherweise einkanalige Systeme) ist die Betrachtung von Ausfällen infolge gemeinsamer Ursachen (CCF) nicht relvant.
Der maximal erreichbare PL, der mit der Kategorie „B“ erreicht werden kann, ist „PL = b“.

⇨ DAS AUFTRETEN EINES FEHLERS KANN ZUM VERLUST DER SICHERHEITSFUNKTION FÜHREN.
⇨ Kapitel 6.2.3 der EN ISO 13849-1

Besondere Anforderungen an die elektromagnetische Verträglichkeit sind in den entsprechenden Produktnormen, zum Beispiel IEC 61800-3 über Abtriebssysteme, zu finden. Besonders für die funktionale Sicherheit der SRP/CS sind die Anforderungen an die Störfestigkeit wichtig.
Wenn keine Produktnorm vorhanden ist, sollten zumindest die Anforderungen der IEC 61000-6-2 an die Störfestigkeit befolgt werden.

Vorgesehene Architektur für Kategorie B:



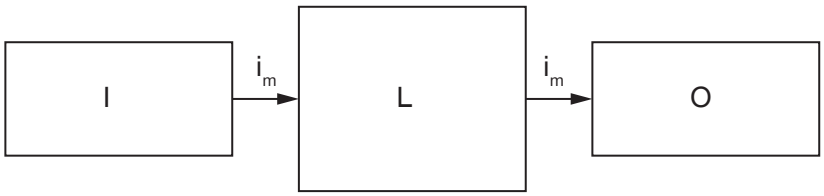
i_m	Verbindungsmittel
I	Eingabeeinheit, z. B. Sensor
L	Logik
O	Ausgabeeinheit, z. B. Hauptschütz

WARNUNG:

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.

4.2 Steuerungskategorie 1

Vorgesehene Architektur für Kategorie 1:



i_m	Verbindungsmittel
I	Eingabeeinheit, z. B. Sensor
L	Logik
O	Ausgabeeinheit, z. B. Hauptschütz

In Sicherheitssystemen der Steuerungskategorie „1“ gibt es keinen DC (DC_{avg} = kein).

WARNUNG:

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Jedoch ist die $MTTF_d$ in jedem Kanal der Steuerungskategorie „1“ größer als in Steuerungskategorie „B“.

Folglich ist der Verlust der Sicherheitsfunktion weniger wahrscheinlich.

4.3 Steuerungskategorie 2

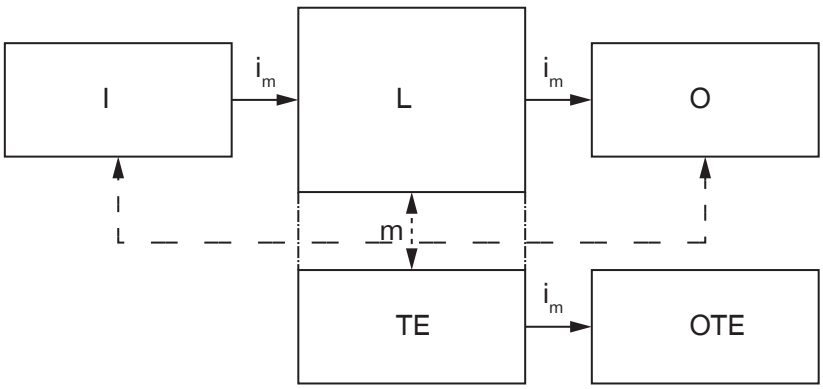
Für die Steuerungskategorie „2“ müssen die identischen Anforderungen erfüllt sein wie diese für Steuerungskategorie „B“. Zusätzlich gelten für die Steuerungskategorie „2“ noch folgende Sicherheitsprinzipien:

- SRP/CS der Steuerungskategorie „2“ müssen so gestaltet sein, dass ihre Funktion in angemessenen Zeitabständen durch die Maschinen- bzw. Anlagensteuerung getestet werden.

⇨ Der Test muss beim Anlaufen der Maschine bzw. Anlage und vor dem Einleiten einer Gefährdungssituatuion durchgeführt werden.

⇨ Die Einleitung dieses Tests kann automatisch erfolgen.

