

Um zu beurteilen, welche Vorschriften wie weit zu beachten sind, sollte der Konstrukteur (Elektro- und/oder Maschinenbautechniker bzw. Ingenieur) eine Risikobeurteilung vornehmen.

Maschinenrichtlinien EN 292: „Allgemeine Gestaltungsgrundsätze Sicherheit von Maschinen“, EN 1050: „Risikobeurteilung der Maschine“ und die EN 954-1: „Sicherheitsbezogene Teile von Maschinen“ sind hierfür anzuwenden.

EN 292 ist eine zweiteilige A-Norm. Sie lässt sich als ein Vertiefungswerk der EU-Maschinen-Richtlinie verstehen. Sicherheit von Maschinen-Grundbegriffen, allgemeine Gestaltungsgrundsätze ist der Titel der harmonisierten Norm. Die Vorschrift hilft dem Hersteller im (rechts) sichereren Bereich zu agieren. Es werden Regelungen zur Risikominderung, bezüglich technischer Schutzmaßnahmen und Benutzerinformation getroffen. Insgesamt ist die Norm eine Art pragmatischer Leitfaden zur Einhaltung der Europäischen Gesetze.

Die Risikominderung durch Konstruktion beinhaltet im Sinne des Nutzers auch ergonomische Grundsätze. Die Annahme, dass das Erfüllen der Norm bereits ein sicheres Produkt ermöglicht, ist eine Risikofalle. Wenn auch das meiste checklistenmäßig berücksichtigt ist, bleiben Gefahren aus spezifischen Nutzungskontexten und durch den allgemein gehaltenen Charakter der DIN EN 292 übrig. Es gilt auch die spezifischen B- und C-Normen zusätzlich zu beachten.

Zusätzlich zur Gefahrenanalyse nach Maschinenrichtlinie, fordert die EN 292 eine Gefährdungsanalyse. Diese stützt sich auf die EN 1050 (Sicherheit von Maschinen – Grundsätze zur Risikobeurteilung). Egal wie man es nennt, das was hinterher aufgesetzt ist, ist im Produkt/Maschinen-Entwicklungsprozess integriert, bei Weitem unterlegen. Alle gefahrenrelevanten Dokumentationspunkte lassen sich erst im Betriebszustand erfassen, denn es gelingt in den seltensten Fällen, d. h. wichtige Hinweise auf Restgefährdungen werden in der Betriebsanleitung fehlen. Im Nachhinein erzeugte Sicherheit ist mit einem mehrfachen Aufwand verbunden, da die Konstruktion in weiten Bereichen noch einmal nachvollzogen werden muss.

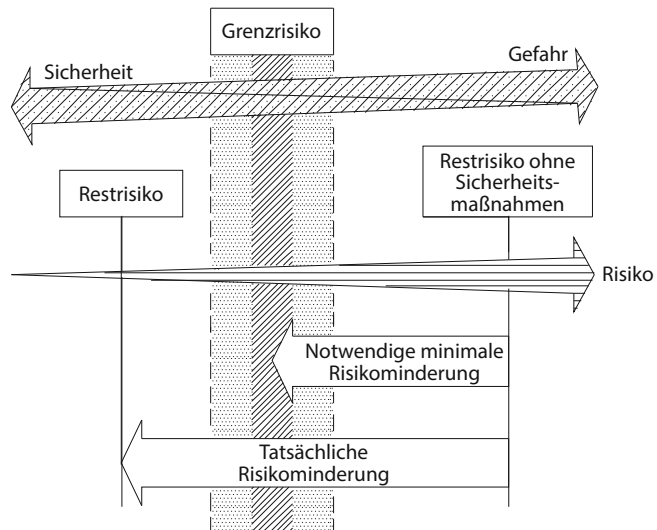
Ein geringeres Produkthaftungsrisiko und bessere Produkte/Maschinen resultieren aus dem Weg, die Gefährdungsanalyse in die Produktentwicklung zu integrieren. Die frühzeitige Modifikation am Produkt auf Grund der parallel laufenden Gefahrenanalyse weicht zwar noch von der derzeitigen Praxis ab, bietet jedoch zahlreiche Mehrwerte.

2.1 Grenzrisiko

Die Norm EN 1050 geht davon aus, dass jede Maschine ein Risiko beinhaltet, und zwar das Risiko ohne MSR-Schutzmaßnahmen (Messen, Steuern, Regeln). Dieses Risiko wird durch die Analyse der Maschine ohne sicherheitstechnische Schutzkomponenten ermittelt. Liegt dieses Risiko über dem vertretbaren Grenzrisiko, müssen Maßnahmen zur Risikoreduzierung vorgenommen werden. Das sind die „MSR-Schutzmaßnahmen“; dadurch soll das tatsächlich verbleibende Risiko unter das vertretbare Grenzrisiko gesenkt werden. Abb. 2.1 zeigt die Beziehung zwischen Sicherheit, Gefahr und Risiko.

- Als Grenzrisiko bezeichnet man das größte noch vertretbare Risiko eines bestimmten technischen Vorgangs oder Zustands. Im Allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen. Es wird in der Regel indirekt durch sicherheitstechnische Festlegungen beschrieben.
- Gefahr wird die Sachlage definiert, bei der das Risiko größer als das Grenzrisiko ist.
- Sicherheit wird die Sachlage definiert, bei der das Risiko nicht größer als das Grenzrisiko ist.
- Restrisiko ist das verbleibende Risiko nach Abzug aller risikoreduzierenden Maßnahmen.

Abb. 2.1 Schema für die Risikoabschätzung



- Risiko ohne Sicherheitsmaßnahmen bezeichnet man das Risiko, wenn eine Maschine keine risikoreduzierenden Maßnahmen aufweist.

2.1.1 Risikobeurteilung

Die Risikobeurteilung (Auszüge aus der EN 1050) von Maschinen oder Anlagen muss einschließen:

- Die Gefährdung, Gefährdungssituation und Ereignisse, die einen Schaden hervorrufen können.
- Die vorhersehbare Wahrscheinlichkeit für das Auftreten eines Schadens und seiner Schwere.
- Die Komplexität der Maschine im Hinblick auf ihre Sicherheit sowie die Komplexität des Zusammenwirkens von Mensch und Maschine während aller Betriebshandlungen einschließlich einer vorhersehbaren nicht bestimmungsgemäßen Verwendung.

Eine Risikobeurteilung umfasst eine Folge von logischen Schritten (EN 1050), welche die systematische Untersuchung von Gefährdungen erlaubt, die von Maschinen ausgehen. Je nach dem Ergebnis folgt der Risikobeurteilung eine Risikominderung nach EN 292. Durch die Wiederholung der Beurteilung ergibt sich ein iterativer Prozess, mit dessen Hilfe die Gefährdung so weit wie möglich beseitigt und Schutzmaßnahmen getroffen werden müssen.

Die Risikobeurteilung umfasst:

- eine Risikoanalyse, die ihrerseits beinhaltet:
 - Bestimmung der konstruktiven (Wirkungs-)Grenzen der Maschine (EN 1050),
 - Identifizierung der Gefährdungen,
 - Risikoeinschätzung,
- sowie eine Risikobewertung.

Die Informationen zur Risikobeurteilung (EN 1050) und zu allen qualitativen und quantitativen Untersuchungen müssen folgende Angaben enthalten:

- die konstruktiven (Wirkungs-)Grenzen der Maschine,
- Sicherheitsanforderungen in den einzelnen Lebensphasen der Maschine (EN 292-1),
- Konstruktionszeichnungen und andere Hilfsmittel zur Beschreibung der Maschine,
- Art der Energieversorgung,
- die Unfall- und Zwischenfallgeschichte (soweit vorhanden),
- Information über eventuelle Gesundheitsschäden, die auf den Betrieb der Maschine zurückgeführt werden können.

Diese Informationen müssen aktualisiert werden, wenn das Fehlen einer Unfallgeschichte, eine bisher geringe Anzahl von aufgetretenen Unfällen oder ein geringes Schadensausmaß dürfen nicht automatisch zu der Annahme führen, dass das Risiko durch die Maschine gering sei.

2.1.2 Iterative Sicherheitserhöhung

Der iterative Prozess zum Erreichen einer erhöhten Sicherheit erfolgt grundsätzlich nach dem Ablauf, wie in Abb. 2.2 dargestellt. Beim n-fachen Durchlaufen des Algorithmus kann man die maximale Sicherheit erreichen.

- S: Schwere der Verletzungen (S1 leichte (normalerweise reversible), S2 schwere (normalerweise irreversible) Verletzung, einschließlich Tod),
- F: Häufigkeit und/oder Dauer der Gefährdungsexposition (F1 selten bis öfters und/oder kurze Dauer der Exposition, F2 häufig bis dauernd und/oder lange Dauer der Exposition),
- P: Möglichkeiten zur Vermeidung der Gefährdung – allgemein bezogen auf die Geschwindigkeit und Frequenz, mit der sich das gefährdende Teil bewegt und auf den Abstand zu dem gefährdenden Teil (P1 möglich unter bestimmten Bedingungen, P2 kaum möglich),
- B 1 bis 4: Kategorien für sicherheitsbezogene Teile von Steuerungen.

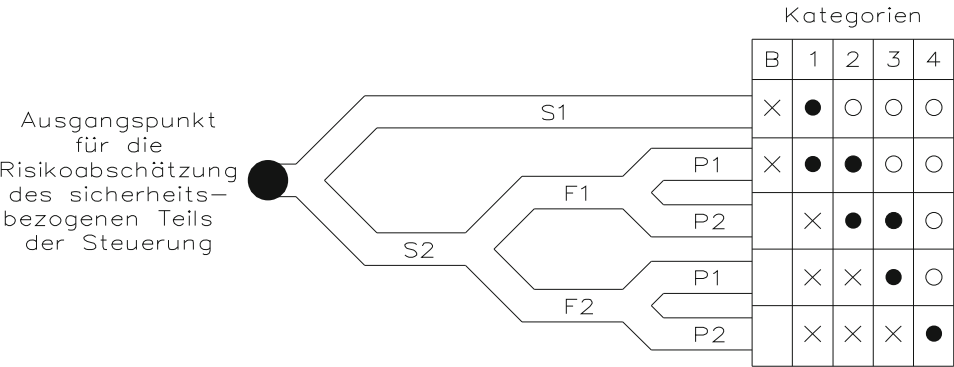


Abb. 2.2 Schema für Risikoabschätzung

Das einer bestimmten Situation oder einem bestimmten technischen Verfahren (EN 1050) immer noch vorhandene Risiko wird als Kombination der folgenden Elemente beschrieben:

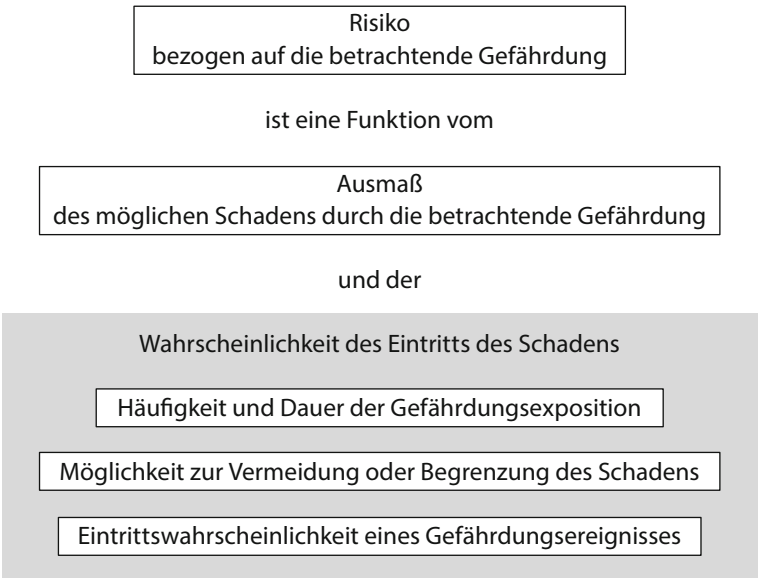
- Ausmaß des möglichen Schadens,
- Eintrittswahrscheinlichkeit dieses Schadens als Funktion mit
 - der Häufigkeit und der Dauer, mit der Personen der Gefährdung ausgesetzt sind,
 - der Wahrscheinlichkeit des Auftretens eines Gefährdungsereignisses und
 - der technischen und menschlichen Möglichkeit zur Vermeidung oder Begrenzung des Schadens.

2.1.3 Risikoelemente

Das Gesamtrisiko, das von technischen Anlagen oder Verfahren ausgeht, wird als Funktion vom Schadensausmaß und der Schadenswahrscheinlichkeit ausgedrückt. Die einzelnen Risikoelemente können nach dem Schema von Tab. 2.1 zusammengefasst werden.

Für die systematische Untersuchung der Risikoelemente wurde eine Reihe von Verfahren entwickelt (EN 1050).

Tab. 2.1 Schadensausmaß und Schadenswahrscheinlichkeit



2.2 Schäden

2.2.1 Schadensausmaß

Das Ausmaß eines möglichen Schadens (EN 1050) kann unter Berücksichtigung der folgenden Kriterien eingeschätzt werden:

- Art des zu schützenden Rechtsgutes
 - Personen
 - Sachen
 - Umwelt
- Ausmaß der erfolgten Verletzung oder Gesundheitsschädigung
 - leicht, üblicherweise reversibel
 - schwer, üblicherweise irreversibel
 - tödlich
- Schadensumfang für jede Maschine
 - eine Person betroffen
 - mehrere Personen betroffen

2.2.2 Eintrittswahrscheinlichkeit eines Schadens

Die Wahrscheinlichkeit für den Eintritt (EN 1050) eines Schadens ist natürlich die alles entscheidende Frage. Nach dem „Gesetz der maximalen Boshaftigkeit“ wird jedes unangenehme Ereignis, das denkbar ist, auch eintreten. Dass diese pauschale Aussage bei der Konstruktion einer Maschine als „überzogen“ angesehen werden kann, weiß auch die Norm. Deshalb lässt sie die Einbeziehung der Häufigkeit und Dauer der Gefährdung sowie die Möglichkeit der Vermeidung der Gefährdung zu. Werden diese Überlegungen gewissenhaft durchgeführt, kann das Ergebnis optimaler Personenschutz und Kostenreduzierung sein.

Abhängig von der Notwendigkeit des Zugangs (EN 1050) zum Gefahrenbereich muss:

- die Art des Zugangs,
- die Zeit, die im Gefahrenbereich verbracht wird, sowie
- die Anzahl der Personen, für die ein Zugang erforderlich ist, beurteilt werden, denn mit diesen Punkten steigt die Wahrscheinlichkeit eines Unfalls.

Die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses (EN 1050) ist entsprechend der Norm ableitbar aus:

- der Zuverlässigkeit der verwendeten Technik,
- anderen statistischen Daten,

- der Unfallgeschichte (soweit schon vorhanden),
- den Daten über Gesundheitsschädigungen ähnlicher Anlagen oder Maschinen und
- den Risikovergleichen.

Zu beachten ist, dass das Eintreten eines Gefährdungsereignisses sowohl technisch als auch menschlich bedingt sein kann.

2.2.3 Möglichkeiten zur Vermeidung oder Begrenzung eines Schadens

Die Möglichkeiten zur Vermeidung oder Begrenzung eines Schadens verbessern sich entsprechend der EN 1050 durch:

- die Art der Bedienung der Maschine:
 - durch ungeübtes Personal,
 - durch geübtes Personal,
 - durch selbsttätigen Betrieb.
- die Schnelligkeit des Eintretens eines Gefährdungsereignisses:
 - plötzlich,
 - schnell,
 - langsam.
- das Risikobewusstsein des Betreibers/Bedieners, der eine Gefahr erkennt:
 - durch allgemeine Informationen,
 - durch direktes Beobachten,
 - durch Anzeigegeräte.
- die menschlichen Reaktionen zur Vermeidung oder Begrenzung eines Schadens (z. B. Reflexe, Beweglichkeit, Möglichkeit der Befreiung):
 - unmöglich,
 - möglich unter bestimmten Bedingungen,
 - möglich.
- die praktischen Erfahrungen und Kenntnisse von Betreiber/Bediener über:
 - keine Erfahrung,
 - konkrete Maschine,
 - ähnliche Maschinen.

