Das Sicherheitskompendium

PILZ
THE SPIRIT OF SAFETY

Für den Umgang mit Normen zur funktionalen Sicherheit.




Das Sicherheitskompendium

1 Vorwort
1.1 Autoren

2 Produkthaftung
2.1 Terminologie
2.2 Produkthaftungsgesetz (ProdHaftG)
2.3 Verschuldenshaftung § 823 Abs. 1 BGB
2.4 § 823 Abs. 2 in Verbindung mit dem Produktsicherheitsgesetz

3 Normen, Richtlinien und Gesetze
3.1 Normen, Richtlinien und Gesetze in der Europäischen Union (EU)
3.2 CE-Kennzeichnung
3.3 Richtlinien
3.4 Normen
3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich
3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)
3.7 Sicheres Programmieren nach EN ISO 13849-1
3.8 Validierung
3.9 Zertifizierung und Akkreditierung

4 Schutzeinrichtungen
4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen
4.2 Trennende Schutzeinrichtungen
4.3 Nicht trennende Schutzeinrichtungen
4.4 Manipulation von Schutzeinrichtungen

5 Sichere Steuerungstechnik
5.1 Sicherheitsschaltgeräte
5.2 Konfigurierbare sichere Kleinsteuerungen
5.3 Sicherheit und Automation
5.4 Mit Sicherheitssteuerungen zur sicheren Steuerungstechnik
5.5 Sichere Steuerungstechnik im Wandel

6 Sichere Kommunikation
6.1 Grundprinzipien sicherheitsgerichteter Kommunikation
6.2 Sichere Ethernet-Kommunikation mit SafetyNET p

Das Sicherheitskompendium

7 Sichere Bewegungssteuerung/Safe Motion
7.1 Definition von Safe Motion
7.2 Grundprinzip
7.3 Norm EN 61800-5-2
7.4 Sicherheitsfunktionen
7.5 Systembetrachtung
7.6 Beispiele für Safe Motion

8 Mechanische, pneumatische und hydraulische Konstruktion
8.1 Einleitung in die mechanische, pneumatische und hydraulische Konstruktion
8.2 Mechanische Konstruktion
8.3 Pneumatische Konstruktion
8.4 Hydraulische Konstruktion
8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik

9 Anhang
9.1 Stichwortverzeichnis
9.2 Haftungsausschluss

1 Vorwort

1 Vorwort

1 Vorwort
1.1 Autoren _____ 1-4

1 Vorwort

Ihre Anwesenheit wird stets vorausgesetzt, aber erst ihre Abwesenheit wird tatsächlich auch bemerkt: die Sicherheit. Sie hat den Schutz von Mensch, Maschine und Umwelt zur Aufgabe.

1787, mit den von Edmond Cartwright erstmals eingesetzten Webmaschinen, begann mit der Mechanisierung die erste industrielle Revolution. Hauptmotivation damals war die Erhöhung der Produktivität, an die Sicherheit des Webers wurde kaum ein Gedanke verschwendet. Heute dagegen stehen die Effizienz des Produktionsablaufs und die Sicherheit des Menschen gleichermaßen im Mittelpunkt.

Neben der Vermittlung aktueller normativer und technischer Grundlagen ist es daher ein wichtiges Anliegen des Sicherheitskompendiums, die zahlreichen Zusammenhänge zwischen Sicherheit und Wirtschaftlichkeit darzustellen. Dabei gilt: Wenn die Sicherheit von Beginn an berücksichtigt und richtig dimensioniert wird, dann führt sie automatisch zu effizienten Abläufen und hoher Akzeptanz beim Anwender.

Mit der vorliegenden 5. Auflage erhalten Sie, lieber Leser, nicht nur eine neu aufgelegte, aktualisierte Version. Unsere Experten haben dieses inzwischen als Standardwerk anerkannte Sicherheitskompendium auch um aktuelle Themen, wie beispielsweise ‚Sicherheit in der Industrie 4.0' und ‚Mensch-Roboter-Kollaboration', erweitert.

Denn digitale Daten und ihr effizienter Austausch definieren künftig den Produktionsprozess der Smart Factory. Dort steigt der Bedarf an abgesicherter Kommunikation, die gleichermaßen die Aspekte der Maschinensicherheit (Safety) wie die Anforderungen der Daten und IT-Sicherheit (Security) umfasst. Und schließlich wird die Rolle des Menschen in der Smart Factory neu interpretiert: Seine besonderen Fähigkeiten tragen dazu bei, die Produktion noch effizienter und besser zu machen. In vielen Bereichen wie zum Beispiel der Robotik bedeutet das, dass der Mensch näher an die Maschine rückt oder sich Mensch und Maschine einen Arbeitsraum teilen. Das vorliegende Sicherheitskompendium verdeutlicht, welche Anforderungen das an die Sicherheit stellt, und erklärt, wie diese erfüllt werden können.

Sicherheit wird dabei nicht mehr nur als eine normative Pflicht betrachtet, die den Zielen der Effizienz oder Anwenderfreundlichkeit entgegensteht. Ausgereifte Sicherheit ist heute vielmehr eine ganz wesentliche Voraussetzung für eine verfügbare und effiziente Produktion.

In diesem Sinne wünsche ich Ihnen eine nutzbringende Lektüre des Sicherheitskompendiums.

Ihre Renate Pilz
Geschäftsführende Gesellschafterin
Pilz GmbH & Co. KG

1.1 Autoren

Christian Bittner, Gruppenleiter der Gruppe Consulting Services innerhalb der Pilz GmbH & Co. KG, ist Mitglied des Normengremiums u. a. zur EN ISO 12100. Er steht in direktem Kontakt zu den Kunden: Die Durchführung von Risikobeurteilungen sowie die Erstellung von Sicherheitskonzepten, CE-Kennzeichnungen und weiteren Sicherheitsdienstleistungen zählen zu seinen Aufgaben.

Holger Bode ist in der Arbeitsgruppe Pressen bei der Pilz GmbH & Co. KG für die internationale Projektierung von Pressenumrüstungen und Neuanlagen zuständig. Dies umfasst die Ausarbeitung von kompletten Umbaumaßnahmen sowie die die Erstellung von Steuerungskonzepten, Gefährdungsbeurteilungen und Sicherheitskonzepten. Daneben ist er Qualitätsmanager der akkreditierten Inspektionsstelle der Pilz GmbH & Co. KG und gehört ihrer Leitung an.

Arndt Christ ist Abteilungsleiter Customer Support bei der Pilz GmbH & Co. KG. Er verantwortet innerhalb dieser Abteilung Gruppen wie den Technischen Support, die Consulting-Bereiche sowie die Systemintegration und den Schulungsbereich. Er kennt die Kundenbedürfnisse in Bezug auf alle sicherheitsrelevanten Themen und gewährleistet so eine anwenderfreundliche Umsetzung im Bereich Sicherheitstechnik.

Roland Gaiser ist Bereichsleiter für Aktorsysteme in der Entwicklung bei der Pilz GmbH & Co. KG. Zusätzlich ist er als Lehrbeauftragter für Systementwicklung und Simulation am Fachbereich Mechatronik und Elektrotechnik an der Hochschule Esslingen tätig. Er verfügt über umfangreiches Wissen im Bereich der Grundlagenentwicklung für Aktorsysteme.

Andreas Hahn ist im Produktmanagement der Pilz GmbH & Co. KG Senior Manager Controller für Netzwerke, Steuerungssysteme und Aktorik. Er ist Mitarbeiter in Normengremien und Arbeitskreisen verschiedener Verbände. Er verfügt über langjährige Erfahrung in der Konstruktion von Automatisierungslösungen.

1.1 Autoren

Jürgen Hasel ist Trainer und Berater bei der Festo Didactic SE. Seine Seminarschwerpunkte sind die Pneumatik, Elektropneumatik, Ventilinseln und die Sicherheitstechnik. Er war früher im Entwicklungsbereich der Festo AG tätig. Seit einigen Jahren arbeitet er eng mit dem Schulungsbereich der Firma Pilz GmbH & Co. KG zusammen. Er unterrichtet bei Pilz im Rahmen der produktneutralen Schulungen den ZMSE (Zertifizierter Machinensicherheitsexperten), der vom TÜV Nord zertifiziert ist.

Prof. Dr. Thomas Klindt ist Partner der internationalen Sozietät NOERR und zudem Honorarprofessor für Produkt- und Technikrecht an der Universität Bayreuth. Er ist Mitglied der kanzleiinternen practice group product safety & product liability, die nationale wie internationale Produkthaftungsprozesse, Produkt-Rückrufe und Schadensersatzklagen betreut.

Michael Moog ist als Fachreferent Normung bei der Pilz GmbH & Co. KG für die Koordinierung der internationalen Normgremienarbeit zuständig. Er ist selbst in Normgremien aktiv und verbindet die theoretische Normenarbeit mit der praxisbezogenen Auslegung und Interpretation von Normen zur Pilz-internen wie auch kundenseitigen Unterstützung. Er setzt sich insbesondere auch mit der weltweit zu beachtenden Sicherheits- und Produktnormung und entsprechenden nationalen gesetzlichen Rahmenbedingungen auseinander und gibt sein Wissen unter anderem im Seminar „Zulassungsverfahren für Maschinen und Anlagen in Nordamerika“ weiter.

Dr. Alfred Neudörfer war Dozent am Fachbereich Maschinenbau an der Technischen Universität Darmstadt. Er war auch als Gastprofessor für Sicherheitstechnik an der Nagaoka University of Technology in Japan tätig. In seinen Vortrags- und Seminartätigkeiten sowie seinen Fachbeiträgen beschäftigte er sich u. a. mit dem Thema Konstruktion von sicherheitsgerichteten Produkten.

Andreas Schott ist innerhalb der Pilz GmbH & Co. KG für den Bereich Training & Didaktik verantwortlich. Als Gruppenleiter erarbeitet er mit seinem Team didaktische und praxisrelevante Schulungskonzepte sowohl für produktneutrale als auch produktspezifische Schulungen.
Durch seine langjährige Tätigkeit als staatlich geprüfter Elektrotechniker und Softwareprogrammierer kennt er die praktischen Anforderungen der Kunden im Bereich Sicherheitstechnik.

1.1 Autoren

Eszter Sieber-Fazakas, LL.M. ist Rechtsanwältin der internationalen Sozietät NOERR. Sie ist zudem Mitglied der kanzleiinternen practice group product safety & product liability, die nationale wie internationale Produkthaftungsprozesse, Produkt-Rückrufe und Schadensersatzklagen betreut.

Klaus Stark verantwortet den Bereich Innovationsmanagement bei der Pilz GmbH & Co. KG. Davor war er ab 1996 Leiter des Produktmanagements, bis er 2008 die Leitung des Vertriebs International übernahm. Er setzt sich in verschiedenen Gremien aktiv für das Thema Automatisierung ein, darunter als Vorsitzender im Technischen Ausschuss „Sicherheitssysteme in der Automation“ des ZVEI oder als Mitglied des Vorstands der Technologie-Initiative SmartFactory KL e. V.

Jochen Vetter ist Teamleiter Robotik Services in der Pilz GmbH & Co. KG. Er steht in direktem Kontakt zum Kunden: Die Durchführung von Dienstleistungen rund um das Thema MRK, das bedeutet: das Erstellen von Risikobeurteilungen und Sicherheitskonzepten für MRK-Applikationen, gehört zu seinen Aufgaben. Bei der Abnahme von MRK-Applikationen gehört daneben das messtechnische Überprüfen der biomechanischen Grenzwerte gemäß TS 15066 zu seinen Aufgaben.

Gerd Wemmer ist als Applikationsingenieur im Customer Support der Pilz GmbH & Co. KG tätig. Er ist zuständig für Beratung, Projektausarbeitung und die Erstellung von Sicherheitskonzepten für Kunden vom Maschinenhersteller bis zum Endkunden und verfügt über langjährige praktische Erfahrung in der Sicherheitstechnik.

Harald Wessels ist Bereichsleiter für produktübergreifende Themen im Produktmanagement der Pilz GmbH & Co. KG. Zu seinen Aufgaben zählt unter anderem die Mitarbeit in internationalen Normengremien, die sich mit der Kommunikation in industriellen Anwendungen beschäftigen. Er verfügt über ein umfangreiches Wissen zu Feldbussystemen und Netzwerken, die in der Automatisierung eingesetzt werden.

1.1 Autoren

Matthias Wimmer sorgt innerhalb der Pilz Standards-Group für einen fundierten Umgang mit Normen und Vorschriften. Er ist Mitglied der internationalen Normungsgruppe ISO/TC199/WG8 und gestaltet die Entwicklung von Normen zur funktionalen Sicherheit (u. a. EN ISO 13849-1) wesentlich mit. Er bringt seine Kenntnisse außerdem durch Trainings und Schulungen in der Pilz Academy sowohl intern als auch extern an ein breites Publikum.

Michael Wustlich verantwortet als Gruppenleiter bei der Pilz GmbH & Co. KG den Bereich Software, Applikation und Tests. In seinen Aufgabenbereich fällt unter anderem die Entwicklung sicherheitsgerichteter Software auf Anwenderebene in Form standardisierter und zertifizierter Produkte. Darüber hinaus ist er mit seinem Team über alle Produktgruppen hinweg für die Spezifikation und Ausführung von systematisierten Anwendungstests zuständig.

2 Produkthaftung

2 Produkthaftung

2	**Produkthaftung**	
2.1	Terminologie	2-4
2.2	Produkthaftungsgesetz (ProdHaftG)	2-5
2.2.1	Einleitung	2-5
2.2.2	Produktfehler	2-5
2.2.3	Hersteller und sonstige Verantwortliche	2-9
2.2.4	Ausschluss der Haftung	2-10
2.2.5	Beweislastverteilung	2-12
2.2.6	Besonderheiten des Produkthaftungsgesetzes	2-12
2.3	Verschuldenshaftung § 823 Abs. 1 BGB	2-13
2.3.1	Inverkehrbringen des fehlerhaften Produktes	2-13
2.3.2	Rechtsgutsverletzung	2-14
2.3.3	Verletzung von Verkehrssicherungspflichten	2-14
2.3.4	Haftung in der arbeitsteiligen Produktion	2-17
2.3.5	Gefahrabwendungsmaßnahme, Warnung, Nachrüstung, Rückruf	2-20
2.4	§ 823 Abs. 2 in Verbindung mit dem Produktsicherheitsgesetz	2-22

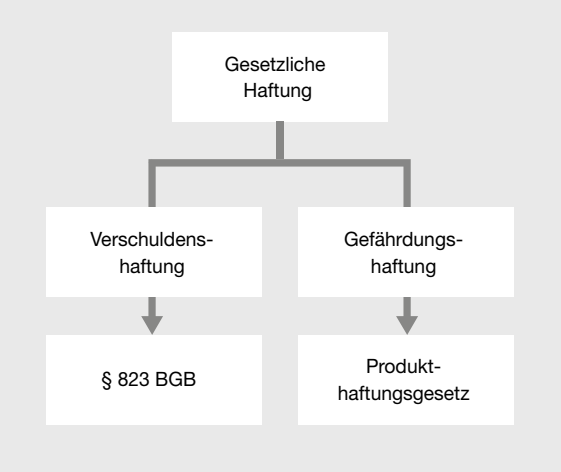
2 Produkthaftung

Das deutsche Produzentenhaftungsrecht kennt seit vielen Jahrzehnten Pflichten der (industriellen) Hersteller im Bereich Konstruktion, Fabrikation, Instruktion und After-Sales-Produktbeobachtung. Mit der europäischen Produkthaftungsrichtlinie 85/374/EWG wurde die Haftung für fehlerhafte Produkte in Europa harmonisiert. Die Umsetzung erfolgte 1990 durch das deutsche Produkthaftungsgesetz. Beide Systeme gelten heute parallel.

2.1 Terminologie

Im deutschen Recht wird aus Sicht der Industrie im Wesentlichen zwischen vertraglicher und gesetzlicher Haftung unterschieden: Die vertragliche Haftung kommt grundsätzlich nur zwischen Vertragspartnern, d. h. in echten Lieferbeziehungen in Betracht. In diesem Beitrag wird darauf nicht weiter eingegangen, wenngleich gerade bei Verträgen im grenzüberschreitenden Warenvertrieb (Cross Border Business) viele Fallstricke lauern, die eine rechtzeitige rechtliche Vertragsprüfung sehr empfehlenswert erscheinen lassen.

Vom Risiko einer Produkt- oder Produzentenhaftung spricht man üblicherweise, wenn es nicht um Verträge und Streit zwischen Lieferanten, sondern um sonstige Personen geht, die einen Schaden geltend machen: Der Hersteller eines Produktes wird verklagt wegen eines Personen- oder eines Sachschadens, den sein Produkt verursacht haben soll (ob dem so ist, ist in der Regel Ergebnis eines komplizierten, häufig durch diverse Sachverständige begleiteten Verfahrens). Der Hersteller wird also vom Geschädigten auf finanziellen Schadensersatz in Anspruch genommen, bei Gesundheitsschäden kommt oft noch ein Anspruch auf Schmerzensgeld hinzu.



Zwei Bereiche der gesetzlichen Haftung

Diese gesetzliche Haftung wird wiederum in zwei Bereiche unterteilt: Die Haftung aus unerlaubter Handlung, die sogenannte deliktische Haftung, basiert auf einem Vorwurf oder, juristisch formuliert, auf einem Verschulden. Das Verschulden wird im Gesetz entweder als „Vertretenmüssen“ oder mit den Schuldbegriffen „Vorsatz“ und „Fahrlässigkeit“ umschrieben. Lässt das Gesetz bereits die pure Verwirklichung eines bestimmten Risikos ausreichen, um eine Herstellerhaftung zu begründen (ohne jedes Interesse an der Fragestellung, ob wenigstens Fahrlässigkeit vorlag), spricht man von Gefährdungshaftung. Diese greift weit früher und ist daher für Hersteller besonders kritisch.

In Deutschland existieren beide Systeme nebeneinander. Die erwähnte Verschuldenshaftung des Produzenten wird in § 823 BGB geregelt. Die Rechtsprechung hat bereits ab den 1950er-Jahren die Grundpfeiler für die Produzentenhaftung gelegt. Daneben gilt seit 1990 das Produkthaftungsgesetz, aus dem sich die Gefährdungshaftung für fehlerhafte Produkte ergibt. Das Produkthaftungsgesetz geht auf die europäische Produkthaftungsrichtlinie zurück, die in allen europäischen Mitgliedstaaten gleichermaßen umgesetzt werden musste. Dennoch ist es selbst im europäischen Kontext nicht egal, ob deutsches oder fremdes Recht zur Anwendung kommt. Man kann sich zwar darauf verlassen, dass die Regelungen der Produkthaftungsrichtlinie in den Mitgliedstaaten der EU durch die jeweiligen Umsetzungsgesetze gelten, allerdings kann die Rechtsprechung der einzelnen Länder durchaus unterschiedliche Schwerpunkte setzen oder sogar die gleiche Problematik unterschiedlich beurteilen. Deutsches Recht kommt zur Anwendung, wenn sich der Unfall respektive Schadensfall in Deutschland ereignet hat. Man spricht hier auch vom „Tatort-Prinzip“. Ereignete sich der Unfall oder Schadensfall dagegen in einem anderen Staat, kommt in den allermeisten Fällen das dortige Haftungsrecht zur Anwendung. Manche nichteuropäische Staaten, wie z. B. Australien, haben die Produkthaftungsrichtlinie als Vorbild für die eigene Gesetzgebung genommen. Allerdings kann das fremde Haftungsrecht im Einzelfall nachgiebiger, oft aber auch strenger als das deutsche Recht ausfallen.
In jedem Fall ist es ein unbekanntes Recht; bei derartigen Vorfällen im Ausland muss schnell rechtlicher Rat eingeholt werden, um hier nicht Fehler aus purer Ahnungslosigkeit zu begehen.

Nachfolgend wird zuerst die Gefährdungshaftung aus dem Produkthaftungsgesetz dargestellt, um anschließend die deliktische Verschuldenshaftung zu skizzieren. Obwohl in der Praxis meistens beide Haftungsgrundlagen nebeneinander angewendet werden, können sich wichtige Unterschiede insbesondere bezüglich des Haftungsumfangs ergeben. Hierauf wird gesondert hingewiesen.

2.2 Produkthaftungsgesetz (ProdHaftG)

2.2.1 Einleitung

Die Gefährdungshaftung für fehlerhafte Produkte wurde in der ganzen EU einheitlich durch die Europäische Richtlinie 85/374/EWG vom 25.06.1985 – EG-Produkthaftungsrichtlinie – eingeführt. Diese Richtlinie wurde in Deutschland durch das Produkthaftungsgesetz umgesetzt, das seit dem 01.01.1990 in Kraft ist.

§ 1 ProdHaftG lautet:

„Wird durch den Fehler eines Produktes jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produktes verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Im Falle der Sachbeschädigung gilt dies nur, wenn eine andere Sache als das fehlerhafte Produkt beschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist.“

Im Rahmen des Produkthaftungsgesetzes wird also für eine Tötung, Körper- oder Gesundheitsverletzung sowie für eine Sachbeschädigung gehaftet, wenn das fehlerhafte Produkt die Ursache dafür war. Allerdings können Schäden an einer Sache, die für unternehmerische, geschäftliche, gewerbliche oder berufliche Zwecke benutzt wird, nicht im Rahmen des Produkthaftungsgesetzes ersetzt werden.

Beispiel: Werden z. B. Messingrohrnippel eines Herstellers in gewerblich genutzte Wasserrohre eingebaut und führen die eingebauten Kleinteile letztlich zu einer Beschädigung der gesamten Wasserleitung, können keine Schadensersatzansprüche aus ProdHaftG hergeleitet werden. Da es sich bei der Wasserleitung um keinen Gegenstand handelt, der seiner Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt ist, ist das ProdHaftG nicht anwendbar.

2.2.2 Produktfehler

2.2.2.1 Arten von Produktfehlern

Der „Fehler“ ist der zentrale Begriff des Produkthaftungsgesetzes, da der Produktfehler Ausgangspunkt für die Haftung ist.

Nach § 3 ProdHaftG gilt folgende Definition für einen Fehler:

„Ein Produkt hat einen Fehler, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere

- *seiner Darbietung,*
- *des Gebrauchs, mit dem billigerweise gerechnet werden kann,*
- *des Zeitpunkts, in dem es in den Verkehr gebracht wurde,*

berechtigterweise erwartet werden kann.“

2.2 Produkthaftungsgesetz (ProdHaftG)

2.2.2.2 Berechtigte Sicherheitserwartung

Festzuhalten ist, dass eine hundertprozentige Sicherheit von niemandem erwartet werden kann. Ganz praxisnah ist somit zwischen einer absoluten und einer relativen Gefährlichkeit eines Produktes zu unterscheiden: Abhängig von der Verwendung im Einzelfall birgt jedes Produkt ein gewisses technisches Gefahrenpotenzial in sich. Entscheidend ist letztlich, wie gefährlich das Produkt – relativ betrachtet – im Vergleich zu anderen am Markt angebotenen Produkten ist.

Absolute Sicherheit muss also nicht gewährleistet werden. Dies folgt dem Gedanken, dass einem Hersteller im Rahmen der Produktion nicht unzumutbare Kosten auferlegt werden dürfen. Deshalb ist er nicht gezwungen, jede technisch mögliche Sorgfaltsvorkehrung praktisch umzusetzen.
Der von ihm einzuhaltende Sicherheitsstandard ist auf das Mögliche und Zumutbare begrenzt:
Ein Hersteller hat diejenigen ihm möglichen Sorgfaltsmaßnahmen zu ergreifen, deren Kosten geringer sind als die Summe der Schäden, die durch sie vermieden werden. Daraus folgt wiederum, dass der Hersteller sorgfältig zwischen drohendem Schaden und notwendigen Sicherungsmaßnahmen abwägen muss.

Beispiel: Bei einer Spülmaschine, die durch Wasseraustritt die gesamte Küche ruinieren kann, ist der Einbau eines Schutzes gegen Durchrostung – der technisch möglich und vom Kostenaufwand her überschaubar ist – auch im Hinblick auf den hohen Wettbewerbsdruck am Markt zumutbar.

Bei der berechtigten Sicherheitserwartung spielt der Preis des Produktes durchaus eine Rolle, wobei selbst von einem Billigprodukt eine gewisse Basissicherheit erwartet werden kann.

Beispiel: Das OLG Naumburg entschied, dass eine Tischfeuerstelle, die für etwas mehr als einen Euro im „Groschenmarkt“ erworben wurde, trotz des geringen Preises von der Konstruktion her nicht gefährlich sein darf. So bejahte das Gericht einen Konstruktionsfehler, da das Brenngefäß und der Übertopf nicht flüssigkeitsundurchlässig verbunden waren und daher bei Verschütten des flüssigen Brennstoffes ein Eindringen in den Übertopf möglich war, das eine Explosion verursachte.

2.2 Produkthaftungsgesetz (ProdHaftG)

2.2.2.3 Technische Normen und Spezifikationen

Für die berechtigte Sicherheitserwartung bei der Konstruktion und Fabrikation von Produkten spielen technische Normen, Standards und Spezifikationen eine Rolle. Ausgangspunkt ist, dass das Produkt zum Zeitpunkt der Inverkehrgabe dem aktuellen Stand von Forschung und Wissenschaft entsprechen muss. Die Behauptung, dass die Einhaltung der technischen Normen den Schadensfall nicht hätten verhindern können, hilft dem Hersteller nicht weiter. Führt der Hersteller z. B. die gem. EN-Normen gebotene Risiko- und Gefährdungsanalyse nicht durch, muss er beweisen, dass die mangelnde Überwachung für das Unfallgeschehen nicht kausal geworden ist. In der Praxis wird es kaum möglich sein, diesen Beweis zu führen.
Die technischen Vorgaben und Normen stellen lediglich einen Mindeststandard dar, dessen Unterschreitung die Verletzung der zu erwartenden Sicherheit nahelegen mag. Doch kann hieraus kein Umkehrschluss gezogen werden: Ein Produkt, das den technischen Normen entspricht, kann dennoch im Rechtssinne fehlerhaft sein. Technische Normen können aufgrund technischer Fortentwicklungen veraltet, ergänzungsbedürftig geworden oder von Anfang an lückenhaft gewesen sein oder aus sonstigen Gründen inhaltlich vom aktuellen Stand der Wissenschaft und Technik abweichen. Deshalb kann man sich bei Auftreten eines Schadensfalles im Zusammenhang mit einem bestimmten Produkt nicht darauf zurückziehen, dass Produktfehler juristisch ausgeschlossen sind, weil die in den technischen Normen vorgesehenen Standards eingehalten worden sind. Wiederholt wurde entschieden, dass die Einhaltung von DIN-Vorschriften zwar die Fehlerfreiheit des Produktes indizieren, die Fehlerhaftigkeit aber keinesfalls ausschließen. Normkonformität ist also nicht identisch mit Rechtskonformität!

Der BGH betonte in diesem Zusammenhang sogar, dass der „neueste Stand von Wissenschaft und Technik“ den Umfang notwendiger Sicherungsmaßnahmen bestimmt. Hierfür ist nicht der übliche Standard in der jeweiligen Branche maßgebend, vielmehr müssen bessere, also sicherheitstechnisch überlegenere Alternativkonstruktionen vom Hersteller eingesetzt werden, sobald diese serienreif sind und dem Hersteller wirtschaftlich zugemutet werden können. Dies gilt allerdings nur für den Hersteller und im Zeitpunkt der Inverkehrgabe. Der BGH stellt klar, dass den Produkteigentümer/-nutzer keine Nachrüstungspflicht gem. den modernsten Erkenntnissen und nach dem neuesten Stand der Technik trifft. So ist eine Bank nicht verpflichtet, die automatische Glastür nachzurüsten, wenn die Glastür den zum Zeitpunkt des Einbaus gültigen technischen Normen entsprach, aber die zwischenzeitlich erlassenen strengeren DIN-Vorschriften nicht mehr eingehalten wurden.

Beispiele: Eine Hebebühne kann z. B. fehlerhaft sein, wenn sie den anwendbaren DIN-Vorschriften oder VDE-Empfehlungen widerspricht und dies nicht durch „intelligentere“ Lösungen ausgeglichen wurde. Die Fehlerhaftigkeit wird auch nicht dadurch behoben, dass den Kunden mit einem Ergänzungsset Sicherheitsteile zum Kauf angeboten werden. Ein Konstruktionsfehler, z. B. eines Garagentorantriebs, liegt auch dann vor, wenn die technischen Normen (DIN- oder EN-Normen) zwar bei der Standardeinstellung eingehalten werden, bei besonderen Einstellungen allerdings die Grenzwerte überschreiten.

Europäische Normen enthalten ebenfalls technikrechtliche Vorgaben. Werden die Anforderungen aus dem europäischen Technikrecht, z. B. bei der Konstruktion einer Fußboden-Abschleifmaschine, nicht eingehalten, ist ein Produktfehler zu bejahen.

Wird bei einer gefährlichen Maschine, z. B. einer Fenster- und Futterstoffeinklebemaschine, die Bandgeschwindigkeit nicht gem. der einschlägigen EN-Norm überwacht, muss der Hersteller beweisen, dass die fehlende Überwachung für den Unfall nicht ursächlich geworden ist.

Wenn aber z. B. ein Gartengerät vorhandenen DIN-Vorschriften entspricht, wird Fehlerfreiheit zwar indiziert, sie steht damit aber keineswegs fest. Die Fehlerhaftigkeit kann sich auch aus Konstruktionsfehlern im technischen Design ergeben, wenn Normen dort nicht umgesetzt wurden oder wenn einzelne Chargen mit Materialfehlern behaftet waren.