Vorgesehene Architektur für Kategorie 2:



i_m	Verbindungsmittel
I	Eingabeeinheit, z. B. Sensor
L	Logik
O	Ausgabeeinheit, z. B. Hauptschütz
m	Überwachung
TE	Testeinrichtung
OTE	Ausgang der TE

4.4 Steuerungskategorie 3

Für die Steuerungskategorie „3“ müssen die identischen Anforderungen erfüllt sein wie diese für Steuerungskategorie „B“. Zusätzlich gelten für die Steuerungskategorie „3“ noch folgende Sicherheitsprinzipien:

- SRP/CS der Steuerungskategorie „3“ müssen so gestaltet sein, dass ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion führt. Wenn immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.
- Der Diagnosedeckungsgrad (DC_{avg}) der gesamten SRP/CS einschließlich der Fehlererkennung muss niedrig sein. Die $MTTF_d$ jedes redundanten Kanal muss, abhängig vom PL_r niedrig bis hoch sein. Maßnahmen gegen CCF müssen angewendet werden (siehe EN ISO 13849-1, Anhang F).

INFORMATION:

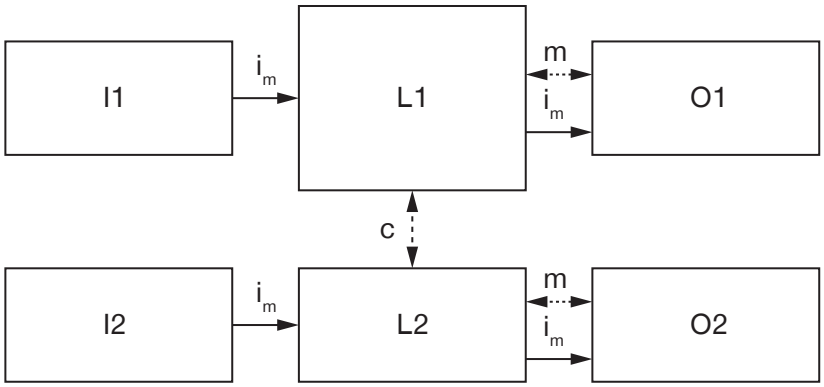
Die Anforderung an die Erkennung einzelner Fehler bedeutet nicht, dass alle Fehler erkannt werden können. Folglich kann die Anhäufung unentdeckter Fehler zu einem unbeabsichtigtem Ausgangssignal un einer Gefährdungssituation an der Maschine führen.

Das Systemverhalten der Steuerungskategorie „3“ lässt folgendes zu:

- bei Auftreten eines einzelnen Fehlers wird die Sicherheitsfunktion immer ausgeführt
- einige, aber nicht alle Fehler erkannt werden
- die Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen

Die verwendete Technologie hat Einfluss auf die Möglichkeiten zur Realisierung der Fehlererkennung.

Vorgesehene Architektur für Kategorie 3:



i_m	Verbindungsmittel
c	Kreuzvergleich
I1, I2	Eingabeeinheit, z. B Sensor
L1, L2	Logik
O1, O2	Ausgabeeinheit, z. B. Hauptschütz
m	Überwachung

Die gestrichelte Linien (m) zeigen die vernünftigerweise durchführbare Fehlererkennung!

4.5 Steuerungskategorie 4

Für die Steuerungskategorie „4“ müssen die identischen Anforderungen erfüllt sein wie diese für Steuerungskategorie „B“. Zusätzlich gelten für die Steuerungskategorie „4“ noch folgende Sicherheitsprinzipien:

- SRP/CS der Steuerungskategorie „4“ müssen so gestaltet sein, dass ...
  - ein einzelner Fehler in jedem dieser sicherheitbezogenen Teile nicht zum Verlust der Sicherheitsfunktion führt.
  - der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird, z. B. unmittelbar, beim Einschalten oder am Ende eines Maschinenzyklus.

WARNUNG:

Wenn die Erkennung von Fehlern nicht möglich ist, dann darf die Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen“.

- Der Diagnosedeckungsgrad (DC_{avg}) der gesamten SRP/CS einschließlich der Fehlererkennung muss niedrig sein. Die $MTTF_d$ jedes redundanten Kanal muss, abhängig vom PL_r niedrig bis hoch sein. Maßnahmen gegen CCF müssen angewendet werden (siehe EN ISO 13849-1, Anhang F).