2.3 Personenschäden

Die Risikoabschätzung für exponierte Personengruppen muss alle der Gefährdung ausgesetzten Personen berücksichtigen (EN 292-1).

Die Einschätzung jeder Gefährdungsexposition erfordert eine Analyse und muss alle Betriebsarten der Maschine umfassen. Dies gilt im Besonderen für die Zugriffsmöglich-

keiten zum Einstellen, Programmieren, Umrüsten, Reinigen, Fehlersuchen und Instandhalten (EN 292-1).

Menschliche Faktoren können das Risiko einer Maschine/Anlage beeinflussen. Es treten beispielsweise auf:

- Wechselwirkungen zwischen Personen und Maschine sowie
- Wechselwirkungen zwischen Personen und Personen.

Das Risiko beeinflussen:

- Psychologische Aspekte und
- ergonomische Aspekte sowie
- die Fähigkeit zur Entwicklung von Risikobewusstsein in einer gegebenen Situation in Abhängigkeit von der Ausbildung, den Erfahrungen und Fertigkeiten.

Ausbildung, Erfahrung und Fähigkeit können das Risiko beeinflussen, aber keine dieser Faktoren darf als Ersatz für die Beseitigung von Gefährdung oder Risikoverminderung durch Konstruktion oder technische Schutzmaßnahmen dienen!

Die Risikoeinschätzung insgesamt muss die Zuverlässigkeit von einzelnen Bauteilen und ganzen Systemen berücksichtigen.

Wenn Schutzmaßnahmen die Arbeitsorganisation, korrekte Verhaltensweisen, Aufmerksamkeit usw. beinhalten, dann muss deren relativ geringe Zuverlässigkeit im Vergleich zu erprobten technischen Schutzmaßnahmen bei der Risikoeinschätzung berücksichtigt werden.

Die Risikoeinschätzung muss auch die Möglichkeit berücksichtigen, dass vorgesehene Schutzmaßnahmen wirkungslos gemacht oder umgangen werden.

Es muss nämlich berücksichtigt werden, dass unter Umständen Interesse besteht, Schutzmaßnahmen zu umgehen, weil:

- die Schutzmaßnahmen evtl. die Produktion verlangsamen oder die Aktivitäten des Bedieners hemmen,
- andere Personen als das Bedienerpersonal davon betroffen sein können oder
- die Schutzmaßnahmen nicht erkannt oder in ihrer Wirkung nicht akzeptiert werden.

Die Anwendung programmierbarer elektronischer Systeme eröffnet eine zusätzliche Möglichkeit, Schutzmaßnahmen wirkungslos zu gestalten oder zu umgehen. Deshalb werden bei programmierbaren Sicherheitssteuerungen die Softwarebausteine mittels Programmquersumme, die das Datum und die Uhrzeit beinhalten, versiegelt (z. B. durch das Automatisierungssystem PSS 4000).

2.4 Risikobewertung

Nach der Risikoeinschätzung als letzten Schritt der Risikoanalyse muss eine Risikobewertung durchgeführt werden, um zu entscheiden, ob eine Risikominderung notwendig ist. Wenn keine genügende Sicherheit erreichbar ist, sind geeignete Schutzmaßnahmen auszuwählen und anzuwenden. Danach ist die Risikobeurteilung zu wiederholen. In diesem iterativen Prozess ist es wichtig zu prüfen, ob durch die Anwendung neuer Schutzmaßnahmen eventuell zusätzliche Gefährdungen geschaffen werden.

2.4.1 Erreichen des Ziels einer Risikominderung

Sind folgende Bedingungen erfüllt, kann der Prozess der Risikominderung als abgeschlossen angesehen werden:

- Gefährdung ist beseitigt oder das Risiko wurde vermindert durch:
 - konstruktive Maßnahmen oder Substitution durch weniger gefährliche Materialien und Stoffe,
 - technische Schutzmaßnahmen.
- Die ausgewählten technischen Schutzmaßnahmen ergeben aus der Erfahrung eine sichere Situation bei einer bestimmungsgemäßen Verwendung
 - die Art der ausgewählten technischen Schutzmaßnahmen für die Anwendung verhindern oder minimieren,
 - die Wahrscheinlichkeit, sie wirkungslos zu gestalten oder umgehen zu können,
 - das Ausmaß des Schadens,
 - die Behinderung bei der Arbeitsausführung.
- Die Informationen über die bestimmungsgemäße Verwendung der Maschinen sind ausreichend klar.
- Die Arbeitsverfahren, die beim Einsatz der Maschine zu befolgen sind, entsprechen den Fähigkeiten des Bedienungspersonals oder anderer Personen, die den von der Maschine ausgehenden Gefährdungen ausgesetzt sein können.
- Die empfohlenen Methoden für ein sicheres Arbeiten mit der Maschine und die entsprechenden Ausbildungsanforderungen sind in angemessener Form festgelegt.
- Anwender ist ausreichend über Restrisiken in den verschiedenen Lebensphasen der Maschine informiert.
- Persönliche Schutzausrüstungen empfohlen werden, wurden die Notwendigkeiten ihrer Benutzung und die entsprechenden Ausbildungsanforderungen festgelegt, die zusätzlichen Vorsichtsmaßnahmen (EN 292-2) sind ausreichend.

2.4.2 Risikovergleich

Als Teil des Verfahrens der Risikobewertung können die Risiken einer Maschine mit denen ähnlicher Maschinen verglichen werden, falls folgende Kriterien erfüllt sind:

- die Vergleichsmaschine ist sicher (Baujahr beachten),
- die bestimmungsgemäße Verwendung und die Art der Konstruktion ist vergleichbar,
- Gefährdung und die Risikoelemente sind vergleichbar,
- die technischen Spezifikationen sind vergleichbar oder
- die Einsatzbedingungen sind vergleichbar.

Die Durchführung eines Risikovergleichs entbindet nicht von der Notwendigkeit einer Risikobeurteilung!

2.5 Dokumentation

Für den Zweck dieser Norm muss die Dokumentation über die Risikobeurteilung, den beschrittenen Weg und die erreichten Ergebnisse informieren. Diese Dokumentation enthält:

- Die Maschine, für die die Beurteilung durchgeführt wurde, inklusiv aller relevanten Annahmen (z. B. Lasten, Festigkeiten, Sicherheitsfaktoren usw.).
- Die festgestellten Gefährdungen, wie
 - die festgestellten Gefährdungssituationen und/oder
 - die bei der Beurteilung in Betracht gezogenen Gefährdungsereignisse.
- Die Informationen, auf denen die Risikobeurteilung beruht, wie die verwendeten Daten und deren Quellen, (z. B. Unfallberichte, Erfahrung und vergleichbare Maschinen) und/oder
 - die Unsicherheit bzw. Fehlergrenzen der verwendeten Daten,
 - die durch Schutzmaßnahmen zu erreichenden Ziele.
- Die in Schutzmaßnahmen zur Beseitigung von festgestellten Gefährdungen oder Minderung von Risiken umgesetzten Anforderungen.
- Restrisiken, die nach der Anwendung von Schutzmaßnahmen verbleiben.
- Das Ergebnis der abschließenden Risikobewertung.

Die Liste in Tab. 2.2 ist nach den wichtigsten Gefährdungsarten selektiert und deshalb nicht vollständig (EN 1050).

Tab. 2.2 Zusammenstellung der Gefährdungen und ihre normenmäßige Behandlung

Nr.	Gefährdungen	Anhang A der EN 292-2:	EN 292-1	EN 292-2
1	Mechanische Gefährdung erzeugt durch Maschinenteile oder Werkstücke; verursacht durch deren	1.3	4.2	3.1, 3.2, 4
a)	Form			
b)	Relative Anordnung			
c)	Masse und Standfestigkeit			
d)	Masse und Geschwindigkeit			
1.1	Gefährdung durch Quetschen	1.3	4.2.1	3.8
1.2	Gefährdung durch Scheren			
1.3	Gefährdung durch Schneiden oder Abschneiden			
1.4	Gefährdung durch Erfassen oder Aufwickeln			
1.5	Gefährdung durch Einziehen oder Fangen			
1.6	Gefährdung durch Stoß			
1.7	Gefährdung durch Durchstich oder Einstich			
1.8	Gefährdung durch Reibung oder Abrieb			
1.9	Gefährdung durch Eindringen oder Herauspritzen von Flüssigkeit unter hohem Druck	1.3.2	4.2.1	
2	Elektrische Gefährdung			
2.1	Direkte Berührung von Personen mit unter Spannung stehenden Teilen	1.5.1, 1.6.3	4.3	3.9, 6.2.2
2.2	Berührung von Personen mit Teilen, die durch Fehlerzustände spannungsführend geworden sind	1.5.1	4.3	3.9
3	Thermische Gefährdung mit der Folge			
3.1	Verbrennungen und Verbrühungen durch Kontakt mit Werkstoffen sehr hoher Temperatur	1.5.5, 1.5.6, 1.5.7	4.4	
4	Gefährdung durch Lärm mit der Folge	1.5.8	4.5	3.2, 4
4.1	Gehörverlust			
4.2	Störung der Sprachkommunikation oder von akustischen Signalen			
5	Gefährdung durch Vibration	1.5.9	4.6	3.2
6	Gefährdung durch Strahlung			
6.1	Strahlung im Niederfrequenz-, Funkfrequenz-, Mikrowellen-Bereich	1.5.10	4.7	
6.5	Laserstrahlen	1.5.12	4.7	
7	Gefährdung durch Werkstoffe und andere Stoffe, die von Maschinen verarbeitet oder verwendet werden	1.1.3, 1.5.13, 1.6.5	4.8	3.3b, 3.4

Tab. 2.2 (Fortsetzung)

Nr.	Gefährdungen	Anhang A der EN 292-2:	EN 292-1	EN 292-2
8	Gefährdung durch Vernachlässigung ergonomischer Grundsätze beim Gestalten von Maschinen			
8.1	Ungesunde Körperhaltung oder besondere Anstrengung	1.1.2d, 1.1.5, 1.6.2, 1.6.4	4.9	3.6.1, 6.2.1–4, 6.2.6
8.6	Menschliches Fehlverhalten, menschliches Verhalten	1.1.2d, 1.2.2, 1.2.5, 1.2.8, 1.5.4, 1.7	4.9	3.6, 3.7.8, 3.7, 9, 5, 6.1.1
9	Kombination von Gefährdungen			
10	Unerwarteter Anlauf, unerwartetes Durch- oder Überdrehen			
10.1	Ausfall oder Störung des Steuerungssystems	1.2.7, 1.6.3		3.7, 6.2.2
10.2	Wiederherstellung der Energiezufuhr nach Unterbrechung	1.2.6		3.7.2
10.5	Softwarefehler	1.2.1		3.7.7
11	Fehlende Möglichkeit, die Maschine unter optimalen Bedingungen stillzusetzen	1.2.4, 1.2.6, 1.2.7		3.7, 3.7.1, 6.1.1
12	Änderung der Umdrehungsgeschwindigkeit von Werkzeugen	1.3.6		3.2, 3.3
13	Ausfall der Energieversorgung	1.2.6		3.7, 3.7.2
14	Ausfall des Steuer- bzw. Regelkreises	1.2.1, 1.2.3–5, 1.2.7, 1.6.3		3.7, 6.2.2
15	Fehlerhafte Montage	1.5.4	4.9	5.5, 6.2.1
16	Bruch bei Betrieb	1.3.2	4.2.2	3.3
22	Ursache beim Steuerungssystem			
22.1	Ungeeignete Positionierung der Steuerungseinheit	3.2.1, 3.3.1, 3.4.5		
25	Ursache durch dritte Personen			
25.1	Unerlaubtes Starten oder Benutzen	3.3.2		
25.2	Bewegung eines Maschinenteils über die Halteposition	3.4.1		
25.3	Fehlen oder mangelhafte Eignung von optischen oder akustischen Warneinrichtungen	1.7.4, 3.6.1		
26	Unzureichende Anweisung für den Fahrer/Bediener	3.6		

2.6 Verfahren zur Untersuchung von Gefährdungen und zur Einschätzung von Risiken

Es gibt es zwei Grundtypen der Risikoanalyse: die deduktiven und die induktiven Verfahren. Bei den deduktiven Verfahren wird das Schlussergebnis angenommen und der Weg gesucht, der zu diesem Schlussergebnis führt. Bei den induktiven Verfahren wird der Ausfall eines Maschinenelements angenommen. Die anschließende Analyse stellt alle Ereignisse fest, die diesen Ausfall verursachen können.

Vorläufige Untersuchung von Gefährdungen: Die „Preliminary Hazard Analysis“ (PHA) ist ein induktives Verfahren mit dem Ziel, für ein System in all seinen Lebensphasen die Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse zu ermitteln, die zu einem eventuellen Unfall führen könnten.

„WAS-WENN“-Verfahren: Dieses Verfahren (WHAT-IF Method) ist für relativ einfache Maschinen geeignet. Es wird bei jedem Prüfschritt die „Was-Wenn“-Frage gestellt.

Fehlzustands- und Auswirkungsanalyse: Diese Analyse, auch als Ausfalleffektanalyse (Failure mode and effect analysis – FMEA) bezeichnet, ist ein induktives Verfahren. Es hilft die Häufigkeit und die Folgen von Ausfällen an Maschinen zu ermitteln.

Fehlersimulation für Steuerungen: Fehlersimulation (Fault simulation for Control Systems) ist ebenfalls ein induktives Verfahren. Es beruht auf zwei Kriterien:

- praktische Prüfung am betreffenden Regelkreis und Fehlersimulation sowie
- Simulation des Regelverhaltens anhand von Hard- und Softwaremodellen.

MOSAR-Verfahren (Method Organized for a Systematic Analysis of Risks) ist ein Verfahren in zehn Schritten. Es wird eine Tabelle benutzt, um die Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse zu identifizieren. Die Eignung der Schutzmaßnahmen wird mit Hilfe einer zweiten Tabelle untersucht, in einer dritten Tabelle wird die gegenseitige Abhängigkeit erarbeitet usw.

Fehlerbaumanalyse/Fehlzustandsbaumanalyse: „Fault Tree Analysis“ (FTA) ist ein deduktives Verfahren, das auf Grund eines als unerwünscht angesehenen Ereignisses durchgeführt wird, um kritische Pfade herauszufinden, die zu dem unerwünschten Ereignis führen.

DELPHI-Methode: Diese Methode ist ein Vorhersageverfahren, das anhand vertrauter Prozessverläufe für bisher unbekannte Prozesse mit Methoden der Wahrscheinlichkeitstheorie hochwahrscheinlich zutreffende prognostische Voraussagen macht. Sie wird auch zur Entwicklung neuer Ideen verwendet.

2.7 Risikobeurteilung

Zurzeit gibt es eine große Anzahl Normen, deren Ziel die Risikobeurteilung ist. Als Anwender ist es fast nicht mehr möglich, die richtige, für sein Produkt anzuwendende Norm auszuwählen. DIN V19250, EN 954, IEC 61508, IEC 61511, IEC 62061 usw. Obwohl nach und nach die EN IEC 61508 zum alles beherrschenden Thema wird, hat die EN 954-1 nach wie vor ihre Berechtigung, wenn es um Maschinensicherheit geht. Diese Berechtigung kann auch von der Tatsache abgeleitet werden, dass im CEN das TC 114/WG 6 die EN 954-1 als EN 150 13849-1 überarbeitet und durch die Einführung von „Performance Level“ an die Denkweise der EN IEC 61508 anpasst.