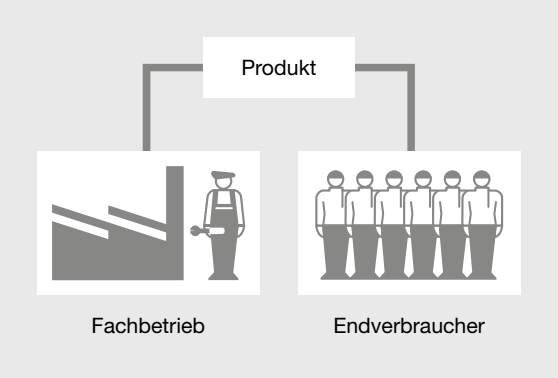
2.2 Produkthaftungsgesetz (ProdHaftG)

2.2.2.4 Bestimmung des Verwenderkreises

In diesem Zusammenhang spielt eine entscheidende Rolle, für wen das Produkt letztlich bestimmt ist. Ist das Produkt nur für einen konkreten Kreis von Anwendern vorgesehen, so ist es auf deren Sicherheitserwartungen abzustellen.

So wurde in der Rechtsprechung entschieden, dass der Hersteller nicht davon ausgehen kann, dass Frischbeton ausschließlich in die Hände von Personen fällt, die mit der Verätzungsgefahr von Frischbeton vertraut sind. Der Hersteller habe sich an dem am wenigsten informierten Abnehmer zu orientieren, deswegen hätte auf das alkalische Verätzungspotenzial warnend hingewiesen werden müssen.

Wird das Produkt beispielsweise nur an Fachbetriebe geliefert, darf der Hersteller davon ausgehen, dass die Produkte auch nur von Fachpersonal benutzt werden. Ein differenzierteres Bild ergibt sich jedoch dann, wenn der Hersteller erfährt, dass – trotz entgegenstehender Vertriebswege – das Produkt auch in die Hände unerfahrener Endverbraucher gelangt („Produktmigration“).



Verwenderkreis eines Produktes

Beispiel: Die ursprünglich für gewerbliche Präsentationszwecke entwickelten Laserpointer haben längst ihren Weg in den Alltag gefunden und werden sogar als Spielzeug verwendet. Der Hersteller hat bei der Sicherheitserwartung zu beachten, dass Laserstrahlen eventuell in die Augen von Menschen projiziert werden. Er muss einen dementsprechend höheren Sicherheitsstandard gewährleisten als bei der ursprünglich geplanten Verwendung.

Schwierigkeiten bereitet die Abgrenzung von Spielzeug und Verbraucherprodukt: Sollen bei einem Kerzenständer, der aus acht miteinander verbundenen Holztieren besteht, die sicherheitsrechtlichen Anforderungen der Spielzeugrichtlinie gelten, obwohl der Hersteller ausdrücklich bestimmt, dass die „Geburtstagskarawane“ nicht zum Spielen geeignet ist? Das erstinstanzliche Gericht VG Münster bejahte dies, mit der Begründung, dass es zu erwarten ist, dass Kinder, für die das Produkt auch konzipiert ist, mit den Holzfiguren spielen werden. Die gegenteilige Instruktion des Herstellers sei nicht ausreichend.

Wenn allerdings bei speziell für Fachleuten bestimmten Produkten – wie z. B. bei einem Relais für Elektrohandwerker – eindeutig angegeben ist, dass das Produkt nur von Fachkräften verwendet, montiert und abgenommen werden darf, müssen Laien nicht über die Montage aufgeklärt werden.

2.2.2.5 Inhärent gefährliche Produkte

Manche sogenannten inhärent gefährlichen Produkte haben gerade in der Gefährlichkeit ihre Zielsetzung und Funktion.

So ist z. B. das Gift fehlerhaft, das nicht tötet – und eben nicht dasjenige, das es tut.

2.2.2.6 Fehlerverdacht als Produktfehler

Die Rechtsprechung schaffte eine besondere Fehlerkategorie – in manchen Fällen muss kein konkreter Produktfehler bewiesen werden, es reicht bereits der Fehlerverdacht, also der potenzielle Fehler einer Produktserie. Der Europäische Gerichtshof befasste sich mit der Frage, ob ein in den menschlichen Körper implantiertes Medizinprodukt bereits dann fehlerhaft ist, wenn bei einer signifikanten Anzahl von Geräten derselben Serie eine Fehlfunktion auftritt, diese Fehlfunktion bei dem im konkreten Fall implantierten Gerät aber nicht festgestellt ist. Der EuGH bejahte diese Frage für Herzschrittmacher und implantierbare Kardioverter-Defibrillatoren, im Wesentlichen mit der Begründung, dass die berechtigte Sicherheitserwartung als besonders hoch einzustufen ist, erstens wegen der Funktion der implantierten

2.2 Produkthaftungsgesetz (ProdHaftG)

Geräte, zweitens wegen der besonderen Verletzlichkeit der betroffenen Patienten. Es ist offen, ob und auf welche Produktgruppen diese Rechtsprechung übertragen werden kann. Das deutsche Kammergericht hat jedenfalls die Fehlerhaftigkeit aufgrund bloßen Fehlerverdachts bei Hüftprothesen bejaht.

2.2.3 Hersteller und sonstige Verantwortliche

Vorrangig haftet nach § 1 Abs. 1 ProdHaftG der Hersteller. Hierbei ist der tatsächliche Hersteller des End-, Teilproduktes oder eines Grundstoffes gemeint. Der Hersteller tritt im Markt zumeist als AG, GmbH oder in sonstiger Form gesellschaftsrechtlich oder körperschaftlich organisiert auf. Demzufolge ist die Haftung auf die Gesellschaft begrenzt.

2.2.3.1 Assembling und bloße Produktkomplettierung

Hersteller des Endproduktes ist auch, wer das Produkt ohne eigene Fertigung aus Teilen, die von anderen Herstellern vorgefertigt wurden, zusammensetzt (oft als Assembler bezeichnet). In der Praxis kann es Schwierigkeiten bereiten, eine solche Assemblertätigkeit von der Produktkomplettierung, die als typische Händlertätigkeit eingestuft wird, abzugrenzen. Es kann davon ausgegangen werden, dass eine Herstellertätigkeit immer dann vorliegt, wenn sicherheitsrelevante Eigenschaften eines Produktes verändert werden. Ein relevanter Anhaltspunkt ist dabei, ob die Verbindung auch von einem Laien ohne Konstruktions- und Fachwissen mit einfachen Handgriffen und ohne Spezialwerkzeug bewerkstelligt werden könnte. Zudem ist relevant, ob das zusammenmontierte Produkt ein eigenständiges Produkt im Vergleich zu den Teilprodukten darstellt.

Der Unternehmer, der Tischgestelle und Glasplatten zu Bistrotischen montiert, ist als Hersteller anzusehen und nicht lediglich als Händler.

Der Unternehmer hingegen, der ein Fertigprodukt, z. B. einen Sicherheitsschalter oder Servoverstärker, nur portioniert und verpackt, ist nicht als Hersteller anzusehen.

Die Abgrenzung kann im Bereich des Medizinprodukterechts Schwierigkeiten bereiten, wenn z. B. bei einer erneuten Operation einem Hüftprothesenpatienten nur Teile der Hüftprothese ausgetauscht werden und damit durch die Kombination der alten und der neuen Prothesenteile ein quasi neues Produkt vom operierenden Arzt geschafften wird. Es liegen zur Einstufung des Arztes oder des Krankenhausbetreibers als Hersteller divergierende (voneinander abweichende) gerichtliche Entscheidungen vor.

2.2.3.2 Haftung des Quasi-Herstellers

Neben dem tatsächlichen Hersteller haftet auch der Quasi-Hersteller. Gemäß § 4 Abs. 1 Satz 2 ProdHaftG gelten aufgrund einer gesetzlichen Gleichstellung als Hersteller auch jene, die sich durch das Anbringen ihres Namens, ihrer Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgeben. Dies ist somit jeder, der nach außen am Markt den Eindruck erweckt, er sei der tatsächliche Hersteller. Diese Haftung des Quasi-Herstellers hat Auswirkungen für Versandhäuser und Handelsketten, die für sich herstellen lassen und das Produkt sodann mit dem eigenen Markenzeichen oder Firmenlabel anbieten. Gleiches gilt für industrielle Anbieter, die ihr Vollsortiment durch Zukauf von Handelsware unter eigenem Label komplettieren.

Der Zusatz „Hergestellt für …“ begründet keine Stellung als Quasi-Hersteller, da gerade dadurch verdeutlicht wird, dass eine andere Person als der Produktanbieter der Hersteller ist.

Es ist unerheblich, ob der tatsächliche Hersteller oder der Quasi-Hersteller den Namen, die Marke oder ein anderes Kennzeichen des Quasi-Herstellers am Produkt anbringt. Es ist auch nicht notwendig, dass der Hersteller vor Anbringung der fremden Marke sein Einverständnis hierzu erteilt. Maßgeblich für die Haftung des Quasi-Herstellers ist nur der Fakt, dass das Produkt mit dem Namen oder der Marke des Quasi-Herstellers und dessen Zustimmung in Verkehr gebracht wird.

2.2 Produkthaftungsgesetz (ProdHaftG)

2.2.3.3 Importeur

Gemäß § 4 ProdHaftG haftet auch der EU-Importeur des Produkts. Dabei muss der Import des Produktes in den Europäischen Wirtschaftsraum im Rahmen der geschäftlichen Tätigkeit des Importeurs zum Vertrieb mit wirtschaftlichem Zweck (z. B. Verkauf, Vermietung, Leasing) geschehen. Mit dieser Vorschrift soll der Verbraucher geschützt werden, einen Produkthaftungsprozess mit einem Hersteller in einem außereuropäischen Drittland führen zu müssen.

Werden z. B. elektronische Überwachungsgeräte aus China importiert und entsteht aufgrund eines Fehlers ein Brand, muss der Geschädigte keinen Produkthaftungsprozess gegen den chinesischen Hersteller führen, sondern kann sich an den EU-Importeur der Geräte als Haftenden wenden.

Stammen dagegen die Überwachungsgeräte aus Italien (also aus einem EU-Land), wird es dem Geschädigten zugemutet, gegen den italienischen Hersteller vorzugehen. Auch ein solcher Prozess kann mit erheblichen rechtlichen und faktischen Schwierigkeiten verbunden sein. Der Gerichtsstand, also der Ort des Prozesses und das anwendbare Recht (italienisches oder deutsches Recht) sind im Vorfeld zu klärende Fragen.

2.2.3.4 Lieferant

Die Haftung des Lieferanten (Händlers) anstelle des Herstellers ist durch das ProdHaftG ausschließlich für den Fall vorgesehen, dass der Hersteller des Produktes nicht festgestellt werden kann. Wurde der Produktnutzer also durch ein anonymes Produkt geschädigt, kann er sich an den Lieferanten wenden, in der Praxis also an den Verkäufer. Der Lieferant haftet aber nur ersatzweise und kann sich durch die fristgerechte Benennung des eigentlichen Herstellers oder seines eigenen Vorlieferanten vollständig entlasten.

2.2.4 Ausschluss der Haftung

2.2.4.1 Keine Haftung für spätere Produktverbesserung

Eine spätere Produktverbesserung führt nicht „rückwärts“ zur Fehlerhaftigkeit der bisherigen Produktlinie. Also hat nicht jeder technische Fortschritt in Sicherheitsfragen zur Folge, dass rückwirkend das Vormodell in juristischem Sinne unsicher und damit fehlerhaft wird. Gibt es aber grundsätzliche Verbesserungen der Sicherheit, so ist von jedem Wettbewerber in jedem Einzelfall die Frage zu stellen, ob er diese möglichst unmittelbar im eigenen Produktsegment einführen muss, um den neuen, just veränderten Sicherheitsstandards zu genügen. Für die Beurteilung der Sicherheit spielt die gesellschaftliche Akzeptanz sowie die gesellschaftliche Sicherheitserwartung eine große Rolle. Produktverbesserungen verbreiten sich mitunter schnell, werden zu Standards und damit Teil der allgemeinen Sicherheitserwartung.

2.2 Produkthaftungsgesetz (ProdHaftG)

Ein Geschädigter kann sich nicht allein darauf berufen, dass das Produkt deswegen fehlerhaft sei, weil der Hersteller eine Produktänderung vorgenommen hat. Dient die Änderung der technischen Weiterentwicklung des Produktes, wird deshalb das Vormodell nicht fehlerhaft. Gelingt es dagegen dem Geschädigten, darzustellen und zu beweisen, dass die Produktänderung lediglich zur Fehlerbeseitigung eines schon vorher existenten Sicherheitsdefizits erfolgte, wird daraus die Fehlerhaftigkeit zum Zeitpunkt der Inverkehrgabe des Vorgängerproduktes gefolgert.

2.2.4.2 Keine Haftung für Entwicklungsfehler

Bei einem Entwicklungsfehler handelt es sich aus juristischer Sicht um einen Fehler, der zum Zeitpunkt des Inverkehrbringens des Produktes nach dem damaligen Stand der Wissenschaft und Technik nicht erkannt und damit niemals vermieden werden konnte. Ein Entwicklungsfehler ist dann objektiv nicht vermeidbar, wenn die potenzielle Gefährlichkeit des Produktes allgemein von keinem – weder in der betreffenden Branche noch auf nationaler oder internationaler Ebene – erkannt werden konnte, weil das Wissen zum Zeitpunkt des Inverkehrbringens nicht verfügbar war. Die Beweislast hierfür trägt der Hersteller. In der Rechtsprechung findet sich daher kaum ein Fall, in dem sich ein Hersteller wegen Vorliegens eines Entwicklungsfehlers wirklich entlasten konnte.

Hinweis: Juristen meinen mit Entwicklungsfehler ausdrücklich etwas anderes als Ingenieure: Wenn diese von einem Entwicklungsfehler sprechen, entspricht dies im Rechtssinne vielmehr einem Konstruktionsfehler. Vorsicht: Produkthaftungsgesetze anderer europäischer Staaten sehen auch eine Haftung für Entwicklungsfehler vor.

2.2.4.3 Haftungsbefreiung bei Anwendung zwingender Rechtsvorschriften

Die Ersatzpflicht des Herstellers ist ausgeschlossen, wenn der Fehler darauf beruht, dass das Produkt zum Zeitpunkt des Inverkehrbringens zwingenden Rechtsvorschriften über die Herstellung entsprach. Diese Haftungsfreistellung hat in der Praxis nur geringe Bedeutung, da es in der Bundesrepublik Deutschland kaum zwingende Rechtsvorschriften für die Produktgestaltung gibt. Insbesondere sind technische Vorschriften, Normungen und Empfehlungen (wie die DIN-, EN-, VDE- oder ETSI-Normen oder VDE-Richtlinien, VDE-Empfehlungen oder VCI-Regeln) weder Rechtsvorschriften noch zwingend. Abgesehen davon, dass technische Normen immer freiwillig eingehalten werden, sind sie auch keine zwingenden Rechtsvorschriften im Sinne des Haftungsausschlusses, da damit nur ein verbindlicher Paragraph im Produkthaftungsgesetz gemeint ist.

2.2 Produkthaftungsgesetz (ProdHaftG)

2.2.5 Beweislastverteilung

Der Erfolg eines Produkthaftungsprozesses hängt meistens von der Darlegungs- und Beweislast ab. Es gilt der Grundsatz, dass immer der Anspruchsteller sämtliche Voraussetzungen seines Anspruches zu beweisen hat. Der Geschädigte muss im Rahmen des Produkthaftungsgesetzes den Fehler, die Kausalität des Fehlers für den Schaden und den Schaden beweisen. Es wird vermutet, dass der Fehler schon bei Inverkehrgabe vorlag. Der Hersteller ist entlastet, wenn er nachweisen kann, dass der Fehler zum Zeitpunkt des Inverkehrbringens dem Produkt noch nicht anhaftete.

Dies ist insbesondere in solchen Konstellationen denkbar, in denen ein Teilprodukt zunächst fehlerfrei ist und wegen der konkreten Art und Weise seiner Verwendung – Einbau in das Endprodukt – fehlerhaft wird. Werden an sich fehlerfreie, aber nur für normale Druckbelastungen geeignete Rohre ohne Abstimmung mit dem Hersteller in eine Maschine verbaut, die hohen Druckbelastungen ausgesetzt ist, haftet der Hersteller der Rohre nicht, wenn diese wegen des hohen Drucks platzen.

2.2.6 Besonderheiten des Produkthaftungsgesetzes

Das Produkthaftungsgesetz sieht einen Haftungshöchstbetrag je Schadensfall von 85 Mio. EUR vor, ein Sockelbetrag in Höhe von 500 EUR wird dabei nicht ersetzt. Die Selbstbeteiligung des Geschädigten am Sachschaden liegt damit bei 500 EUR.

Die Ansprüche aus dem Produkthaftungsgesetz verjähren nach drei Jahren. Die Verjährung beginnt mit Kenntnis bzw. fahrlässiger Unkenntnis vom Schaden, dem Produktfehler und der Person des Ersatzpflichtigen. Sämtliche Ansprüche enden zehn Jahre nach dem Inverkehrbringen.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

Der vom Wortlaut her sehr weit gefasste § 823 Abs. 1 BGB begründet die Produzentenhaftung bei Verschulden:

> *„Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet."*

Diese generelle Formulierung erfasst auch die Haftung für Schäden, die durch ein fehlerhaftes Produkt bei dem Käufer, einem Produktbenutzer oder sonstigen Dritten entstanden sind. Überträgt man die einzelnen Haftungsvoraussetzungen in eine Struktur, ergibt sich folgendes Prüfungsschema:

1. Handlung oder Unterlassung des Täters = Inverkehrbringen eines fehlerhaften Produktes
2. Körper- oder Gesundheitsverletzung, Eigentumsverletzung
3. Körper- oder Gesundheitsverletzung bzw. Eigentumsverletzung durch fehlerhaftes Produkt verursacht
4. Rechtswidrigkeit
5. Verschulden (wobei leichteste Fahrlässigkeit genügt!)
6. Rechtsfolge: Schadensersatz

2.3.1 Inverkehrbringen des fehlerhaften Produktes

Die Verschuldenshaftung knüpft, genauso wie das Produkthaftungsgesetz, an das Inverkehrbringen des fehlerhaften Produktes an. Nichtsdestotrotz ist es nicht gesetzlich definiert, wann das Produkt in Verkehr gebracht wird. Die Inverkehrgabe liegt spätestens dann vor, wenn das Produkt am Markt in Erscheinung tritt. Allerdings ist dies keine Voraussetzung: Es genügt, wenn der Hersteller einer anderen Person außerhalb seiner Herstellersphäre das Produkt übergibt.

Das Produkt gilt als in Verkehr gebracht, wenn es einer rechtlich vom Hersteller unabhängigen Vertriebsgesellschaft überlassen, an den Frachtführer bzw. an die Spedition übergeben oder das Teilprodukt an den Weiterverarbeiter ausgeliefert wurde. Noch keine Inverkehrgabe liegt vor, wenn das Produkt lediglich angeboten, vorrätig gehalten oder einer Materialprüfungsanstalt für Testzwecke übergeben wird.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

2.3.2 Rechtsgutsverletzung

Schadensersatz unter § 823 Abs. 1 BGB kann nur verlangt werden, wenn die aufgezählten Rechtsgüter – Körper, Gesundheit, Eigentum – verletzt werden.

Aus Sicht der Rechtsprechung ist für eine Eigentumsverletzung nicht zwingend eine Beschädigung oder Zerstörung der betreffenden Sache erforderlich. Ausreichend ist vielmehr, wenn der bestimmungsgemäße Gebrauch eingeschränkt wird. Prinzipiell ist jedoch der Schadensersatz für die Zerstörung anderer Sachen durch die „Hersteller-Ware“ zu zahlen: Schäden an dem eigentlich fehlerhaften Produkt – ein eingebauter Motor fängt Feuer und zerstört nicht nur die Maschine, sondern auch sich selbst – werden dagegen nur unter höchst eingeschränkten Voraussetzungen ersetzt. Dies ist deshalb so, weil anderenfalls die Grenze zwischen der rein vertraglichen Haftung des Verkäufers und der hier interessanten deliktischen Haftung des Herstellers aufgeweicht würde. Die sehr schwierigen Einzelheiten lassen sich nicht im Umfang dieses Sicherheitskompendiums beschreiben.

2.3.3 Verletzung von Verkehrssicherungspflichten

Die Rechtsprechung hat im Rahmen des § 823 BGB eine Kategorisierung des fehlerhaften Herstellerverhaltens (Verletzung von Verkehrssicherungspflichten) in Fehlergruppen vorgenommen: Man unterscheidet zur technischen Abgrenzung potenzieller Fehlerkausalitäten vier Fehlergruppen:

- Konstruktionsfehler
- Fabrikationsfehler
- Instruktionsfehler
- Produktbeobachtungsfehler

2.3.3.1 Konstruktionsfehler

Von einem Konstruktionsfehler sprechen Juristen, wenn die gesamte Produktlinie denselben Fehler im technischen Design aufweist. Der Hersteller muss organisatorisch sicherstellen, dass alle sicherheitsrechtlichen Konstruktionsvorgaben (z. B. aus EU-Richtlinien) sowie technischen Regeln beachtet werden. Hierzu werden oft auch Material- und Produktprüfungen nach dem neuesten Stand der Wissenschaft und Technik erforderlich sein.

Der Hersteller ist verpflichtet, sein Produkt so zu konstruieren, dass es der durchschnittliche Verwender nach dem bestimmungsgemäßen Verwendungszweck gefahrlos gebrauchen kann, wobei auch Gefahren durch eine vorhersehbare Fehlanwendung mitzubedenken sind.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

So ist z. B. bei Aufzügen oder Beförderungsmitteln zu bedenken, dass sie in gewissem Maße Überlastungen ausgesetzt sind. Deshalb läge ein Konstruktionsfehler vor, würden Halteseile von Aufzügen bereits bei geringer Überlastung reißen. Evidenter Fehlgebrauch kann dagegen den Anspruch auf Schadenersatz vollständig entfallen lassen. So wurde die Klage eines Landwirts abgewiesen, der den Düngerstreuer bei laufender Zapfwelle zu reinigen versuchte und dessen Hand von dem laufenden Rührfinger des Düngerstreuers schwer verletzt wurde. Das Gericht führte dazu aus, dass „selbst Schulkinder" wissen, dass man bei Benutzung eines Rührgerätes nicht in den Rührfinger greift.

2.3.3.2 Fabrikationsfehler

Fabrikationsfehler werden durch eine mangelhafte Fertigung einzelner Stücke gekennzeichnet und haben nichts mit dem Konstruktions-, sondern mit dem Fabrikationsprozess zu tun.

Beispiele für Fabrikationsfehler: ein mangelhaft geschmiedeter Kondenstopf, eine fehlerhafte Schweißnaht beim Motor, im Einzelfall auftretende Materialfehler bei einem Lichtgitter, falsche Granulatmischung von Bimetall-Ummantelungen, zu hohe Bedampfung auf Platinen.

Eine Besonderheit stellt dabei der sogenannte Ausreißer dar. Ausreißer sind Fertigungs- und Fabrikationsfehler, die trotz aller zumutbaren Vorkehrungen unvermeidbar bzw. unauffindbar sind. Für diese Fehlergruppe hat die Rechtsprechung in den 50er- und 60er-Jahren eine Haftungsfreistellung eingeführt, Hersteller haften für solche Ausreißer mangels Verschulden nicht. Dennoch ist zu betonen, dass im Rahmen des Produkthaftungsgesetzes auch für Ausreißer gehaftet wird, weil dort ja das Verschulden keinerlei Rolle spielt.

Beispiel: So wurde von dem OLG München jüngst entschieden, dass Risse in Glasflaschen, die weder technisch feststellbar noch hundertprozentig vermieden werden können, einen Ausreißer darstellen. Der Hersteller – sowohl Flaschenproduzent als auch Abfüller – haften zwar nicht nach § 823 BGB, sind aber bei Explosion der Flasche gem. dem Produkthaftungsgesetz schadenersatzpflichtig.

2.3.3.3 Grundsätze zur Instruktionspflicht

Dass bestimmte Risiken (bau-)technisch unvermeidbar sind, ist auch Juristen klar. Dem Nutzer muss ein Eigenschutz durch richtiges Verhalten möglich sein, er muss aber gleichzeitig über das Restrisiko Bescheid wissen. Die Rechtsprechung hat deshalb den Herstellern sogenannte Instruktionspflichten auferlegt: Damit ist die Pflicht gemeint, mithilfe von Bedienungsanleitungen, Warnhinweisen, Piktogrammen, Schulungsvorgaben etc. die verbleibende Gefährdung weiter zu minimieren. Grundsätzlich gilt hier, dass ein Produkt fehlerfrei und sicher zu konstruieren ist, wann immer die Möglichkeit dazu besteht. Der Hersteller kann sich also nicht damit begnügen, diese Möglichkeiten ungenutzt zu lassen und lediglich auf die Gefahren hinzuweisen. Die Instruktionspflicht weist auf die Restrisiken hin, die bei einem Produkt selbst unter Ausnutzung aller Möglichkeiten bei Konstruktion und Fabrikation dennoch bleiben.

Bei der Bestimmung der Instruktionspflichten des Herstellers ist stets die am wenigsten informierte Gruppe zugrunde zu legen. Je größer das Ausmaß potenzieller Schadensfolgen und je versteckter die Gefährlichkeit, umso deutlicher müssen Warnhinweise ausfallen. Birgt das Produkt Gesundheitsgefahren, müssen Warnhinweise so deutlich erfolgen, dass die Gefahren für den Verwender plausibel werden. In solchen Fällen reichen keine allgemeinen Hinweise zum richtigen Verhalten, hier sind zutreffend die Folgen und Gesundheitsrisiken darzustellen, die bei Nichtbeachtung drohen.

Beispiel: Ein Hinweis, dass vor der Benutzung der Maschine der Sicherheitsspalt richtig einzustellen und diese Einstellung zu überprüfen ist, genügt nicht. Entsprechende Warnhinweise müssen deutlich machen, dass eine ernsthafte Verletzung der Hand droht, sollte der Sicherheitsspalt falsch eingestellt werden.

Keine Hinweispflicht besteht für solche Informationen, die für die Allgemeinheit oder für spezifische Benutzergruppen offenkundig sind.

So ist z. B. offenkundig und erkennbar, dass ein Messer schneiden kann.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

Der Hersteller kann sich nicht damit verteidigen, dass die Instruktion nicht gelesen wird oder sowieso nicht eingehalten worden wäre. Es ist ständige Rechtsprechung, dass aufklärungskonformes Verhalten der Nutzer vermutet wird.

Instruktionspflichten erstrecken sich auch auf den naheliegenden Fehlgebrauch des Produktes. Allerdings muss der Hersteller nicht mit unvernünftiger, unvorhersehbarer und missbräuchlicher Produktverwendung rechnen.

Eine Bedienungsanleitung hat daher nicht nur darzustellen, wie der richtige Weg der Montage bzw. des Zusammenbaus ist. Vielmehr muss sie vor falschen Handgriffen, die naheliegend sind und oft vorkommen, gesondert warnen.

Andererseits wird von der Rechtsprechung betont, dass der Hersteller sich darauf verlassen kann, dass der fachlich geschulte Bediener sich auf die ihm dezidiert bekannten Vorgaben der Bedienungsanleitung hält. So wurde eine „grobe Fehlbedienung" angenommen, als der Bediener einer Knetmaschine die Deckel-Verklebung dadurch zu öffnen versuchte, dass er die Knetmasse erhitzte, bis ein Überdruck im Anlageninneren den Deckel lösen sollte.

Die Warnung vor potenziellen Gefahren des Produktes ist ohne jegliche Beschönigung an jener Stelle auszusprechen, an der sie konzeptionell vom Verwender auch erwartet wird. Unzulässig wäre es deshalb, Hinweise auf mögliche Produktgefahren versteckt irgendwo in der Gebrauchsanweisung zu platzieren.

Gleichzeitig muss der Hersteller dafür Sorge tragen, dass der Verwender des Produktes die Gebrauchsanleitung auch versteht. Zunächst ist also von Bedeutung, ob der Verwender überhaupt lesen kann bzw. welche Sprachen er beherrscht. Dies impliziert unmittelbar die Frage, in welche Sprachen die Sicherheitshinweise einer Gebrauchsanleitung zu übersetzen sind. Selbstverständlich ist dabei, dass die Sicherheitshinweise einer Gebrauchsanleitung in jedem Fall in die Sprache des Landes zu übersetzen ist, in dem das Produkt vertrieben werden soll. Der Hersteller kann sich nicht darauf verlassen, dass die Gesellschaft, die in einem bestimmten Land für den internationalen Vertrieb eines Produktes verantwortlich zeichnet, auch für eine adäquate Übersetzung einschließlich relevanter Warnhinweise in die jeweilige Landessprache sorgt.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

2.3.3.4 Produktbeobachtungspflicht

Die deliktische Haftung kennt eine weitere Fehlergruppe, nämlich Fehler bei der Produktbeobachtung. Diese Pflicht trifft den Hersteller erst nach Inverkehrgabe des von ihm entwickelten und hergestellten Produktes. Hinter diesem von der Rechtsprechung entwickelten Begriff verbirgt sich die Verpflichtung des Herstellers, das Produkt auch nach erfolgreicher Inverkehrgabe hinsichtlich seines sicherheitsrelevanten Verhaltens am Markt zu beobachten.

Der Hersteller hat die Verwendung seines Produktes in der Praxis beispielsweise durch Auswertung fachwissenschaftlicher Erkenntnisse in Branchenzeitschriften, Medien oder auch auf Fachveranstaltungen und Messen zu verfolgen. Zur aktiven Produktbeobachtungspflicht gehört ferner die Beobachtung der Produktentwicklung bei den wichtigsten Mitbewerbern.

Es ist also eine gut strukturierte betriebliche Organisation erforderlich, damit

- die Beobachtung des Marktes sichergestellt wird,
- die relevanten Informationen ausgewertet werden und
- der Bericht die Entscheidungsträger erreicht.

Eine gut durchdachte Organisation der Produktbeobachtung kann im Rahmen eines Qualitätssicherungsmanagements für das Unternehmen erreicht werden.