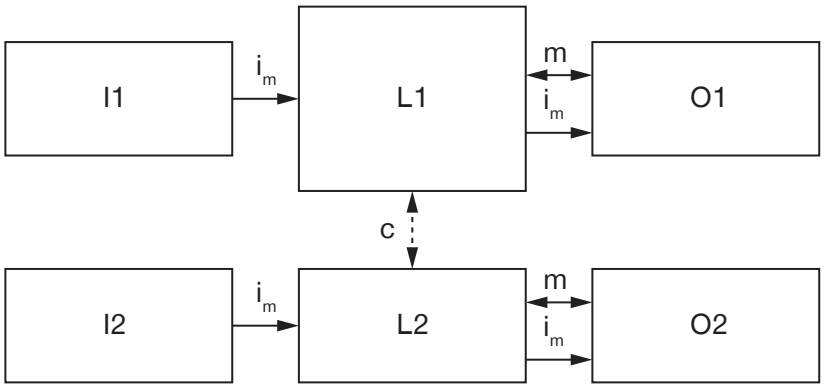
INFORMATION:

Das Systemverhalten der Steuerungskategorie „4“ lässt folgendes zu:

- bei Auftreten eines einzelnen Fehlers wird die Sicherheitsfunktion immer ausgeführt
- die Fehler rechtzeitig erkannen, um den Verlust der Sicherheitsfunktion zu verhindern
- die Anhäufung unerkannter Fehler in Betracht gezogen werden

Der Unterschied zwischen der Steuerungskategorie „3“ und „4“ ist der höhere DC_{avg} in der Steuerungskategorie „4“ und die ausschließlich erforderlichen “hohen” $MTTF_d$-Werte für jedes Element.

Vorgesehene Architektur für Kategorie 4:



i_m	Verbindungsmittel
c	Kreuzvergleich
I1, I2	Eingabeeinheit, z. B Sensor
L1, L2	Logik
O1, O2	Ausgabeeinheit, z. B. Hauptschütz
m	Überwachung

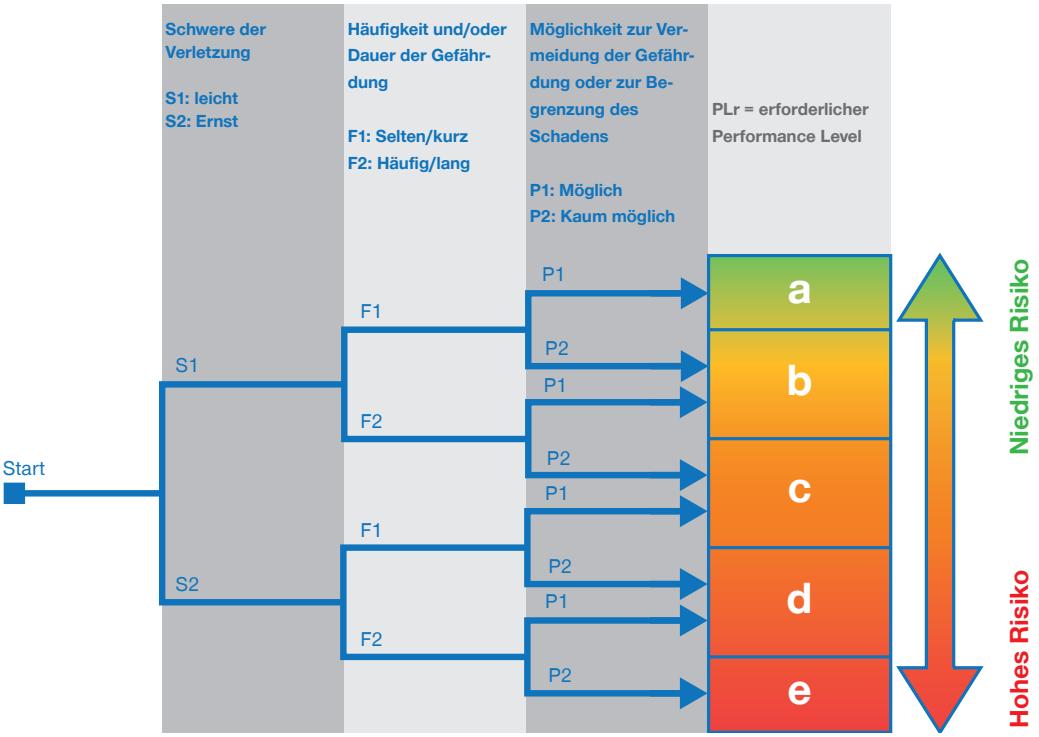
Die durchgezogennen Linien (m) für die Überwachung stellen einen höheren Diagnosedeckungsgrad als bei der vorgesehenen Architektur der Kategorie 3 dar.