Die europäische Norm EN 954-1, EN 954-2 enthält die Definitionen von Kategorien und Anforderungen und beschreibt Eigenschaften von Sicherheitsfunktionen und Gestaltungsleitsätzen für sicherheitsbezogene Teile von Steuerungen. Sie bezieht programmierbare Systeme für alle Maschinenarten und darauf bezogene Schutzeinrichtungen ein. Sie gilt für alle sicherheitsbezogenen Teile von Steuerungen, unabhängig von der verwendeten Energieart (z. B. elektrisch, hydraulisch, pneumatisch, mechanisch). Sie legt jedoch nicht fest, welche Sicherheitsfunktionen und welche Kategorien im Einzelfall anzuwenden sind.

Sie enthält sicherheitstechnische Anforderungen und Orientierungshilfen für die Gestaltung, Konstruktion, Programmierung, den Betrieb, die Wartung und Reparatur von sicherheitsbezogenen Teilen von Steuerungen für Maschinen.

Sie gilt für alle Maschinen im gewerblichen und privaten Bereich. Sie kann, wo dies angebracht ist, auch für Steuerungen mit sicherheitsbezogenen Teilen gelten, die zu anderen technischen Zwecken mit ähnlichen Gefahren verwendet werden.

Die Norm sieht vor, bei der Konzeption der Steuerungskategorien Fehler an Bauteilen vorzusehen bzw. Fehlerausschlüsse anzunehmen (Fehlerausschluss bedeutet, dass ein solcher Fehler auszuschließen ist, weil davon ausgegangen werden kann, dass er weder entsteht noch auftritt.). Um für diesen Zweck objektive und nachprüfbare Kriterien zu haben, werden in EN 954 Listen von möglichen Bauteilfehlern aufgeführt. Diese Fehlerlisten sind bei der Bewertung von sicherheitsbezogenen Teilen von Steuerungen zu berücksichtigen. Die dort aufgeführten Fehlerlisten erheben keinen Anspruch auf Vollständigkeit und gegebenenfalls müssen zusätzliche Fehler berücksichtigt werden.

Im Allgemeinen sind folgende Fehlerbetrachtungen zu berücksichtigen:

- Zwei unabhängige zufällige Fehler treten nicht gleichzeitig auf.
- Falls als Folge eines Fehlers weitere Bauteile ausfallen, sind der erste Fehler und alle sich darauf ergebenden Fehler als einzelne Fehler zu betrachten.
- Systematische Mehrfachausfälle werden als einzelne Fehler betrachtet.

- Bei elektrischen/elektronischen Bauteilen sind folgende Fehler anzunehmen:
- Kurzschluss oder Unterbrechung von Stromkreisen (z. B. Kurzschluss zum Schutzleiter oder zu einem blanken leitfähigen Teil), Unterbrechung von jedem Leiter,
 - Kurzschluss oder Unterbrechung in einzelnen Bauteilen (z. B. Positionsschalter),
 - Nichtabfallen oder Nichtanziehen von elektromagnetischen Bauelementen (z. B. Schütze, Relais, Magnetventile),
 - Nichtstarten oder Nichtstoppen von Motoren, mechanisches Blockieren von bewegten Teilen (z. B. Positionsschalter),
 - Driften über die Toleranzgrenzen hinweg von analogen Bauelementen (z. B. Widerstände, Kondensatoren),
 - Oszillieren von instabilen Ausgangssignalen im Falle von integrierten, nicht programmierbaren Bauteilen,
 - Fehler in der Gesamtfunktion oder von Teilfunktionen im Falle von programmierbaren Bauteilen (Worst-Case-Verhalten).

Anmerkungen

- Die Kategorien sind nicht dazu bestimmt, in irgendeiner gegebenen Reihenfolge oder hierarchischen Anordnung in Bezug auf die sicherheitstechnischen Anforderungen angewendet zu werden.
- Aus der Risikobeurteilung wird sich ergeben, ob der gesamte oder teilweise Verlust der Sicherheitsfunktion auf Grund von Fehlern akzeptabel ist.

Hieraus kann man ableiten, dass die bisweilen geführten Diskussionen, ob jetzt die ganze Firma XY in Kategorie 2, 3 oder 4 einzustufen ist, am Willen der Normengeber vorbei geht und nicht im Sinn der Norm ist. Meistens hat jede Maschine eine Vorder- und eine Rückseite. Die gefährliche ist die Frontseite, weil dort in der Regel die Maschine bestückt und bedient wird, während die Rückseite weniger gefährlich ist, weil sie meist durch Bleche und Schutzgitter verkleidet ist.

Tab. 2.3 Einstufungen gemäß EN 954-2 (EN ISO 13849-2)

Anhang	Technologie	Liste der grundlegenden Sicherheitsprinzipien	Liste der bewährten Sicherheitsprinzipien	Liste der bewährten Bauteile	Fehlerlisten und Fehlerausschlüsse
A	Mechanik	A.1	A.2	A.3	A.4
B	Pneumatik	B.1	B.2	B.3	B.4
C	Hydraulik	C.1	C.2	C.3	C.4
D	Elektrik	D.1	D.2	D.3	D.4

Tab. 2.4 Vergleich der drei gültigen Risikobeurteilungsnormen

DIN AK V 19250	DIN EN Kat 954	DIN EN IEC SIL 61508
1, 2	B	–
2, 3	1, 2	1
4	3	2
5, 6	4	3
7	–	4
8	–	–

Um für diesen Zweck objektive und nachprüfbare Kriterien zu haben, werden in der EN 954-2 (EN ISO 13849-2) Listen für die Technologien Mechanik, Pneumatik, Hydraulik und Elektrik aufgeführt werden. Tab. 2.3 zeigt die Einstufungen gemäß EN 954-2 (EN ISO 13849-2).

2.7.1 Vergleich verschiedener Risikobeurteilungsnormen

Es gibt verschiedene Normen, die auf einen Risikographen verweisen: DIN V 19 250, EN 954-1, DIN EN IEC 61508 und bis vor kurzem auch EN 1050. Mit Ratifizierung der EN 1050 sind in dieser Norm die Risikographen entfallen. Die DIN V 19 250, die eine deutsche Norm ist, wird nach den EU-Beschlüssen von 1993 als nationale Norm nicht mehr ratifiziert. Da diese jedoch in der Anlagentechnik häufig verwendet wird, im Maschinenbau jedoch die EN 954 zur Anwendung kommt, entsteht immer wieder die Frage, wie diese Normen zu vergleichen sind. Tab. 2.4 zeigt den Vergleich der drei gültigen Risikobeurteilungsnormen.

2.7.2 Prozess für Auswahl

Es ist wichtig, die Schnittstellen zwischen den sicherheitsbezogenen und den nicht sicherheitsbezogenen Teilen der Steuerung und nicht zu allen anderen Teilen der Maschine festzulegen. Somit kann der Beitrag der sicherheitsbezogenen Teile zur Risikoverringung in Übereinstimmung mit der Risikobeurteilung der Maschine nach EN 1050 festgelegt werden.

- Schritt 1 (Gefährdungsanalyse und Risikobeurteilung): Die Gefährdungsanalyse und Risikobeurteilung erfolgt durch:
 - Festlegen der Gefährdung an der Maschine,
 - Beurteilen des durch diese Gefährdung aufgetretenen Risikos.

- Schritt 2 (Entscheiden über Maßnahmen zur Risikoverminderung durch Steuerungsmaßnahmen): Das Entscheiden über Maßnahmen zur Risikoverminderung durch Steuerungsmaßnahmen erfolgt über gestalterische Maßnahmen an der Maschine.
- Schritt 3 (Festlegen der sicherheitstechnischen Anforderungen für sicherheitsbezogene Teile der Steuerung): Das Festlegen der sicherheitstechnischen Anforderungen für sicherheitsbezogene Teile der Steuerung erfolgt in den beiden Schritten:
 - Festlegen der Sicherheitsfunktionen, die in der Steuerung vorzusehen sind.
 - Festlegen wie die Sicherheitsfunktionen erreicht werden und Auswählen der Kategorien.
- Schritt 4 (Gestalten und Verifizieren): Gestalten der nach den in Schritt 3 getroffenen Festlegungen und nach der in EN 954-1 beschriebenen Vorgehensweise. Verifizieren der Gestaltung muss in jeder Phase erfolgen, um sicherzustellen, dass die sicherheitsbezogenen Teile die Anforderungen der vorhergehenden Stufe im Zusammenhang mit den festgelegten sicherheitsbezogenen Funktionen und Kategorien erfüllen.
- Schritt 5 (Validieren): Validieren der bei der Gestaltung erreichten Sicherheitsfunktionen und Kategorien. Werden bei der Gestaltung sicherheitsbezogener Teile der Steuerung programmierbare Systeme verwendet, sind andere detaillierte Verfahren erforderlich (EN 954-1). Diese Verfahren sind derzeit in Vorbereitung.

2.8 Übersicht der Risikokategorien

Schwerpunkt dieses Verfahrens ist, die sicherheitstechnische Anforderung von Steuerungen, unabhängig von der Technologie, in fünf sicherheitstechnisch sinnvolle Kategorien einzustufen. Diese reichen von einfachen bis zu aufwendigen Anforderungen, wie Einfehlersicherheit, Redundanz, Diversität oder/und Selbstüberwachung.

Die sicherheitsbezogenen Teile von Steuerungen (EN 954-1 und EN 954-2) müssen mit den Anforderungen (Tab. 2.5) einer oder auch mehrerer der fünf nachfolgend beschriebenen Kategorien übereinstimmen. Die fortlaufende Nummerierung der Kategorien B, 1, 2, 3 und 4 soll keine hierarchische Anordnung sein bzw. soll nicht im hierarchischen Sinn angewendet werden.

Die sicherheitsbezogenen Teile der Kategorie B von Steuerungen (EN 954-1 und EN 954-2) müssen nach den zutreffenden Normen unter Verwendung der zugrundgelegten Sicherheitsprinzipien gestaltet und validiert werden.

Anmerkung

Diese Forderung scheint auf den ersten Blick verwirrend und ist auch nicht für Hersteller in den klassischen Industrieländern gedacht. Da jedoch zunehmend Produkte aus so genannten Dritte-Welt-Ländern, die andere, meist jedoch keinerlei Normen zu berücksichtigen haben, in den Wirtschaftsbereich der EU importiert werden, soll für diese hiermit ein gewisser Mindeststandard festgeschrieben werden.

Tab. 2.5 Anforderungen und Auswirkungen von Risikokategorien

Kategorie	Kurzfassung der Anforderung	Systemverhalten	Wesentliches
B	Die sicherheitsbezogenen Teile von Maschinensteuerungen und/oder ihre Schutzeinrichtung als auch ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, konstruiert, ausgewählt, zusammengestellt und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können	Wenn ein Fehler auftritt, kann er zum Verlust der Sicherheitsfunktion führen	Überwiegend durch Auswahl von Bauteilen charakterisiert
1	Die Anforderung von B muss erfüllt sein Verwendung von sicherheitstechnisch bewährten Bausteinen und Prinzipien	Wie für Kategorie B beschrieben, aber mit einer höheren sicherheitsbezogenen Zuverlässigkeit der Sicherheitsfunktionen	
2	Die Anforderung von B und die Verwendung sicherheitstechnisch bewährter Prinzipien müssen erfüllt sein Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung geprüft werden	Das Auftreten eines Fehlers kann zum Verlust der Prinzipien der Sicherheitsfunktion zwischen den Prüfungsabständen führen Der Verlust der Sicherheitsfunktion wird durch die Prüfung erkannt	Überwiegend durch Struktur charakterisiert
3	Die Anforderung von B und die Verwendung sicherheitstechnisch bewährter Prinzipien müssen erfüllt sein, dass – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und – wann immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird	Wenn der einzelne Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen	Überwiegend durch Struktur charakterisiert
4	Die Anforderung von B und die Verwendung sicherheitstechnisch bewährter Prinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, dass: – ein einzelner Fehler in der Steuerung nicht zum Verlust der Sicherheitsfunktion führt und – der einzelne Fehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktionen erkannt wird. Falls dies nicht möglich ist, darf eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen	Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktionen zu verhindern	Überwiegend durch Struktur charakterisiert

Die Anforderungen der Kategorie 1 von B müssen nach EN 954-1 und EN 954-2 erfüllt sein. Die sicherheitsbezogenen Teile der Kategorie 1 müssen unter Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien gestaltet, gebaut und validiert werden.

Ein Bauteil für eine sicherheitsbezogene Anwendung gilt als bewährt, wenn dies in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen verwendet worden ist.

Bewährte Sicherheitsprinzipien sind z. B.

- Vermeiden bestimmter Fehler durch Konstruktion, z. B. Kurzschluss durch Abstand,
- Verringerung der Wahrscheinlichkeit von Fehlern, z. B. durch Überdimensionierung der Bauteile,
- Festlegung der Ausfallrichtung, z. B. Not-Aus-Taster mit Öffnerfunktion oder
- frühe Fehlererkennung, z. B. durch Verwenden von Relais mit zwangsgeführten Kontakten, oder durch Erdung von Schaltkreisen usw.

Der Feuermelder ist, obwohl das große Gehäuse etwas anderes vermuten lässt, nichts anderes als ein Druckknopf, der auf einen elektrischen Kontakt wirkt. Dieser elektrische Kontakt ist nicht wie bei der Türklingel an unserer Haustüre ein Schließerkontakt, der einen Stromkreis schließt um eine Glocke läuten zu lassen, sondern ein Öffnerkontakt. Wie kann dies funktionieren? Ein Steuerstromkreis, der bei nicht betätigten Feuermeldern geschlossen ist, lässt ein Relais anziehen, dessen Öffnerkontakt mit einem elektrischen Läutwerk verbunden ist. Wird jetzt ein Feuermelder betätigt oder die Zuleitung zu einem Feuermelder gekappt, fällt das Relais in seine Ruhelage zurück und der Stromkreis zu dem elektrischen Läutwerk wird geschlossen. Dieses System hat sich als so zuverlässig erwiesen, dass Sicherheitsschaltkreise wie Not-Aus oder Positionsschalter von beweglichen Verdeckungen nach dem selben Prinzip erstellt werden. Auch hier sind die Steuerkontakte, wie z. B. die des Not-Aus-Tasters, Öffnerkontakte. Das Schaltrelais jedoch ist hierbei nicht ein einfaches Relais, sondern eine Relaisgruppe, die so beschaffen ist, dass Fehler erkannt werden können.

Die Anforderung der Kategorie 2 von B und die Verwendung bewährter Sicherheitsprinzipien EN 954-1 und EN 954-2 müssen erfüllt sein.

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie 2 müssen so gestaltet werden, dass ihre Sicherheitsfunktionen in geeigneten Zeitabständen durch die Maschinensteuerung geprüft werden.

Diese Prüfung der Sicherheitsfunktion muss

- beim Anlaufen der Maschine und vor dem Einleiten eines gefährlichen Zustands, und
- periodisch während des Betriebs, wenn dies notwendig ist, erfolgen.

Jede Prüfung der Sicherheitsfunktion muss entweder

- Betrieb zulassen, wenn kein Fehler erkannt wird, oder
- einen Ausgang für die Einleitung angemessener Steuerungsmaßnahmen erzeugen, wenn ein Fehler erkannt wurde, und

- wann immer möglich am Ausgang einen sicheren Zustand einleiten oder eine Warnung vor der Gefährdung vorsehen.

Die Prüfeinrichtung darf als Bestandteil des sicherheitsbezogenen Teils der Steuerungen oder getrennt davon vorgesehen werden.

Nach Erkennen eines Fehlers muss ein sicherer Zustand bis zur Beseitigung des Fehlers aufrechterhalten bleiben.

Die Anforderung der Kategorie 3 von B und die Verwendung bewährter Sicherheitsprinzipien (EN 954-1 und EN 954-2) müssen erfüllt sein.

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie 3 müssen so gestaltet werden, dass ein einzelner Fehler in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt. Wann immer in angemessener Weise durchführbar, muss der einzelne Fehler bei der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Diese Forderung kann z. B. durch Redundanz erreicht werden.

Das Systemverhalten ist so, dass

- einige, jedoch nicht alle Fehler erkannt werden,
- eine Anhäufung unerkannter Fehler zum Verlust der Sicherheitsfunktion führen kann.