In einem zweiten Schritt müssen Entscheidungsträger die Konsequenzen aus etwaigen Schadensmeldungen ziehen. Folgende Fragestellungen sind dabei zu beantworten:

- Ist die bisherige Konstruktion für künftige Produktreihen zu ändern?
- Sind zusätzliche Gefahrenhinweise für bisherige und künftige Abnehmer aufzunehmen?
- Ist eine Gefahrenabwendungsmaßnahme (z. B. eine öffentliche Warnung, eine Nachrüstungsaktion oder ein Rückruf) wegen unerkannt gebliebener Produktgefahren angezeigt?

Stellt sich z. B. erst nach Inverkehrgabe aufgrund vermehrter Schadensmeldungen und neuer wissenschaftlicher Berichte in der Fachpresse heraus, dass z. B. ein bestimmter Sicherheitsriegel bei hohen Temperaturen an Wirksamkeit verliert, wird der Hersteller bei seinen noch nicht verkauften Produkten ggf. darauf hinweisen, dass während der Sommermonate ein zusätzlicher Schutz notwendig ist. Gleichzeitig wird er seine Kunden über das Risiko informieren. Sind die Kunden namentlich bekannt (in der Praxis leider eher selten), ist dies problemlos durchführbar. Bei nicht namentlich bekannten Kunden ist die nachträgliche Warnung über die Hauptverkaufsorte, Fachzeitschriften oder über andere öffentliche Medien zu erwägen.

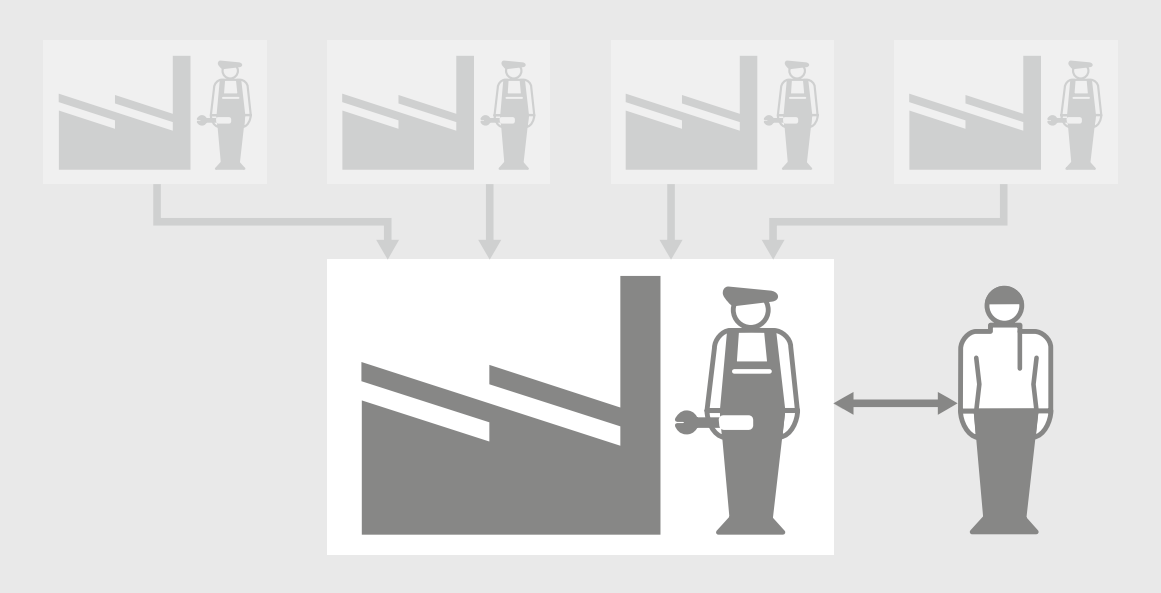
Auf missbräuchliche Arten der Verwendung braucht der Hersteller aber auch im Rahmen der Produktbeobachtung keine Rücksicht zu nehmen. Wird das Produkt zweckentfremdet oder eigenmächtig umgebaut, besteht keinerlei Handlungspflicht im Rahmen der Produktbeobachtung.

Beispiel: Kauft ein industrieller Betreiber eine komplizierte technische Maschine und baut sie eigenmächtig und ohne Abstimmung mit dem Hersteller um, muss der ursprüngliche Hersteller ihn nicht auf mit dem Umbau in Verbindung stehende Sicherheitsmängel hinweisen.

2.3.4 Haftung in der arbeitsteiligen Produktion

Das gesetzliche Leitbild des Alleinherstellers, der jedes Teil seines Produktes selbst herstellt und es anschließend zusammenbaut, wirkt längst wie eine historische Beschreibung und kommt in der Praxis mit ihrer immer geringeren Fertigungstiefe kaum mehr vor. Die Arbeitsteilung in der Produktion wirft neue Fragen auf, insbesondere in Bezug auf die Verteilung der Verantwortungsbereiche zwischen Zulieferer und Endhersteller.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB



Haftung des Endproduktherstellers

2.3.4.1 Haftung des Endproduktherstellers

Der Endhersteller bzw. der Assembler, der die einzelnen Teile des Produktes zusammenbaut, haftet insgesamt für die Fehlerfreiheit des Endproduktes.

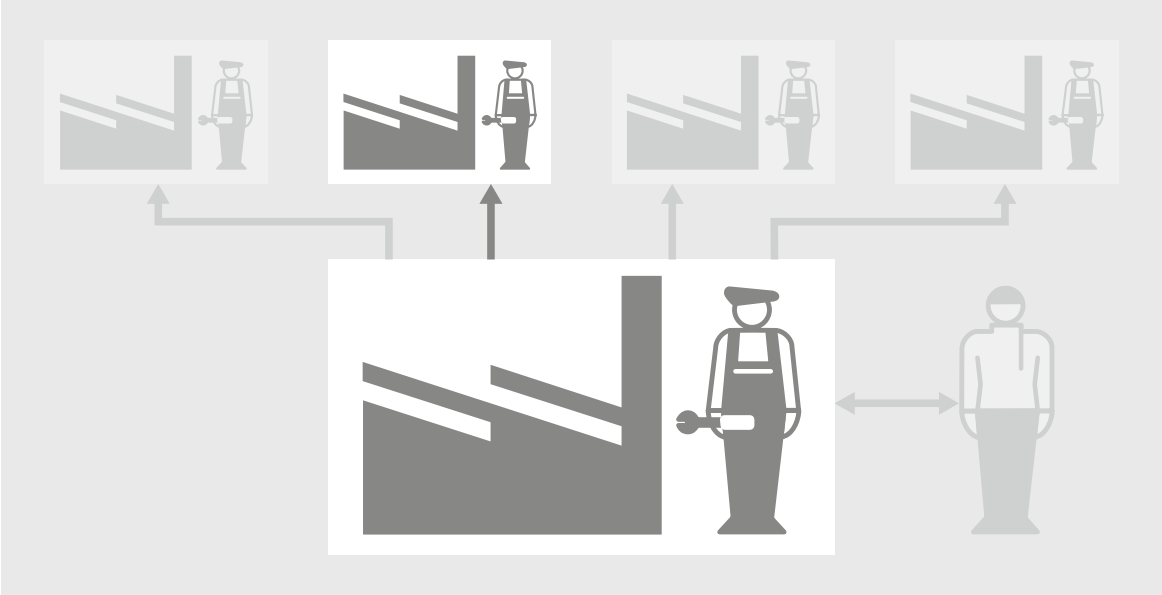
Im Bereich der Konstruktion muss der Endhersteller dafür sorgen, dass das Produktteil, das er von seinem Zulieferer bezieht, nach Materialvorgaben und Belastbarkeitsparametern jene Funktion erfüllen kann, für die sein Endprodukt verwendet werden soll. Hierbei ist eine der wichtigsten Aufgaben des Endherstellers, das Zulieferprodukt richtig und durchdacht zu spezifizieren. Er muss dieses präzise beschreiben (z. B. Werkstoffart, Materialeigenschaften, Härtegrade, Maße, Toleranzbereiche, Gewicht, Fertigungsvorgaben, Belastbarkeit, Ausschuss-ppm-Werte, Prüfmethodologien etc.). Darüber hinaus muss er durch konkrete Zielvorgaben sicherstellen, dass das Zulieferprodukt keine sicherheitsrelevanten Mängel aufweist (z. B. Beschreibung aller Betriebsbedingungen, Einsatzorte, Betriebsstunden, Hinweise auf Spitzenbelastung, mögliche Überbeanspruchung, möglicher Fehlgebrauch durch den Nutzer).

Im Rahmen der Fabrikation liegt es im Verantwortungsbereich des Endherstellers, sicherzustellen, dass bei der Produktion der Zulieferprodukte ordnungsgemäßes Material ausgewählt und verwendet wird. Stellt der Endhersteller nicht durch Weisungen oder vertragliche Vereinbarungen mit dem Zulieferer sicher, auf welche Art und Weise die Fabrikation erfolgen soll, so hat er eine Typenprüfung des Zulieferproduktes nach dem neuesten Stand der Wissenschaft und Technik durchzuführen.

Beispiel: Schrauben sind nach Material, Durchmesser und Gewinde auf ihre Belastbarkeit, Mineralwasserflaschen auf ihre Druckbeständigkeit, Tragegriffe und Haltebügel auf ihre Reißfestigkeit zu testen.

Diese Prüfungspflichten können partiell auf den Zulieferer übertragen werden, in der Praxis geschieht dies häufig durch Qualitätssicherungsvereinbarungen. Diese betreffen Konstruktion und Fabrikation des Produktes und schreiben bestimmte qualitätssichernde Maßnahmen und Prüftechniken vor. Die Details sind in der Praxis juristisch sehr anspruchsvoll.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB



Haftung des Zulieferers

Für die notwendigen Spezifikationen und Prüfungen bzw. Tests wird oft auf eine technische Norm Bezug genommen. Zusätzliche Qualitätssicherungsmaßnahmen wie eine Herstellbarkeitsanalyse (Feasibility Study) ergeben das Pflichtenprogramm des Zulieferers.

Der BGH bestätigte, dass der Endhersteller sich darauf verlassen kann, dass der Zulieferer die Bauteile nach den vertraglich vereinbarten Qualitätsanforderungen baut und deren Qualität selbst überprüft. Die ordnungsgemäße Wahl eines renommierten Zulieferunternehmens, dessen vorherige eingehende Überprüfung, Sicherstellung der erforderlichen Zertifizierung des Bauteils und Abschluss von Qualitätssicherungsvereinbarungen ermöglichen, den eigenen Prüfaufwand des Endherstellers herabzusetzen. Kann also der Endhersteller nachweisen, dass er die geschilderten Maßnahmen zur Auswahl und Überwachung des Zulieferers getroffen hat, sind die Fehler für ihn ein Ausreißer, für die er nicht gem. § 823 BGB haftet (wohl aber gegenüber Verbrauchern nach dem ProdHaftG).

Ein Endhersteller hat auch vor solchen Gefahren zu warnen, die auf die Gefährlichkeit des zugelieferten Produktes zurückgehen. Erst recht ist der Endhersteller verpflichtet, die vom Zulieferer beigefügten Gebrauchs- oder Warnhinweise an den Verwender des Produktes weiterzuleiten und in seine insgesamt zu erstellende Bedienungsanleitung zu integrieren.

2.3.4.2 Haftung des Zulieferers

Der Zulieferer ist Hersteller eines Teilproduktes. Folglich muss er für alle Gefahren einstehen, die von seinem Teilprodukt ausgehen.

Die Konstruktionspflichten für das Zulieferteil hängen in besonderem Maße von den Sicherheitserwartungen der Abnehmer ab. Kennt der Zulieferer den Verwendungszweck des Endproduktes, muss er das dafür geeignete Teil herstellen. Er hat dabei auch ihm bekannte oder denkbare Fehlanwendungen des Endproduktes durch den Endnutzer zu berücksichtigen. Ausdrücklich hat er die vorgegebenen Spezifikationen und Qualitätssicherungsvorgaben seines Auftraggebers zu beachten.

Der Zulieferer hat darüber hinaus die Verpflichtung, seinen Auftraggeber vor solchen Gefahren seines Zulieferproduktes zu warnen, die in der Branche des Endherstellers nicht allgemein bekannt sind. Der Zulieferer muss die Anfragen seines Abnehmers zu konkreten Gefahren ohne jede Beschönigung beantworten. Allerdings darf der Zulieferer Fragen nach der Produkteignung, sofern keine weitere Aufklärungspflicht besteht, auch mit Nichtwissen erklären.

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

Der BGH entschied: Ein Hersteller bezog vom Zulieferer sogenannte 25-kg-Hobbocks, das sind Blecheimer mit zwei beweglichen Tragegriffen. Ein Malermeister verunglückte beim Tragen eines solchen Hobbocks, den er mit 50 kg Plastikmasse befüllt hatte. Der Endhersteller hatte sich zuvor beim Zulieferer erkundigt, ob die Eimer mit 50 kg belastbar seien. Der Zulieferer antwortete, dass die Eimer für 25 kg geeignet seien, ob er diese mit 50 kg befüllen möchte, müsse er selbst entscheiden. Der BGH traf die Entscheidung, dass der Zulieferer zu dieser Antwort berechtigt war und daraus klar hervorging, dass die Produkteignung lediglich bis zu einer Befüllung von 25 kg gesichert war.

2.3.5 Gefahrabwendungsmaßnahme, Warnung, Nachrüstung, Rückruf

Wird im Zuge der After-Sales-Produktbeobachtung festgestellt, dass ein in Verkehr gebrachtes Produkt nicht den Sicherheitserwartungen entspricht, ist herstellerseitig zu prüfen, ob zur Vermeidung von Haftungsrisiken eine Gefahrabwendungsmaßnahme in Bezug auf das entsprechende Produkt angezeigt ist. Darunter werden im Rahmen dieses Sicherheitskompendiums alle Maßnahmen zur Abwendung, Beseitigung oder Verminderung von Gefahren verstanden, die von bereits im Verkehr befindlichen Produkten ausgehen (z. B. Warnungen, neue Bedienungsanleitungen, Safety-Uploads, Nachrüstungen vor Ort oder Rückrufe ins Werk).

2.3.5.1 Voraussetzungen für die Gefahrabwendungsmaßnahme

Wann eine solche Gefahrabwendungsmaßnahme durchgeführt werden muss, kann nicht allgemein beantwortet werden. Dabei kommt es auf die Umstände des Einzelfalles unter Berücksichtigung des Ausmaßes des drohenden Schadens und des Grades ihrer Realisierungsgefahr an. In ökonomischer Terminologie ausgedrückt ist der „Schadenerwartungswert“ entscheidend, d. h. das Produkt aus Schadenshöhe und Eintrittswahrscheinlichkeit. Der Hersteller muss also analysieren:

1. Wie hoch ist die Eintrittswahrscheinlichkeit des Schadens:

Sind einzelne Chargen betroffen oder haftet der Fehler der gesamten Serie an? Tritt der Schaden bei bestimmungsgemäßer Verwendung oder nur bei vorhersehbarer Fehlanwendung auf? Müssen mehrere zufällige Verhaltensweisen kumuliert vorliegen? Tritt der Schaden erst nach längerer Nutzungsdauer auf? Wird vor dem Verhalten in der Bedienungsanleitung gewarnt?

2. Welcher Schaden droht:

Vorausgesetzt, der Produktfehler führt zum Schaden: Sind lediglich Sachschäden, leichte oder schwere Personenschäden zu erwarten?

2.3 Verschuldenshaftung § 823 Abs. 1 BGB

Rein wirtschaftliche Erwägungen sind kein Argument, um die Durchführung einer Gefahrabwendungsmaßnahme abzulehnen (so etwa hohe Rückrufkosten oder Imageverlust), insbesondere dann nicht, wenn bedeutende Rechtsgüter auf dem Spiel stehen.

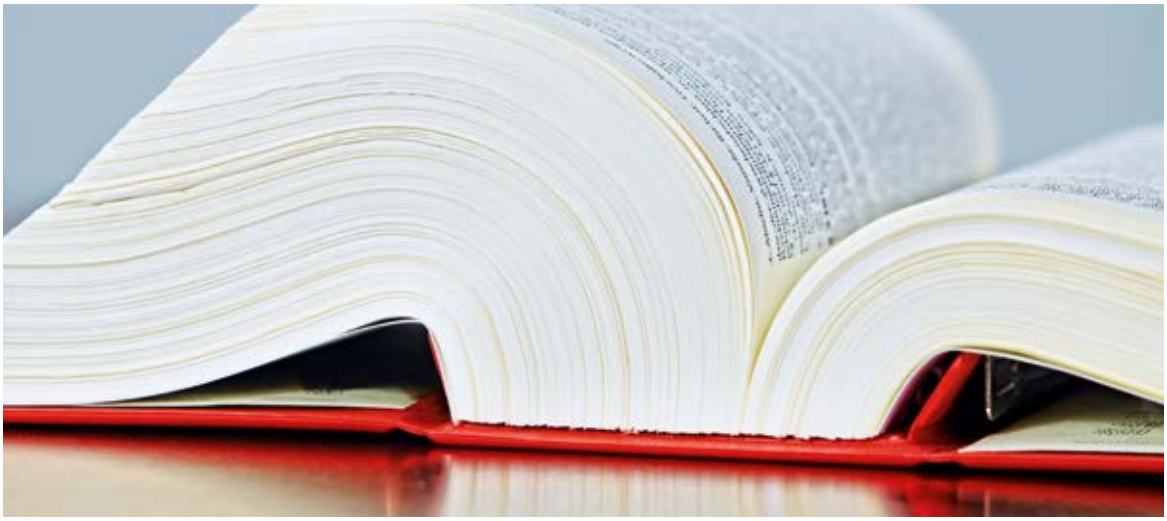
Es ist auch ohne Bedeutung, ob die eigentliche Schadensursache bereits im Einzelnen festgestellt werden konnte, solange die Schadensfälle in Zusammenhang mit der Verwendung des Produktes aufgetreten sind. Es ist also nicht zulässig, so lange zu warten, bis man einen feststehenden Schadensursachenverlauf auch ingenieurtechnisch durchdrungen hat. Allerdings wird dem Hersteller selbstredend die Möglichkeit zugebilligt, vor Einführung von Maßnahmen zu prüfen, ob überhaupt ein Produktfehler vorliegt. Hals-über-Kopf-Maßnahmen sind also nicht notwendig.

Erreichen den Hersteller Schadensmeldungen z. B. im Rahmen seiner Produktbeobachtung, kann er zunächst Prüfungen einleiten, ob die berichteten Schäden (z. B. Brüchigkeit eines Glasteiles) tatsächlich auf Produktfehler zurückzuführen sind oder etwa nur Transportschäden oder Schäden infolge unsachgemäßer Benutzung vorliegen. Steht fest, dass ein Produktfehler für die Schadensfälle verantwortlich ist, muss der Hersteller Gegenmaßnahmen einleiten, selbst wenn nicht feststeht, ob der Fehler z. B. bei der Temperatureinstellung oder in anderen Bereichen des Glasblasprozesses aufgetreten ist.

2.3.5.2 Unternehmensinterne Risiko-Prävention

Um im Ernstfall schnell und effizient auf auftretende Produktgefahren reagieren zu können, bietet sich die betriebsinterne Einrichtung eines Rückrufmanagements an. Ferner ist der Abschluss einer Rückrufversicherung in Betracht zu ziehen.

2.4 § 823 Abs. 2 in Verbindung mit dem Produktsicherheitsgesetz



Neben der allgemein gefassten Generalklausel in § 823 Abs. 1 BGB kann sich eine Schadensersatzhaftung auch gemäß § 823 Abs. 2 BGB ergeben:

§ 823 Abs. 2 BGB

„Die gleiche Verpflichtung (gemeint ist die Pflicht zum Schadensersatz) trifft denjenigen, der gegen ein Gesetz verstößt, das den Schutz eines anderen bezweckt.“

Die rechtsgutsverletzende Handlung ist hierbei die Verletzung eines sogenannten „Schutzgesetzes“: Schutzgesetz bedeutet, dass die jeweilige gesetzliche Bestimmung aus irgendeinem anderen Gesetzeswerk (auch) zum Schutz des Einzelnen bestimmt ist und deshalb im Schadensfall die Gesetzesverletzung selbst bereits zum Schadensersatz verpflichtet.

Im Rahmen der Haftungsrisiken wegen Schutzgesetzes-Verletzung spielen Spezialgesetze eine Rolle, die für bestimmte Produktgruppen Sicherheitsanforderungen festlegen. Am bedeutendsten ist das Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Produktsicherheitsgesetz/ProdSG), da es eine breite Palette von Produkten erfasst: Haarfön, Wasserkocher und Minibagger fallen genauso in seinen Anwendungsbereich wie Atemschutzgeräte und komplexe Anlagen. Da zudem über das ProdSG und seine nachgeordneten Verordnungen diverse EG-Richtlinien zur CE-Kennzeichnung national „gespiegelt“ wurden (u. a. Niederspannungs-, ATEX-, Maschinen-, Spielzeug-, Druckgeräte-, Sportboote-, Aufzugs-, Gasverbrauchseinrichtungs-Richtlinie), drohen hier unversehens Haftungsrisiken bei Missachtung der in den CE-Vorschriften enthaltenen Sicherheitsvorgaben. Weitere CE-Richtlinien wurden über gesonderte Gesetze umgesetzt, die im Schadensfall ebenfalls mit § 823 Abs. 2 BGB kombiniert werden können (z. B. EMV-Gesetz/EMVG), Medizinproduktegesetz/MPG), Funk- und Telekommunikationsendeinrichtungs-Gesetz/FTEG).

Beim Bereitstellen von unsicheren Produkten am Markt kann sich also die Haftung – zusätzlich zu der Haftung aus dem Produkthaftungsgesetz und § 823 Abs. 1 BGB – wegen Verstoßes gegen derartige technikrechtliche Sicherheitsvorschriften ergeben.

3

Normen, Richtlinien und Gesetze

3 Normen, Richtlinien und Gesetze

3	**Normen, Richtlinien und Gesetze**	
3.1	Normen, Richtlinien und Gesetze in der Europäischen Union (EU)	3-3
3.2	CE-Kennzeichnung	3-5
3.2.1	Die Basis der Maschinensicherheit: Maschinenrichtlinie und CE-Zeichen	3-5
3.2.2	Rechtliche Grundlagen	3-5
3.2.3	CE-Kennzeichnung von Maschinen	3-6
3.3	Richtlinien	3-16
3.3.1	Maschinenrichtlinie	3-17
3.4	Normen	3-18
3.4.1	Herausgeber und Geltungsbereich	3-18
3.4.2	EN-Sicherheitsnormen im Maschinenbau	3-19
3.4.3	Grundnormen und Designvorgaben	3-21
3.4.4	Produktnormen	3-36
3.4.5	Anwendungsnormen	3-39
3.5	Normen, Richtlinien und Gesetze im internationalen Vergleich	3-40
3.5.1	Richtlinien und Gesetze in Amerika	3-40
3.5.2	Richtlinien und Gesetze in Asien	3-45
3.5.3	Richtlinien und Gesetze in Ozeanien	3-49
3.5.4	Zusammenfassung	3-51
3.6	Industrieroboter, Mensch-Roboter-Kollaboration (MRK)	3-52
3.6.1	Normative Vorgaben für den Einsatz von Industrierobotern	3-53
3.6.2	Die Roboterapplikation aus Sicht der EN ISO 10218-2	3-54
3.6.3	Mensch-Roboter-Kollaboration und ISO/TS 15066	3-54
3.6.4	Validierung	3-57
3.6.5	Sinn der Messung	3-58
3.7	Sicheres Programmieren nach EN ISO 13849-1	3-60
3.7.1	Safety Related Software	3-60
3.7.2	Software in Bezug auf die Risikobeurteilung	3-61
3.7.3	Basisanforderungen an die Softwareentwicklung	3-62
3.7.4	Weitere fehlervermeidende Maßnahmen für steigende Performance Level	3-63
3.7.5	Programmierwerkzeuge, Sprachen und Bibliotheken	3-63
3.7.6	Strukturierung und Modularität der Software	3-63
3.7.7	SRASW und Nicht-SRASW in einer Komponente	3-64
3.7.8	Softwareimplementierung und Codierung	3-64
3.7.9	Testen	3-65
3.7.10	Dokumentation	3-66
3.7.11	Verifikation	3-66
3.7.12	Konfigurationsmanagement	3-66
3.7.13	Änderungen	3-66
3.7.14	Zusammenfassung	3-66

3 Normen, Richtlinien und Gesetze

3.8 Validierung 3-67
3.8.1 Verifikation von Sicherheitsfunktionen nach EN ISO 13849-1/2 3-68
3.8.2 Verifikation von Sicherheitsfunktionen nach EN 62061 3-68
3.8.3 Allgemeines zum Validierungsplan 3-69
3.8.4 Validieren durch Analyse 3-70
3.8.5 Validieren durch Prüfung 3-70
3.8.6 Verifikation von Sicherheitsfunktionen 3-70
3.8.7 Validierung von Software 3-72
3.8.8 Validieren der Widerstandsfähigkeit gegenüber Umgebungsanforderungen 3-73
3.8.9 Erstellen des Validierungsberichtes 3-73
3.8.10 Fazit 3-73
3.8.11 Anhang 3-74
3.9 Zertifizierung und Akkreditierung 3-76
3.9.1 Akkreditierung: Qualitätssiegel für Kunden 3-76
3.9.2 Akkreditierung oder Zertifizierung 3-79
3.9.3 Prüfungen gemäß BetrSichV und Akkreditierung 3-80
3.9.4 Fazit 3-81

3.1 Normen, Richtlinien und Gesetze in der Europäischen Union (EU)

Die Europäische Union wächst immer mehr zusammen. Dies äußert sich für Maschinenbauer in einer zunehmenden Harmonisierung von Gesetzen, Regeln und Bestimmungen. Noch vor gar nicht langer Zeit hat jedes Land eigene Vorgaben zu den unterschiedlichen Bereichen des täglichen Lebens und der Wirtschaft herausgebracht, heute findet man mehr und mehr einheitliche Regelungen in Europa.

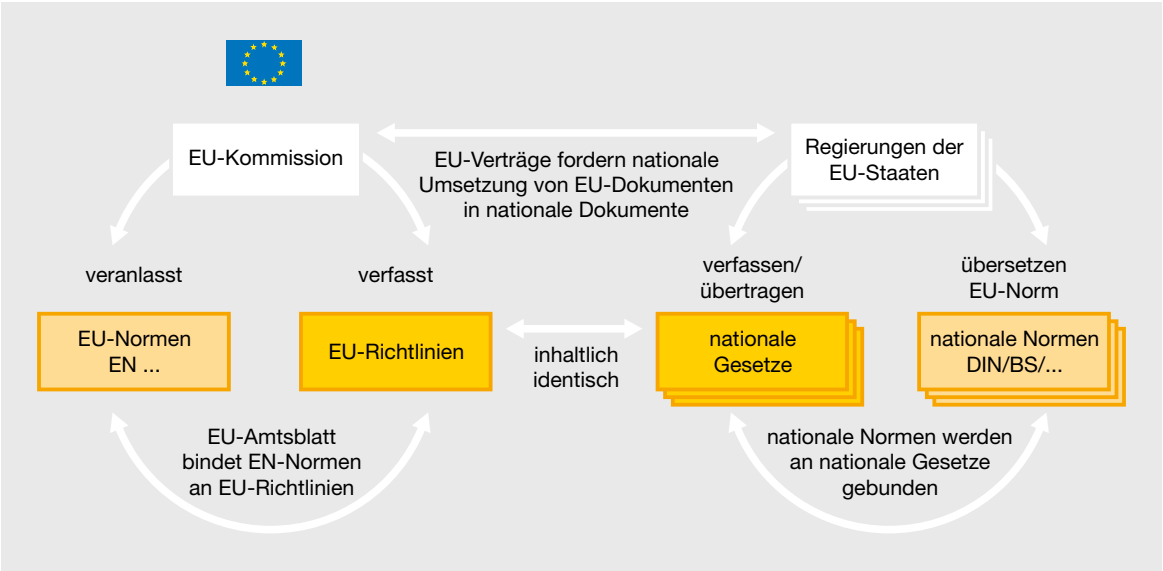
Wie hängen Gesetze, Richtlinien und Normen in Europa zusammen?

Zunächst formuliert die EU mittels Richtlinien allgemeine Schutzziele. Diese Schutzziele bedürfen einer genaueren Spezifizierung, die konkrete Regelung erfolgt über Normen.

Üblicherweise verfasst die EU Richtlinien zu speziellen Themen. Diese Richtlinien haben an sich noch keine direkte Auswirkung auf den einzelnen Bürger oder auf eine Firma. Wirksam werden diese erst im Zusammenhang mit den Vereinbarungen der einzelnen Länder innerhalb der EU, die diese Richtlinien in nationales Recht umsetzen. In jedem Land der EU verweist also ein Gesetz oder eine Bestimmung auf die entsprechende EU-Richtlinie und erhebt diese damit zu nationalem Recht. Zwischen der Verabschiedung einer Richtlinie und der Umsetzung in nationales Recht gibt es daher zwangsläufig Übergangsfristen, innerhalb derer die Richtlinie in den einzelnen Ländern in nationales Recht umgewandelt wird. Dies ist jedoch in der Regel für einen Anwender unerheblich, da die Richtlinien selbst klare Regelungen zum jeweiligen Gültigkeitsdatum treffen. In der Praxis haben somit innerhalb der EU die ihrem Titel nach fast harmlos als Richtlinien bezeichneten Dokumente den Status von Gesetzen.

Damit ist zwar geklärt, wie Gesetze und Richtlinien zusammenhängen, die Frage der Normen ist jedoch noch offen.