4.6 Zusammenfassung der Anforderungen für Kategorien

Eine Zusammenfassung der einzelnen Anforderungen für die Kategoreien sind der Tabelle 10 der EN ISO 13849-1 zu entnehmen.

5. Erforderlicher PLr - Erreichter PL

5.1 Schritt 1

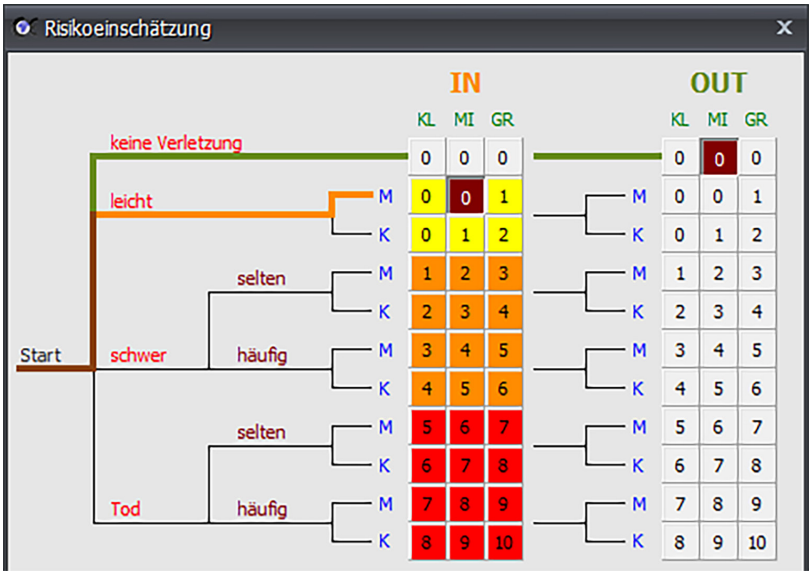


Die EN ISO 13849-1 verwendet zur Bestimmung des erforderlichen Sicheitsniveaus **PLr** ebenfalls einen Risikographen. Für die Bestimmung der Risikohöhe werden die Parameter S,F und P verwendet.
Das Ergebnis des Verfahrens ist der **erforderliche Performance Level (PLr: required Performance Level)**.
Der PLr ist in der Praxis sehr oft im Lastenheft des Kunden definiert.

HINWEIS:

Die Struktur des Risikographen zur Bestimmung des PLr begegnet uns in der Praxis bei der Beurteilung der Wirksamkeit der getroffenen Maßnahmen zur Risikobeurteilung erneut. Anstelle der Spalte für den PLr steht hier nun eine Klassifizierung der erreichten Risikominderung, in Form einer Zahl, als abstraktes Kennzeichen für die Risikohöhe.

Siehe hierzu folgende Abbildung „Risikoeinschätzung“.