Die Anforderung der Kategorie 4 von B und die Verwendung bewährter Sicherheitsprinzipien (EN 954-1 und EN 954-2) müssen erfüllt sein.

Die sicherheitsbezogenen Teile von Steuerungen der Kategorie 4 müssen so gestaltet werden, dass

- ein einzelner Fehler in jedem dieser sicherheitsbezogenen Teile nicht zum Verlust der Sicherheitsfunktion führt,
- der einzelne Fehler bei der nächsten Anforderung der Sicherheitsfunktion erkannt wird, und falls dies nicht möglich ist, eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen darf,
- Fehler gemeinsamer Ursache berücksichtigt werden müssen, z. B. durch Anwendung von Diversität, Verhindern von EMV-Einflüssen usw.

2.9 Funktionen in Sicherheitskreisen

Weitere Punkte aus dieser Norm gehen auf einzelne Funktionen in Sicherheitskreisen ein und fordern deren Realisierung wie folgt:

Eine durch Schutzeinrichtungen ausgelöste Stopp-Funktion muss die Maschine nach Betätigung dieser Funktion so schnell wie nötig in einen sicheren Zustand überführen. Diese Stopp-Funktion muss funktionellen Vorrang vor einem Betriebsstopp aufweisen.

Beim Zusammenwirken einer Gruppe von Maschinen muss dafür gesorgt werden, dass dem übergeordneten Stellteil und/oder den anderen Maschinen das Anstehen einer sicheren Stopp-Bedingung signalisiert wird.

Beim Zusammenwirken einer Gruppe von Maschinen müssen die sicherheitsbezogenen Teile die Möglichkeit haben, eine Not-Aus-Funktion an alle Teile des zusammenwirkenden Systems zu signalisieren.

Wo Bereiche des zusammenwirkenden Systems deutlich voneinander getrennt sind (z. B. durch Schutzeinrichtungen oder durch ihre physikalische Anordnung) ist es nicht immer erforderlich, die Not-Aus-Funktion auf das gesamte System auszudehnen, sondern lediglich auf bestimmte, durch die Risikobeurteilung festgelegte Bereiche.

Nach dem Wirksamwerden eines Not-Aus-Vorgangs für einen Bereich des zusammenwirkenden Systems darf an den Schnittstellen zwischen diesem Bereich und anderen Bereichen des Systems keine Gefährdung vorhanden sein.

Nach dem Einleiten eines Stopp-Befehls durch eine Schutzeinrichtung muss der Stopp-Befehl aufrechterhalten bleiben, bis sichere Bedingungen für einen erneuten Start gegeben sind.

Die Rückstellung der Sicherheitsfunktion von der Schutzeinrichtung hebt einen Stopp-Befehl auf. Falls dies in der Risikobeurteilung angezeigt ist, muss das Aufheben des Stopp-Befehls durch eine manuelle, getrennte und absichtliche Betätigung (manuelle Rückstellung) bestätigt werden.

Die manuelle Rückstellung muss über eine getrennte, handbetriebene Einrichtung der sicherheitsbezogenen Teile der Steuerung vorgenommen werden, muss sicherstellen, dass alle Sicherheitsfunktionen und Schutzeinrichtungen betriebsbereit sind. Ist das nicht der Fall, darf eine Rückstellung nicht möglich sein. Die manuelle Rückstellung darf keine Bewegung oder keinen gefährlichen Zustand verursachen. Die Rückstellung muss durch absichtliche Betätigung erfolgen, die Steuerung auf die Annahme eines getrennten Anlaufbefehls vorbereiten und wird nur akzeptiert durch die Betätigung eines Freigabeschalters.

Der Rückstell-Schalter muss außerhalb des Gefahrenbereiches an einem sicheren Ort angebracht sein, von dem gute Sicht über die gesamte Anlage gegeben ist, um sicherzustellen, dass sich niemand innerhalb des Gefahrenbereichs befindet.

Wenn eine sicherheitsbezogene Einrichtung einen Befehl für einen Start oder einen erneuten Start erzeugt, hat der Start oder erneute Start nur dann automatisch zu erfolgen, wenn kein gefährlicher Zustand vorliegen kann. Diese Anforderungen für Start und erneuten Start sind auch für Maschinen einzuhalten, die ferngesteuert werden können.

Bei Schwankungen des Energieniveaus außerhalb des zulässigen Bereichs einschließlich eines Totalausfalls der Energieversorgung müssen sicherheitsbezogene Teile der Steuerung weiterhin Ausgangssignale vorsehen oder abgeben, sodass andere Maschinenteile einen sicheren Zustand erreichen können.

Die Aufhebung (muting) darf nicht dazu führen, dass Personen gefährlichen Zuständen ausgesetzt sind.

Nach Beendigung der Aufhebung müssen Sicherheitsfunktionen der sicherheitsbezogenen Teile der Steuerung wiederhergestellt werden.

Die Kategorie der sicherheitsbezogenen Teile, die eine Aufhebungsfunktion ausführen, muss so ausgewählt werden, dass die Einbeziehung der Aufhebungsfunktion die für die relevante Sicherheitsfunktion erforderliche Sicherheit nicht verringert, d. h. ein in die

Kategorie 3 eingestuftter Sicherheitsschaltkreis darf nur mit Komponenten, die auch mindestens die Forderungen der Kategorie 3 erfüllen, überbrückt werden.

Anmerkung

Bei einigen Anwendungen ist ein Hinweissignal für die Aufhebungsfunktion erforderlich.

Soll nach diesen Kriterien für eine Anwendung eine Teilkomponente ausgewählt werden, ist festzustellen, dass das nicht einfach ist. Nur im Zusammenspiel aller Teile, die eine Steuerung bilden, kann die Risikobeurteilung vorgenommen werden. Die optimalen Eigenschaften von Einzelkomponenten nützen nichts, wenn diese zwar funktionsrichtig, aber sicherheitstechnisch falsch eingesetzt werden. Aus diesem Grund kann man nicht gewährleisten, dass Teilkomponenten der Risikokategorie 3 oder 4 entsprechen, sondern lediglich feststellen, dass mit diesen Teilkomponenten bei richtigem Einsatz in Verbindung mit anderen Teilkomponenten die Risikokategorie 3 bzw. 4 erreichbar ist.

Diese Einstufungspflicht zieht sich wie ein roter Faden vom kleinsten Endschalter bis zum Gesamtkonzept der ganzen Maschine durch, wobei der permanente Konflikt zwischen dem „technisch Machbaren“ und dem nach der „reinen-Lehre-Zulässigen“ ausgefochten werden muss.

2.10 Risikograph

Vielfach erkennen die Normenmacher, dass so manche Forderung einer Norm erklärungsbedürftig ist. Da sich aber auch Normenmacher an eine Norm zu halten haben, und zwar an die DIN 820, können sie dann diese Norm in einen normativen Teil und einen informativen Teil aufteilen. Der informative Teil ist dann der Anhang, und dient zur erleichterten Anwendung der betreffenden Norm und ihrer technischen Festlegungen. Zum besseren Verständnis dient die Grafik von Abb. 2.1.

Das Risiko ist eine Wahrscheinlichkeitsaussage, die die zu erwartenden Häufigkeiten des Auftretens einer Gefährdung und Verletzungsschwere durch diese berücksichtigt. Das zu erwartende Risiko muss durch geeignete Maßnahmen so verringert werden, dass das für diese Anwendung geforderte Sicherheitsniveau erreicht wird.

2.10.1 Gestaltung und Auswahl von Sicherheitsmaßnahmen nach EN 954-1

Da es zahlreiche Möglichkeiten gibt, um das Risiko an einer Maschine zu verringern und es ebenso viele Möglichkeiten gibt, um die sicherheitsbezogenen Teile einer Steuerung zu gestalten, handelt es sich hierbei um einen interaktiven Prozess. Hierfür wird ein schrittweises Vorgehen empfohlen.

- Schritt 1 (Gefährdungsanalyse und Risikobeurteilung):
 - Feststellen der Gefährdung an einer Maschine bei allen Betriebsarten und während jeder Lebensphase der Maschine entsprechend den Normen EN 292-1 und EN 1050,
 - Beurteilung des durch diese Gefährdung aufgetretenen Risikos und Entscheiden über die Risikoreduzierung für diese Anwendung nach den Normen EN 292-1 und EN 1050.
- Schritt 2 (Entscheiden über Maßnahmen zur Risikoreduzierung durch Steuerungsmittel):
 - Entscheiden über gestalterische Maßnahmen an der Maschine wie das Vorsehen von Schutzeinrichtungen, um die Risikoreduzierung zu bewirken.
- Schritt 3 (Festlegen der sicherheitstechnischen Anforderungen für die sicherheitsbezogenen Teile der Steuerung):
 - Festlegen der Sicherheitsfunktionen, die in der Steuerung vorzusehen sind,
 - Festlegen, wie die Sicherheitsfunktionen erreicht werden,
 - Auswählen der Kategorie für jedes Teil und für jede Kombination von Teilen innerhalb der sicherheitsbezogenen Teile der Steuerung.

Anmerkung

Hier kann abgeleitet werden, dass die Teile einer risikoreduzierenden Maßnahme nicht alle der gleichen Kategorie entsprechen müssen.

- Schritt 4 (Gestalten):
 - Gestalten der sicherheitsbezogenen Teile der Steuerung; Auflisten der berücksichtigten Gestaltungsmerkmale für die zu erreichenden Kategorien,
 - Verifizieren der Gestaltung in jeder Phase, um sicherzustellen, dass die sicherheitsbezogenen Teile den Anforderungen der festgelegten Funktionen und Kategorien entsprechen.
- Schritt 5 (Validieren):
 - Validieren der bei der Gestaltung erreichten Sicherheitsfunktion und Kategorie im Vergleich zu den Festlegungen in Schritt 3; erneute Gestaltung, falls erforderlich,
 - werden bei der Gestaltung sicherheitsbezogene Teile der Steuerung als programmierbare elektronische Systeme verwendet, sind andere detaillierte Verfahren erforderlich.

Anmerkung

Derzeit ist man der Auffassung, dass die Zuverlässigkeit des fehlerfreien Betriebs einer einkanaligen, programmierbaren, elektronischen Ausrüstung nicht zugesichert werden kann, deshalb ist es nicht ratsam, sich alleine auf den fehlerfreien Betrieb einer solchen Einkanal-Einrichtung zu verlassen.

2.10.2 Validieren durch Analyse

Im Allgemeinen ist eine Analyse zum Validieren (Betätigen) der erreichten Risikominde-
rung notwendig.

Prüfung der festgelegten Sicherheitsfunktionen: Ein wichtiger Schritt für die Bestäti-
gung ist die Prüfung der Sicherheitsfunktionen (EN 954-1) auf ihre vollständige Über-
einstimmung mit den festgelegten Eigenschaften. Ziel der Prüfung ist es sicherzustellen,
dass sicherheitsbezogene Ausgangssignale in eindeutiger und logischer Weise von den
Eingangssignalen abhängig sind.

Prüfung der festgelegten Kategorien: Grundlage für eine festzulegende Kategorie ist
das Verhalten im Fehlerfall. Die Prüfung muss zeigen, dass die notwendigen Anforderun-
gen erfüllt sind.

Grundsätzlich sind folgende Verfahren anzuwenden:

- eine theoretische Prüfung und Verhaltensanalyse der Schaltpläne,
- praktische Prüfung der Originalschaltung und Fehlersimulation an Originalbauteilen,
- Simulation des Verhaltens der Steuerung anhand von Hard- und Software-Modellen.

Prüfung der Dimensionierung: Die Prüfung muss zeigen, dass die bei der Gestaltung
festgelegte Leistungsfähigkeit bei allen festgelegten Betriebsarten erreicht wird. Folgende
Normen sind zu berücksichtigen: EN 60 204-1, EN 60 529, EN 60 721-3-0, EN 61 000-
4-1, IEC 68.

Nach Abschluss des Validierungsverfahrens muss ein Validierungsbericht erstellt wer-
den. In dem Bericht sollte insbesondere festgehalten werden:

- alle zu prüfenden Gegenstände,
- für die Prüfung zuständiges Personal,
- die zu benutzenden Prüfeinrichtungen,
- durchgeführte Analysen und Prüfungen,
- die festgestellten Probleme und deren Lösungen,
- die Ergebnisse.

Alle Ergebnisse müssen dokumentiert und in nachvollziehbarer Form aufbewahrt wer-
den (EN 1050).

Der Validierungsplan (EN 954) muss die Anforderungen für die Durchführung des
Validierungsverfahrens für die festgelegten Sicherheitsfunktionen und deren Kategorien
beschreiben:

- a) Identität der Dokumente für die Festlegungen,
- b) Betriebs- und Umgebungsbedingungen,
- c) grundlegende Sicherheitsprinzipien (A.1, B.1, C.1 und D.1),
- d) bewährte Sicherheitsprinzipien (A.2, B.2, C.2 und D.2),

- e) bewährte Bauteile (A.3 und D.3),
- f) Fehler, die aus den Fehlerlisten in A.4, B.4, C.4 und D.4 zu berücksichtigen sind,
- g) alle Analysen und Prüfungen, die angewandt wurden.

Dokumente, die für die Validierung erforderlich sein können, sind:

- a) Festlegung(en) über die angenommene Leistungsfähigkeit der Konstruktion, einschließlich der Sicherheitsfunktionen und Kategorien,
- b) Zeichnungen und Festlegungen, z.B. für mechanische, hydraulische und pneumatische Teile, gedruckte Steuerkreislpläne, Montagepläne, interne Verdrahtung, Gehäuse, Materialien, Aufstellung,
- c) Blockdiagramm(e) mit Funktionsbeschreibung der Blöcke,
- d) Steuerkreisdigramm(e) einschließlich ihrer Verknüpfungen/Verbindungen,
- e) Funktionsbeschreibung der Steuerkreisdigramme,
- f) Zeitfolgediagramm(e) für schaltende Bauteile, für Signale, die für die Sicherheit zuständig sind,
- g) Bauteilliste mit Stückbezeichnung, Nennwerten, Toleranzen, relevanten weiteren Daten, die für die Sicherheit relevant sind,
- h) Analyse aller relevanten Fehler, die in A.4, B.4, C.4 und D.4 aufgelistet sind, einschließlich der Begründung aller ausgeschlossenen Fehler,
- i) Analyse des Einflusses der im Verfahren verwendeten Materialien,
- j) spezielle Information für die Kategorie nach Tab. 2.6,
- k) wo angebracht, muss die Software-Dokumentation beinhalten:
 - 1. eine Festlegung, die klar und eindeutig ist, und die das Erreichen der geforderten sicherheitstechnischen Leistungsfähigkeit der Software bestätigt, und
 - 2. den Beweis, dass die Software so gestaltet ist, dass sie die geforderte sicherheitstechnische Leistungsfähigkeit erreicht, und Einzelheiten über Prüfungen (insbesondere Prüfberichte), die durchgeführt wurden, um zu bestätigen, dass die geforderte sicherheitstechnische Leistungsfähigkeit erreicht wurde. Tab. 2.6 zeigt eine Übersicht über Anforderungen und Notwendigkeit einer Dokumentation.

2.10.3 Validierungsverfahren

Die Validierung soll für die Bereiche Mechanik, Pneumatik, Hydraulik und Elektrik durchgeführt werden. Hierfür gibt es in den Anhängen A, B, C und D für die Kategorien B, 1, 2, 3 und 4 jeweils eine

- Liste der grundlegenden Sicherheitsprinzipien,
- Liste der bewährten Sicherheitsprinzipien,
- Liste bewährter Bauteile,
- Liste von Fehlern und Fehlerausschlüsse.