Normen an sich sind zwar interessant zu lesen, haben aber für sich allein noch keine direkte rechtliche Relevanz. Diese erhalten Normen erst durch eine Veröffentlichung im Amtsblatt der EU oder durch nationale Gesetze und Bestimmungen, die diese Normen nennen. Mittels einer solchen Veröffentlichung kann eine Norm die sogenannte Vermutungswirkung erlangen. Diese Vermutungswirkung besagt, dass ein Hersteller davon ausgehen kann, dass die von der Norm erfassten Anforderungen



Zusammenhang von harmonisierten Normen und Gesetzen in der EU

3.1 Normen, Richtlinien und Gesetze in der Europäischen Union (EU)

der zugehörigen Richtlinie dann erfüllt sind, wenn er die Vorgaben der Norm erfüllt. Die Vermutungswirkung bescheinigt also quasi korrektes Verhalten. Im formalrechtlichen Zusammenhang spricht man dabei von der Umkehrung der Beweislast. Wird vom Hersteller eine harmonisierte Norm angewandt, so muss ihm im Zweifel ein Fehlverhalten nachgewiesen werden. Andernfalls muss der Hersteller nachweisen, dass er sich richtlinienkonform verhalten hat.
Erfüllt ein Hersteller eine Norm nicht, bedeutet das noch lange nicht, dass er sich nicht korrekt verhalten hätte. Gerade in innovativen Branchen existieren entweder noch keine Normen oder greifen nur unzureichend. Der Hersteller muss dann individuell nachweisen, dass er die notwendige Sorgfalt walten ließ und die Schutzziele der entsprechenden Richtlinien damit einhält. Ein solcher Weg ist meist aufwendiger, aber gerade in innovativen Branchen häufig nicht vermeidbar.

Hierbei muss besonders betont werden, dass die EU nicht alle Normen im Amtsblatt veröffentlicht und viele damit nicht harmonisiert sind. Selbst wenn einer derartigen Norm erhebliche technische Relevanz beigemessen wird, eine Vermutungswirkung hat sie dennoch nicht. Mitunter erlangt aber auch eine nicht im EU-Amtsblatt gelistete Norm einen mit der Harmonisierung vergleichbaren Status. Das ist beispielsweise dann der Fall, wenn eine bereits harmonisierte Norm auf die betreffende Norm verweist. Die nicht im Amtsblatt der EU gelistete Norm wird dann quasi durch die Hintertür harmonisiert.

3.2 CE-Kennzeichnung

3.2.1 Die Basis der Maschinensicherheit: Maschinenrichtlinie und CE-Zeichen

1993 wurde die Maschinenrichtlinie (MRL) mit dem Ziel ratifiziert, Handelshemmnisse abzubauen und damit den freien Binnenmarkt in Europa zu ermöglichen. Nach einer Übergangsfrist von zwei Jahren ist die Maschinenrichtlinie seit dem 01.01.1995 in Europa bindend. Sie beschreibt einheitliche Anforderungen an die Sicherheit und Gesundheit bei der Interaktion von Mensch und Maschine und ersetzt so die vielen einzelstaatlichen Regelungen, die zur Maschinensicherheit existierten. Seit dem 29.12.2009 gilt die Maschinenrichtlinie 2006/42/EG.

Das CE-Zeichen steht für „Communauté Européenne“. Mit diesem Zeichen dokumentiert ein Hersteller, dass er alle für sein Produkt relevanten europäischen Binnenmarktrichtlinien berücksichtigt hat und dass alle zutreffenden Verfahren zur Konformitätsbewertung angewendet wurden. Mit dem CE-Zeichen versehene Produkte dürfen ohne Rücksicht auf nationale Vorschriften eingeführt und vertrieben werden. Man spricht beim CE-Zeichen daher auch vom „Reisepass für Europa“.

In der Regel sehen alle Richtlinien nach dem neuen Konzept („new approach“) die Anbringung der CE-Kennzeichnung vor. Gelten für ein Produkt mehrere Richtlinien, die eine CE-Kennzeichnung nahelegen, bedeutet diese Kennzeichnung, dass von der Konformität des Produktes mit den Bestimmungen all dieser Richtlinien auszugehen ist.

3.2.2 Rechtliche Grundlagen

Die Pflicht zur Anbringung der CE-Kennzeichnung erstreckt sich auf alle Produkte, die unter Richtlinien fallen, die diese Kennzeichnung vorsehen und für den gemeinschaftlichen Markt bestimmt sind. Demnach sind folgende Produkte, die unter eine Richtlinie fallen, mit einer CE-Kennzeichnung zu versehen:

- alle neuen Produkte, unabhängig davon, ob sie in den Mitgliedstaaten oder in Drittländern hergestellt wurden
- aus Drittländern importierte gebrauchte Produkte und Produkte aus zweiter Hand
- wesentlich veränderte Produkte, die als neue Produkte unter die Richtlinien fallen

Die Richtlinien können bestimmte Produkte von der CE-Kennzeichnung ausnehmen.

Mit der EG-Konformitätserklärung bestätigt der Hersteller u. a., dass sein Produkt die Anforderungen der entsprechenden Richtlinie(n) erfüllt.

Im Folgenden soll die CE-Kennzeichnung unter Betrachtung der Maschinenrichtlinie erläutert werden.

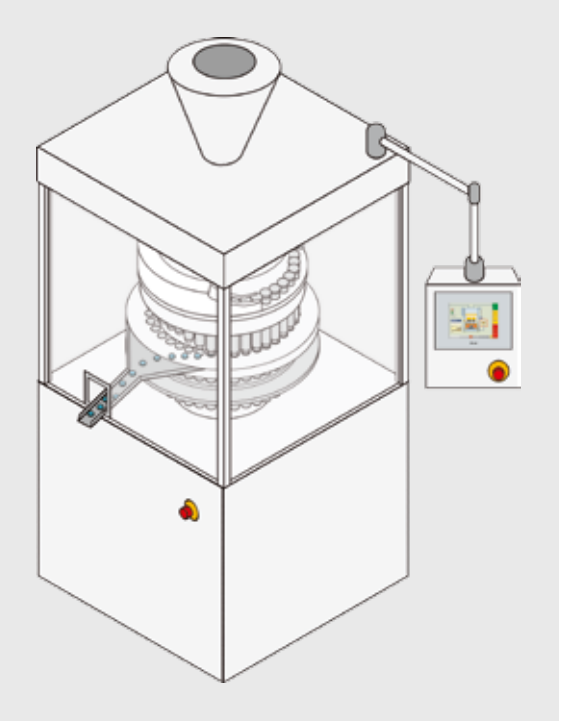
3.2 CE-Kennzeichnung

3.2.3 CE-Kennzeichnung von Maschinen

3.2.3.1 Was ist eine Maschine?

Im Sinne der Richtlinie gilt als Maschine u. a.

eine Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist, und die für eine bestimmte Anwendung zusammengefügt sind (siehe Artikel 2 der Maschinenrichtlinie).



Beispiel für eine Maschine im Sinne der Richtlinie

Ebenfalls zu Maschinen im Sinne der Maschinenrichtlinie zählen:

- Gesamtheiten von Maschinen oder komplexen Anlagen (zu komplexen Anlagen gehören ebenfalls Fertigungsstraßen und aus mehreren Maschinen bestehende Spezialmaschinen)
- Sicherheitsbauteile (Welche Bauteile als Sicherheitsbauteile zu klassifizieren sind, wird dabei sehr kontrovers diskutiert. Der Anhang V der Maschinenrichtlinie enthält eine äußerst umfangreiche Liste von Sicherheitsbauteilen.)
- auswechselbare Ausrüstungen, mit denen die Grundfunktionen einer Maschine geändert werden können
- unvollständige Maschinen, die dazu bestimmt sind, in andere Maschinen(teile) eingebaut zu werden, um gemeinsam eine Maschine zu bilden

3.2.3.2 CE-Kennzeichnung von Maschinen und Anlagen

Gemäß Maschinenrichtlinie wird derjenige zum Hersteller einer Maschine, der Maschinen oder Maschinenteile unterschiedlichen Ursprungs zusammenbaut und diese dem Markt zur Verfügung stellt.

Hersteller kann entweder der Maschinenbauer selbst oder – bei Änderungen an der Maschine – der Betreiber sein, der dadurch zum Hersteller wird. Im Falle von zusammengesetzten Maschinen kann dies der Hersteller, ein Montageunternehmen, der Projektleiter, ein Ingenieurbüro oder der Betreiber selbst sein, der eine neue Anlage aus unterschiedlichen Maschinen zusammenstellt, sodass verschiedene Teil-Maschinen eine neue Maschine bilden.

Laut Maschinenrichtlinie gibt es aber nur einen Hersteller, der für Konstruktion und Herstellung der Maschine verantwortlich ist. Dieser Hersteller oder sein Bevollmächtigter zeichnet für die Durchführung der administrativen Verfahren für die gesamte Anlage verantwortlich. Der Hersteller kann Bevollmächtigte benennen, um die Verantwortung für die Verfahren zu übernehmen, die notwendig sind, um das Produkt auf den Markt zu bringen:

- Zusammenstellung der technischen Unterlagen der Anlage
- Erstellen der technischen Dokumentation
- Bereitstellung einer Betriebsanleitung der Anlage
- Anbringung der CE-Kennzeichnung an einer repräsentativen Stelle der Anlage und Ausstellung einer EG-Konformitätserklärung für die gesamte Anlage

3.2 CE-Kennzeichnung

Wichtig ist, dass der Hersteller den Sicherheitsaspekt bereits bei der Formulierung der Aufträge oder in den Lastenheften für die Bauteile berücksichtigt. Die Unterlagen dürfen nicht ausschließlich unter dem Gesichtspunkt der maschinellen Leistungen abgefasst werden. Der Hersteller ist für die technischen Gesamtunterlagen verantwortlich und muss für jeden seiner Zulieferer den Anteil bestimmen, den dieser übernehmen soll.

3.2.3.3 Einsatz von Maschinen im europäischen Wirtschaftsraum

Unabhängig von Herstellungsort und -datum unterliegen alle Maschinen, die erstmals ab dem 01.01.1995 im europäischen Wirtschaftsraum eingesetzt werden, der EU-Maschinenrichtlinie und müssen somit mit einer CE-Kennzeichnung versehen sein.

3.2.3.4 Zusammengesetzte Maschinen

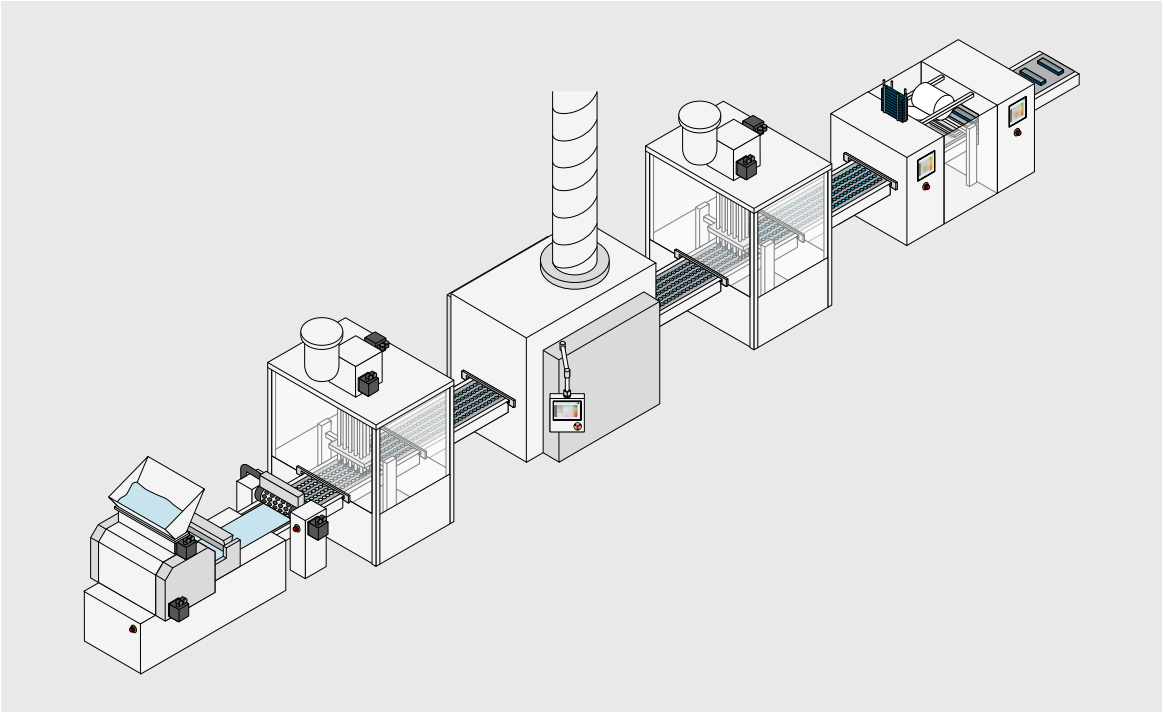
Bei großen Produktionslinien besteht eine Maschine oftmals aus mehreren zusammengesetzten Einzelmaschinen. Auch wenn jede für sich eine CE-Kennzeichnung trägt, so muss die Gesamtanlage ebenfalls einen CE-Kennzeichnungsprozess durchlaufen.

3.2.3.5 Import einer Maschine aus einem Land außerhalb der EU

Beim Import einer Maschine aus einem Drittland, die auf dem Gebiet der EU verwendet werden soll, muss die Maschine bei der Bereitstellung auf dem EU-Markt konform zur Maschinenrichtlinie sein. Wer eine Maschine erstmals im Europäischen Wirtschaftsraum in Verkehr bringt, muss über die notwendige Dokumentation zur Feststellung der Konformität verfügen oder zu dieser Zugang haben. Dies gilt unabhängig davon, ob es sich um eine „Altmaschine“ oder um eine neue Maschine handelt.

3.2.3.6 Maschinen für die Eigenverwendung

Die Maschinenrichtlinie verpflichtet auch jene Anwender zu deren Einhaltung, die eine neue Maschine für den Eigengebrauch herstellen. Obwohl hinsichtlich des freien Verkehrs keinerlei Probleme entstehen – die Maschine wird ja nicht in den Handel gebracht – ist die Maschinenrichtlinie anzuwenden, damit sichergestellt ist, dass das Sicherheitsniveau der neuen Maschinen dem der auf dem Markt vorhandenen Maschinen entspricht.

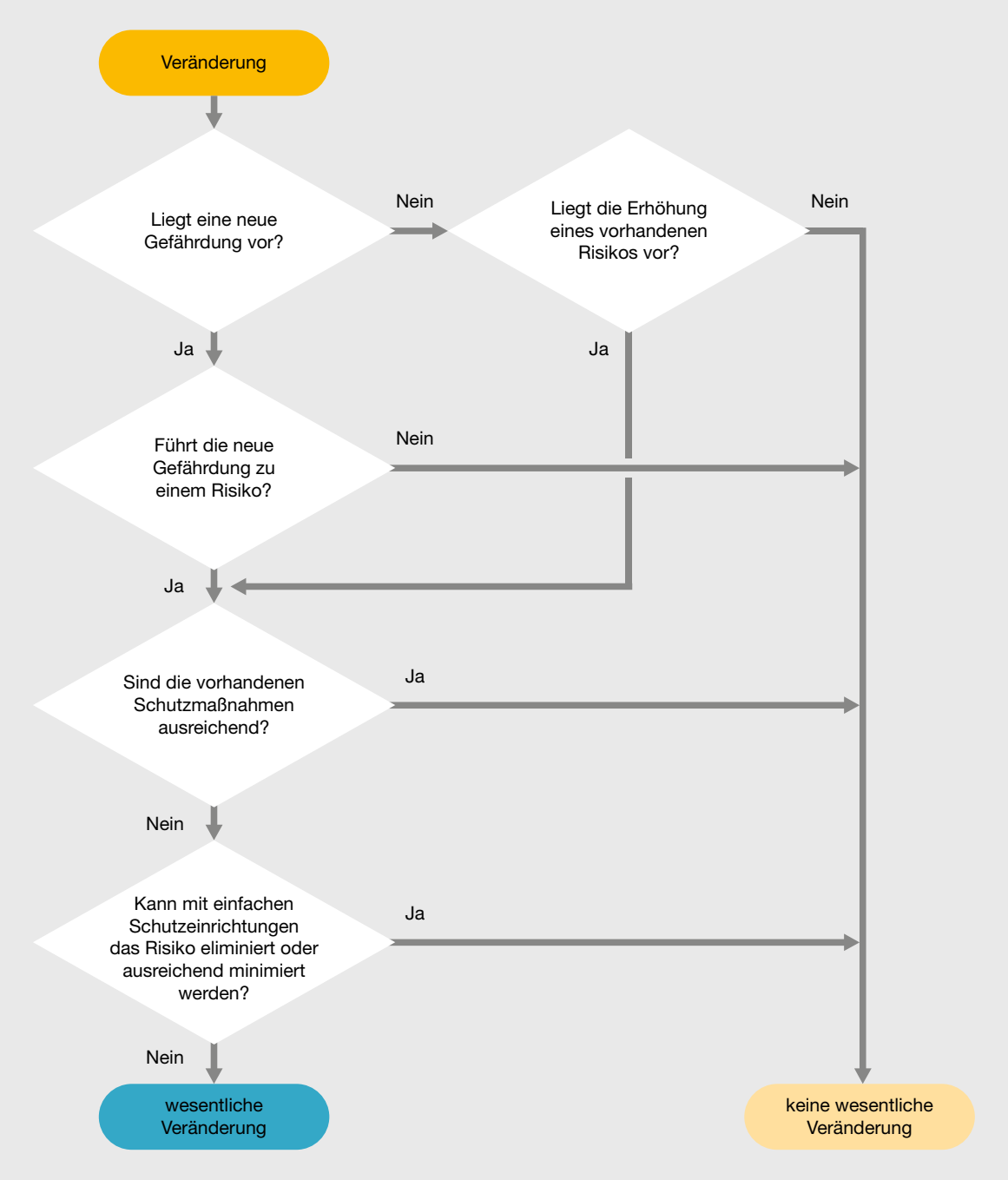


CE-Kennzeichnung für Einzelmaschinen und die Gesamtanlage

3.2 CE-Kennzeichnung

3.2.3.7 Umbau von Maschinen

Grundsätzlich beschreibt die Maschinenrichtlinie Anforderungen an neue Maschinen. Wird eine Maschine jedoch so verändert, dass neue Gefährdungen zu erwarten sind, muss im Rahmen einer Analyse festgestellt werden, ob es sich beim Umbau um eine sogenannte wesentliche Änderung handelt. In diesem Fall sind dieselben Maßnahmen wie für neue Maschinen einzuleiten.



Entscheidungsdiagramm „Wesentliche Veränderung von Maschinen“, Quelle: Bundesministerium für Arbeit und Soziales

3.2 CE-Kennzeichnung

3.2.3.8 Verkettung von Maschinen

Eine Anlage kann dann nicht mehr als Einzelmaschine betrachtet werden, wenn ein Ereignis an einer Maschine sicherheitstechnische Auswirkungen auf eine andere Maschine hat.

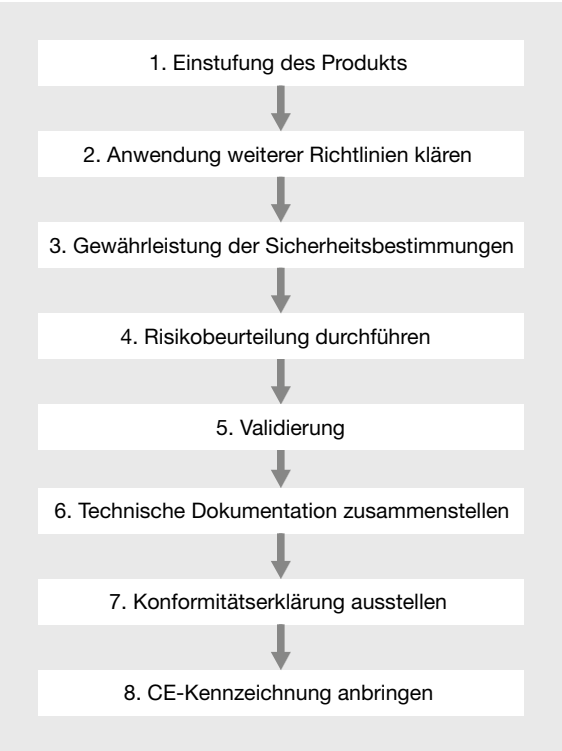
Grundsätzlich gilt, dass auch eine verkettete Anlage der aktuellen Gesetzeslage (insbesondere unter Berücksichtigung der Maschinenrichtlinie) entsprechen und der Prozess zur Konformitätsbewertung der Gesamtanlage erneut durchgeführt werden muss.

In der Regel muss für die neu hinzugefügte Maschine sowie die Schnittstelle zwischen alter und neuer Maschine zuerst eine Risikobeurteilung durchgeführt werden, um entsprechende Sicherheitsmaßnahmen ableiten zu können. Basierend darauf folgt die Entwicklung eines Sicherheitskonzepts, das Safety Design (Spezifikation der Sicherheitsanforderungen) und die Systemintegration. Am Ende des Prozesses steht die Validierung der Sicherheitsfunktionen, um nachzuweisen, dass die umgesetzten Sicherheitsmaßnahmen alle Anforderungen erfüllen. Am Ende muss also auch bei verketteten Maschinen die EG-Konformitätserklärung für die gesamte Anlage stehen.

Vor einer besonderen Herausforderung steht man, wenn Bestandsmaschinen mit Neumaschinen verkettet werden sollen, die unter Berücksichtigung unterschiedlicher Normenlagen gebaut wurden. Dies ist insbesondere der Fall, wenn eine Maschine nach der EN 954-1 mit einer weiteren Maschine, die nach 13849-1 gefertigt wurde, verbunden werden soll. Die EN 954-1 war bis 31.12.2011 gültig. Sie sah den Einbau von Sicherheitstechnik vor, nicht jedoch die Validierung der Komponenten. Die aktuell gültige EN ISO 13849-1 fordert die Validierung der Sicherheitsfunktionen. In diesem Fall liegen die Angaben zu den Sicherheitsfunktionen für beide Maschinen somit in unterschiedlicher Form vor, was die Validierung der neuen, verketteten Maschine deutlich erschwert. Pilz kann hier aufgrund umfangreicher Erfahrung unterstützen. Stets unter Berücksichtigung der aktuellen Normenlage kann Pilz als Bevollmächtigter das gesamte EG-Konformitätsbewertungsverfahren für einen Dritten durchführen.

3.2 CE-Kennzeichnung

3.2.3.9 In acht Schritten zum CE-Zeichen



Schritt 1: Einstufung des Produkts

Zu Beginn der CE-Kennzeichnung steht die Einstufung des Produkts. Dabei sind folgende Fragen zu beantworten:

- Unterliegt das Produkt der Maschinenrichtlinie?

Hierbei ist zu beachten, dass in der Maschinenrichtlinie 2006/42/EG (im Gegensatz zur Vorgängerversion) einige Produkte neu aufgenommen wurden (wie z. B. Druckbehälter, Dampfkessel und Seilbahnen), während andere weggefallen sind (wie z. B. elektrische Haushalts- und Bürogeräte).

- Ist das Produkt im Anhang IV der Maschinenrichtlinie gelistet?

Im Anhang IV der Maschinenrichtlinie finden sich „besonders gefährliche“ Maschinen wie Pressen, Holzbearbeitungsmaschinen, Hubarbeitsbühnen etc. In diesem Fall muss die CE-Kennzeichnung bzw. die Konformitätserklärung besondere Anforderungen erfüllen.

- Handelt es sich bei der Maschine um eine Teil- oder unvollständige Maschine?

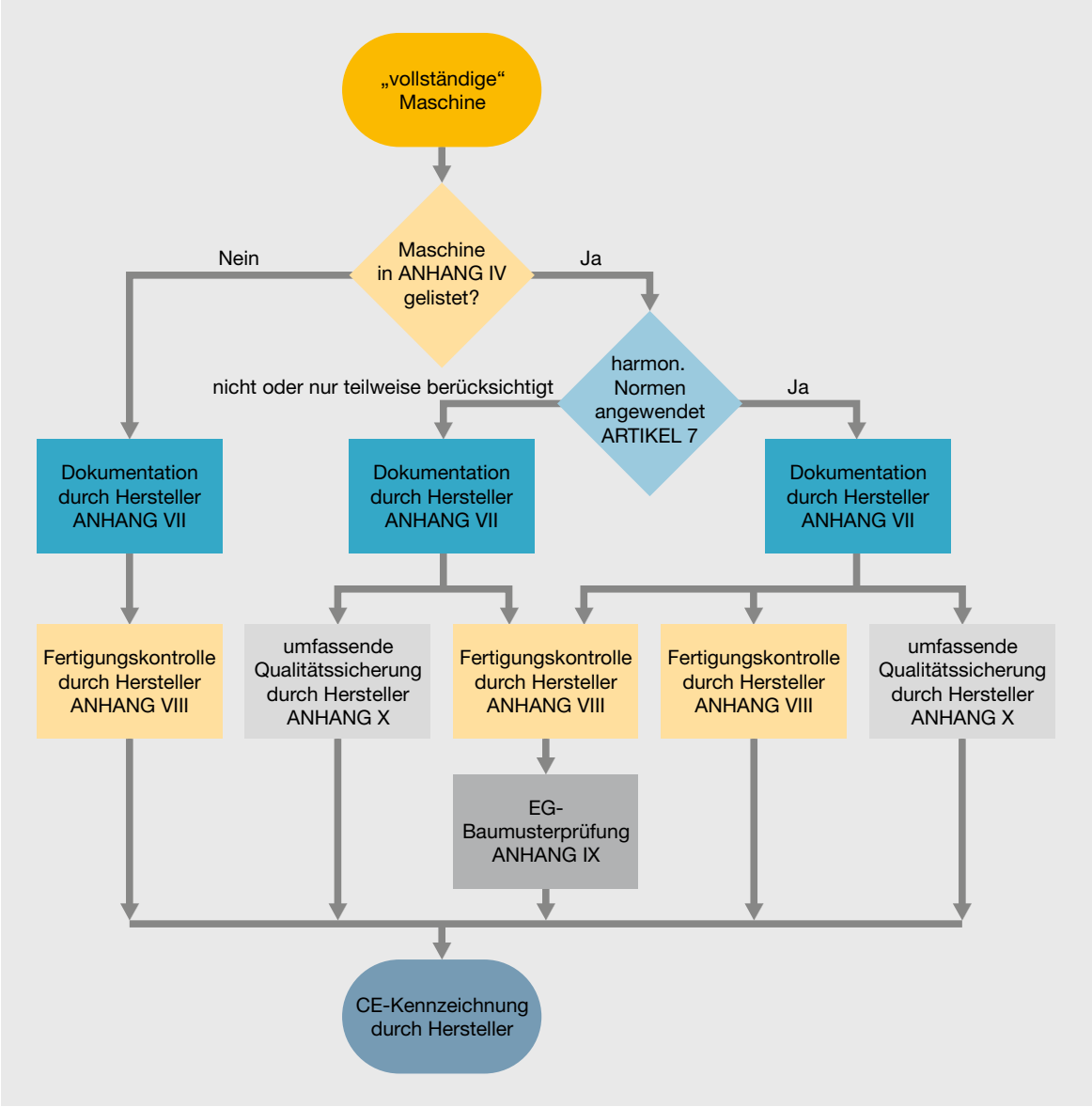
Für funktionsfähige Maschinen, die in vollem Umfang dem Anhang I der Maschinenrichtlinie entsprechen, stellt der Hersteller eine EG-Konformitätserklärung aus. Für Teilmaschinen, wie z. B. Roboter, die noch nicht in vollem Umfang den Anhang I erfüllen können, stellt der Hersteller eine Einbauerklärung gemäß Anhang II B aus.

Ab Gültigkeit der Maschinenrichtlinie 2006/42/EG muss allen unvollständigen Maschinen eine Einbauerklärung nach Anhang II beigefügt werden. Gleichzeitig müssen deren Hersteller eine Risikobeurteilung durchführen und eine Montageanleitung gemäß Anhang VI mitliefern. Praktisch handelt es sich bei der Hersteller- bzw. Einbauerklärung also um ein „Verbot der Inbetriebnahme“, da die Maschine unvollständig ist und somit nicht verwendet werden darf.

3.2 CE-Kennzeichnung

▸ Handelt es sich um ein Sicherheitsbauteil?

Sicherheitsbauteile werden nach der Maschinenrichtlinie 2006/42/EG wie Maschinen behandelt und erhalten daher ein CE-Zeichen.



Mögliche Bewertungsverfahren gemäß der neuen Maschinenrichtlinie

3.2 CE-Kennzeichnung

Schritt 2: Anwendung weiterer Richtlinien klären

Falls die Maschinen auch von EU-Richtlinien erfasst werden, die andere Aspekte behandeln und in denen die CE-Kennzeichnung vorgesehen ist, müssen vor der Kennzeichnung auch die Bestimmungen dieser Richtlinien eingehalten werden. Enthält die Maschine z. B. auch elektrische Ausrüstungen, fällt die Maschine häufig auch unter die Niederspannungsrichtlinie und ggf. unter die EMV-Richtlinie.

Schritt 3: Gewährleistung der Sicherheitsbestimmungen

Der Hersteller einer Maschine ist verpflichtet, die grundlegenden Sicherheits- und Gesundheitsanforderungen nach Anhang I der Maschinenrichtlinie einzuhalten. Diese relativ abstrakt formulierten Anforderungen werden durch EU-Normen konkretisiert.

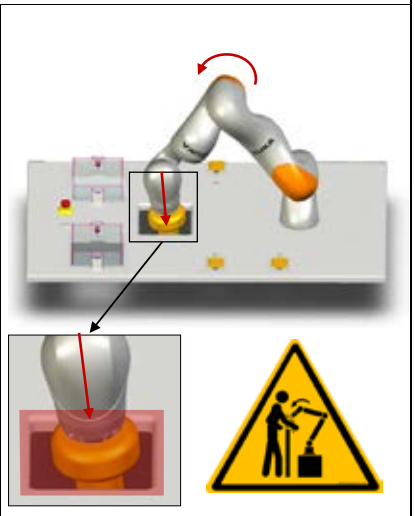
Die EU veröffentlicht hierzu Listen mit Richtlinien zu harmonisierten Normen. Die Anwendung dieser Normen ist freiwillig, jedoch führt deren Einhaltung zur Vermutung der Konformität mit der Rechtsvorschrift. Dies kann die Beweisführung beträchtlich reduzieren, der Aufwand zur Einarbeitung in die Risikobeurteilung fällt wesentlich geringer aus.