5.2 Schritt 2

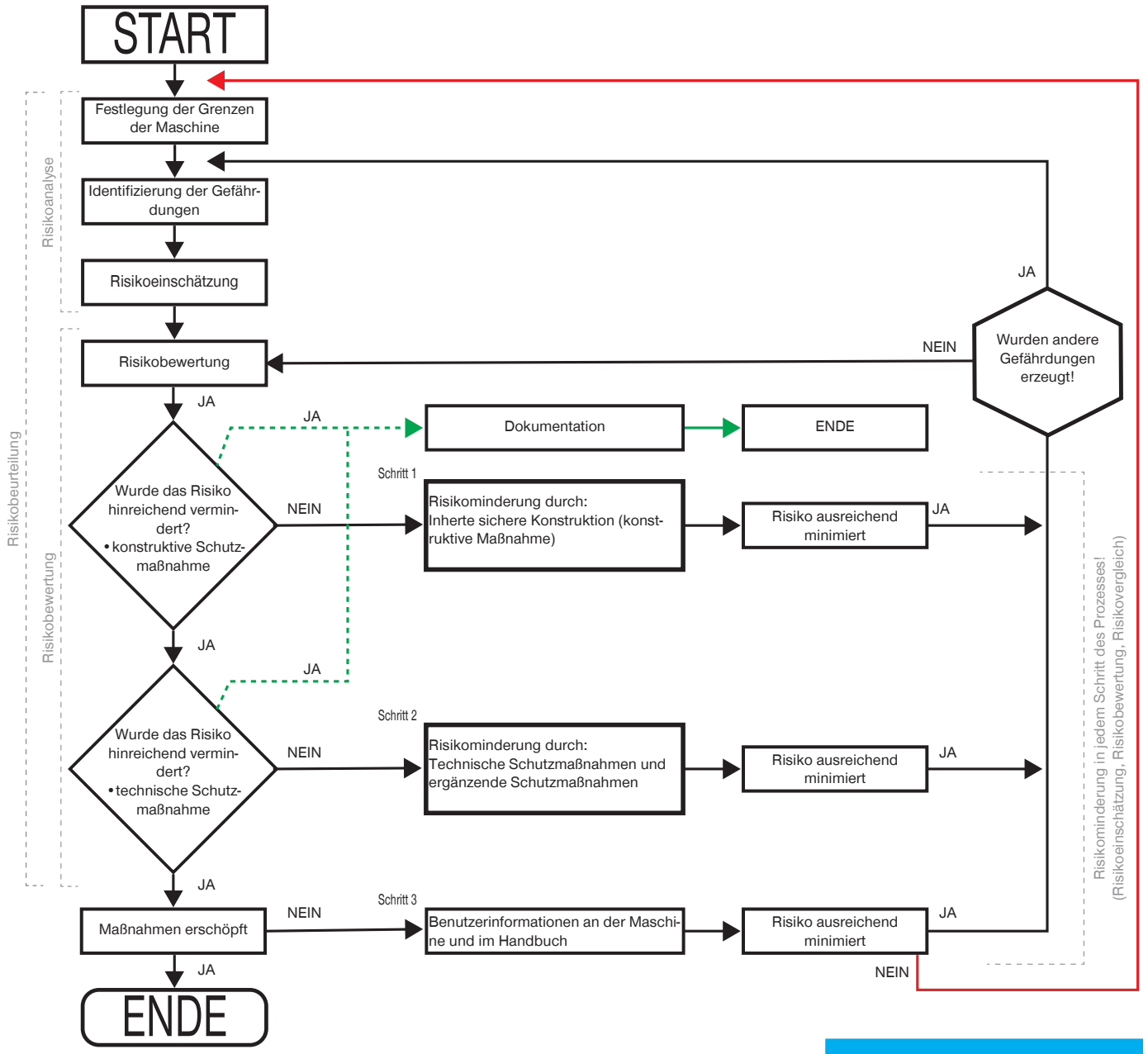
Für alle risikomindernden Maßnahmen, die **steuerungstechnische Komponente** enthalten, sind im Rahmen der Risikobeurteilung der erreichte Performance Level zu bestimmen.

Dazu steht in der Praxis beispielhaft das Programm SISTEMA der DGUV zur Verfügung.

INFORMATION:

Das Ergebnis dieser Bestimmung muss in jedem Fall lauten:

PL ≥ PLr (erreichter Performance Level ≥ erforderlicher Performance Level)



QUELLE: EN ISO 12100

6. Risikobeurteilung

Jeder Hersteller ist verpflichtet eine Risikobeurteilung für sein Produkt durchzuführen.
In der Risikobeurteilung erfolgt eine Risikobewertung, bei der entsprechende Maßnahmen zur Risikominderung durchgeführt werden müssen.
Hier liegt der Fokus im Bereich der technischen Schutzmaßnahmen, die zur Minderung beitragen.

Grenzen der Maschine:	Verwendungsgrenzen, räunliche Grenzen, zeitliche Grenzen, ...
Gefährdungen:	Ermitteln/Definieren
Risikoeinschätzung:	Eingreifen durch Personen, Betriebszustände, Unbeabsichtigtes Verhalten, vorhersehbare Fehlanwendung

Leerseite

Zimmer GmbH · Im Salmenkopf 5 · 77866 Rheinau · +49 7844 9138 0 · +49 7844 9138 80 · www.zimmer-group.com