Tab. 2.6 Übersicht über Anforderungen und Notwendigkeit einer Dokumentation

Anforderungen an die Dokumentation	Kategorien, für die eine Dokumentation erforderlich ist				
	B	1	2	3	4
Grundlegende Sicherheitsfunktionen	X	X	X	X	X
Zu erwartende Betriebsbeanspruchung	X	X	X	X	X
Einfluss des zu verarbeitenden Materials	X	X	X	X	X
Leistungsfähigkeit während anderer relevanter externer Einflüsse	X	X	X	X	X
Bewährte Bauteile	X	–	–	–	–
Bewährte Sicherheitsprinzipien	–	X	X	X	X
Prüfverfahren für die Sicherheitsfunktion	–	–	X	–	–
Festgelegte Prüfintervalle	–	–	X	–	–
Berücksichtigte, vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	–	–	–	X	X
Alle identifizierten Fehler gemeinsamer Ursache und wie diese verhindert werden	–	–	–	X	X
Alle vorhersehbaren ausgeschlossenen Einzelfehler	–	–	–	X	X
Wie Sicherheitsfunktionen bei jedem Fehler aufrechterhalten bleiben	–	–	–	X	X
Fehler, die zu erkennen sind	–	–	X	X	X
Verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	–	–	–	–	X
Wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	–	–	–	–	X

Die Validierung durch Analyse und Prüfung muss aufgezeichnet werden. Die Aufzeichnung muss das Validierungsverfahren aller sicherheitstechnischen Anforderungen ersichtlich machen. Es lassen sich Querverweise zu anderen Dokumenten durchführen.

Für jedes System oder Bauteil, das einen Teil des Validierungsverfahrens nicht bestanden hat, muss die Aufzeichnung zeigen, inwieweit Übereinstimmung mit dieser Norm besteht.

Die Validierung durch Prüfungen muss systematisch geplant werden. Ein Prüfplan muss vor Beginn der Prüfungen ausgearbeitet werden, der Folgendes beinhaltet:

- die Prüfspezifikation,
- zu erwartende Ergebnisse der Prüfungen,
- die Reihenfolge der Testungen.

Prüfaufzeichnungen müssen erstellt werden, die Folgendes beinhalten:

- den Namen des Prüfers,
- die Umgebungsbedingungen,

- die Vorgehensweisen bei der Prüfung und die benutzten Ausrüstungen,
- die Ergebnisse der Prüfungen.

2.10.4 Fehlerlisten

Das Validierungsverfahren schließt die Überlegung des Verhaltens von sicherheitsbezogenen Teilen der Steuerungen im Fehlerfall ein. Zu berücksichtigende Fehler sind in den allgemeinen Fehlerlisten in A.4, B.4, C.4 und D.4 zu finden, die sich auf Erfahrungen stützen. Die allgemeinen Fehlerlisten enthalten:

- die einzubeziehenden Bauteile und Elemente, z. B. Leiter, Kabel,
- die zu berücksichtigenden Fehler, z. B. Kurzschlüsse zwischen Leitern,
- die erlaubten Fehlerausschlüsse,
- eine Spalte für Bemerkungen, die die Begründungen für Fehlerausschlüsse enthält.

Nur permanente Fehler sind berücksichtigt.

Das Ziel der Validierung von Sicherheitsfunktionen ist sicherzustellen, dass sicherheitsbezogene Ausgangssignale abhängig von den Eingangssignalen entsprechend den Festlegungen korrekt und logisch sind. Die Validierung sollte alle normalen und vorhersehbare abnormale Bedingungen durch statische und dynamische Simulation abdecken.

2.11 Risikobewertung anhand eines Beispiels

Für das Beispiel einer Risikobewertung soll eine CNC- oder SPS-gesteuerte Drehmaschine dienen. Das zu bearbeitende Werkstück wird vor jedem Arbeitsgang von Hand in die Spannzange eingelegt. Dann wird der Arbeitsvorgang gestartet und nach Ablauf des Bearbeitungsvorgangs wird das Werkstück wieder von Hand entnommen. Das Bearbeitungsprogramm läuft automatisch ab. In der EN 954-1 wird vorgeschrieben, dass das Betrachten der Maschine ohne risikoreduzierende Maßnahmen zu erfolgen hat. Abb. 2.3 zeigt eine Drehmaschine (≈ 50 Jahre alt) ohne Schutzmaßnahmen.

Die Risikobeurteilung erfolgt nach EN 1050. Bestimmung der Grenzen der Maschine: Der Wirkungsbereich der Gefährdungen der Maschine muss erfasst werden, einschließlich des vorhersehbaren Missbrauchs oder einer Fehlfunktion nach EN 292-1:

- Das vorhersehbare Fehlverhalten infolge normaler Unachtsamkeit, aber nicht infolge absichtlichen Missbrauchs der Maschine.
- Das reflexartige Verhalten einer Person im Falle einer Fehlfunktion, eines Zwischenfalls, eines Ausfalls usw. während des Gebrauchs der Maschine.
- Das menschliche Verhalten, das darauf zurückzuführen ist, dass u. U. der „Weg des geringsten Widerstands“ beim Ausführen einer Aufgabe gewählt wird.

Abb. 2.3 Drehmaschine ohne Schutzmaßnahmen

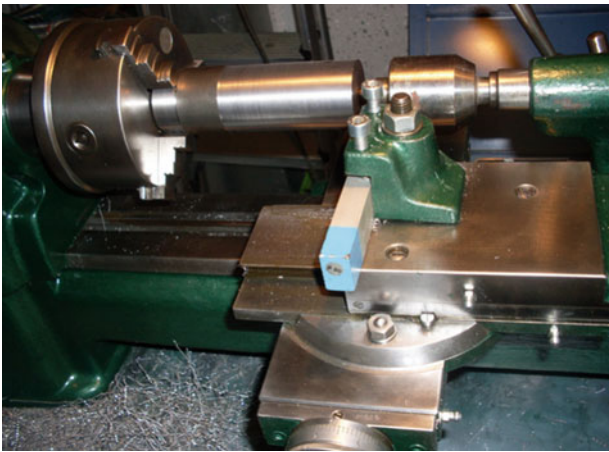


Abb. 2.4 Drehmaschine mit mechanischer Abdeckhaube für Schutzmaßnahmen



Im Fall der Beispielmachine ist der Wirkungsbereich eng begrenzt und überschaubar wie Abb. 2.4 zeigt. Der wirklich gefährliche Bereich ist der Bearbeitungsbereich, die Spannzange bzw. das Backenfutter, das u. U. mit sehr hoher Drehzahl rotiert.

Identifizierung der Gefährdungen: Es müssen alle Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse festgestellt werden, die beim Einsatz der Maschine auftreten können. Tab. 2.7 zeigt die Auswahl nach EN 1050.

Tab. 2.7 Auswahl nach EN 1050

Tabelle A. 1	1,4	Gefährdung durch Erfassen oder Aufwickeln	EN 292-1
Tabelle A. 1	1,5	Gefährdung durch Einziehen oder Fangen	EN 292-1
Tabelle A. 1	8,6	Menschliches Verhalten/Fehlverhalten	EN 292-2

Risikoeinschätzung (EN 1050): Zur Risikoabschätzung sind folgende Faktoren zu berücksichtigen:

- Schadensausmaß,
- Eintrittswahrscheinlichkeit eines Gefährdungsereignisses,
- Möglichkeit zur Vermeidung oder Begrenzung eines Schadens,
- Art, Häufigkeit und Dauer der Gefährdungsexposition,
- menschliche Faktoren,
- Zuverlässigkeit von Schutzfunktionen,
- Möglichkeit zur Ausschaltung oder Umgehung von Schutzmaßnahmen.

Abb. 2.5 zeigt Schutzmaßnahmen an einer neuen Drehmaschine. Die Art der Gefährdung wurde wie folgt eingeschätzt:

- Es ist mit sehr hohen Drehzahlen zu rechnen.
- Es entstehen scharfe Kanten am Werkstück.
- Es entstehen scharfe Stahlspäne.
- Bei vorzeitigem Griff nach dem Werkstück kann es zum Erfassen von Kleidungsstücken oder Haaren kommen und dann ist mit erheblichen Verletzungen zu rechnen.
- Auch ohne direkte Berührung kann es durch fliegende, heiße, scharfkantige Späne zu Augenverletzungen kommen.

Deshalb muss dieser Gefahrenbereich abgedeckt werden. Ein direktes festes Verschließen der Gefahrenstelle ist die effektivste Lösung. Dies ist jedoch nur bei einer automati-

Abb. 2.5 Schutzmaßnahmen an einer Drehmaschine, denn durch die mechanische Konstruktion ist ein vorzeitiger Zugriff auf das Werkstück nicht möglich und es ist oben rechts der NOT-Aus-Taster vorhanden



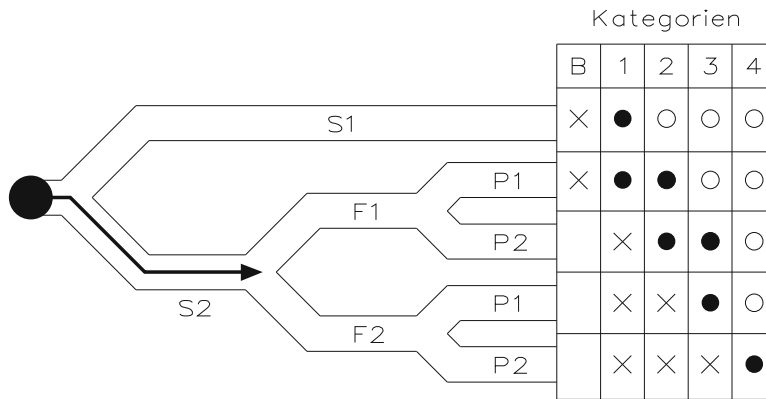


Abb. 2.6 Fortschritt der Risikoabschätzung anhand des Beispiels mit der Verletzungsschwere S2

schen Bestückung möglich. Das ist aber bei der Beispielmachine nicht vorgesehen, denn diese wird von Hand bestückt. Somit muss der Gefahrenbereich zu öffnen sein. Für diesen Fall kann eine Schutztür als beste Lösung angesehen werden.

Risikobewertung (EN 1050): Nach der Risikoeinschätzung als letztem Schritt der Risikoanalyse muss eine Risikobewertung durchgeführt werden, um zu entscheiden, ob eine Risikominderung notwendig ist. Wenn keine Sicherheit erreicht ist, sind geeignete Schutzmaßnahmen auszuwählen und anzuwenden. Hiernach ist die Risikobeurteilung zu wiederholen. In diesem iterativen Prozess ist es wichtig zu prüfen, ob durch die Anwendung neuer Schutzmaßnahmen zusätzliche Gefährdungen geschaffen wurden.

Für die Anwendung des Risikographen ist die Schwere der Verletzung S1 oder S2 (EN 954) zuständig. Die Norm unterscheidet zwischen zwei Möglichkeiten:

- S1: nur leichte, sogenannte reversible, wieder verheilende Verletzungen. Solche Verletzungen können sein: Prellungen, Schnittwunden usw.
- S2: schwere Verletzung, so genannte irreversible, nicht wieder verheilende Verletzung. Solche Verletzungen können sein: Amputation oder auch Tod.

Die Risikoanalyse des Beispiels ergibt eine Verletzungsschwere S2, da mit irreversiblen Verletzungen zu rechnen ist, wie Abb. 2.6 zeigt.

Häufigkeit und Dauer der Gefährdungsexposition F1 oder F2 (EN 954). Die Norm unterscheidet zwischen den beiden Möglichkeiten F1 oder F2, legt jedoch nicht fest, welcher Zeitraum für F1 oder F2 anzunehmen ist.

- F1: der Zugang ist von Zeit zu Zeit erforderlich.
- F2: zyklischer Betrieb erfordert in regelmäßigen Abständen einen Eingriff in den Gefahrenbereich.

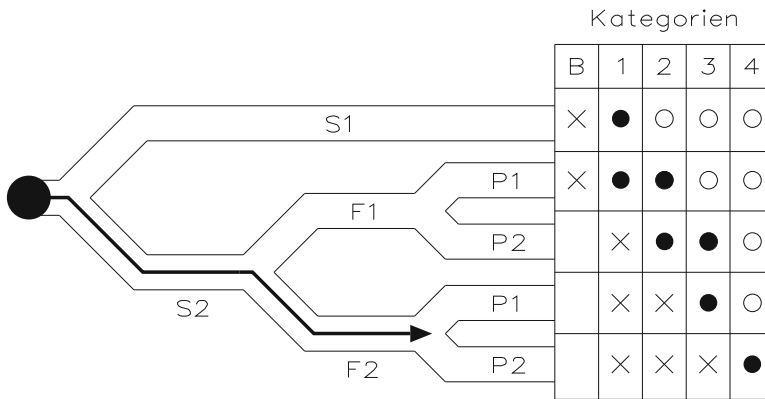


Abb. 2.7 Fortschritt der Risikoabschätzung mit der Gefährdungsexposition F2

Es ist ein zyklischer Betrieb gegeben, die Beispielmachine wird von Hand bestückt. Abb. 2.7 zeigt den Fortschritt der Risikoabschätzung mit einer Gefährdungsexposition F2.

Möglichkeit zur Vermeidung der Gefährdung P1 und P2 (EN 954): Die Norm unterscheidet auch hier zwischen zwei Möglichkeiten:

- P1: wenn keine realistische Möglichkeit besteht, den Unfall zu vermeiden.
- P2: wenn fast keine Möglichkeit besteht, die Gefährdung zu vermeiden.

Ist die Gefahrenstelle offen und auch während des Fertigungsprozesses zugänglich, ist immer mit einem Unfall zu rechnen. Dies kann aus Erfahrungs- und Unfallberichten entnommen werden, wie Abb. 2.8 zeigt.

Als Ergebnis ist die Kategorie 4 ermittelt worden.

Sind hier keine Sicherheitsvorrichtungen angebracht worden, ist die Unfallgefahr sehr hoch. Denn bei gleichmäßigen eintönigen Arbeiten ist schnell ein Flüchtigkeitsfehler zu erwarten. Die Statistik belegt, dass bei Menschen etwa jede tausendste Handlung eine Fehlhandlung ist, d. h., dass beginnend mit dem morgendlichen Aufstehen uns stetig mehr oder weniger kleine Fehler unterlaufen (z. B. Stolpern, Danebengreifen, Übersehen, falsches Einschätzen usw.). Solche Fehlhandlungen werden aus Gewohnheit selbst nicht mehr registriert. Unter Berücksichtigung dieser Fakten kann ausgerechnet werden, wie lange es dauert, bis es zu einem Arbeitsunfall kommt.

Nach dem Produkthaftungsgesetz wird dem Hersteller oder Inverkehrbringer einer Maschine nach einem Arbeitsunfall ein Verschulden unterstellt. Dieser muss dann beweisen, dass ihn keine Schuld trifft. Wurden die Normen nicht eingehalten oder richtig ausgelegt, dürfte diese Beweisspflicht sehr schwer zu erfüllen sein.

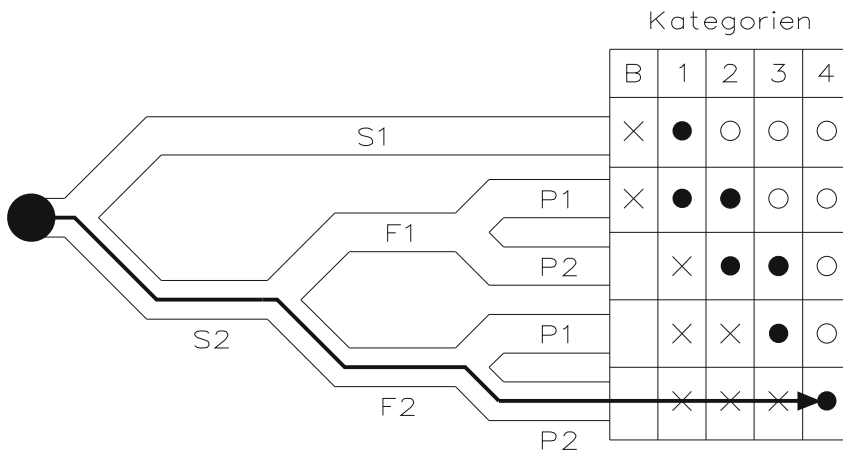


Abb. 2.8 Ergebnis des Beispiels einer Risikoabschätzung nach Berücksichtigung der Gefährdungsgruppe

2.12 Risikobeurteilung

Was ändert sich durch die ISO 13 849-1?