3.2 CE-Kennzeichnung

Schritt 4: Risikobeurteilung durchführen

PILZ
THE SPIRIT OF SAFETY

Pilz GmbH & Co. KG

Identifizierung der Gefährdung		**Gefahren-Nr.:**	**2.14**
Titel	Gefährdungen durch quasi-statischen Kontakt zwischen Roboter und Anlagenteilen		
Ort	Kamera-Öffnung in der Tischplatte		
Gefährdungs-auswirkung	Obere Extremitäten		
Lebensphase	Normalbetrieb, Einrichten, Wartung, Instandhaltung, und Reparatur		
Tätigkeit	Be-, Entladen der Applikation, Bergen von losgelassenen Teilen, Rüsten/Einstellen, Programmieren/ Testen, Beseitigen von Störungen im Arbeitsablauf, Beobachten von Fertigungsläufen, Fehlersuche und -beseitigung, Reinigung/Wartung		
Tätigkeits-Erklärung	Manuelle Tätigkeit in dem Arbeitsbereich des Roboters, bei bestimmungsgemäßem Betrieb.		
Art der Gefährdung	Mechanische Gefährdung		
Ursprung oder Folgen	Quetschen		
Beschreibung	Während des Betriebes und der damit verbundenen Bewegungen des Roboterarms besteht die Gefahr, dass Gliedmaßen zwischen Roboterarm und festen Anlagenteilen bei der Fahrt zur Kamera gequetscht werden können.		

Risikoeinschätzung und -bewertung			
Schwere der möglichen Verletzung:	11	Möglichkeit zur Vermeidung:	2.5
Möglichkeit des Auftretens eines Gefahr bringenden Ereignisses:	2.5	Häufigkeit der Exposition:	5
Pilz Hazard Rating (PHR):	**343**	**Risikohöhe:**	Hohes Risiko

Konzept zur Risikominderung	**Referenz**
Risikominderung 1: Konstruktive Schutzmaßnahmen: Anlagenteile müssen so gestaltet werden, dass sie gemäß EN 349 mit dem Roboter keine gefährlichen Quetsch- und Scherstellen bilden. Wenn dies konstruktiv nicht möglich ist, müssen die möglichen Kollisionsflächen möglichst groß sein. **Risikominderung 2: Technische Schutzmaßnahmen:** Quetsch- und Scherstellen sind durch Begrenzung der Freiheitsgrade des Robotersystems so weit als möglich zu vermeiden. Verbleibende Quetschstellen sind durch Begrenzung der Roboter-Dynamik und -Leistung abzusichern. Es müssen die biomechanischen Grenzwerte der TS 15066 eingehalten werden.	EN 349 EN ISO 10218-2 TS 15066

Risikobeurteilung – Roboter-Fertigungsapplikation/Messe CORB 1

Auszug aus einer Risikobeurteilung der Pilz GmbH & Co. KG

3.2 CE-Kennzeichnung

Der Hersteller ist verpflichtet, eine Risikobeurteilung vorzunehmen, um alle mit seiner Maschine verbundenen Gefahren zu ermitteln. Das Ergebnis dieser Beurteilung muss dann sowohl im Entwurf als auch im Bau der Maschine berücksichtigt werden. Inhalt und Umfang von Risikobeurteilungen werden prinzipiell in keiner Richtlinie vorgegeben, jedoch beschreibt die EN ISO 12100 die generelle Vorgehensweise.

Ausgehend von der bestimmungsgemäßen Verwendung gilt es, sämtliche relevanten Gefährdungen zu ermitteln – unter Berücksichtigung aller Lebensphasen nach dem erstmaligen Bereitstellen auf dem Markt. Dabei werden alle unterschiedlichen Personengruppen, wie z. B. Bedienungs-, Reinigungs- oder Wartungspersonal, die mit der Maschine in Berührung kommen, beachtet.

Für jede Gefährdung wird das Risiko abgeschätzt und bewertet. Maßnahmen, die das Risiko reduzieren, werden nach dem Stand der Technik und unter Beachtung der Normen festgesetzt. Gleichzeitig wird das Restrisiko abgeschätzt: Ist das von einer Gefahrenstelle ausgehende Restrisiko auf kein vertretbares Maß gemindert, sind weitere Maßnahmen erforderlich. Dieser iterative Prozess wird fortgeführt, bis die notwendige Sicherheit erreicht ist.

Schritt 5: Validierung

Die Validierung ist einer der maßgeblichsten Schritte im Zuge des Verfahrens zur Konformitätsbewertung. Sie ist essenziell für den Beweis, dass eine Maschine den Sicherheitsbestimmungen entspricht. Alle Informationen zur Validierung finden Sie in Kapitel 3.6.

Schritt 6: Technische Dokumentation zusammenstellen

Die technische Dokumentation nach der Maschinenrichtlinie umfasst im Einzelnen:

- einen Gesamtplan der Maschine sowie die Steuerkreispläne
- detaillierte und vollständige Pläne (eventuell mit Berechnungen, Versuchsergebnissen usw. für die Überprüfung der Übereinstimmung der Maschine mit den grundlegenden Sicherheits- und Gesundheitsanforderungen)
- eine Liste der grundlegenden Anforderungen dieser Richtlinie, der Normen und der anderen technischen Spezifikationen, die bei der Konstruktion der Maschine berücksichtigt wurden, sowie eine Beschreibung der Lösungen, die zur Verhütung der von der Maschine ausgehenden Gefahren gewählt wurden (in der Regel durch die Risikobeurteilung abgedeckt)
- technische Berichte oder ausgestellte Zertifikate, Berichte oder Prüfungsergebnisse zur Konformität
- die Betriebsanleitung der Maschine
- eine allgemeine Beschreibung der Maschine
- Konformitätserklärung oder Einbauerklärung und Montageanleitung
- Konformitätserklärungen der in die Maschine eingebauten Maschinen oder Geräte

Die Dokumentation muss nicht ständig und tatsächlich vorhanden sein. Sie muss jedoch innerhalb eines Zeitraums, welcher der Wichtigkeit der Unterlage angemessen ist, zusammengestellt und zur Verfügung gestellt werden können. Sie muss mindestens zehn Jahre ab Herstellung der Maschine aufbewahrt und für die zuständigen nationalen Behörden bereitgehalten werden. Falls es sich um eine Serienmaschine handelt, so beginnt die Frist mit der Herstellung des letzten Exemplars der Maschine.

3.2 CE-Kennzeichnung

Schritt 7: EG-Konformitätserklärung ausstellen

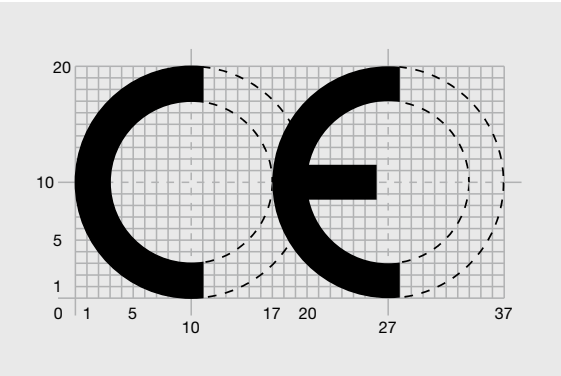
Mit der Ausstellung der EG-Konformitätserklärung erklärt der Hersteller, dass er alle für das Produkt zutreffenden Richtlinien berücksichtigt hat. Derjenige, der eine EG-Konformitätserklärung unterschreibt, muss zur Vertretung seines Unternehmens befugt sein. Dies bedeutet, dass der Unterzeichner ein Rechtsgeschäft wie die Unterzeichnung der EG-Konformitätserklärung aufgrund seiner Funktion rechtswirksam tätigen darf.

Bringt ein beauftragter Angestellter des Unternehmens auf einer EG-Konformitätserklärung rechtsgültig seine Unterschrift an, löst er damit die Haftung der verantwortlichen natürlichen Person und gegebenenfalls des Unternehmens als juristische Person aus.

Die Erklärung kann auch durch einen Bevollmächtigten unterschrieben werden.

Die Maschinenrichtlinie fordert in der Erklärung die Nennung einer Person, die bevollmächtigt ist, die technischen Unterlagen zusammenzustellen. Diese Person muss in der EU ansässig sein.

Schritt 8: CE-Kennzeichnung anbringen



Merkmale des CE-Zeichens

Nach Ausstellung der EG-Konformitätserklärung darf das CE-Zeichen angebracht werden.

Wichtig ist dabei, dass die CE-Kennzeichnung für die vollständige Maschine von anderen CE-Zeichen z. B. auf Bauteilen deutlich unterschieden werden kann. Um Verwechslungen mit anderen Zeichen zu vermeiden, ist es ratsam, die CE-Kennzeichnung für die vollständige Maschine auf dem Maschinenschild anzubringen, auf dem auch der Name und die Anschrift des Herstellers enthalten sein müssen.

3.3 Richtlinien

Von den inzwischen fast 30 aktiven Richtlinien ist für den typischen Maschinenbauer lediglich eine kleine Auswahl relevant. Einige Richtlinien haben außer der Richtliniennummer (z. B. 2006/42/EC) teilweise nur einen sehr langen oder bürokratischen Titel. Varianten bestehen dabei im letzten Teil der Richtliniennummer. Je nach Sprachraum und Ausgabedatum steht hier ein EC, EU, EG, EWG oder andere Kürzel. Dies macht die Benennung der Richtlinie in der Regel sehr schwer. Häufig werden diese langen Titel individuell abgekürzt, auch und obwohl dies immer wieder zu Missverständnissen führen kann. Hier die wichtigsten Richtlinien mit deren offiziellem Titel sowie ihrem gebräuchlichen, aber nicht offiziellen Kurztitel:

Richtlinie	Kurztitel (nicht offiziell)	Offizieller Titel
2006/42/EG	Maschinenrichtlinie	Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)
2001/95/EG	Produktsicherheitsrichtlinie	Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit
2014/30/EU	EMV-Richtlinie	Richtlinie 2014/30/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit (Neufassung)
2014/53/EU	Funkanlagenrichtlinie	Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG
2003/10/EG	Lärmrichtlinie	Richtlinie 2003/10/EG des Europäischen Parlaments und des Rates vom 6. Februar 2003 über Mindestvorschriften zum Schutz von Sicherheit und Gesundheit der Arbeitnehmer vor der Gefährdung durch physikalische Einwirkungen (Lärm)
2014/35/EU	Niederspannungsrichtlinie	Richtlinie 2014/35/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen auf dem Markt
Verordnung (EU) 2016/425	PSA-Richtlinie	Verordnung (EU) 2016/425 des Europäischen Parlaments und des Rates vom 9. März 2016 über persönliche Schutzausrüstungen und zur Aufhebung der Richtlinie 89/686/EWG des Rates (89/686/EWG mit Übergangsfrist bis 20. April 2019 anwendbar)

Ziel der Richtlinien ist, den freien Warenverkehr innerhalb der EU zu gewährleisten. Die Richtlinien selbst sind im Volltext im Internet erhältlich. Außer der Maschinenrichtlinie soll im Folgenden keine der Richtlinien näher betrachtet werden. Dennoch wird in der Liste der relevanten Normen natürlich auch auf Normen, die andere Richtlinien betreffen, verwiesen.

3.3 Richtlinien

3.3.1 Maschinenrichtlinie

Im Rahmen der funktionalen Sicherheit von Maschinen kommt der 2006/42/EG eine besondere Bedeutung zu. Die Richtlinie, allgemein als Maschinenrichtlinie bezeichnet, beschäftigt sich mit der Standardisierung der europäischen Sicherheitsanforderungen an Maschinen.

3.3.1.1 Inhalt

Die Maschinenrichtlinie behandelt die wesentlichen Aspekte der Sicherheit von Maschinen. Die Inhalte der Maschinenrichtlinie sind:

- Anwendungsbereich, Inverkehrbringen, freier Warenverkehr
- Bescheinigungsverfahren
- CE-Kennzeichnung
- grundlegende Sicherheits- und Gesundheitsanforderungen
- Typen von Maschinen und die anwendbaren Bescheinigungsverfahren
- EG-Konformitätserklärung und Baumusterprüfung
- Anforderungen an Prüfstellen

3.3.1.2 Gültigkeit

Die Maschinenrichtlinie 2006/42/EG hat die Vorgängerversion 98/37/EG mit Wirkung vom 29.12.2009 abgelöst. Eine Übergangsfrist gab es nicht.

3.3.1.3 Normen mit Bezug zur Maschinenrichtlinie

An dieser Stelle alle Normen zu nennen, die unter der Maschinenrichtlinie gelistet sind und somit als harmonisiert gelten, ist nicht sinnvoll. Mit Stand Winter 2016 waren über 750 Normen direkt gelistet. Würden noch all die Normen hinzugezählt werden, die indirekt über die direkt gelisteten Normen hinaus relevant sind, würde das den Rahmen dieses Kompendiums sprengen. Die folgenden Kapitel konzentrieren sich daher auf diejenigen Normen zur Maschinenrichtlinie, die von allgemeiner Bedeutung sind.

3.4 Normen

3.4.1 Herausgeber und Geltungsbereich

Auf europäischer Ebene wurde mit der Harmonisierung der Gesetzgebung auch eine Harmonisierung der Normung angestoßen. Traditionell hat fast jedes Land ein oder mehrere eigene Normungsinstitute. Zusätzlich existieren einige internationale Kooperationen. Hierbei wird dieselbe Norm auf unterschiedlichen Ebenen unter unterschiedlichen Namen herausgegeben. In aller Regel, wenn auch nicht immer, wird dabei der übergeordnete Normenname als Teil des nationalen Normennamens erkennbar fortgeführt. Dazu jedoch im Folgenden mehr.

3.4.1.1 Internationale Normen

Auf internationaler Ebene sind die wohl wichtigsten Herausgeber von Normen für den Maschinenbau die International Electrotechnical Commission (IEC) und die International Organization for Standardization (ISO), die beide ihren Sitz in Genf haben. Während sich die IEC hauptsächlich um Themen der Elektrik und Elektronik kümmert, beschäftigt sich die ISO vornehmlich mit Themen der Mechanik. Derzeit sind weit über 100 Länder in den beiden Organisationen vereint, was den von IEC und ISO erarbeiteten Normen ein erhebliches Gewicht verleiht.

Auf europäischer Ebene kommen die EN-Normen zur Anwendung. Die EN-Normenentwicklungen geschehen normalerweise auf Initiative der EU durch CEN und CENELEC. Wie auch bei IEC und ISO teilen sich CEN und CENELEC die Normen auf. CENELEC ist hierbei für die elektrischen Themen zuständig.

Viele der Normen werden heute quasi im Paket als IEC- oder ISO-Norm in Kooperation mit der EU durch CEN und CENELEC entwickelt. Als Ergebnis dieser Bemühungen entstehen EN-IEC- oder EN-ISO-Normen.

3.4.1.2 Nationale Normen

Die Vielfalt der nationalen Normen und Normeninstitute im gesamten europäischen Raum ist fast unüberschaubar. Zumindest in der EU wird die Mehrzahl der Normen direkt als EN-Norm angestrebt und nur noch auf die nationale Ebene gespiegelt, d. h. die EN-Norm zur nationalen Norm erklärt oder die nationale Norm als EN-Norm eingebracht.

In Deutschland ist beispielsweise das Deutsche Institut für Normung (DIN) für die Herausgabe der nationalen Normen verantwortlich. Die gängige Praxis ist heute, dass Normen vom DIN direkt in Zusammenarbeit mit CEN oder CENELEC als DIN EN ISO oder DIN EN entwickelt werden. Diese Normen unterscheiden sich in aller Regel nur im nationalen Vorwort von der EN-, ISO- oder IEC-Norm.

Dieselbe Norm kommt also auf EU-Ebene als EN-ISO- oder EN-IEC-Norm zum Tragen, während die identische deutsche Norm DIN EN ISO oder DIN EN heißt. In den übrigen europäischen Ländern unterscheidet sich das Vorgehen meist nur darin, dass ein anderes Institut die Norm herausgibt. Für Österreich ist dies das Österreichische Normungsinstitut (ÖNorm), für Großbritannien ist es das British Standards Institute (BSI).

Wird eine ISO-Norm zur EN-Norm, so trägt diese den Titel EN ISO. Wird diese nun noch zur DIN-Norm, so ist der volle Titel DIN EN ISO. Je lokaler das Institut, desto weiter vorne im Namen wird es genannt. Ein kleines Kuriosum am Rande: Wird eine IEC-Norm zur EN-Norm, so entfällt die Nennung der IEC. Die IEC 61508 wird also zur Europäischen EN ~~IEC~~ 61508 oder zur deutschen DIN EN ~~IEC~~ 61508.

Während in vielen Ländern wie beispielsweise China oder der Schweiz das europäische Verfahren eines zentralen Normungsinstituts ebenfalls verfolgt wird, kann man in manchen Ländern Überraschungen erleben. In den USA werden Normen unter anderem von ANSI, OSHA, RSA und UL herausgegeben.

3.4 Normen

3.4.2 EN-Sicherheitsnormen im Maschinenbau

Auf eine vollständige Liste der Sicherheitsnormen für den europäischen Maschinenbau wird hier verzichtet. Allein unter der Maschinenrichtlinie sind über 760 Normen als harmonisiert gelistet. Im Folgenden wird auf eine Auswahl der allgemeinen Sicherheitsnormen eingegangen. Je nach Bedeutung der einzelnen Normen werden diese in unterschiedlicher Detaillierung erläutert.

Norm	Harmonisiert	Titel
EN 349:2008	Ja	Sicherheit von Maschinen Mindestabstände – zur Vermeidung des Quetschens von Körperteilen
EN 547-1 bis -3:2008	Ja	Sicherheit von Maschinen Körpermaße des Menschen
EN 574:2008	Ja	Sicherheit von Maschinen Zweihandschaltungen – Funktionale Aspekte Gestaltungsleitsätze
DIN EN ISO 14120:2016 ersetzt EN 953:2009	Ja	Sicherheit von Maschinen Trennende Schutzeinrichtungen – Allgemeine Anforderungen an Gestaltung und Bau von feststehenden und beweglichen trennenden Schutzeinrichtungen
EN 1005-1 bis -4:2008 EN 1005-5:2007	Ja Nein	Sicherheit von Maschinen Menschliche körperliche Leistung
EN 1037:2008 identisch mit ISO 14118:2000	Ja	Sicherheit von Maschinen Vermeidung von unerwartetem Anlauf
EN ISO 14119 (Ersatz für EN 1088:2008 und ISO 14119:2006)	Ja	Sicherheit von Maschinen Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
DIN EN ISO 11161:2010	Ja	Sicherheit von Maschinen Integrierte Fertigungssysteme – Grundlegende Anforderungen
EN ISO 12100:2010 Ersatz für EN ISO 12100-1 und 2; EN ISO 14121; EN 292	Ja	Sicherheit von Maschinen Allgemeine Gestaltungsleitsätze, Risikobewertung und Risikominderung
EN 12453:2000	Nein	Tore Nutzungssicherheit kraftbetätigter Tore – Anforderungen
EN ISO 13849-1:2015 ersetzt EN ISO 13849-1:2009	Ja	Sicherheit von Maschinen Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
EN ISO 13849-2:2012	Ja	Sicherheit von Maschinen Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung
EN ISO 13855:2010	Ja	Sicherheit von Maschinen Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen
EN ISO 13857:2008	Ja	Sicherheit von Maschinen Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen

3.4 Normen

Norm	Harmonisiert	Titel
ISO/TR 23849:2010 identisch mit IEC/TR 62061-1:2009	Nein	Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
EN 60204-1:2010	Ja	Sicherheit von Maschinen Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen
EN 60947-5-1:2009 EN 60947-5-2:2012 EN 60947-5-3:2005 EN 60947-5-4:2003 EN 60947-5-5:2013 EN 60947-5-6:2001 EN 60947-5-7:2003 EN 60947-5-8:2006 EN 60947-5-9:2007	Ja	Niederspannungsschaltgeräte Teil 5: Steuergeräte und Schaltelemente
EN 61326-3 Teile 1+2:2008	Nein	Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen
EN 61496-1:2010	Ja	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen
IEC 61496-2:2013 CLC/TS 61496-2:2006	Nein	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven optoelektronischen Prinzip arbeiten
CLC/TS 61496-3:2008 ersetzt EN 61496-3:2003	Nein	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 3: Besondere Anforderungen an aktive optoelektronische, diffuse Reflektion nutzende Schutzeinrichtungen (AOPDDR)
EN 61508 Teile 1-7:2010	Nein	Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme
EN 61511 Teile 1-3:2004	Nein	Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie
EN 61784-3:2010	Nein	Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen
EN 61800-5-2:2007	Ja	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit
IEC/TS 62046:2008	Nein	Sicherheit von Maschinen Anwendung von Schutzausrüstungen zur Anwesenheitserkennung von Personen
EN 62061:2016	Ja	Sicherheit von Maschinen Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme
IEC/TR 62685:2010	Nein	Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safe communication profiles (FSCPs)
NFPA 79:2013	Nein	Industrielle Maschinen

3.4 Normen

3.4.3 Grundnormen und Designvorgaben

3.4.3.1 EN ISO 12100 und EN ISO 14121

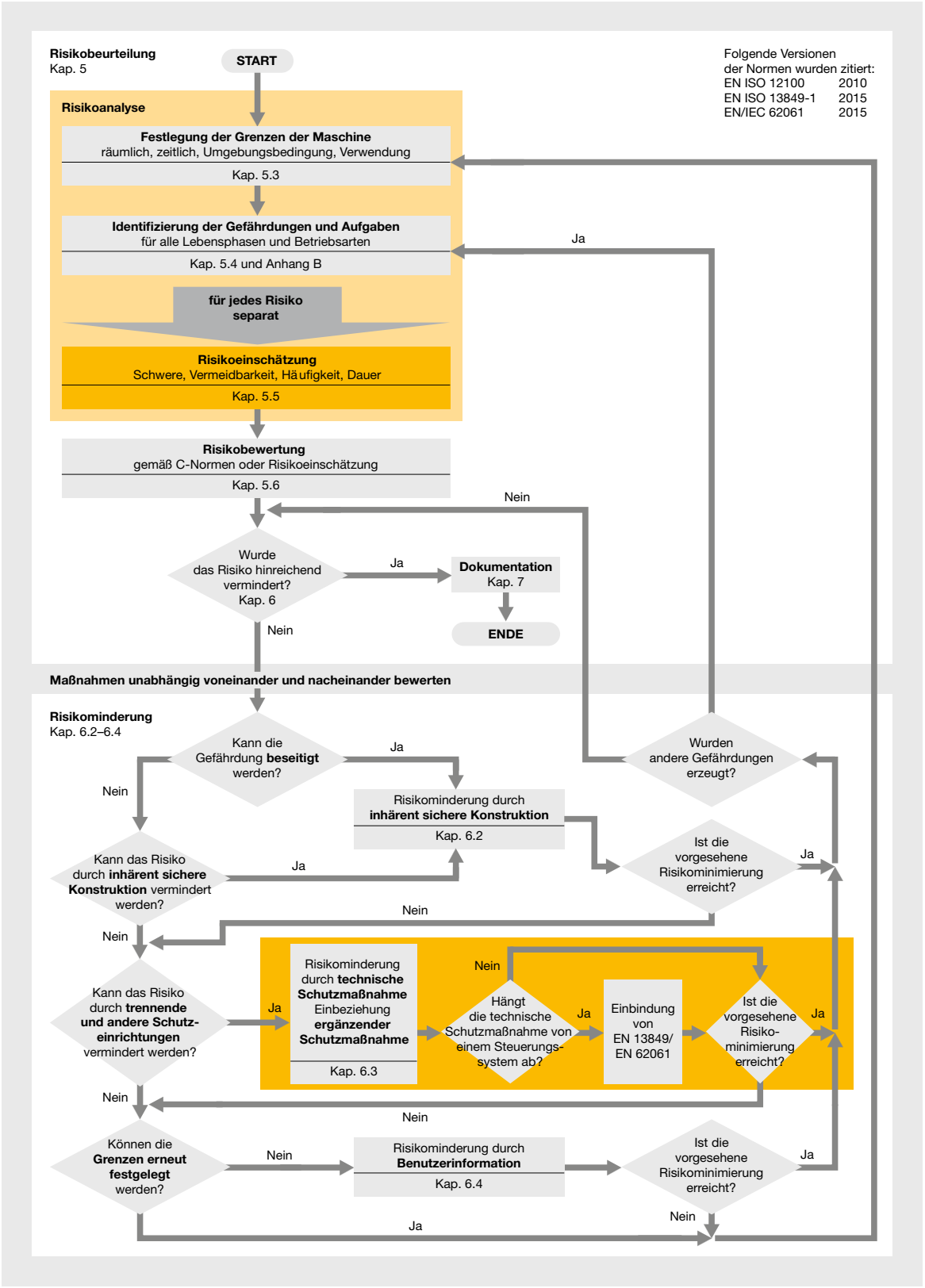
Norm	Harmonisiert	Titel
EN ISO 12100:2010 ersetzt EN ISO 12100-1 und -2; EN ISO 14121-1	Ja	Sicherheit von Maschinen Allgemeine Gestaltungsleitsätze, Risikobewertung und Risikominderung

Mit EN ISO 12100 wurde 2010 eine weitergehende Zusammenfassung von EN 12100-1 und -2 und EN 14121-1 bereitgestellt. Diese Norm ist inhaltlich identisch mit den genannten Normen und fasst diese lediglich in einem Dokument zusammen.

Das beigefügte Diagramm (siehe Seite 3-22) zeigt die einzelnen in dieser Norm betrachteten Elemente auf. Die Norm bietet eine gute Sammlung zu beachtender Gefährdungen, Risikofaktoren und Designgrundsätze.

Die dunkel-gelb hinterlegten Elemente des Diagramms sind die von den Anwendernormen EN ISO 13849-1 und EN/IEC 62061 erfassten Bereiche und werden dort näher betrachtet. Sofern möglich, wurde im Diagramm bereits auf die entsprechenden Kapitel der Normen verwiesen, die den jeweiligen Aspekt behandeln. Dabei sind einige Punkte durchaus in mehreren Normen zu finden. Meist ist aber die Detaillierungstiefe unterschiedlich.

3.4 Normen



Risikoeinschätzung und Risikominderung nach EN ISO 12100

3.4 Normen

3.4.3.2 IEC/TR 62685 Prüfanforderungen und EMV

Norm	Harmonisiert	Titel
IEC/TR 62685:2010	Nein	Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safe communication profiles (FSCPs)

Die IEC/TR 62685 ist aus den Prüfanforderungen des deutschen BGIA-Dokuments GS-ET-26 entstanden und behandelt Anforderungen an Sicherheitskomponenten innerhalb einer Sicherheitsfunktion. Sie deckt neben mechanischen und klimatischen Tests auch die Themen Beschriftung und EMV ab. Damit werden einige Lücken der EN ISO 13849-1 und EN 61784-3 geschlossen. Insgesamt ist das Dokument eher für den Hersteller von Sicherheitskomponenten relevant als für den Maschinen- und Anlagenbauer. Da aber eine gute Gegenüberstellung der EMV-Anforderungen Teil des Dokuments ist, mag es auch für Maschinenbauer von Interesse sein.

3.4.3.3 EN 61784-3 Sichere Feldbusse

Norm	Harmonisiert	Titel
EN 61784-3:2010	Nein	Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen

Die Normenreihe der EN 61784-3 umfasst eine ganze Reihe von Sicherheitserweiterungen zu unterschiedlichen Feldbusprofilen, basierend auf den Vorgaben der EN 61508. Diese Erweiterungen werden als sogenannte Sicherheitsprofile behandelt und beschreiben die Mechanismen und technischen Details dieser Profile. Für den normalen Maschinenbauer ist davon maximal der Basisteil EN 61784-3 von Interesse, in dem allgemeine Sicherheitsprinzipien beschrieben werden. Gedacht sind die Profildokumente EN 61784-3-x vor allem für Geräte-hersteller, die selbst Sicherheitsgeräte gemäß einem der publizierten Profile bauen möchten. Dann ist allerdings die Zusammenarbeit mit den entsprechenden Nutzerorganisationen, die hinter diesen Profilen stehen, sowie die Kenntnis der Basisprofile sinnvoll, die in den Reihen EN 61784-1 und -2 sowie EN 61158 beschrieben sind. Ein komplettes Profil, bestehend aus den entsprechenden Teilen von EN 61784 und EN 61158, umfasst zwischen 500 und 2 000 Seiten. Alle Profile zusammen kommen auf etwa 10 000 Seiten.

3.4 Normen

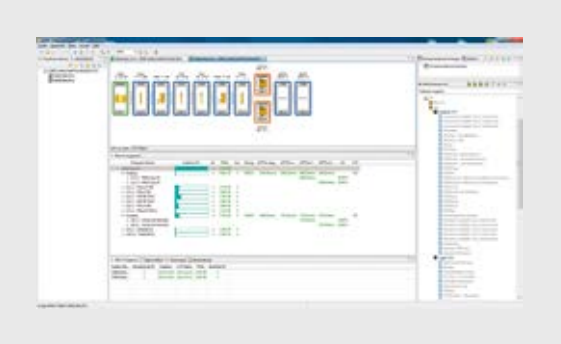
3.4.3.4 EN ISO 13849-1

Norm	Harmonisiert	Titel
EN ISO 13849-1:2015	Ja	Sicherheit von Maschinen Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
EN ISO 13849-2:2012	Ja	Sicherheit von Maschinen Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung

Inhalt

Die EN ISO 13849-1 befasst sich mit der Zuordnung geeigneter Zuverlässigkeitsklassen von Risiken anhand eines Risikographen sowie mit der Bewertung von Sicherheitsfunktionen mittels struktureller und statistischer Methoden. Ziel hierbei ist, die Eignung von Sicherheitsmaßnahmen zur Minderung von Risiken festzustellen. Die EN ISO 13849-2 beschreibt hierbei den zur EN ISO 13849-1 gehörigen Aspekt der Validierung. Beide Normen zusammen sind damit praktisch gleichwertig (aber nicht identisch) zu der EN 62061.

Der Aufwand, die im Rahmen dieser Norm erforderlichen Berechnungen durchzuführen, kann erheblich verringert werden, wenn eine geeignete Software verwendet wird. Hier bieten sich Berechnungstools wie der Safety Calculator PAScal als frei verfügbare Software an: https://www.pilz.com/de-INT/eshop/00105002187038/PAScal-Safety-Calculator, Webcode: web150431



Safety Calculator PAScal

Geltungsbereich

Bei der EN ISO 13849-1 handelt es sich um eine Grundnorm für die funktionale Sicherheit. Sie ist auf ISO-Ebene verabschiedet und innerhalb der EU als Norm innerhalb der Maschinenrichtlinie harmonisiert. Damit gilt für sie im Rahmen der EU die Vermutungswirkung. Als Anwendungsbereich ist die elektrische, elektronische, programmierbare elektronische, mechanische, pneumatische und hydraulische Sicherheit von Maschinen genannt.

Risikobewertung/Risikoanalyse

Die Bewertung von Risiken geschieht in der EN ISO 13849-1 anhand eines Graphen. Dabei werden unter anderem die Schwere von möglichen Verletzungen, die Häufigkeit der Risiko-Exposition und die Vermeidbarkeit von Risiken bewertet. Als Ergebnis der Bewertung erhält man den erforderlichen Performance Level (PL_r) für die einzelnen Sicherheitsfunktionen, die die Risiken minimieren sollen.

Die mithilfe des Graphen bestimmten Levels werden in späteren Schritten der Risikobewertung mit den gewählten Maßnahmen der Risiko-Reduktion abgeglichen. Es müssen dann für jedes klassifizierte Risiko eine oder mehrere Maßnahmen angewendet werden, die das Eintreten des Risikos vermeiden oder hinreichend reduzieren. Dabei muss die Qualität der Maßnahme, ausgedrückt als Performance Level, dem für das jeweilige Risiko bestimmten Level mindestens entsprechen.

3.4 Normen

Bestimmung des erforderlichen Performance Levels PL_r

Beim Performance Level (PL) reicht zur Bewertung die Betrachtung von drei Aspekten:

Schwere der Verletzung	**S**
leichte Verletzung (normalerweise reversibel)	S_1
schwere Verletzung, einschließlich Tod (normalerweise irreversibel)	S_2

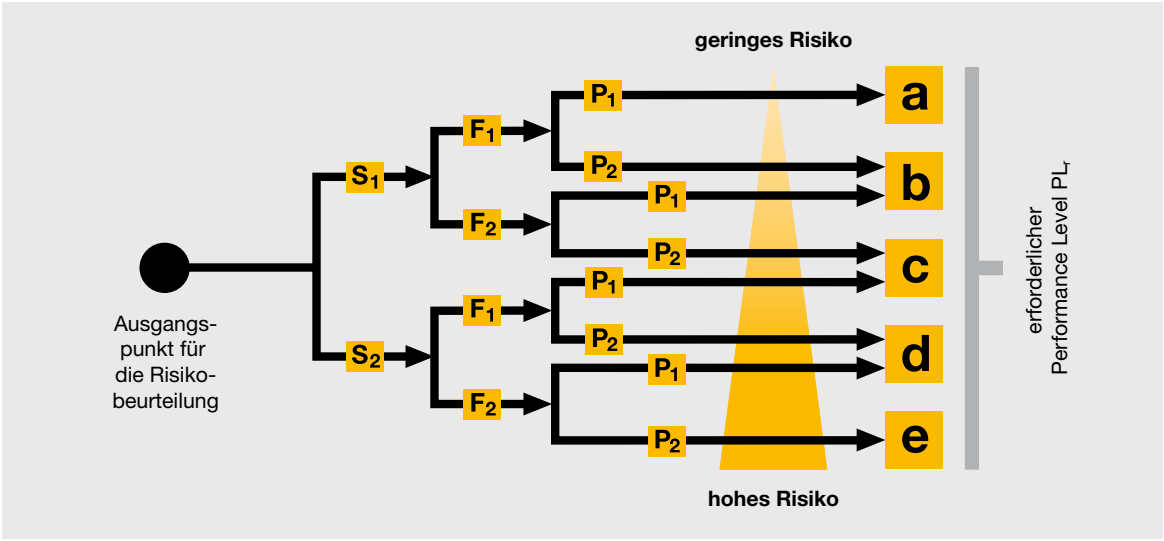
Häufigkeit und/oder Dauer der Gefährdungsexposition	**F**
selten bis öfter und/oder kurze Dauer	F_1
häufig bis dauernd und/oder lange Dauer	F_2

Möglichkeiten zur Vermeidung der Gefährdung	**P**
möglich unter bestimmten Bedingungen	P_1
kaum möglich	P_2

Mittels des folgenden Graphen und den Klassifizierungen der einzelnen Aspekte erhält man den erforderlichen Performance Level PL_r.

Hierzu beginnt die Bewertung des Risikos am Ausgangspunkt des Graphen und folgt den entsprechenden Pfaden, je nach Einordnung des Risikos. Nach Bewertung aller Aspekte ist der erforderliche Performance Level PL_r a, b, c, d oder e bestimmt.

Neu hinzugekommen ist in der letzten Ausgabe der Norm die Möglichkeit, die Wahrscheinlichkeit des Auftretens einer Gefährdung zu bewerten. Kommt man zu dem Schluss, dass diese Wahrscheinlichkeit niedrig ist, kann der bis dahin bestimmte PL_r um eine Stufe reduziert werden. Die Schwierigkeit liegt dabei im Detail: So soll man sich zur Bewertung dieser Frage an vergleichbaren Maschinen orientieren. Diese vergleichbaren Maschinen sind aber mit adäquaten Sicherheitsmaßnahmen ausgerüstet, sonst dürften sie ja nicht am Markt sein. Es ist also eine niedrige Unfallzahl an vergleichbaren Maschinen keine Begründung, die damit verbundenen Gefährdungen als niedrig einzustufen. Vielmehr wäre das der Beweis, dass die realisierten Sicherheitsmaßnahmen angemessen waren (und besser nicht verringert werden sollten).



Risikograph nach EN ISO 13849-1

3.4 Normen

Bewertung der Realisierung/Systembetrachtung

In der EN ISO 13849-1 wird davon ausgegangen, dass es sichere Geräte nicht gibt. Geräte werden erst durch geeignetes Design für die Anwendung in Applikationen mit erhöhten Ansprüchen ertüchtigt. Dabei erhält jedes Gerät im Rahmen einer Bewertung einen PL (Performance Level), der dessen Eignung beschreibt. Einfache Komponenten können dabei auch über deren $MTTF_d$ (Mean time to dangerous failure – mittlere Zeit bis zu einem gefahrbringenden Ausfall) oder den $B10_d$-Wert (mittlere Schalthäufigkeit, bis 10 % der Komponenten gefahrbringend ausfallen) beschrieben werden.

In den folgenden Betrachtungen wird untersucht, wie Ausfälle von Geräten oder deren Komponenten sich auf die Sicherheit des Systems auswirken, wie wahrscheinlich diese Ausfälle sind und wie man zum PL kommt.

Ermittlung der Ausfälle aufgrund gemeinsamer Ursache – CCF-Faktor

Die Bewertung der Maßnahmen gegen Fehler gemeinsamer Ursache setzt sich aus mehreren Einzelfaktoren zusammen. Strukturell kommen Aspekte wie Trennung der Kanäle, aber auch organisatorische Aspekte wie die Ausbildung der Konstrukteure zum Tragen. Dies geschieht nach einem Bewertungsschlüssel, bei dem 0 bis 100 % erreichbar sind.

Anforderung	Bewertung
physikalische Trennung zwischen den Sicherheitskreisen und zu anderen Kreisen	15 %
Diversität (Verwendung verschiedener Technologien)	20 %
Entwurf/Applikation/Erfahrung	20 %
Beurteilung/Analyse	5 %
Kompetenz/Ausbildung	5 %
Umwelteinflüsse (EMV, Temperatur …)	35 %

Bei der EN ISO 13849-1 gilt der CCF-Einfluss als akzeptabel, wenn eine Summe von ≥ 65 % bei der Bewertung erreicht wird.

PL-Bewertung

Die IEC ISO 13849-1 verwendet für die Bestimmung des PL den Diagnosedeckungsgrad (DC), die Systemkategorie sowie die $MTTF_d$ des Systems. Der DC ist abhängig von λ_{DD} (Fehlerrate der erkannten gefährlichen Ausfälle) und λ_{Dtotal} (Fehlerrate aller gefährlichen Ausfälle).
Im einfachsten Fall ist diese gegeben als:

$$DC = \Sigma\lambda_{DD}/\Sigma\lambda_{Dtotal}$$

Bei komplexen Systemen wird ein durchschnittlicher DC_{avg} ermittelt:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

Dem DC-Wert wird ein Größenbereich zugeordnet:

Deckungsgrad	Bereich des DC
ohne	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Der $MTTF_d$-Wert ist bei homogenen oder einkanaligen Systemen näherungsweise als Summe der Kehrwerte der einzelnen Komponenten zu ermitteln und entspricht dem $MTTF_d$-Wert eines einzelnen Kanals:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}}$$

3.4 Normen

Bei zweikanaligen, diversitären Systemen ist der $MTTF_d$-Wert beider Kanäle separat zu bestimmen. Beide Werte gehen mittels folgender Formel in die Berechnung der kombinierten $MTTF_d$ ein.

$$MTTF_d = \frac{2}{3}\left[MTTF_{d,C_1} + MTTF_{d,C_2} - \frac{1}{\frac{1}{MTTF_{d,C_1}} + \frac{1}{MTTF_{d,C_2}}}\right]$$

Auch hier wird aus dem Zahlenwert eine qualitative Bewertung über eine Tabelle abgeleitet, die in den folgenden Betrachtungen weiterverwendet wird.

$MTTF_d$-Bewertung	**$MTTF_d$**
niedrig	3 Jahre ≤ $MTTF_d$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_d$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_d$ < 100 Jahre

Die verwendete Architektur des Systems lässt sich in fünf unterschiedliche Kategorien einteilen. Dabei hängt die erreichte Kategorie nicht nur von der Architektur, sondern auch von den verwendeten Bauelementen und Diagnosedeckungsgraden ab. Zu beachten ist, dass die Sicherheitsfunktionen in der Form in Teile zerlegt werden, dass der Ausfall eines Teils die Sicherheitsfunktion komplett außer Funktion setzen würde (oft Subsystem genannt). Jedes dieser Subsysteme kann eine eigene Kategorie besitzen.

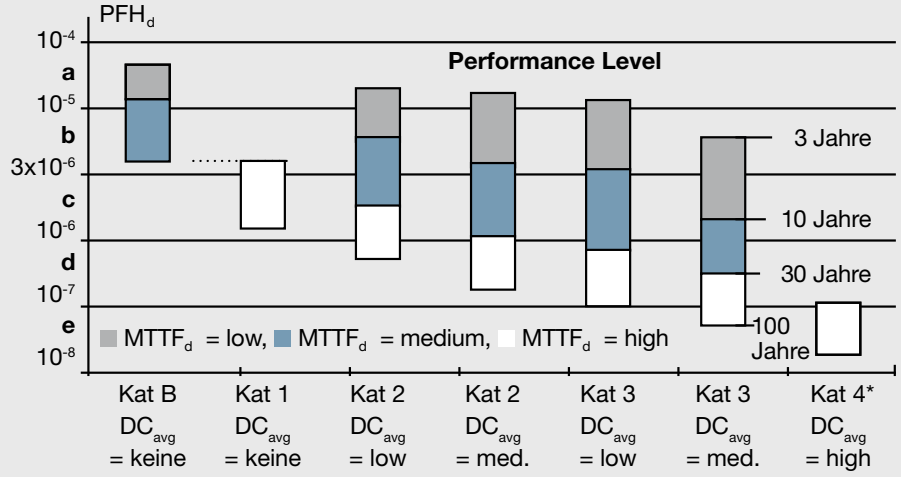
In einem letzten Bewertungsschritt wird aus den eben bestimmten Werten der PL über eine Grafik zugewiesen.

Am zweckmäßigsten ist es, als Erstes die zu Kategorie und DC passende Spalte zu wählen. Danach wird aus dem Balken der zutreffende $MTTF_d$-Bewertungsbereich ausgesucht. Das PL-Ergebnis kann nun an der linken Skala abgelesen werden. In den meisten Fällen ist es noch interpretationsbedürftig, da in vielen Fällen keine eindeutige Beziehung zwischen dem $MTTF_d$-Bewertungsbereich und dem PL besteht.

Befindet man sich in der Kategorie 4, können auch größere $MTTF_d$-(und damit kleinere PFH_d-)Werte als in der Grafik gezeigt genutzt werden. Dafür mussder Anhang K der Norm DIN EN ISO 13849-1 herangezogen werden.

In einem letzten Schritt ist der in der Risikobewertung bestimmte erforderliche PL_r-Level mit dem erreichten PL zu vergleichen. Dabei gilt die Anforderung an die Realisierung als erfüllt, wenn der erreichte PL größer oder gleich dem erforderlichen PL_r ist.

Beziehung zwischen den Kategorien, DC, $MTTF_d$ und PL



* in Kat. 4 ist $MTTF_d$ bis zu 2500 a möglich

Graph zur Bestimmung des PL nach EN ISO 13849-1

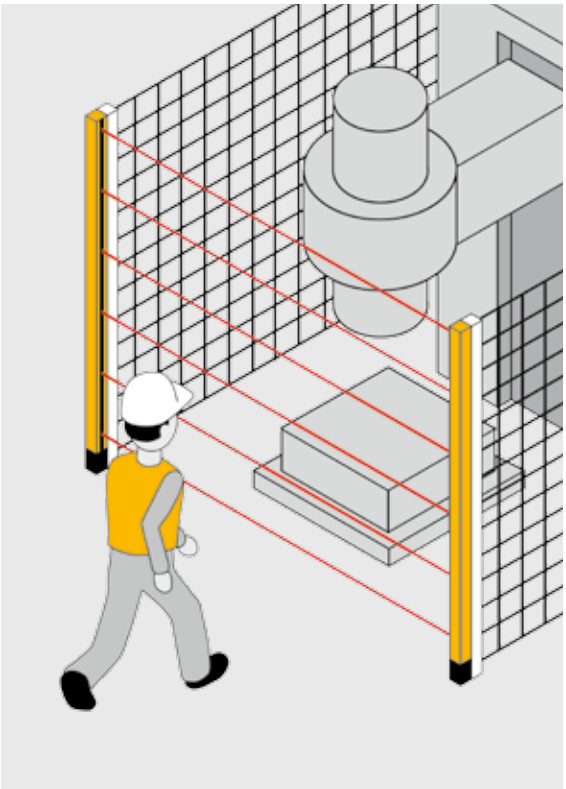
3.4 Normen

3.4.3.5 EN ISO 13855

Norm	Harmonisiert	Titel
EN ISO 13855:2010 ersetzt EN 999	Ja	Sicherheit von Maschinen Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen

In der EN ISO 13855 werden in erster Linie sogenannte Annäherungsgeschwindigkeiten des Menschen definiert. Diese Annäherungsgeschwindigkeiten sind bei der Auslegung von Sicherheitsmaßnahmen und der Wahl geeigneter Sensorik zu berücksichtigen. Hierbei werden, je nach Annäherungsrichtung und Art, unterschiedliche Geschwindigkeiten und Schutzgrößen festgelegt. Auch der Aspekt der indirekten Annäherung wird betrachtet.

Neben der Bemessung von Sicherheitsabständen wird auch die Problematik der Nachlaufmessung betrachtet. Hierzu gibt es klare Vorgaben, wie eine Nachlaufmessung erfolgen kann bzw. nicht erfolgen darf.



Schutzeinrichtungen verhindern das Annähern an gefahrbringende Bewegungen.

3.4.3.6 EN ISO 13857

Norm	Harmonisiert	Titel
EN ISO 13857:2008	Ja	Sicherheit von Maschinen Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen

Die 2008 neu herausgegebene EN ISO 13857 betrachtet die Sicherheitsabstände, die sich durch das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen ergeben. Es ist hervorzuheben, dass diese Norm deutlich macht, dass für andere Bevölkerungs- oder Personengruppen (z. B. asiatische Länder, Skandinavien, Kinder) andere anthropometrische Daten (Größe, Länge von Gliedmaßen …) gelten können und dadurch andere Risiken gegeben sein können. Insbesondere im öffentlichen Raum oder beim Export in andere Länder kann daher die Anwendbarkeit dieser Norm eingeschränkt sein.

3.4 Normen

3.4.3.7 EN 61511 Sicherheitstechnische Systeme für die Prozessindustrie

Norm	Harmonisiert	Titel
EN 61511 Teile 1-3:2004	Nein	Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

Die Normenreihe der EN 61511 beschäftigt sich mit Sicherheitsthemen rund um Anlagen und Systeme der Prozessindustrie. Als Sektornorm der EN 61508 ist die EN 61511 Serie eine Schwesternorm der EN 62061. Dies spiegelt sich in ähnlichen Betrachtungen und mathematischen Grundlagen der drei Normenserien wider. Eine wesentliche Variante für die meisten Endanwender, aber auch für Komponentenhersteller ist die Differenzierung der Anforderungsraten. Während im Maschinenbau stets von hohen Anforderungsraten ausgegangen wird, kennt die EN 61511 auch einen „Low Demand Mode“. Das zentrale Kennzeichen für diesen Modus ist die Anforderung (Betätigung) einer Sicherheitsfunktion seltener als einmal pro Jahr. Als Konsequenz hiervon wurde in der EN 61511 neben dem PFH (Probability of failure on high demand) und SILcl auch ein PFD (Probability of failure on low demand) eingeführt. Es ist insbesondere zu beachten, dass der SILcl für den „Low Demand Mode“ vom SILcl für den „High Demand Mode“ abweichen kann.

3.4.3.8 EN 62061

Norm	Harmonisiert	Titel
EN 62061:2016	Ja	Sicherheit von Maschinen Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

Inhalt

Die EN 62061 befasst sich mit der Bewertung von Risiken anhand eines Risikographen, der hier die Form einer Tabelle hat. Außerdem wird die Validierung von Sicherheitsfunktionen mittels struktureller und statistischer Methoden betrachtet. Wie auch bei der EN ISO 13849-1 lautet das Ziel, die Eignung von Sicherheitsmaßnahmen zur Minderung von Risiken festzustellen.

Wie auch bei der EN 13849-1 ist der Aufwand der im Rahmen dieser Norm erforderlichen Berechnungen beachtlich. Dieser kann durch Verwendung einer passenden Software wie dem Safety Calculator PAScal deutlich verringert werden. https://www.pilz.com/de-INT/eshop/00105002187038/PAScal-Safety-Calculator, Webcode: web150431

Geltungsbereich

Die EN IEC 62061 ist eine der Grundnormen für die funktionale Sicherheit. Sie ist auf IEC-Ebene verabschiedet und innerhalb der EU als Norm innerhalb der Maschinenrichtlinie harmonisiert. Damit gilt für sie im Rahmen der EU die Vermutungswirkung. Als Anwendungsbereich ist die elektrische, elektronische und programmierbare elektronische Sicherheit von Maschinen genannt. Für mechanische, pneumatische oder hydraulische Energiequellen ist sie nicht vorgesehen. In diesen Fällen ist die Verwendung der EN ISO 13849-1 anzuraten.

3.4 Normen

Risikobewertung/Risikoanalyse

Die Bewertung von Risiken geschieht in der IEC 62061 anhand von Tabellen und Risikographen. Dabei werden unter anderem die Schwere von möglichen Verletzungen, die Häufigkeit der Gefährdungsexposition, die Vermeidbarkeit eines Risikos sowie die Wahrscheinlichkeit eines Eintritts des Risikos für jedes einzelne Risiko bewertet. Als Ergebnis der Bewertung erhält man den erforderlichen Safety Integrity Level (SIL) für die einzelnen Risiken.

Die mittels Risikographen bestimmten Levels werden in späteren Schritten der Risikobewertung mit den gewählten Maßnahmen der Risiko-Reduktion abgeglichen. Es müssen dann für jedes klassifizierte Risiko eine oder mehrere Maßnahmen angewendet werden, die das Eintreten des Risikos vermeiden oder hinreichend reduzieren. Dabei muss der SIL der Maßnahme mindestens dem erforderlichen SIL entsprechen, der aufgrund des Risikos bestimmt wurde.

Bestimmung des erforderlichen SIL

Gemäß der EN IEC 62061 gilt es vier verschiedene Aspekte zu bewerten. Jeder Aspekt erhält dabei Punkte gemäß den Bewertungen in den folgenden Tabellen.

Die Klassifizierung des SIL geschieht, basierend auf obigen Eingaben, mithilfe der nachstehenden Tabelle. Es wird hierbei die Auswirkung/Schwere der Klasse K gegenübergestellt. Die Klasse K versteht sich als Summe der Bewertungen für Häufigkeit, Dauer, Wahrscheinlichkeit und Vermeidung. Die als AM gekennzeichneten Bereiche sind in der Norm als Empfehlung für die Anwendung anderer Maßnahmen beschrieben.

Häufigkeit und Dauer	F < 10 Min	F ≤ 10 Min
≤ 1 Std.	5	5
> 1 Std. – ≤ 1 Tag	5	4
> 1 Tag – ≤ 2 Wo.	4	3
> 2 Wo. – ≤ 1 Jahr	3	2
> 1 Jahr	2	1

Wahrscheinlichkeit gef. Ereignis	W
häufig	5
wahrscheinlich	4
möglich	3
selten	2
vernachlässigbar	1

Vermeidung	P
unmöglich	5
möglich	3
wahrscheinlich	1

Auswirkungen und Schwere		Klasse K = F+W+P				
	S	3-4	5-7	8-10	11-13	14-15
Tod, Verlust eines Auges oder Armes	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
permanent, Verlust von Fingern	3		AM	SIL 1	SIL 2	SIL 3
reversibel, medizinische Behandlung	2			AM	SIL 1	SIL 2
reversibel, Erste Hilfe	1				AM	SIL 1

AM = andere Maßnahmen empfohlen

Risikograph nach EN IEC 62061

3.4 Normen

Bewertung der Realisierung/Systembetrachtung

Prinzipiell wird davon ausgegangen, dass es sichere Geräte nicht gibt. Geräte werden erst durch geeignetes Design für die Anwendung in Applikationen mit erhöhten Ansprüchen ertüchtigt. Dabei erhält jedes Gerät im Rahmen einer Bewertung einen SIL, der dessen Eignung beschreibt. Einfache Komponenten können dabei auch über deren $MTTF_d$- oder $B10_d$-Wert beschrieben werden.

In den folgenden Betrachtungen wird untersucht, wie Ausfälle von Geräten oder deren Komponenten sich auf die Sicherheit des Systems auswirken, wie wahrscheinlich diese Ausfälle sind und wie man zum SIL kommt.

Ermittlung der Ausfälle aufgrund gemeinsamer Ursache – CCF-Faktor

Die Ermittlung des CCF-Faktors setzt sich aus mehreren Einzelbewertungen zusammen. Ein erster zentraler Parameter für die Betrachtung ist die verwendete Systemarchitektur. Dabei kommen insbesondere systematische Einflüsse, wie Ausfälle mehrerer Komponenten aufgrund einer Ursache, zur Bewertung. Aber auch die Kompetenz der Entwickler, deren Erfahrung und die Analyseverfahren werden bewertet. Dies geschieht nach einem Bewertungsschlüssel, der jeweils 100 Punkte zu vergeben hat.

Anforderung	Punkte
physikalische Trennung zwischen den Sicherheitskreisen und zu anderen Kreisen	25
Diversität (Verwendung verschiedener Technologien)	38
Entwurf/Applikation/Erfahrung	2
Beurteilung/Analyse	18
Kompetenz/Ausbildung	4
Umwelteinflüsse (EMV, Temperatur …)	18

Im nächsten Schritt ist der β-Faktor (Beta) in Abhängigkeit der erzielten Punkte anhand folgender Tabelle zu bestimmen.

	β-Faktor – Common-Cause-Faktor
< 35	10 % (0,1)
35–65	5 % (0,05)
66–85	2 % (0,02)
86–100	1 % (0,01)

3.4 Normen

SIL-Bewertung

In der EN 62061 wird der maximal erreichbare SIL über eine Abhängigkeit der Hardware-Fehlertoleranz und dem Anteil sicherer Ausfälle (SFF) ermittelt. Der SFF wird berechnet, indem alle möglichen Arten von Komponentenausfällen bewertet werden und jeweils ermittelt wird, ob diese Ausfälle zu einem sicheren oder nicht sicheren Zustand führen. Als Ergebnis erhält man den SFF des Systems.

Daneben ergibt die strukturelle Analyse, ob eine Fehlertoleranz existiert. Das Auftreten von N+1 Fehlern kann dabei bei einer Fehlertoleranz von N zum Verlust der Sicherheit führen. Die folgende Tabelle zeigt den maximal möglichen SIL abhängig von Fehlertoleranz und SFF.

Anteil sicherer Ausfälle (SFF)	Hardware Fehlertoleranz 0	Hardware Fehlertoleranz 1	Hardware Fehlertoleranz 2
< 60 %	nicht erlaubt	SIL 1	SIL 2
60 %–< 90 %	SIL 1	SIL 2	SIL 3
90 %–< 99 %	SIL 2	SIL 3	SIL 3
99 %	SIL 2	SIL 3	SIL 3

Die Ausfallraten λ der einzelnen Komponenten und deren Anteil λ_D (gefahrbringende Ausfälle) lassen sich über architekturabhängige Formeln PFH_D bestimmen. Die Formeln sind teils recht komplex, haben aber stets die Form:

$$PFH_D = f(\lambda_{Di}, \beta, T_1, T_2, DC_i)$$

mit

T_2 Diagnose-Testintervall

T_1 Minimum-Testintervall und Gebrauchsdauer

Durch die kombinierte Betrachtung von Hardware, Fehlertoleranz, Kategorie, DC, PFH_D und SFF kommt man zu folgender Zuordnung der SIL-Level. Dabei sind immer alle Bedingungen zu erfüllen. Wird eine einzelne Bedingung nicht erfüllt, so gilt der SIL als nicht erreicht.

PFH_D	Kat	SFF	Hardware Fehlertoleranz	DC	SIL
≥ 10^{-6}	≥ 2	≥ 60 %	≥ 0	≥ 60 %	1
≥ $2x10^{-7}$	≥ 3	≥ 0 %	≥ 1	≥ 60 %	1
≥ $2x10^{-7}$	≥ 3	≥ 60 %	≥ 1	≥ 60 %	2
≥ $3x10^{-8}$	≥ 4	≥ 60 %	≥ 2	≥ 60 %	3
≥ $3x10^{-8}$	≥ 4	> 90 %	≥ 1	> 90 %	3

In einem letzten Schritt ist der in der Risikobewertung bestimmte erforderliche SIL mit dem erreichten SIL zu vergleichen. Dabei gilt die Anforderung an die Realisierung als erfüllt, wenn der erreichte SIL größer oder gleich dem erforderlichen SIL ist.

3.4 Normen

3.4.3.9 EN 60204-1

Norm	Harmonisiert	Titel
EN 60204-1:2010	Ja	Sicherheit von Maschinen Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen

Die harmonisierte EN 60204-1 betrachtet die elektrische Sicherheit von nicht handgeführten Maschinen mit Spannungen bis 1 000 V DC und 1 500 V AC. Damit ist ihr Anwendungsbereich derart gestaltet, dass nur wenige industrielle Maschinen nicht von ihr betroffen sind.