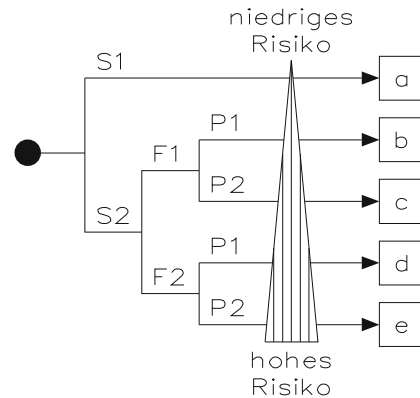
1. Durch Übernahme der Norm zum ISO ändert sich die Nummerierung von 954 in 13849,
2. Bewertung der Zeit bis zum gefährlichen Ausfall,
3. Qualifizierung der Diagnose,
4. Einführung von „Performance Level“,
5. Berücksichtigung Fehler gemeinsamer Ursache,
6. Änderung des Risikographen.

Die Risikoparameter S, F und P werden weiterhin ein wichtiges Auswahlkriterium sein, aber nicht mehr zur Kategorie, sondern zum Performance Level führen. Dies ist dann der so genannte „erforderliche“ PLr, der mit dem „erreichten“ PL validiert werden muss.

Die Risikoparameter S, F und P sind

- **S_Schwere der Verletzung:**
 - S1 = leichte (normalerweise reversible) Verletzung,
 - S2 = schwere (normalerweise irreversible) Verletzung einschließlich Tod.
- **F_Häufigkeit und/oder Dauer der Gefährdungsexposition**
 - F1 = selten bis öfters und/oder kurze Dauer,
 - F2 = häufig bis dauernd und/oder lange Dauer.

Abb. 2.9 Risikograph zum Ermitteln des erforderlichen „Performance Level“



- **P**_Möglichkeiten zur Vermeidung der Gefährdung
 - P1 = möglich unter bestimmten Bedingungen,
 - P2 = kaum möglich.
- **a, b, c, d, e** = sicherheitsrelevante „Performance Level“.

Abb. 2.9 zeigt den Risikograph zum Ermitteln des erforderlichen „Performance Level“. Hat man jetzt einen „Performance Level“ und es stehen als nächstes mehrere Entscheidungen an:

- Welche Struktur soll die Steuerung und deren Verdrahtung aufweisen?
- Welche Prüftiefe bzw. welchen Diagnosedeckungsgrad DC hat diese Steuerung?
- Welche Qualität bzw. $MTTF_d$ haben die verwendeten Komponenten?
- Welcher Fehler gemeinsamer Ursache bzw. welcher CCF wird akzeptiert?

Hierzu ist es natürlich wichtig zu wissen, was DC, CCF und $MTTF_d$ überhaupt bedeuten.

Der Diagnosedeckungsgrad DC ist die teilweise Verminderung der Wahrscheinlichkeit von gefahrbringenden Hardwareausfällen aufgrund der Anwendung automatischer diagnostischer Prüfung. Ermittelt werden kann dieser aus der Wahrscheinlichkeit λ_{DD} von erkannten gefahrbringenden Ausfällen und der Wahrscheinlichkeit Σ_{Dtotal} aller gefahrbringenden Ausfälle mit folgender Gleichung:

$$DC = \frac{\sum \lambda_{DD}}{\sum \Sigma_{Dtotal}}$$

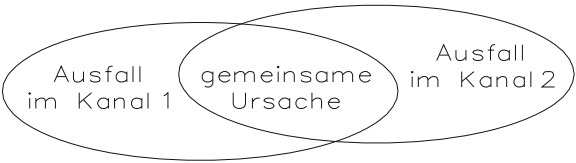
Der Diagnosedeckungsgrad wird in Stufen unterteilt, wie Tab. 2.8 zeigt.

Genaugenommen geht es hierbei um die Prüftiefe und die Fehlererkennung. Es gibt Fehler, die relativ leicht zu erkennen sind, und es gibt Fehler, die nur mit sehr viel Aufwand erkannt werden. Auch gibt es Fehler, die in ihrer Auswirkung harmlos sind und eigentlich gar nicht als Fehler eingestuft werden, jedoch im Zusammenspiel mit anderen „harmlosen“ Fehlern einen gefährlichen Zustand hervorrufen können.

Tab. 2.8 Deckungsgrad im Bereich des DC

Deckungsgrad	Bereich des DC
Ohne	DC < 60 %
Niedrig	60 % = DC < 90 %
Mittel	90 % = DC < 99 %
Hoch	99 % = DC

Abb. 2.10 Ausfälle gleicher Ursache in homogenen Systemen, CCF



Die Praxis hat gezeigt, dass auch redundante Systeme frühzeitig gefährlich ausfallen können. Die Ursachen sind dann in der Regel nicht systematische Fehler, sondern Frühaustritte. Diese sind dann meist nicht auf Verschleiß oder Überalterung, sondern auf einen Herstellerfehler zurückzuführen. Handelt es sich bei diesem Herstellerfehler nicht um einen Ausreißer, sondern um einen Chargenfehler, sind alle Bauteile mit demselben Herstellerdatum, aus demselben Fertigungsprozess usw. betroffen. Wird dies nicht erkannt und kommen solche Bauteile in Schaltkreisen, die der Sicherheit dienen, zum Einsatz, wird redundanzbedingtes Duplizieren die Ausfallwahrscheinlichkeit nicht wesentlich verändern. Denn warum soll ein fehlerbehaftetes Bauteil im Kanal A zuverlässiger sein als im identisch aufgebauten Kanal B. Abb. 2.10 zeigt Ausfälle gleicher Ursache in homogenen Systemen.

Die Wahrscheinlichkeit von gefährlichen Ausfällen gemeinsamer Ursache ist:

$$\lambda_{DU} \cdot CCF + \lambda_{DD} \cdot CCF_D,$$

- λ_{DU} : Wahrscheinlichkeit unentdeckter zufälliger gefährlicher Ausfälle eines einzelnen Kanals,
- λ_{DD} : Wahrscheinlichkeit aufgedeckter zufälliger gefährlicher Ausfälle eines einzelnen Kanals,
- CCF: Anteil von Ausfällen, die eine gemeinsame Ursache aufweisen (Common Cause Failure),
- CCF_D : CCF-Faktor aufgedeckter gefährlicher Ausfälle, steigt mit steigender Testrate.

Es gibt eigentlich nur ein Mittel um Ausfälle gleicher Ursache zu beherrschen, und das ist Diversität. Diversität ist Redundanz mit unterschiedlichen Bauteilen, Techniken oder Prinzipien.

Der Mathematiker A. A. Markov entwickelte Anfang des 20. Jahrhundert ein Wahrscheinlichkeitsmodell mit der Absicht, in Puschkins Werk „Onegin“ die Häufigkeit der Konsonanten zu ermitteln. Dieses Modell geht davon aus, dass jeder Zustand lediglich

vom vorherigen Zustand abhängig ist. Das Ziel des Markov-Modells ist die Berechnung der Wahrscheinlichkeit, dass sich ein System zu einem bestimmten Zeitpunkt in einem bestimmten Zustand befindet, somit ist auch die Zuverlässigkeit sowie die Sicherheit oder die Verfügbarkeit gegeben.

Das Ziel und die Technik dieses Markov-Modells ist, die Zuverlässigkeit sowie die Sicherheit oder Verfügbarkeit zu bewerten. Es ist anwendbar zur Modellierung redundanter Systeme, in denen der Grad der Redundanz sich in zeitlicher Abhängigkeit von Komponentenausfällen oder Reparaturen ändert. Denn die Wahrscheinlichkeit, dass sich ein System nach Ablauf eines Zeitraums Δt in einem Zustand i_{k+1} befindet, hängt nur von den Zustandswahrscheinlichkeiten im aktuellen Zeitpunkt t_k sowie den Übergangsraten ab, jedoch nicht von den Zustandswahrscheinlichkeiten zu den weiter zurückliegenden Zeitpunkten.

2.12.1 Ausfallwahrscheinlichkeit

Mit Hilfe des Markov-Modells kann die durchschnittliche Wahrscheinlichkeit PDF (Probability of dangerous Failures ist eine gefährliche Ausfallwahrscheinlichkeit und Wahrscheinlichkeit des Eintretens eines gefährlichen Systemausfalls) eines gefährlichen Ausfalls pro Stunde errechnet werden:

$$PDF_{avg} \approx \frac{1}{2} \lambda_{DF} \cdot T_i = T_i / (2 \cdot MTBF_{FTD}),$$

T_i = Zeitabstand zwischen den funktionalen Prüfungen eines Bestandteils,

$MTBF$ = ist die mittlere Zeit bis zum Bauteileausfall ($MTBF$ = mean time between failures),

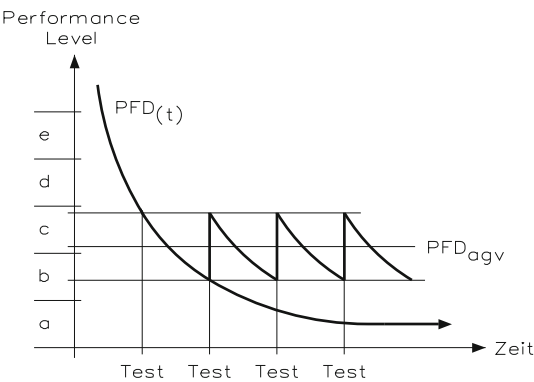
λ_{DF} = ist die Summe aller gefährlichen Fehler.

Das Modell geht von der Tatsache aus, dass jedes System ausfällt, wenn man nur lange genug wartet. Statistisch gesehen kann angenommen werden, dass nach Ablauf der MTTF von 63,2 % ($MTTF$ = mean time to failures) die betreffenden Komponenten ausgefallen sind. Wobei die typischen Frühausfälle und Alterungsprozesse nicht berücksichtigt sind. Man kann sogar unterstellen, dass sich ein System im Laufe seiner Lebensphasen von einem hochsicheren System zu einem unsicheren System wandeln kann. Um diesem Phänomen entgegenzuwirken, hat man zwei Möglichkeiten:

- das System qualitativ so hochwertig zu gestalten, dass der gefährliche Ausfall erst nach Ablauf der Benutzungsdauer eintritt oder
- das System regelmäßig zu testen um sicherzustellen, dass die geforderten Funktionen bei der nächsten Anforderung noch gewährleistet sind.

Abb. 2.11 zeigt die Abhängigkeit zwischen $MTTF_d$ und DC, denn je nach Testrate verändert sich die Zeit bis zum gefährlichen Ausfall eines Systems. Ein anfänglich sicheres

Abb. 2.11 PFD_{avg} ist der mittlere Ausfall, Versagenswahrscheinlichkeit bei Anforderung



System mit einem „Performance Level“ rutscht im Laufe der Zeit durch Defekt und Verlust von Eigenschaften und Funktionen nach und nach auf das Niveau von „Performance Level“ a. Natürlich werden verlorengegangene Eigenschaften nicht mehr erreicht, durch Tests nicht wieder zurückgeholt, aber wenn das geforderte „Performance Level“ nicht mehr erreicht wird, geht das System in Betriebshemmung und stellt so einen sicheren Zustand her. Die Bezeichnung PFD steht für „Probability of Failure on Demand“ und definiert die Ausfallwahrscheinlichkeit bei Anforderung (Versagungswahrscheinlichkeit der Sicherheitsfunktion) bei ihrer Anforderung bzw. Auslösung nach DIN EN 61508, die für Betriebsarten mit niedriger Anforderungsrate der Sicherheitsfunktion eine Rolle spielt.

Allgemein kann die MTTF (mean time to failures) für ein System bestehend aus Einzelkomponenten wie folgt beschrieben werden:

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{d,i}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{d,j}}.$$

Die Zeit bis zum gefährlichen Ausfall wird in drei Bereiche aufgeteilt, wie Tab. 2.9 zeigt.

Bei den Kategorien hat sich nicht viel verändert, außer, dass nicht mehr der Weg zur Kategorie das Ziel ist, sondern die Kategorie auf dem Weg zum „Performance Level“ helfen soll. Folgende Parameter sind hierfür heranzuziehen:

Tab. 2.9 Zeit bis zum gefährlichen Ausfall

Bewertung	$MTTF_d$
Niedrig	3 Jahre = $MTTF_d < 10$ Jahre
Mittel	10 Jahre = $MTTF_d < 30$ Jahre
Hoch	30 Jahre = $MTTF_d < 100$ Jahre

- S = Schwere der Verletzung,
- F = Häufigkeit und/oder Dauer der Gefährdungsexposition,
- P = Möglichkeiten zur Vermeidung der Gefährdung,
- DC = Diagnosedeckungsgrad,
- $MTTF_d$ = Zeit bis zum gefährlichen Ausfall,
- $MTTF_{oc}$ = Zeit bis zum gefährlichen Ausfall eines Kanals,
- CCF = Fehler gemeinsamer Ursache.

2.12.2 Kategorie B

Abb. 2.12 zeigt die Funktionen der Kategorie B.

Kategorie	Anforderung	Systemverhalten	$MTTF_{oc}$	DC_{avg}	PL	CCF in %
B	Die sicherheitsbezogenen Teile von Steuerungen müssen nach den zutreffenden Normen unter Verwendung grundlegender Sicherheitsprinzipien gestaltet/validiert werden	Wenn ein Fehler auftritt, kann er zum Verlust der Sicherheitsfunktion führen	Low–medium	–	a–b	–



Abb. 2.12 Einfaches System, Kategorie B. *I* Input bzw. Sensor, *L* Logic, *O* Output bzw. Actuator

Abb. 2.13 zeigt die Funktionen der Kategorie 1.

Kategorie	Anforderung	Systemverhalten	$MTTF_{oc}$	DC_{avg}	PL	CCF in %
1	Die Anforderungen von B müssen erfüllt sein. Die sicherheitsbezogenen Teile der Kategorie 1 müssen unter Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien gestaltet, gebaut und validiert werden	Das Ereignis eines Fehlers kann zu dem Verlust der Sicherheitsfunktion führen, aber mit höherer Zuverlässigkeit als bei Kategorie B	High	–	a–b	–



Abb. 2.13 Einfaches System mit hoher Zuverlässigkeit, Kategorie 1. *I* Input bzw. Sensor, *L* Logic, *O* Output bzw. Actuator

Abb. 2.14 zeigt die Funktionen der Kategorie 2.

Kategorie	Anforderung	Systemverhalten	MTTF _{oc}	DC _{avg}	PL	CCF in %
2	Die Anforderungen von B müssen erfüllt sein und die Sicherheitsfunktion muss in geeigneten Zeitabständen von der Maschinensteuerung geprüft werden	Das Ereignis eines Fehlers kann zu dem Verlust der Sicherheitsfunktion führen. Der Verlust der Sicherheit wird erkannt	Low–high	–	a–b	>65

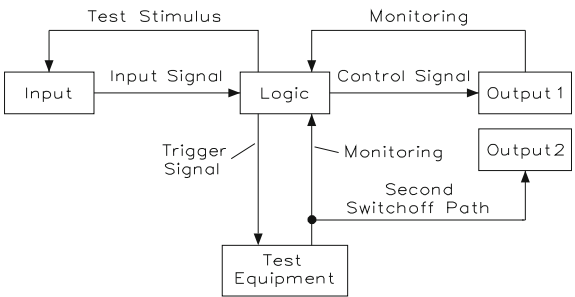


Abb. 2.14 Einkanaliges System mit Testung, Kategorie 2. *I* Input bzw. Sensor, *L* Logic, *O* Output bzw. Actuator, *TE* Test Equipment

Ob auch für den Hauptstromkreis, wie aus Abb. 2.14 entnommen werden kann, tatsächlich Redundanz gefordert sein wird, steht vermutlich erst nach Ratifizierung der ISO 13849-1 fest.