3.4.3.10 EN 61508

Norm	Harmonisiert	Titel
EN 61508-1:2010 EN 61508-2:2010 EN 61508-3:2010 EN 61508-4:2010 EN 61508-5:2010 EN 61508-6:2010 EN 61508-7:2010	Nein	Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

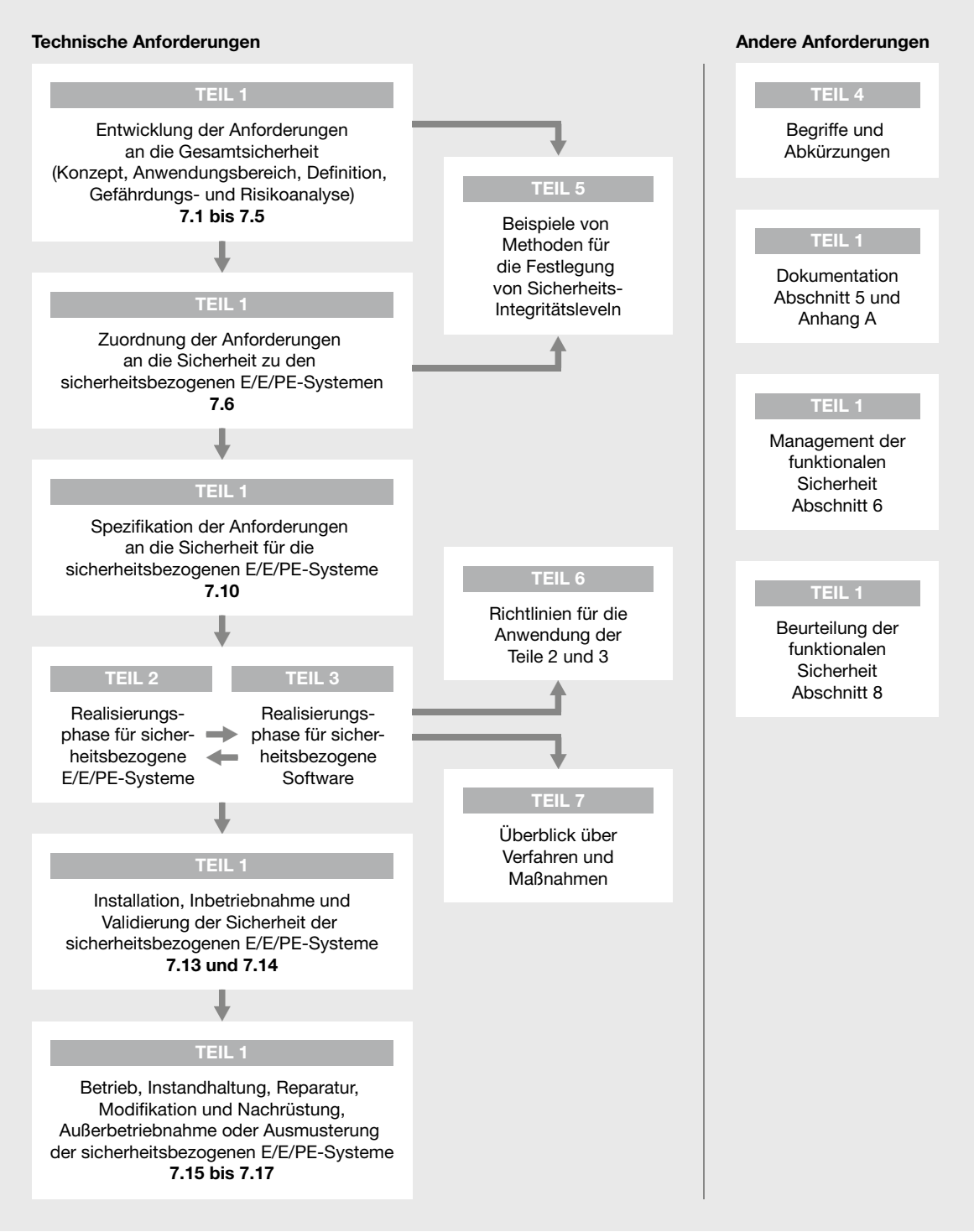
Bei der EN 61508 handelt es sich um die zentrale Norm zum Thema funktionaler Sicherheit von Steuerungssystemen. Insgesamt handelt es sich um sieben Teile, die gemeinsam etwa 1 000 Seiten Normungstext beinhalten. Das gesamte Normenpaket der EN 61508 wurde 2010 komplett überarbeitet und ist in der Edition 2 erhältlich.

Ein zentraler Inhalt der EN 61508, nämlich die Betrachtung des kompletten Lebenszyklus (im Teil 1) aus Sicherheitssicht mit detaillierten Anforderungen an Vorgehen und Inhalt der einzelnen Schritte, ist für den Maschinenbauer und Hersteller von Sicherheitskomponenten gleichermaßen essenziell.

Ein anderer Fokus dieser Norm liegt auf dem Entwurf von elektrischen Systemen und der zugehörigen Software. Dennoch wird diese Norm in der Praxis weiter gefasst und häufig auch für andere Systeme zur Anwendung gebracht (Mechanik, Pneumatik, Hydraulik). Den größten Nutzen dieser Norm haben vermutlich Hersteller von Sicherheitskomponenten wie Sicherheitsschaltgeräten, Sicherheitssteuerungen, Sicherheitssensorik und -aktorik. Insgesamt sind Endanwender oder Systemintegratoren für die Bestimmung von Sicherheitslevels besser beraten, wenn sie statt der EN 61508 die deutlich weniger komplexe EN 62061 oder EN ISO 13849-1 einsetzen.

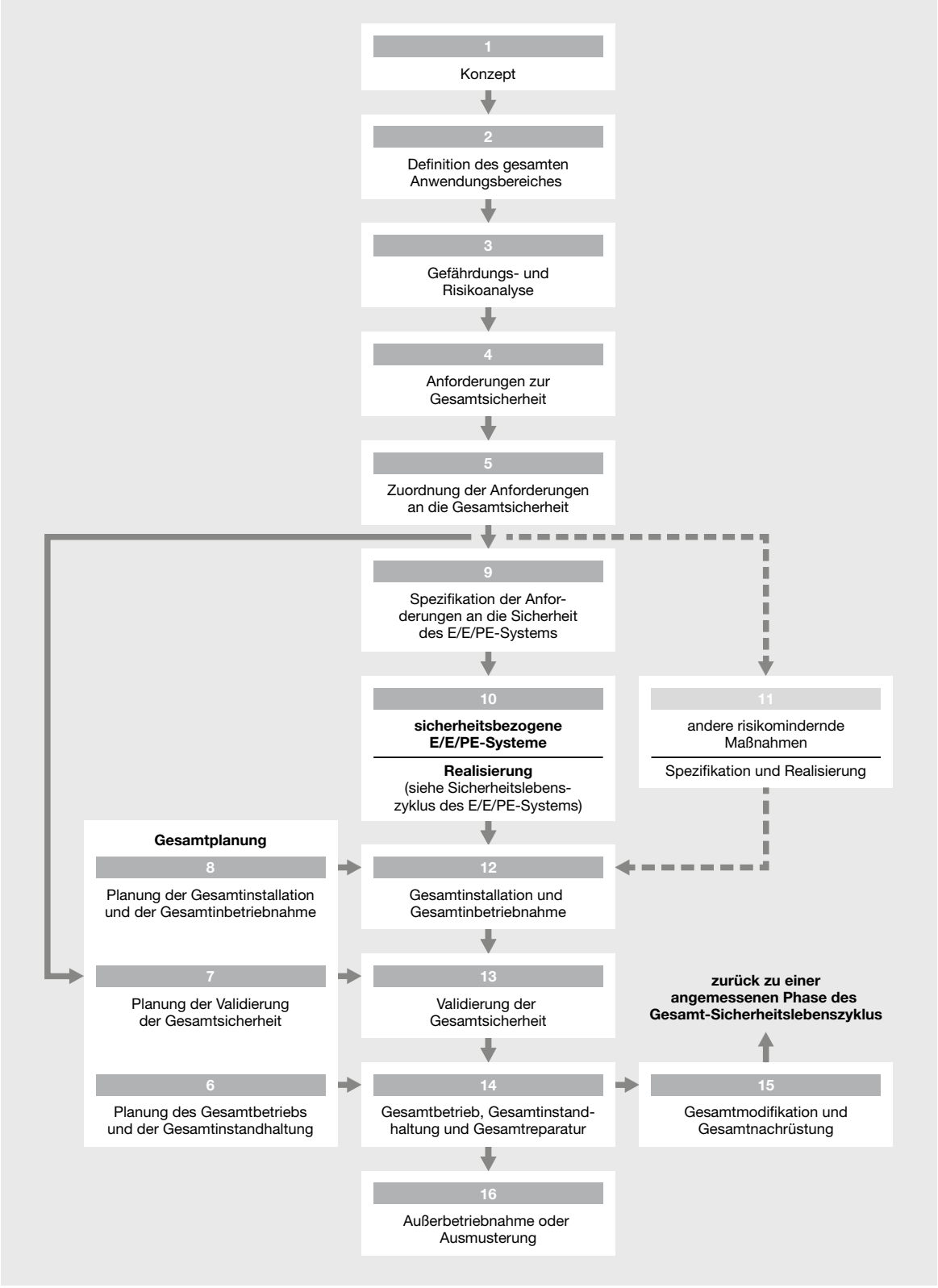
Eine weitere Sektornorm der EN 61508 ist die EN 61511, die für den Bereich der Prozessindustrie anzuwenden ist.

3.4 Normen



Entnommen DIN EN 61508-1, Gesamtrahmen der Sicherheitsbetrachtung nach EN 61508. Gesamtrahmen der Normenreihe IEC 61508

3.4 Normen



Gesamter Sicherheitslebenszyklus nach EN 61508-1

3.4 Normen

3.4.3.12 EN 61326-3

Norm	Harmonisiert	Titel
EN 61326-3 Teil 1 und 2:2008	Nein	Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen

Mit den Ausgaben EN 61326-3-1 und EN 61326-3-2 gibt es seit 2008 zwei Normen, die Aussagen über die erforderliche Störfestigkeit bezüglich des EMV-Levels von Sicherheitsgeräten liefern. Hierbei wurden die zwei Teile mit unterschiedlichen Störfestigkeitsanforderungen spezifiziert. Der Teil EN 61326-3-1 ist der allgemeine Teil mit den schärferen Anforderungen. Dieser Teil wurde insbesondere mit Blick auf den Maschinen- und Anlagenbau entworfen. Im Gegensatz dazu ist der Teil EN 61326-3-2 mit Blick auf die Prozessindustrie geschrieben und stellt deutlich geringere Anforderungen an die Störfestigkeit. Im Maschinenbau sollte daher stets darauf geachtet werden, dass mindestens die Prüfanforderungen nach EN 61326-3-1 erfüllt sind. Da diese beiden Normen aber noch sehr jungen Ursprungs sind und auf keine Vorläufer zurückgreifen können, wird es noch einige Zeit dauern, bis sich diese in den entsprechenden Gerätezertifikaten widerspiegeln. Generell ist zu beachten, dass Produkt- oder Sektornormen ebenfalls EMV-Anforderungen stellen, die meist jedoch unterhalb der in EN 61326-3-1 genannten Anforderungen liegen.

3.4.4 Produktnormen

3.4.4.1 EN ISO 14119

Norm	Harmonisiert	Titel
EN ISO 14119:2013	Ja	Sicherheit von Maschinen Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
ISO/TR 24119	Nein	Sicherheit von Maschinen Bewertung der Fehlerverdeckung in Verbindung mit Verriegelungseinrichtungen mit potenzialfreien Kontakten

Durch die Veröffentlichung der EN ISO 14119:2013 wurden die beiden Vorgänger EN 1088 und ISO 14119 zusammengefasst. Die Norm beschäftigt sich mit trennenden Schutzeinrichtungen, also Türen, Hauben oder Klappen, sowie der Sensorik zur Erkennung der Position dieser Einrichtungen. Außerdem wird auf Zuhaltungen eingegangen.

Zweck der Norm ist außerdem, genaue Anforderungen festzulegen, mit denen die Vorkehrungen zur Verringerung von Umgehungsmöglichkeiten durch den Maschinenbediener verbessert werden. Untersuchungen haben gezeigt, dass Bediener durch Umgehen von Verriegelungseinrichtungen oft versuchen, die Sicherheitsfunktion einer verriegelten und trennenden Schutzeinrichtung zu umgehen. Die Umgehungsmöglichkeit ist in erster Linie den Unzulänglichkeiten in der Maschinenkonstruktion zuzuschreiben. Zeitgleich mit der EN ISO 14119 wird der ISO/TR 24119 veröffentlicht, der eine Abspaltung aus der EN ISO 14119 darstellt. Der ISO/TR 24119 hat lediglich ein Thema: die Bewertung der Verkettung von Schutztürschaltern. Hintergrund sind die immer wieder auftauchenden Fehleranhäufungen im Zusammenhang mit derartigen Anwendungen, die zum Verlust der Sicherheit von Anlagen führen können.

3.4 Normen

3.4.4.2 EN 61496 und IEC/TS 62046

Norm	Harmonisiert	Titel
IEC/TS 62046:2008	Nein	Sicherheit von Maschinen Anwendung von Schutzausrüstungen zur Anwesenheitserkennung von Personen
EN 61496-1:2012	Ja	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen
IEC 61496-2:2013	Nein	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven optoelektronischen Prinzip arbeiten
CLC/TS 61496-3:2008	Nein	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an aktive optoelektronische, diffuse Reflektion nutzende Schutzeinrichtungen (AOPDDR)

Während die 61496-Serie die produktspezifischen Anforderungen an berührungslos wirkende Schutzeinrichtungen beschreibt, hat die IEC/TS 62046 die Auswahl und Bemessung von berührungslos wirkende Schutzeinrichtungen wie Lichtschranken, Lichtgitter oder Scanner im Fokus. Damit ist sie für den Maschinenbauer eine der zentralen Normen für die Gestaltung von Zugangsbereichen zu Maschinen wie auch der Absicherung von Materialschleusen.

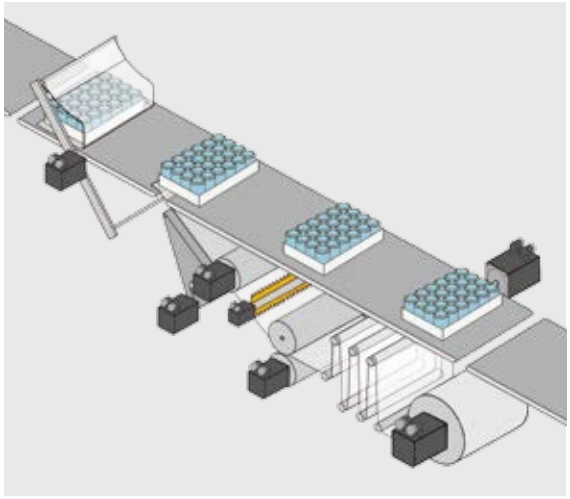
Die Serie der EN 61496-Normen betrachtet die berührungslos wirkenden Schutzeinrichtungen. Hierunter fallen Geräte wie Lichtgitter, Laserscanner, Lichtschranken, sichere Kamerasysteme und andere Sensoren, die zur berührungslosen Absicherung eingesetzt werden können. Da es sich bei der EN 61496 um eine Produktnorm für Sicherheitskomponenten handelt, ist diese Norm für den typischen Anwender nur insofern von Bedeutung, als die von ihm eingesetzten Sicherheitskomponenten diesen Normen entsprechen sollten.

3.4 Normen

3.4.4.3 EN 61800-5-2

Norm	Harmonisiert	Titel
EN 61800-5-2:2007	Ja	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit

Die EN 61800-5-2 richtet sich sowohl an Hersteller von Antrieben als auch an Anwender. Sie behandelt das Thema der Sicherheit von und in Antrieben, ohne jedoch konkrete Forderungen an die sicherheitstechnische Eignung zu stellen. So werden weder Sicherheitslevel festgelegt, noch bestimmte Gefahren- oder Risikobewertungen durchgeführt. Stattdessen beschreibt die Norm Mechanismen und Sicherheitsfunktionen von Antrieben im applikativen Umfeld sowie deren Prüfbarkeit und Planung im Lebenszyklus des Antriebs. Technologisch orientiert sich die Norm an der EN 61508, auch wenn durch den stets vorhanden mechanischen Aspekt der Antriebe eine Nähe zur EN ISO 13849-1 zu erwarten gewesen wäre.



Hersteller von sicheren Antrieben orientieren sich an der EN 61800-5-2.

3.4 Normen

3.4.5 Anwendungsnormen

3.4.5.1 EN ISO 11161 Integrierte Fertigungssysteme

Norm	Harmonisiert	Titel
EN ISO 11161:2010	Ja	Sicherheit von Maschinen Integrierte Fertigungssysteme – Grundlegende Anforderungen

Diese Norm beschäftigt sich mit den Sicherheitsaspekten bei der Verbindung von Maschinen und Bauteilen zu einem Fertigungssystem (IMS). Die Anforderungen an die einzelnen Bauteile und Maschinen werden dabei nicht thematisiert.

Die Norm ist insbesondere für Betreiber und Systemintegratoren von Interesse, die Maschinenparks und Anlagen mit Maschinen und Bauteilen betreiben oder konzipieren. Diese Norm ist in enger Wechselwirkung zur EN ISO 12100 anzuwenden.

3.4.5.2 NFPA 79

Norm	Harmonisiert	Titel
NFPA 79:2015	Nein	Elektrischer Standard für industrielle Maschinen

Diese Norm ist hauptsächlich für den US-Markt von Bedeutung, kommt aber durchaus auch in Asien zur Anwendung. Sie enthält große Ähnlichkeiten zur europäischen EN 60204-1.

Inhalt der Norm sind das sichere elektrische Design, der Betrieb und die Inspektion industrieller Maschinen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

Das in Europa etablierte und sehr umfassende System der EU-Richtlinien mit den dazu harmonisierten Normen, kombiniert mit dem CE-Konformitätsbewertungsverfahren und CE-Kennzeichnungsverfahren für Sicherheitsbauteile, Maschinen und Anlagen, wird nicht automatisch weltweit akzeptiert. In einigen Ländern der Welt gelten andere verbindliche Gesetze, Richtlinien und Normen, die dann für einen problemlosen Export zu beachten und umzusetzen sind. Sichere Maschinen und Anlagen tragen auch in diesen Ländern grundsätzlich zur Erhöhung der Arbeitssicherheit bei, wenn auch das länderspezifische Anforderungs- und Durchsetzungsniveau durchaus sehr unterschiedlich einzustufen ist und in aller Regel das hohe europäische Sicherheitsniveau sicher nicht erreicht wird. Das vorliegende Sicherheitskompendium geht hauptsächlich auf die europäischen Normen, Richtlinien und Gesetze ein. Nachfolgend dennoch ein kurzer Überblick über die Situation in außereuropäischen Ländern und anderen Erdteilen.

3.5.1 Richtlinien und Gesetze in Amerika

3.5.1.1 Nordamerika (USA + Kanada)

USA

In den USA gelten grundsätzlich andere Gesetze, Richtlinien und Normen zu Sicherheitsanforderungen an Maschinen und Anlagen als in Europa. CE-Zeichen und CE-Konformitätserklärung haben keinerlei rechtliche Akzeptanz. Ein Export allein auf Basis einer CE-Konformität ist definitiv illegal und aus Produkthaftungsgründen als sehr kritisch zu bewerten.

Grundsätzlich darf in den USA keine Maschine oder Anlage ohne eine Abnahme durch spezielle Behördenvertreter der Bundestaaten, Bezirke oder Kommunen, den sogenannten Authorities Having Jurisdiction (AHJ), in Betrieb genommen werden. Diese Inspektoren sind etwa für die Abnahme der elektrischen Gebäude- und Maschinensicherheit (Electrical Building/Field Inspector), den Explosionsschutz (Hazardous Location Inspector) oder die Druckgerätesicherheit (Pressure and Vessels Code Inspector) verantwortlich. Ohne deren Freigabe gibt es in der Regel keine Inbetriebnahme. Bei festgestellten Sicherheitsabweichungen ist eine Stilllegung bis zur Mängelbeseitigung durch einen Red Tag (roter Aufkleber/rotes Etikett) prinzipiell möglich. Die Folge sind aufwendige und teure Nachrüst- und Umbaumaßnahmen vor Ort in den USA durch den Hersteller und gegebenenfalls fällige vertraglich vereinbarte Konventionalstrafen wegen verzögerter Inbetriebnahme.

Für die Festlegung und Überwachung von grundlegenden Arbeitsschutzmaßnahmen ist in den USA die Occupational Safety and Health Administration (OSHA), eine Unterbehörde des US-Arbeitsministeriums, zuständig. Diese legt Mindestanforderungen in sogenannten OSHA-Standards fest, die im US-amerikanischen Bundesgesetzbuch Code of Federal Regulations (CFR) unter 29 CFR 1910 hinterlegt sind. Diese richten sich primär an den Maschinen- und Anlagenbetreiber.

Für die Maschinen- und Anlagensicherheit aus Herstellersicht stellt sich die Situation etwas komplizierter dar.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

Zum einen gibt es in den USA kein einheitliches Normungssystem mit einem einzigen Normherausgeber, wie das in Europa mit CEN/CENELEC und den EN-Normen der Fall ist. Es gibt eine Vielzahl von akkreditierten Normerstellern, die Normen erarbeiten und veröffentlichen dürfen. Meist handelt es sich dabei um Herstellerverbände. Die von der Bedeutung her wichtigsten und auch in Europa bekanntesten sind:

- ANSI American National Standards Institute
- NEMA National Electrical Manufacturers Association
- NFPA National Fire Protection Association
- UL Underwriters Laboratories

Eine gesetzliche Anwendungspflicht derartiger Normen besteht in den allermeisten Fällen im Maschinen- und Anlagenbereich allerdings nicht. Aus Sicht des kritischen US-amerikanischen Produkthaftungsrechts muss ein Hersteller dennoch immer durch eine Normenrecherche sicherstellen, welche für seine Maschinen und Anlagen heranziehbaren Normen anwendbar sind. Ist die produktbezogene Anwendbarkeit gegeben, dann sollten die Normanforderungen auch vollständig und korrekt in der Maschine und Anlage umgesetzt werden. Das vermeidet unnötige Produkthaftungsrisiken.

Grundsätzlich immer zu berücksichtigende und anzuwendende Normen sind zum Beispiel:

- NFPA 70 – National Electrical Code (NEC)
- NFPA 79 – Electrical Standard for Industrial Machinery
- UL 508A – Industrial Control Panels

Diese Aufzählung macht deutlich, dass die elektrische Sicherheit bei Maschinen und Anlagen besonders im Fokus steht.

Die mechanische Sicherheit hat verglichen mit der europäischen harmonisierten Normung eine untergeordnete Bedeutung und spielt auch bei der Abnahme durch die o. a. Inspektoren keine Rolle.

Eine umfassende Produktnormung für die elektrische und mechanische Sicherheit von Maschinen und Anlagen, wie in Europa üblich, gibt es deshalb in USA nicht. Lediglich für Maschinen und Anlagen zur Metallverarbeitung, wie Werkzeugmaschinen oder Umformmaschinen, gibt es die Normenreihe ANSI B11, die neben elektrischen auch klare mechanische Sicherheitsanforderungen enthält.

Grundsätzlich lässt sich mit Blick auf die mechanische Maschinen- und Anlagensicherheit in USA sagen, dass eine konsequente Umsetzung von mechanischen Sicherheitsanforderungen auf Basis der harmonisierten A-, B- und C-Normen nach europäischer Maschinenrichtlinie eine wesentliche Grundlage zur Erfüllung der in den USA geltenden Sicherheitsanforderungen darstellt.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in USA gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

Kanada

In Kanada gelten grundsätzlich andere Gesetze, Richtlinien und Normen zu Sicherheitsanforderungen an Maschinen und Anlagen als in Europa. CE-Zeichen und CE-Konformitätserklärung haben keinerlei rechtliche Akzeptanz. Ein Export allein auf Basis einer CE-Konformität ist definitiv illegal und aus Produkthaftungsgründen ist auch davon abzuraten.

Grundsätzlich geht in Kanada keine Maschine oder Anlage ohne eine Abnahme durch spezielle Behördenvertreter der Provinzen, den sogenannten Safety Authority Officers (SAO), in Betrieb. Aber auch der Begriff der Authorities Having Jurisdiction (AHJ) ist in Kanada gebräuchlich. Diese Sicherheitsinspektoren sind etwa für die Abnahme der elektrischen Gebäude- und Maschinensicherheit (Electrical Building/Field Inspector), den Explosionsschutz (Hazardous Location Inspector) oder die Druckgerätesicherheit (Pressure, Vessels and Vessels Code Inspector) verantwortlich. Ohne deren Freigabe gibt es grundsätzlich keine Inbetriebnahme-Freigabe. Bei festgestellten Sicherheitsabweichungen ist eine Stilllegung bis zur Mängelbeseitigung prinzipiell möglich.

Die Folge sind aufwendige und teure Nachrüst- und Umbaumaßnahmen vor Ort in Kanada durch den Hersteller und gegebenenfalls fällige vertraglich vereinbarte Konventionalstrafen wegen verzögerter Inbetriebnahme.

Für die Festlegung und Überwachung von grundlegenden Arbeitsschutzmaßnahmen ist in Kanada das Canadian Centre for Occupational Health and Safety (CCOHS) zuständig. Diese kanadische Behörde ist vergleichbar mit der US-amerikanischen OSHA (siehe 3.5.1.1/USA) und legt Mindestanforderungen für den Arbeitsschutz auch für Maschinen und Anlagen fest, die sich aber primär an den Maschinen- und Anlagenbetreiber richten.

Für die Maschinen- und Anlagensicherheit aus Herstellersicht stellt sich die Situation in Kanada etwas einfacher als in den USA dar.

In Kanada gibt es im Gegensatz zu den USA ein einheitliches Normungssystem mit einem einzigen Normherausgeber, der Canadian Standards Association (CSA), wie das in Europa mit CEN/CENELEC und EN-Normen auch der Fall ist. Es gibt also in Kanada nur eine Art von Normen, die sogenannten CSA Standards. Eine gesetzliche Anwendungspflicht derartiger Normen besteht in den allermeisten Fällen im Maschinen- und Anlagenbereich allerdings nicht. Trotz des weniger scharfen kanadischen Produkthaftungsrechts sollte ein Hersteller dennoch immer durch eine Normenrecherche sicherstellen, welche für seine Maschinen und Anlagen heranziehbaren Normen anwendbar sind. Ist die produktbezogene Anwendbarkeit gegeben, dann sollten die Normanforderungen auch vollständig und korrekt in der Maschine und Anlage umgesetzt werden. Das vermeidet unnötige Produkthaftungsrisiken.

Grundsätzlich immer zu berücksichtigende und anzuwendende kanadische Normen sind zum Beispiel:

- CSA 22.1 – Canadian Electrical Code (CEC)
- CSA 22.2 No.286 – Industrial Control Panels and Assemblies
- SPE 1000 Model Code for the Field Evaluation of Electrical Equipment

Diese Aufzählung macht deutlich, dass die elektrische Sicherheit bei Maschinen und Anlagen besonders im Fokus steht.

Die mechanische Sicherheit hat, verglichen mit der europäischen harmonisierten Normung, eine untergeordnete Bedeutung und spielt auch bei der Abnahme durch die o. a. Inspektoren keine Rolle.

Eine umfassende Produktnormung für die elektrische und mechanische Sicherheit von Maschinen und Anlagen, wie in Europa üblich, gibt es deshalb in Kanada nicht.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

Es gibt aber eine wichtige zu beachtende kanadische Norm, die sich mit Maschinen--Schutzeinrichtungen befasst:

- Z432 – Safeguarding of Machinery

Diese Norm enthält sowohl elektrische als auch mechanische grundlegende Anforderungen an derartige Schutzeinrichtungen, unabhängig von Maschinen- und Anlagenart, und ist mit dem Status einer europäischen A- oder höchstens B-Norm vergleichbar.

Grundsätzlich lässt sich mit Blick auf die mechanische Maschinen- und Anlagensicherheit in Kanada sagen, dass eine konsequente Umsetzung von mechanischen Sicherheitsanforderungen auf Basis der harmonisierten A-, B- und C-Normen nach europäischer Maschinenrichtlinie eine wesentliche Grundlage zur Erfüllung der in Kanada geltenden Sicherheitsanforderungen darstellt.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in Kanada gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5.1.2 Südamerika

Für die südamerikanischen Länder gibt es außer für Brasilien derzeit keine produktspezifischen Sicherheitsanforderungen für Maschinen und Anlagen, die konkret und belastbar sind. Es gibt zwar nationale Normorganisationen, die nationale Normen erarbeiten und insbesondere auch ISO- oder IEC-Normen in nationale Normen überführen. Der Schwerpunkt liegt hier aber derzeit praktisch ausschließlich auf Normen für Verbraucherprodukte. Für den Export von Maschinen und Anlagen nach Südamerika ist deshalb eine fallbezogene Überprüfung der zu erfüllenden Sicherheitsanforderungen etwa durch konkretes, schriftliches Hinterfragen beim Auftraggeber/Besteller und/oder Betreiber anzuraten. Auch wenn in Südamerika die europäischen Richtlinien und deren harmonisierten Normen eine gewissen Stellenwert in puncto Sicherheit genießen, darf man eine grundlegende Akzeptanz nicht automatisch voraussetzen.

Brasilien

In Brasilien gibt es seit 2010 ein nationales Gesetz, das Mindestsicherheitsanforderungen für Maschinen und (Maschinen-)Ausrüstungen fordert:

- Norma Regulamentadora 12 (NR-12) – MÁQUINAS E EQUIPAMENTO

Eigentlich existiert das Gesetz schon seit 1978, ohne wirklich konsequent durch die Behörden umgesetzt und eingefordert worden zu sein. Aber erst mit der letzten, praktisch vollständigen Überarbeitung in 2010 erlangte NR-12 einen verbindlicheren Charakter durch Implementierung behördlicher Überwachungsmaßnahmen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

Im Zuge der Überarbeitung erfolgte eine sehr starke Anpassung an die europäische Maschinenrichtlinie 2006/42/EG. Faktisch wurden die Sicherheitsanforderungen von Anhang I der Maschinenrichtlinie einschließlich einzelner spezieller Anforderungen für bestimmte Maschinenarten weitestgehend übernommen. In Europa wird dieses Gesetz deshalb auch als „brasilianische Maschinenrichtlinie“ bezeichnet.

NR-12 richtet sich grundsätzlich an den Maschinenbetreiber und gilt, im Gegensatz zur europäischen Maschinenrichtlinie, für Alt-, Gebraucht- und Neumaschinen.

Eine Konformitätserklärung als Bestätigung der umgesetzten Sicherheitsanforderungen nach NR-12, wie in Europa vorgeschrieben, wird bisher weder vom Betreiber noch vom Hersteller gefordert. Der Betreiber muss in diesem Fall nachweisen, dass die jeweilige Maschine oder Anlage den Anforderungen nach NR-12 gerecht wird. Im Umkehrschluss heißt das, dass man beim Brasilien-Export von Maschinen in der Regel vom Betreiber mit entsprechenden Forderungen konfrontiert wird. Der Betreiber wird nämlich bei Nichteinhaltung der NR-12 seitens der Behörden mit entsprechenden Zwangsmaßnahmen zur Umsetzung belegt.

Eine der einfachen, aber nicht zu unterschätzenden Forderungen ist das Vorliegen von Betriebs-, Installations- und Wartungsanleitungen in brasilianischem Portugiesisch. Und das ist eben nicht identisch mit der Sprachversion des EU-Landes Portugal.

Eine harmonisierte Normung zur NR-12 existiert derzeit nicht, aber es gibt erste Denk- und Diskussionsansätze auf nationaler Ebene, zukünftig die NR-12 schrittweise mit harmonisierten Normen zu ergänzen und dabei auf dem europäischen Harmonisierungssystem aufzusetzen. In diesem Zusammenhang wird auch die Möglichkeit von Zertifizierungen, etwa für Sicherheitsbauteile, in Erwägung gezogen. Eine praktische Umsetzung ist aber derzeit definitiv noch nicht absehbar.