Abb. 2.15 zeigt die Funktionen der Kategorie 3.

Kategorie	Anforderung	Systemverhalten	MTTF _{oc}	DC _{avg}	PL	CCF in %
3	Die sicherheitsbezogenen Teile von Steuerungen müssen nach den zutreffenden Normen unter Verwendung der grundlegenden Sicherheitsprinzipien gestaltet/validiert werden	Wenn ein Fehler auftritt, kann er zum Verlust der Sicherheitsfunktion führen	Low–high	Low–medium	a–e	>65

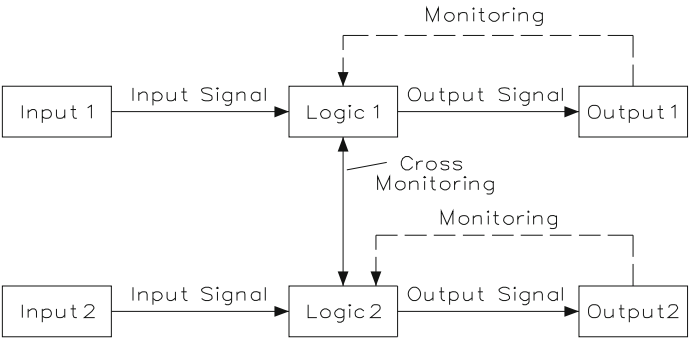


Abb. 2.15 Zweikanaliges System mit partieller Fehlererkennung, Kategorie 3. *I1, I2* Input bzw. Sensor, *L1, L2* Logic, *O1, O2* Output bzw. Aktuator

Ob auch für den Hauptstromkreis, wie Abb. 3.18 entnommen werden kann, tatsächlich Redundanz gefordert sein wird, steht vermutlich erst nach Ratifizierung der ISO 13849-1 fest.

Abb. 2.16 zeigt die Funktionen der Kategorie 4.

Kategorie	Anforderung	Systemverhalten	MTTF _{oc}	DC _{avg}	PL	CCF in %
4	Die sicherheitsbezogenen Teile von Steuerungen müssen nach den zutreffenden Normen unter Verwendung der grundlegenden Sicherheitsprinzipien gestaltet/validiert werden	Wenn ein Fehler auftritt, kann er zum Verlust der Sicherheitsfunktion führen	High	High	e	>65

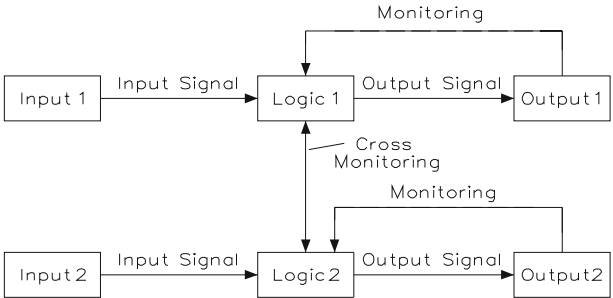


Abb. 2.16 Zweikanaliges System mit Einfehlersicherheit, Kategorie 4. *I1, I2* Input bzw. Sensor, *L1, L2* Logic, *O1, O2* Output bzw. Aktuator

Tab. 2.10 Zusammenfassung der meisten sicherheitsrelevanten Anforderungen nach ISO 13849-1

Struktur	CCF	DC _{avg}	MTTF _{OC}	Kategorien	PL
Mono	/	/	Low	B	a
Mono	/	/	Medium	B	b
Mono	/	/	High	1	c
Mono	Erreicht	Low	Low	2	a–b
Mono	Erreicht	Low	Medium	2	b–c
Mono	Erreicht	Low	High	2	c–d
Mono	Erreicht	Medium	Low	2	c
Mono	Erreicht	Medium	Medium	2	c–d
Mono	Erreicht	Medium	High	2	d
Redundant	Erreicht	Low	Low	3	b
Redundant	Erreicht	Low	Medium	3	c–d
Redundant	Erreicht	Low	High	3	d
Redundant	Erreicht	Medium	Low	3	b–c
Redundant	Erreicht	Medium	Medium	3	d
Redundant	Erreicht	Medium	High	3	d–e
Redundant	Erreicht	High	High	4	e

2.12.3 Zusammenfassung der meisten sicherheitsrelevanten Anforderungen

DC_{avg} = Diagnosedeckungsgrad bei Anforderung,
 CCF = Fehler gemeinsamer Ursache,
 MTTF_{OC} = Zeit bis zum gefährlichen Ausfall eines Kanals,
 r_t = Diagnose-Testrate,
 r_d = Anforderungsrate der Sicherheitsfunktion,
 r_r = Reparaturrate,
 PL = Performance Level.

Da die hier aufgezeigte Vorgehensweise von der EN IEC 61508 abgeleitet ist, liegt es natürlich nahe, die SIL der EN IEC 61508 mit den PL der ISO 13849 zu vergleichen. Diese Vergleichstabelle ist nicht wie Vergleiche der EN 954-1 mit der EN IEC 61508 nur eine Näherung, sondern direkt der ISO 13849 entnommen. Tab. 2.11 zeigt den Vergleich SIL der EN IEC 61508 mit PL der ISO 13849.

Beispiel einer Risikobestimmung nach ISO 13849

Unter Verwendung eines Beispiels wird versucht eine Risikoanalyse nach ISO 13849 durchzuführen.

Aufgabe: Überwachung einer Schutztür in Kategorie 3 oder 4 Verwendung (Abb. 2.17) einer Sicherheitssteuerung vom Typ PSS

Tab. 2.11 Vergleich SIL der EN IEC 61508 mit PL der ISO 13849

Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde [1/h]	PL, – ISO 13849-1, Performance Level	SIL, – EN IEC 61508 Safety Integrity Level
$10^{-3} < \text{PDF} < 10^{-4}$	a	
$3 \cdot 10^{-3} < \text{PDF} < 10^{-5}$	b	1
$10^{-6} < \text{PDF} < 3 \cdot 10^{-6}$	c	1
$10^{-7} < \text{PDF} < 10^{-6}$	d	2
$10^{-8} < \text{PDF} < 10^{-7}$	e	3

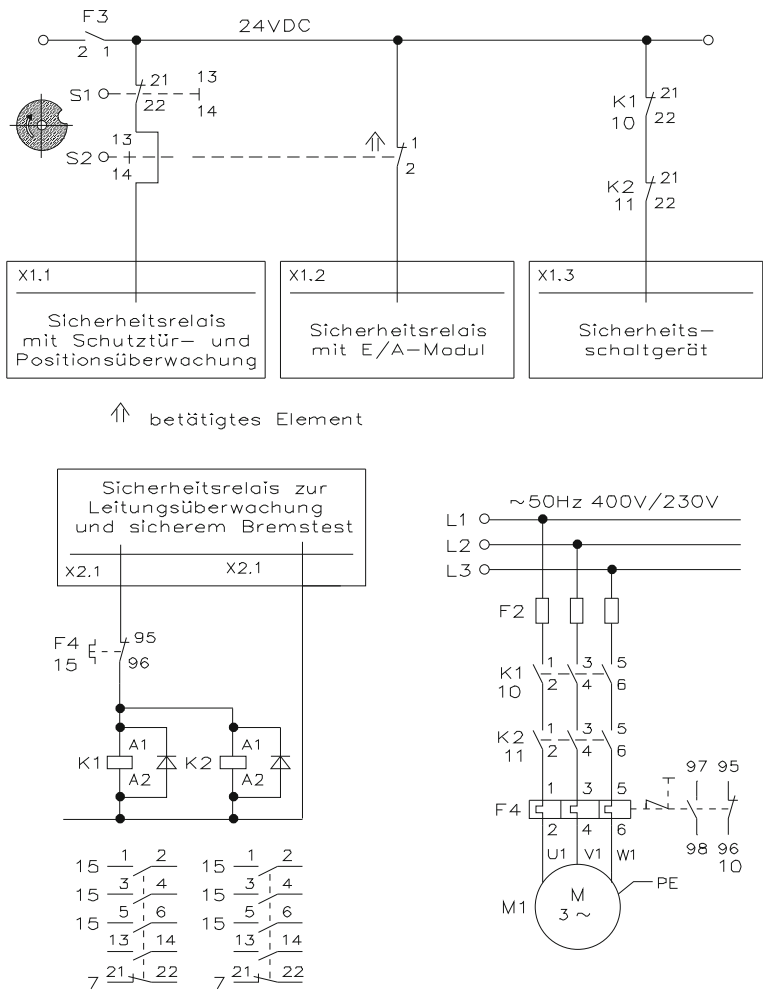


Abb. 2.17 Anschlussbeispiel einer Ansteuerung für eine Drehmaschine

Struktur: Redundanz bei Positionsschalter und Verdrahtung

Bestimmung der $MTTF_{oc}$ -Zeit bis zum gefährlichen Ausfall eines Kanals

Zur Ermittlung der $MTTF_{oc}$ ist zu klären ob das System in

1. einkanaliger Struktur,
2. redundanter homogener Struktur,
3. redundanter diversitärer Struktur

realisiert werden soll. Handelt es sich um eine einkanalige Struktur, dann ist $MTTF_{oc} = MTTF_d$.

Wird eine homogene redundante Struktur ausgewählt, ist die $MTTF_{oc}$ für alle Kanäle gleich.

Bei diversitärer redundanter Struktur ist entweder die ungünstige der ermittelten $MTTF_{oc}$ auszuwählen oder deren Mittelwert anzuwenden.

Eine diversitäre Struktur liegt z. B. vor, wenn Positionsschalter unterschiedlichen Typs, unterschiedlicher Hersteller und/oder somit auch, unterschiedlicher $MTTF_d$ eingesetzt werden.

Die Quelle der $MTTF_d$ -Werte für Geräte sollte in der Regel deren Hersteller sein. Ist dies nicht möglich, kann man entsprechende Datenbanken heranziehen, die typische Werte enthalten. Für die Worst-Case-Abschätzung der $MTTF_d$ wird in der Regel ein Sicherheitsfaktor von 10 eingerechnet.

Für das Beispiel nimmt man folgende $MTTF_d$ für die einzelnen Geräte an, wie Abb. 2.18 zeigt.

- a) Positionsschalter S1 hat eine $MTTF_d$ von 15 Jahren (geschätzter Wert für diese Konstellation).
- b) Positionsschalter S2 hat eine $MTTF_d$ von 30 Jahren (geschätzter Wert für diese Konstellation).
- c) Sicherheitssteuerung hat eine $MTTF_d$ von 60 Jahren (vermuteter Worst-Case-Wert).
- d) Schütz K1/K2 hat eine $MTTF_d$ von 32 Jahren (ISO 13849-1).

$$\begin{aligned} \text{Kanal 1: } \frac{1}{MTTF_{d,C1}} &= \frac{1}{MTTF_{d,S1}} + \frac{1}{MTTF_{d,PSS}} + \frac{1}{MTTF_{d,K1}} \\ \frac{1}{MTTF_{d,C1}} &= \frac{1}{15 \text{ Jahre}} + \frac{1}{60 \text{ Jahre}} + \frac{1}{32 \text{ Jahre}} = 0,11 \Rightarrow MTTF_{d,C1} = 8,7 \\ \text{Kanal 2: } \frac{1}{MTTF_{d,C2}} &= \frac{1}{MTTF_{d,S2}} + \frac{1}{MTTF_{d,PSS}} + \frac{1}{MTTF_{d,K2}} \\ \frac{1}{MTTF_{d,C2}} &= \frac{1}{30 \text{ Jahre}} + \frac{1}{60 \text{ Jahre}} + \frac{1}{32 \text{ Jahre}} = 0,08125 \\ &\Rightarrow MTTF_{d,C2} = 12,3 \text{ Jahre} \end{aligned}$$

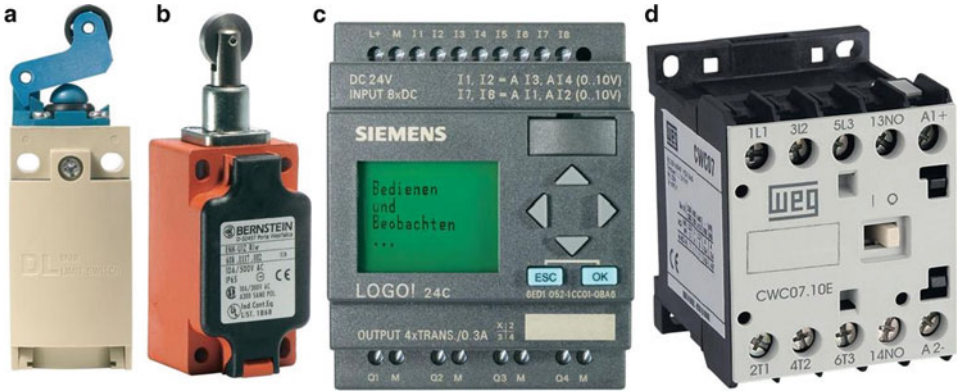


Abb. 2.18 $MTTF_d$ für zwei Positionsschalter, eine Sicherheitssteuerung und zwei Schütze K1/K2

Mit Hilfe der Mittelungsformel lässt sich näherungsweise eine gleichwertige homogene Struktur errechnen:

$$MTTF_d = \frac{2}{3} \left[MTTF_{d,C1} + MTTF_{d,C2} - \frac{1}{\frac{1}{MTTF_{d,C1}} + \frac{1}{MTTF_{d,C2}}} \right] = 10,5 \text{ Jahre.}$$

Ermittlung von DC_{avg} :

Berücksichtigung von $DC_{avg} = S1_{DD} / S1_{total}$ lässt sich der durchschnittliche DC bestimmen.

Für das Beispiel von Abb. 2.18 nimmt man folgende DC_{avg} Werte an:

- Positionsschalter S1 hat einen DC von 90 %.
- Positionsschalter S2 hat einen DC von 90 %.
- Sicherheitssteuerung PSS hat einen DC von 99 %.
- Schütze K1/K2 haben einen DC von 99 %.

Die Quelle der DC_{avg} -Werte sind:

- Positionsschalter können je nach Beschaltung einen unterschiedlichen Diagnosedegrad haben. Werden Positionsschalter mit intelligenter Elektronik verknüpft, so kann wie im Beispiel ein geeigneter Softwarebaustein Plausibilitätstests durchführen. Da Positionsschalter nur durch Öffnen und Schließen der Schutztüren getestet werden können, erreicht man bei diesem Beispiel mangels Testrate nur ein mittleres $DC = 90 \%$.
- Schütze, die zwangsgeführt sind, lassen sich durch Rückführung eines Öffnerkontakts zur Sicherheitssteuerung auf Stellung überwachen. Deshalb kann für dieses Bauteil ein hoher $DC = 99 \%$ eingesetzt werden. Dieser hohe DC ist jedoch nur gegeben, wenn

die Zwangsführung nach EN 50205 zwischen den Hauptkontakten (Schließer) und den Hilfskontakten (Öffner) gegeben ist. Die Praxis zeigt jedoch, dass bei Schützen größer 5,5 kW in der Regel die Zwangsführung nur zwischen den Hauptkontakten (Schließer) besteht. Dies entspricht dann nicht den Forderungen der EN 50205.

- Schütze ohne Rückführung (ohne Zwangsführung) können weil Ruhestromprinzip in DC = 60 % eingestuft werden. Mit 60 % fallen die Schütze in den Bereich „gering“.
- Sicherheitssteuerung, wie alle variablen Systeme verändert sich auch bei dieser je nach Konstellation der Diagnosedeckungsgrad, (z. B. für Eingangskreise, Mikroprozessor und Ausgänge). Daher müssten für bestimmte PSS-Konfigurationen die Werte für I_{DD} und I_{total} angegeben werden. Angenommener Wert des DC für diese Konstellation ist 99 %.

Um den DC_{avg} bestimmen zu können, muss jede an der Sicherheitsfunktion beteiligte Komponente mit einbezogen werden. Die PSS bekommt aufgrund ihrer redundanten Struktur einen Faktor von 2, denn sie ist wie zwei Sicherheitskreise zu betrachten.

Daraus ergibt sich

$$DC_{avg} = \frac{0,9 \cdot \frac{1}{MTTF_{S1}}}{\frac{1}{MTTF_{S1}}} + \frac{0,9 \cdot \frac{1}{MTTF_{S2}}}{\frac{1}{MTTF_{S2}}} + \frac{2 \cdot 0,99 \cdot \frac{1}{MTTF_{PSS}}}{2 \cdot \frac{1}{MTTF_{PSS}}} + \frac{0,99 \cdot \frac{1}{MTTF_{K1}}}{\frac{1}{MTTF_{K1}}} + \frac{0,99 \cdot \frac{1}{MTTF_{K2}}}{\frac{1}{MTTF_{K2}}} = 0,94.$$

Nach Tabelle „Diagnosedeckungsgrad“ sind 94 % DC als „mittel“ einzustufen.

Hierdurch ist zu erkennen, dass fehlende Rückführung der Schütze K1/K2 oder das Verwenden von Schützen ohne Zwangsführung das Gesamtergebnis entscheidend ins Negative korrigiert. Der DC_{avg} würde ca. 80 % fallen und somit nach Tabelle „Diagnosedeckungsgrad“ als „gering“ einzustufen sein.

Der „Common Cause Faktor“ (CCF) wird in ISO 13849-2 abgehandelt. Es hat sich jedoch gezeigt, dass der CCF bis zu einem bestimmten Wert (2 %) das Gesamtergebnis nur unwesentlich beeinflusst. Ein vereinfachtes Verfahren zur Ermittlung der maximalen Wertigkeit von risikoreduzierenden Maßnahmen zeigt in Anlehnung an den Teil 6 der EN IEC 61508 Tabelle. Wird mehr als 65 % Übereinstimmung erreicht, so können die Anforderungen für den CCF als erfüllt betrachtet werden.

Nach Tab. 2.12 ist bei folgendem Design ein CCF von größer 65 % gegeben.

Es wurde ein redundantes System mit partieller Fehlererkennung ausgewählt und dies ergibt Kategorie 3.

Tab. 2.13 zeigt typische Werte nach Kategorie 3.

Bei diesem Beispiel wurden alle Komponenten und deren Verschaltung so ausgewählt, dass maximale Sicherheit und ein hoher Diagnosedeckungsgrad erreicht wurde. Dass dieser Wunschraum nicht immer erfüllt werden kann, liegt an der Tatsache, dass die ausgewählten Komponenten oftmals die in sie gesetzten Erwartungen nicht erfüllen.

Tab. 2.12 Prozentuale Punktevergabe für Maßnahmen zur Vermeidung von Fehlern gemeinsamer Ursache

Nr.	Anforderung	Punkte
1	Trennung	
	Physikalische Trennung zwischen den Sicherheitskreisen und zu anderen Kreisen, z. B. getrennte Verlegung, Mantelleitungen, Einhaltung der Luft und Kriechstrecken auf Platinen für Trennung nach DIN VDE 0100	15 %
2	Diversität	
	Verschiedene Technologien verwenden, verschiedenartiges Design oder Prinzipien. Komponenten verschiedener Hersteller	20 %
3	Entwurf/Applikation/Erfahrung	
	Schutz gegen Überspannung, Überdruck, Überstrom, usw.	15 %
	Anwendung hinsichtlich Umwelteinflüssen bewährter Prinzipien	5 %
4	Beurteilung/Analyse	
	Wurden die Ergebnisse einer Fehleranalyse in Betracht gezogen, um Fehler gemeinsamer Ursache im Entwurf zu vermeiden?	5 %
5	Kompetenz/Ausbildung	
	Sind Entwickler geschult worden, die Ursachen und Folgen von Ausfällen gemeinsamer Ursache, zu erkennen, zu verstehen und zu vermeiden?	5 %
6	Umwelteinflüsse	
	EMV getestet	25 %
	Temperatur, Schock, Vibration, Luftfeuchtigkeit getestet, Einhaltung von Produktnormen	10 %

Tab. 2.13 Hoher AC_{avg} ergibt einen „Performance Level“ von d und eine Kategorie von 3

Kanal 1	Kanal 2	MTTF/Jahre	DC %	CCF	Redundanz	Jahre	MTTF _d	Einstufung
S1	–	15	90	88	Redundant	8,7	MTTF _{d,C1}	Low
–	S2	30	90			12,3	MTTF _{d,C2}	Medium
PSS	–	60	99					
–	PSS	60	99			> 65 %	CCF	Erreicht
K1	–	32	99			11	MTTF _d	Medium
–	K2	32	99			0,94	DC _{avg}	Medium
							Kategorie	3
							Per. Level	d

Beispielsweise ist man bei den Schützen von $DC_{avg} \approx 99 \%$ ausgegangen. Dieser Wert ist jedoch nur zu erreichen, wenn Stellungsüberwachung gegeben ist. Stellungsüberwachung eines Schützes erreicht man durch Abfragen eines Öffnerkontakts, ob dieser in Ruhstellung geschlossen ist. Dies funktioniert jedoch nur, wenn die Hilfskontakte, denn der Öffner ist ein Hilfskontakt, und die Lastkontakte nach EN 50205 zwangsgeführt sind. Erfüllt das Schütz diese Anforderung nicht, so kann es, weil das Ruhestromprinzip angewendet wird, in $DC_{avg} \approx 60 \%$ eingestuft werden. In der Regel liegt die Grenze bei 5,5 kW,

Tab. 2.14 Ungünstiger Wert von DC_{avg} ergibt einen „Performance Level“ von c und eine Kategorie von 3

Kanal 1	Kanal 2	MTTF/Jahre	DC %	CCF	Redundanz	Jahre	MTTF _d	Einstufung
S1	–	15	90	88	Redundant	8,7	MTTF _{d,C1}	Low
–	S2	30	90			12,3	MTTF _{d,C2}	Medium
PSS	–	60	99					
–	PSS	60	99			> 65 %	CCF	Erreicht
K1	–	32	60			11	MTTF _d	Medium
–	K2	32	60			0,82	DC_{avg}	Low
							Kategorie	3
							Per. Level	c

d. h. hat das Schütz eine größere Schaltleistung als 5,5 kW, ist nicht von Zwangsführung aller Kontakte auszugehen.

Änderung für nachfolgendes Beispiel ohne Zwangsführung: Schütze K1/K2 haben einen DC von 60 %.

Tab. 2.14 zeigt die Reduzierung des DC der Schütze wegen mangelnder Zwangsführung.

2.13 Neue Risikobewertung

Der Zweck des Bewertungs- und Validierungsverfahrens ist, die Spezifikation und die Konformität der Gestaltung der sicherheitsbezogenen Teile der Steuerung innerhalb der Gesamtspezifikation für die Sicherheitsanforderungen an der Maschine zu bestätigen. So beschreibt sich die Norm und zeigt mit einem Flussdiagramm (Abb. 2.19) die Vorgehensweise auf.

Die Tab. 2.15 2.16, 2.17 und 2.18 zeigen die Möglichkeiten zur Validierung für mechanische Systeme, pneumatische Systeme, hydraulische Systeme und elektrische Systeme. Die Auflistung ist nicht vollständig und soll nur aufzeigen, was mit grundlegenden oder bewährten Sicherheitsprinzipien, bewährten Bauteilen und Fehlerausschlüssen bezeichnet wird. Auch hier lautet die Empfehlung, „Norm kaufen und lesen“.

Bei Anwendung mechanischer Systeme für die Validierung (Tab. 2.15) sind die einzelnen Punkte einzuhalten.

Bei Anwendung von pneumatischen Systemen für die Validierung (Tab. 2.16) sind die einzelnen Punkte einzuhalten.

Bei Anwendung hydraulischer Systeme für die Validierung (Tab. 2.17) sind die einzelnen Punkte einzuhalten.

Bei Anwendung von elektrischen Systemen für die Validierung (Tab. 2.18) sind die einzelnen Punkte einzuhalten.

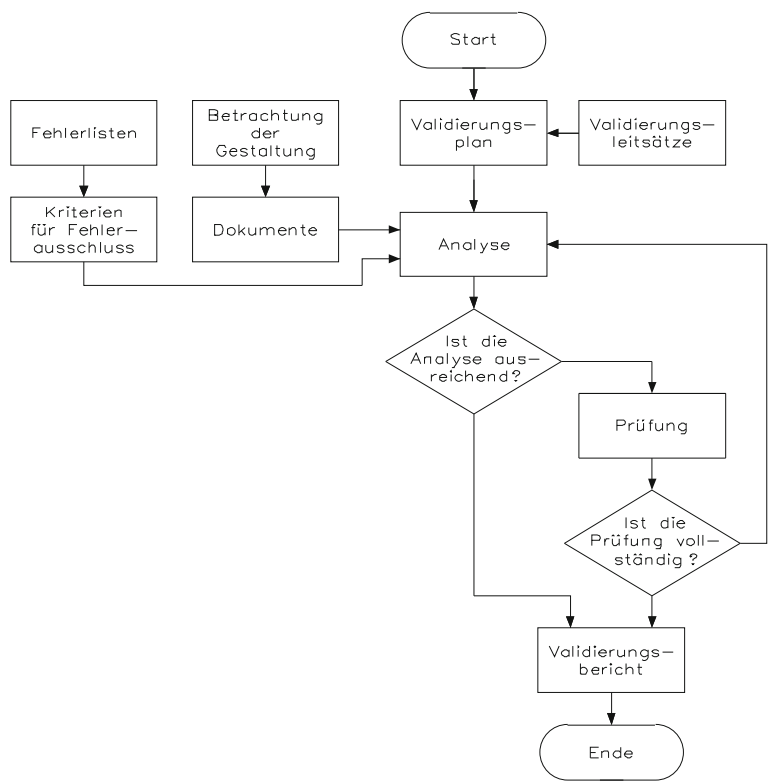


Abb. 2.19 Flussdiagramm über das Validierungsverfahren

Tab. 2.15 Anwendung für mechanische Systeme

Grundlegende Sicherheitsprinzipien	Bewährte Sicherheitsprinzipien	Bewährte Bauteile	Fehlerlisten und Fehlerausschlüsse
– Anwendung geeigneter Werkstoffe und Herstellungsverfahren, – richtige Dimensionierung und Formgebung, – geeignete Befestigung, – geeignete Reaktionszeit, usw.	– Anwendung des Prinzips der Energietrennung, – Anwendung von Bauteilen mit definiertem Ausfallverhalten, – Überdimensionierung, – zwangsläufige mechanische Wirkung/Betätigung, – Vervielfachung von Teilen, usw.	Schrauben, Federn, Nocken und Abscherstifte, wenn diese den Anforderungen entsprechen	– Fehlerannahmen wie z. B. Verschleiß/Korrosion, Bruch, Verformung usw., – Fehlerausschluss durch Überdimensionierung usw.

Tab. 2.16 Anwendung für pneumatische Systeme

Grundlegende Sicherheitsprinzipien	Bewährte Sicherheitsprinzipien	Bewährte Bauteile	Fehlerlisten und Fehlerausschlüsse
– Anwendung geeigneter Werkstoffe und Herstellungsverfahren, – richtige Dimensionierung und Formgebung, – Anwendung des Prinzips der Energietrennung, – geeignete Befestigung, – ausreichende Maßnahmen zur Vermeidung von Verunreinigung der Druckluft, – geeigneter Schaltbereich, – Schutz gegen unerwarteten Anlauf, usw.	– Durch Lastdruck schließendes Ventil, – Überdimensionierung, – zwangsläufige mechanische Wirkung/Betätigung, – Vervielfachung von Teilen, – geeignete Vermeidung von Verunreinigung der Druckluft	Z. Z. ist keine Liste von bewährten Bauteilen vorhanden, denn ein für eine bestimmte Anwendung bewährtes Bauteil kann für eine andere Anwendung ungeeignet sein	Tabellen für Wegeventile, Absperrventile, Stromregelventile, Druckventile, Rohrleitungen, Schlauchleitungen, Verbindungselemente, Druckwandler, Filter, Öler, Schalldämpfer, Druckbehälter, Sensoren usw.

Tab. 2.17 Anwendung für hydraulische Systeme

Grundlegende Sicherheitsprinzipien	Bewährte Sicherheitsprinzipien	Bewährte Bauteile	Fehlerlisten und Fehlerausschlüsse
– Anwendung geeigneter Werkstoffe und Herstellungsverfahren, – richtige Dimensionierung und Formgebung, – Anwendung des Prinzips der Energietrennung, – geeignete Befestigung, – Druckbegrenzung, – geeigneter Schaltzeitbereich, – Vereinfachung, – Trennung, usw.	– Überdimensionierung, – gesicherte Position, – durch Lastdruck schließendes Ventil, – zwangsläufige mechanische Wirkung/Betätigung, usw.	Z. Z. ist keine Liste von bewährten Bauteilen vorhanden, denn ein für eine bestimmte Anwendung bewährtes Bauteil kann für eine andere Anwendung ungeeignet sein	– Fehlerannahmen wie z. B. Verändern der Schaltzeiten, Nichtschalten bzw. Hängenbleiben usw., – Fehlerausschluss durch zwangsläufige mechanische Betätigung usw.

Tab. 2.18 Anwendung für elektrische Systeme

Grundlegende Sicherheitsprinzipien	Bewährte Sicherheitsprinzipien	Bewährte Bauteile	Fehlerlisten und Fehlerausschlüsse
– Anwendung geeigneter Werkstoffe und Herstellungsverfahren, – richtige Dimensionierung und Formgebung, – richtige Schutzleiterverbindung, – Isolationüberwachung, – Anwendung des Prinzips der Energieabschaltung, – unterdrücken von Spannungsspitzen, – Verringern der Ansprechzeit, – sichere Befestigung der Eingabegeräte, – Schutz gegen Wiederanlauf nach Wiederherstellung der Energieversorgung, – Schutz des Steuerstromkreises, usw.	– Mechanisch verbundene Kontakte, Zwangsführung, – Fehlervermeidung in Kabeln, Querschluss, – Vermeidung undefinierter Zustände, – zwangsläufiger Betätigungsmodus, – gerichteter Ausfall, – Überdimensionierung, – zwangsläufiger Betätigungsmodus	– Schalter mit zwangsläufigem Betätigungsmodus nach EN 60947-5-1, – Not-Aus-Einrichtungen nach EN 418/ISO 13850, – Sicherungen nach EN 60269-1, – Leistungsschalter nach EN 60947-2, – Hauptschutz nach EN 60947-4-1 sind bewährt wenn: andere Einflüsse berücksichtigt sind, z. B. Schwingen, und – der Ausfall durch geeignete Verfahren vermieden wird, z. B. durch Überdimensionierung, und – der Strom zur Last durch eine thermische Schutzeinrichtung begrenzt ist, und – Schaltung mit einer Sicherung gegen Überlastung geschützt werden. – Hilfsschutz nach EN 50205, EN 60204-1 und EN 60947-5-1 sind bewährt wenn: – andere Einflüsse berücksichtigt sind, z. B. Schwingen, und – zwangsläufig erregte Funktion vorliegt, und – der Ausfall durch geeignete Verfahren vermieden wird, z. B. durch Überdimensionierung, und – der Strom in den Kontakten durch Sicherungen oder Schutzschalter begrenzt ist, um ein Verschleifen der Kontakte zu vermeiden, und die Kontakte mechanisch verbunden sind, wenn sie für Überwachungen angewendet werden	– Kurzschluss zwischen beliebigen Leitern, – Kurzschluss zwischen beliebigen Leitern und der Erde oder dem Schutzleiter, – Kurzschluss zwischen benachbarten Klemmen, – nichtschließen von Kontakten, – nichtöffnen von Kontakten, usw.

Sicherheits- und Antriebstechnik
Umweltgerechte Konstruktion und Normung der
Maschinensicherheit

Bernstein, H.

2016, XI, 437 S. 317 Abb., 30 Abb. in Farbe., Hardcover

ISBN: 978-3-658-12933-0