Auf dem Gebiet der Normung erarbeitet die brasilianische Normungsorganisation Associação Brasileira de Normas Técnicas (ABNT) die länderspezifischen nationalen Normen NBR (Norma Brasileira Regulamentadora), aber überführt auch in zunehmendem Maße ISO- und IEC-Normen in nationale Normen. Oft werden aber nicht die aktuell gültigen Normfassungen von ISO und IEC übernommen, sondern ältere Versionen. Das Normungssystem ist deshalb zwar als sehr umfangreich anzusehen, aber meist nicht auf dem aktuellen Stand der internationalen oder europäischen Normung.

Im Umkehrschluss lässt sich zwar ableiten, dass nach aktuellen europäischen Richtlinien und harmonisierten Normen gebaute Maschinen und Anlagen mit CE-Konformität grundsätzlich sehr gute Voraussetzungen für eine problemlose Inbetriebnahme in Brasilien mitbringen. Dennoch ist für den Export von Maschinen und Anlagen nach Brasilien eine fallbezogene Überprüfung der zu erfüllenden Sicherheitsanforderungen, etwa durch konkretes schriftliches Hinterfragen beim Auftraggeber/Besteller und/oder Betreiber, anzuraten.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in Brasilien gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

3.5.2 Richtlinien und Gesetze in Asien

3.5.2.1 Russland/Russische Föderation

Bis 2011 mussten Maschinen und Anlagen unter bestimmten Voraussetzungen ein sogenanntes GOST-R-Zertifikat vorweisen, um in die Russische Föderation eingeführt werden zu dürfen. Die (internationale) Zoll-Warentarifnummer (HS-Code – Harmonized Commodity Description and Coding System) wurde als Kriterium für die Festlegung der zertifizierpflichtigen Produkte zugrunde gelegt.

Im September 2009 trat ein Erlass der Russischen Föderation in Kraft, der für Maschinen und Ausrüstungen grundlegende Mindestanforderungen an die Sicherheit sowie ein verpflichtendes Konformitätsbewertungsverfahren kombiniert mit einem Zertifizierverfahren vorschreibt:

- N 753 Decree of the Government of the Russian Federation – Technical Regulation (TR) on safety of machines and equipment

Basis ist ein vertragliches Annäherungsverfahren zwischen der EU und der Russischen Föderation zur Angleichung der unterschiedlichen sicherheitstechnischen Vorschriften und Konformitätsbewertungsverfahren für Maschinen in der Russischen Föderation. Bestandteil des Erlasses sind auch zwei Anhänge, je eine Liste der zertifizierungspflichtigen Maschinen und eine solche mit Maschinen, für die eine russische Konformitätserklärung genügt.

Zertifizierungspflicht
Bei Zertifizierungspflicht muss die Maschine durch ein lokal akkreditiertes Prüflabor geprüft und ein TR-Zertifikat ausgestellt werden. Das Verfahren ist in etwa vergleichbar mit einer Baumusterprüfung nach Maschinenrichtlinie.

Konformitätserklärung
Ist eine Konformitätserklärung ausreichend, muss diese trotzdem zusätzlich durch eine national akkreditierte Zertifizierungsstelle geprüft, freigegeben und registriert werden. Diese Art von Konformitätserklärung ist also definitiv KEINE Eigenerklärung des Maschinenherstellers, wie in Europa nach Maschinenrichtlinie und dazu harmonisierten Normen zulässig und üblich.

Die Zoll-Warentarifnummer spielt weiterhin eine gewisse Rolle, da es hierfür eine umfassende Liste gibt, in der alle Produkte, also nicht nur Maschinen, mit Zertifizierungspflicht oder Konformitätspflicht aufgeführt sind.

Basis für die Sicherstellung der Maschinensicherheit sind die russischen Normen GOST (Gossudarstwenny Standart). Es steht hier mittlerweile eine Vielzahl maschinenspezifischer Sicherheitsnormen zur Verfügung. Neben nationalen russischen Normen vom Typ GOST-R werden zunehmend ISO- und IEC-Normen als GOST R ISO, GOST ISO, GOST R IEC oder GOST IEC mit Abweichungen oder sogar weitestgehend unverändert übernommen. Darüber hinaus wurden und werden auch EN-Normen aus dem harmonisierten Bereich der europäischen Maschinenrichtlinie als russische Normen GOST EN übernommen, wenn keine vergleichbaren maschinenbezogenen ISO- und IEC-Normen existieren.

Seit Juli 2010 ist eine Zollunion (Customs Union CU) zwischen den drei eurasischen Ländern Russland, Weißrussland und Aserbaidschan in Kraft getreten, die 2015 um die beiden Länder Armenien und Kirgistan erweitert wurde. Mittel- bis langfristig soll diese Zollunion weitere postsowjetische Staaten einbeziehen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

Die TR für Maschinen gilt in allen Ländern der Zollunion und auch die relevanten russischen GOST-Normen werden als Konformitätsgrundlage anerkannt.

Als nach außen sichtbare Kennzeichnung gibt es ein eigenes eurasisches Konformitätszeichen EAC (EuraAsian Conformity):

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in Russland gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5.2.2 Japan

Das japanische Gesetz über Arbeits- und Gesundheitsschutz (Industrial Safety and Health Law) stellt einige konstruktionstechnische Anforderungen an bestimmte Maschinen (Krane, Aufzüge etc.). Das Gesetz legt darüber hinaus fest, dass der Maschinenbetreiber verantwortlich für die Durchführung von Risikoanalysen ist. Zudem hat er für die Sicherheit am Arbeitsplatz Sorge zu tragen. Man geht davon aus, dass der Betreiber den Maschinenhersteller beim Erwerb zur Ausstellung eines Risikoanalyseberichtes auffordert und die Maschine sicher konstruiert ist. Darüber hinaus enthält das Gesetz Anforderungen an Druckbehälter, Verpackungsmaschinen der Nahrungsmittelindustrie sowie an mobile Maschinen.

Japan übernimmt in der Regel IEC- und ISO-Normen als nationale JIS-Normen (Japanese Industrial Standards), das Gesetz über Arbeits- und Gesundheitsschutz verweist jedoch nicht direkt auf jede dieser Normen. Es gibt demzufolge keine gesetzliche Verpflichtung, diese JIS-Normen auch tatsächlich anzuwenden und umzusetzen.

Für Maschinen und Anlagen gibt es derzeit keine konkreten Abnahme- oder Zulassungsverpflichtungen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

3.5.2.3 China

In China ist die State Administration of Work Safety für die Festlegung und Überwachung von Arbeitsschutzmaßnahmen zuständig. Die Überwachung wird durch lokale Arbeitsschutzinspektoren gewährleistet. Für Maschinen und Anlagen werden dazu chinesische Maschinensicherheitsnormen herangezogen.

Darüber hinaus hat China seit Mai 2002 ein eigenes chinesisches Zertifizierungssystem – Chinese Compulsory Certificate (CCC) – eingeführt. Die Kennzeichnung zertifizierter Produkte erfolgt durch das CCC Mark:

Eine Zertifizierungspflicht besteht derzeit für 23 Produktkategorien mit 132 Produktgruppen aus dem Bereich der Verbraucher-, Elektronik- und Industrieprodukte.

Maschinen und Anlagen fallen aber nicht darunter. Wichtiges Suchkriterium für eine bestehende Zertifizierungspflicht ist dabei die international harmonisierte Zoll-Warentarifnummer, kurz HS-Code (Harmonized Commodity Description and Coding System) im chinesischen Zoll-Handbuch. Ein weiteres Kriterium ist die Prüfung, ob die für ein Produkt geltende chinesische Norm als verpflichtend gekennzeichnet ist.

China hat ein eigenständiges nationales Normsystem, für dessen Erarbeitung die Standardization Administration of China (SAC) verantwortlich ist. Diese Normorganisation gibt die nationalen GB- oder GB/T-Normen heraus.

- GB = Guobiao, bedeutet nationaler Standard
- GB/T = Guobiao/Tujiàn, bedeutet empfohlener, nationaler Standard. Wird verpflichtend bei Referenzierung in GB-Normen

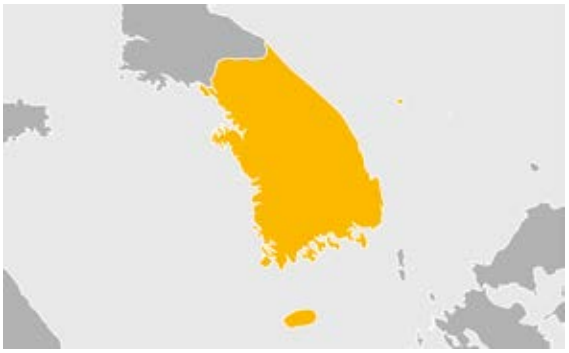
Auf dem Gebiet der Maschinensicherheit übernimmt SAC in der Regel internationale ISO- und IEC-Normen, wenn auch in vielen Fällen nur mit nationalen Abweichungen und nicht auf Basis der aktuellsten internationalen Normfassungen.

Fehlen internationale Normen, werden teilweise auch zur Maschinenrichtlinie harmonisierte europäische EN-Normen in gleicher Weise in nationale chinesische Normen überführt. Ein Anwendungsproblem ergibt sich aus der Veröffentlichung in chinesischer Sprache, englischsprachige offizielle Normfassungen stehen dagegen derzeit nur in Einzelfällen zur Verfügung.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in China gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

3.5.2.4 Südkorea



In Südkorea ist für die Erarbeitung, Umsetzung und Überwachung von Arbeitsschutzmaßnahmen die Korea Occupational Safety & Health Agency (KOSHA) als Regierungsbehörde zuständig. Das koreanische Gesetz Occupational Safety & Health Act bildet die Grundlage für die Arbeit von KOSHA. Ein wichtiges Element der Überwachung durch KOSHA sind Zulassungsverfahren für verschiedene Sicherheitsbauteile, Maschinen und Anlagen. Dazu wurde das bis zum Dezember 2008 existierende System von 13 bereits existierenden und rechtlich verpflichtenden Zertifizierungen in ein neues, einheitliches Zertifiziersystem überführt, das mit einer Übergangsfrist ab Juni 2011 verbindlich umgesetzt wurde. Signalisiert wird das bei Maschinen und Anlagen durch das sogenannte KCs-Mark (Korean Certification Safety Mark)

und dokumentiert durch ein Zertifikat. Die Durchführung der Zertifizierung obliegt den national akkreditierten Prüfinstituten:

- ERI – EMC Research Institute
- KETI – Korea Electronics Technology Institute
- KTL – Korea Testing Laboratory

Es gibt zwei unterschiedliche Zertifizier- oder Zulassungsverfahren, die vom Maschinen- und Anlagenhersteller als Importeur vor dem Export zu beantragen und mit positivem Prüfergebnis durchzuführen sind:

Verpflichtende Zertifizierung für gefährliche Maschinen
Hier muss die Maschinenprüfung vollständig durch ein unabhängiges, lokal akkreditiertes Prüflabor selbst durchgeführt werden. Dieses Prüfverfahren ist gesetzlich vorgeschrieben für Krane, Druckbehälter, Aufzüge, mobile Hubplattformen bestimmte Schrägaufzüge, Pressen, Abkant-/Gesenkbiegepressen, Walzmaschinen, Spritzgießmaschinen und tragbare Kettensägen. Dieses Prüfverfahren ist vom Umfang her grob vergleichbar mit einer Baumusterprüfung nach Anhang IV der Maschinenrichtlinie.

Eigenerklärung des Maschinenherstellers
Hier muss der Maschinenhersteller gegenüber einem lokal akkreditierten Prüflabor durch eine umfassende Dokumentation nachweisen, dass die in Südkorea relevanten Sicherheitsanforderungen/-normen für den jeweiligen Maschinentyp angewandt, umgesetzt, geprüft, dokumentiert und somit erfüllt sind. Dieses Verfahren darf für folgende stationäre Maschinenarten angewandt werden: Industrieroboter, Schleifmaschinen, Werkzeugmaschinen, Holzbearbeitungsmaschinen, Druckerpressen, Misch- und Zerkleinerungsmaschinen, Nahrungsmittelverarbeitungs-Maschinen, Förderbänder und Fahrzeughebebühnen. Die bereitzustellenden Unterlagen sind vom Umfang her vergleichbar mit der Dokumentationserstellung für ein vollständiges EU-Konformitätsbewertungsverfahren.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in Südkorea gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

3.5.3 Richtlinien und Gesetze in Ozeanien

3.5.3.1 Australien

Seit 2013 gilt in vier der sechs Staaten und den zwei Territorien des Kontinents ein weitgehend vereinheitlichtes Recht für notwendige und umzusetzende Arbeitsschutzmaßnahmen. Die Erarbeitung und Festlegung der gesetzlichen Rahmenbedingungen sowie die Überwachung obliegen der nationalen Behörde Safe Work Australia. Grundlage für den Arbeitsschutz ist das nationale Gesetz Work Health and Safety Act (WHS).

Lediglich die Staaten Victoria und West Australia haben eigenständige Arbeitsschutzanforderungen als Occupational Health and Safety Acts erarbeitet und umgesetzt.

Grundsätzlich sind die definierten Arbeitsschutzmaßnahmen gesetzlich verpflichtend und damit zwingend zu beachten. Es gibt diverse Anwendungs- und Umsetzungsleitfäden, Model Codes of Practice genannt. Diese richten sich in erster Linie direkt an den lokalen Betreiber und nicht an den Hersteller von Maschinen und Anlagen. Gleichwohl muss sich ein Hersteller damit auseinandersetzen, um mögliche Probleme bei der Inbetriebnahme in Australien zu vermeiden.
Die Überwachung erfolgt durch Inspektoren in den jeweiligen Staaten und Territorien.

Als Mitgliedsland des britischen Commonwealth folgt Australien traditionell den administrativen Vorgehensweisen Großbritanniens. Das macht sich auch bei den Arbeitsschutzmaßnahmen durch – für den Maschinen- und Anlagenbauer wichtige – Gemeinsamkeiten mit der europäischen Maschinenrichtlinie und der zugehörigen harmonisierten Normung bemerkbar.

Australien hat ein eigenständiges Normungssystem, für dessen Erarbeitung Standards Australia verantwortlich ist. Diese Normorganisation gibt die nationalen Normen Australian Standards (AS) heraus. Für den Bereich der Maschinensicherheit gibt es folgende AS-Normen:

- Normenreihe AS 4024.xxxx – Safety of machinery
- AS 60204.1 – Electrical equipment of machines, general requirements
- Normenreihe AS IEC 61511.x – Functional safety in process industry
- AS 62061 Safety of machinery – Functional safety electrical, electronic and programmable electronic control systems

Diese Normen sind auf jeden Fall zu beachten, auch wenn es derzeit keine konkreten Anforderungen zur rechtsverbindlichen Umsetzung aus der australischen Arbeitsschutzgesetzgebung dazu gibt. Die australische Maschinensicherheitsnormung basiert im Wesentlichen – aber nicht durchgängig – auf der Übernahme von ISO- oder IEC-Normen und auch zur europäischen Maschinenrichtlinie harmonisierten Normen. Aber nicht immer ist bereits die aktuelle Ausgabe einer internationalen oder europäischen Norm übertragen worden.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in Australien gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

3.5.3.2 Richtlinien und Gesetze in Neuseeland

Seit 2015 gilt in Neuseeland für notwendige und umzusetzende Arbeitsschutzmaßnahmen der Health and Safety Work Act (HSW). Die Erarbeitung und Festlegung der gesetzlichen Rahmenbedingungen sowie die Überwachung obliegen der nationalen Behörde WorkSafe New Zealand.

Grundsätzlich sind die definierten Arbeitsschutzmaßnahmen gesetzlich verpflichtend und damit zwingend zu beachten. Es gibt diverse Anwendungs- und Umsetzungsleitfäden, diese richten sich in erster Linie direkt an den lokalen Betreiber und nicht an den Hersteller von Maschinen und Anlagen. Gleichwohl muss sich ein Hersteller damit auseinandersetzen, um mögliche Probleme bei der Inbetriebnahme in Neuseeland zu vermeiden.
Die Überwachung erfolgt auch in Neuseeland durch lokale Inspektoren.

Als Mitgliedsland des britischen Commonwealth folgt Neuseeland traditionell den administrativen Vorgehensweisen Großbritanniens. Das macht sich auch bei den Arbeitsschutzmaßnahmen durch – für den Maschinen- und Anlagenbauer wichtige – Gemeinsamkeiten mit der europäischen Maschinenrichtlinie und der zugehörigen harmonisierten Normung bemerkbar. Neuseeland hat ein eigenständiges Normungssystem, für dessen Erarbeitung Standards New Zealand verantwortlich ist. Diese Normorganisation gibt die nationalen Normen New Zealand Standards (NZS) heraus.

Für den Bereich der Maschinensicherheit werden dabei in der Regel die entsprechenden australischen AS-Normen als AS/NZS-Normen übernommen:

- Normenreihe AS/NZS 4024.xxxx – Safety of machinery

Diese Normen sind auf jeden Fall zu beachten, auch wenn es derzeit keine konkreten Anforderungen zur rechtsverbindlichen Umsetzung aus der neuseeländischen Arbeitsschutzgesetzgebung dazu gibt.

Die neuseeländische Maschinensicherheitsnormung basiert damit ebenso wie die AS-Normen auf der Übernahme von ISO- oder IEC-Normen und auch zur europäischen Maschinenrichtlinie harmonisierten Normen. Aber nicht immer ist bereits die aktuelle Ausgabe einer internationalen oder europäischen Norm übertragen worden.

Bei konkreten Fragestellungen zu den nationalen Besonderheiten in der Maschinen- und Anlagensicherheit sprechen Sie einfach Pilz an. Die Pilz Tochtergesellschaft in Neuseeland gemeinsam mit dem international aufgestellten Pilz Dienstleistungsservice für Automation, Anlagen- und Maschinensicherheit kann Sie in landesspezifischen Fragestellungen zu diesen Themen zielgerichtet unterstützen.

3.5 Normen, Richtlinien und Gesetze im internationalen Vergleich

3.5.4 Zusammenfassung

Die kurze und sicher nicht umfassende Gegenüberstellung europäischer und weltweiter Anforderungen an die Maschinen- und Anlagensicherheit soll lediglich die teils sehr unterschiedliche und vor allem uneinheitliche Situation bei außereuropäischen Sicherheitsanforderungen an Maschinen und Anlagen aufzeigen.

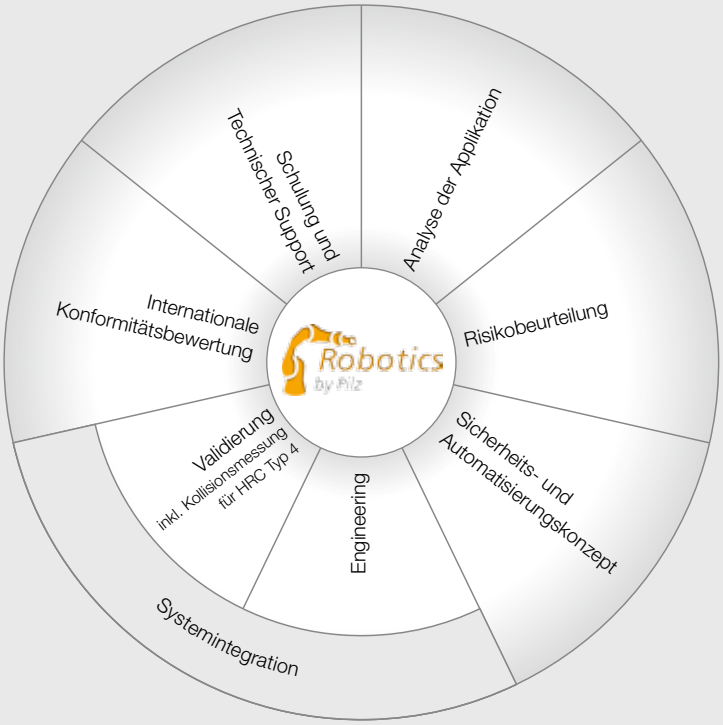
Der Maschinen- und Anlagenhersteller muss sich deshalb frühzeitig mit den speziellen länderspezifischen und für das eigene Produkt relevanten Gesetzen, Richtlinien und Normen auseinandersetzen und vertraut machen. Das ist die Grundvoraussetzung für den dann weitestgehend problemlosen Maschinen- und Anlagenexport außerhalb Europas.

Grundsätzlich kann man aber sagen, dass die Beachtung und die tatsächliche Umsetzung der für die jeweilige Maschine und Anlage relevanten EU-Richtlinien und harmonisierten Normen eine wesentliche Voraussetzung ist, um mit relativ überschaubarem Zeit- und Kostenaufwand Maschinen und Anlagen weltweit exportieren zu können.

Das zeigt insbesondere auch den grundsätzlichen Stellenwert des europäischen Richtlinienkonzepts mit den sehr detaillierten harmonisierten Normungssystemen auch im internationalen Bereich. Es gibt derzeit kein Land auf der Welt außerhalb der EU, das ein derart umfassendes und praktisch alle sicherheitsrelevanten Bereiche abdeckendes und zudem noch einheitliches Sicherheitskonzept für Maschinen und Anlagen aufweisen kann. Darauf kann man als Maschinen- und Anlagenhersteller setzen, auch wenn das CE-Zeichen und die CE-Konformitätserklärung international definitiv keine wirkliche rechtliche Akzeptanz besitzen. Die immer noch weit verbreitete Sichtweise von Maschinen- und Anlagenherstellern, mit einer CE-Konformität praktisch einen Freibrief für den weltweiten Export zu haben, ist deshalb schlichtweg falsch. Schließlich handelt sich es dabei in aller Regel ja „nur“ um die Eigenerklärung des Herstellers, mit der behauptet wird, alle für sein Produkt anzuwendenden Richtlinien und harmonisierten Normen beachtet, angewandt und auch tatsächlich umgesetzt zu haben. Und da ist das Vertrauen in verschiedenen außereuropäischen Ländern durchaus nur eingeschränkt vorhanden.

3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

Lebenszyklus



Analyse der Applikation
Dokumentation der wichtigsten Peripheriegeräte der geplanten Roboterapplikation. Die prozess- und sicherheitstechnischen Anforderungen wie z. B. Taktzeit, Wiederholgenauigkeit, Arbeitsplatz, Gefahrenbereiche etc. werden in die grobe Systemplanung integriert. Es folgt die technische sowie wirtschaftliche Evaluierung.

Risikobeurteilung
Überprüfung der Roboterapplikation in Übereinstimmung mit den geltenden Normen und Richtlinien und Beurteilung bestehender Gefahren.

Sicherheitskonzept
Erarbeitung einer detaillierten technischen Lösung für die Sicherheit der Roboterapplikation durch mechanische, elektronische und organisatorische Maßnahmen.

Sicherheitsdesign
Durch eine detaillierte Ausarbeitung der notwendigen Schutzmaßnahmen wird eine Reduzierung oder Beseitigung der Gefahrenstellen der Applikation erreicht.

Systemintegration
Die Ergebnisse aus Risikobeurteilung und Sicherheitskonzept werden durch ausgewählte Sicherheitsmaßnahmen maßgeschneidert umgesetzt.

Validierung
Überprüfung und Spiegelung der Risikobeurteilung und des Sicherheitskonzepts sowie Durchführung der Kollisionsmessung gemäß der Grenzwerte der ISO/TS 15066.

Internationale Konformitätsbewertung
Gewährleistung der Konformität mit den behördlichen Anforderungen wie z. B. CE-Kennzeichnung in Europa oder OSHA in den USA, NR-12 in Brasilien, KOSHA in Korea, GOST in Russland oder CCC in China.

Schulung und Technischer Support
Vermittlung von Know-how rund um die sichere Anwendung von Robotern.

3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

3.6.1 Normative Vorgaben für den Einsatz von Industrierobotern

Gemäß Maschinenrichtlinie 2006/42/EG ist ein Robotersystem eine unvollständige Maschine. Das bedeutet, dass Robotersysteme zunächst als nicht sicher einzustufen sind und eine CE-Kennzeichnung benötigen.

Dies liegt daran, dass ein Roboter für sich allein gesehen keinen bestimmten Verwendungszweck hat. Erst durch den Integrator, der die Roboterapplikation erstellt und den Roboter mit einem Werkzeug versieht, definiert sich dessen bestimmungsgemäße Verwendung.

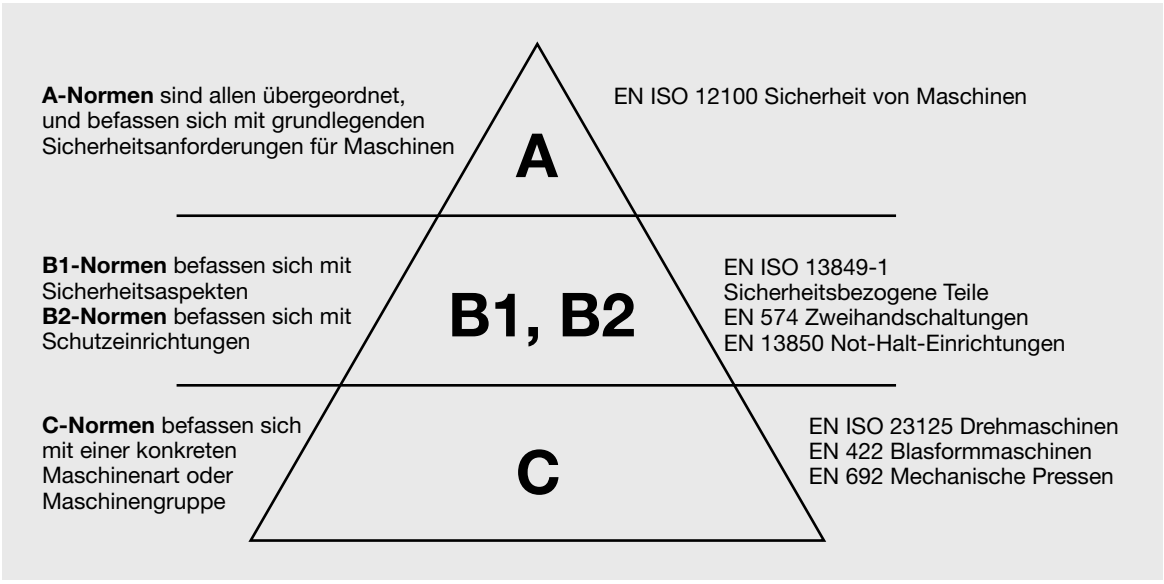
Der Integrator ist der Inverkehrbringer der Maschine (Roboterzelle). Er muss das Konformitätsbewertungsverfahren, an dessen Ende die EG-Konformitätserklärung steht, durchlaufen.

Für detaillierte Sicherheitsanforderungen standen bislang die beiden Normen ISO 10218 „Safety of Industrial Robots“ Teil 1: „Robots“ und Teil 2: „Robot systems and integration“ zur Verfügung. Die deutschen Fassungen beider Teile sind als EN ISO 10218-1:2011 und EN ISO 10218-2:2011 veröffentlicht und unter der Maschinenrichtlinie 2006/42/EG gelistet.

Die EN ISO 10218-1 befasst sich ausschließlich mit dem eigentlichen Robotersystem.

Im Gegensatz dazu erweitert die EN ISO 10218-2 den Blickwinkel auf die gesamte Roboterapplikation.

Die beiden genannten Normen sind Typ-C-Normen. Das bedeutet, es sind produktspezifische Normen, die in der Hierarchie über den Typ–A- und Typ-B-Normen stehen.



In der Praxis erwiesen sich diese Normen aber als nicht ausreichend, um eine tatsächliche Kollaboration von Mensch und Maschine, bei der sich die jeweiligen Arbeitsräume zeitlich und räumlich überschneiden können, sicher umzusetzen. Hier klaffte eine normative Lücke, die durch die Veröffentlichung der ISO/TS 15066 geschlossen werden konnte.

MRK erfordert Schutzmaßnahmen, damit während des kollaborierenden Betriebs die Sicherheit des Menschen jederzeit gewährleistet ist. Dafür sind in der ISO/TS15066 vier Kollaborationsarten als Schutzprinzipien genauer beschrieben. Zudem werden hier die maximal erlaubten biomechanischen Grenzwerte für eine Kollision zwischen Mensch und Roboter definiert.

3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

3.6.2 Die Roboterapplikation aus Sicht der EN ISO 10218-2

Wie schon erwähnt, hat die EN ISO 10218-2 einen breiteren Fokus. Sie betrachtet die gesamte Roboterapplikation.

Eine Roboterzelle kann aus folgenden Komponenten bestehen:

- Industrieroboter
- Endeffektor (Werkzeug des Roboters)
- Werkstück
- maschinelle Ausrüstung

Im Vergleich zur rotativen Antriebstechnik sind in der Robotik die Sicherheitsfunktionen normativ nicht eindeutig benannt und spezifiziert.

Sicherheitsfunktionen des Industrierobotersystems können u. a. sein:

- sicherer Halt
- sicher reduzierte Geschwindigkeit
- sichere Achsbegrenzung
- sichere Arbeitsraumüberwachung
- usw.

Die Benennung im Detail ist jedoch immer herstellerspezifisch und kann variieren. Aus diesem Grund ist es sehr wichtig, die Zertifikate der jeweiligen Hersteller zu sichten, um das Leistungsniveau der Sicherheitsfunktionen einordnen zu können.

Das Leistungsniveau von sicherheitsgerichteten Teilen von Steuerungen ist im Kapitel 5.2 der EN ISO 10218-2 beschrieben. Hier wird unter 5.2.2 eine zweikanalige Steuerungsstruktur, PL d, Kat. 3 gemäß EN ISO 13849-1 gefordert.

3.6.3 Mensch-Roboter-Kollaboration und ISO/TS 15066

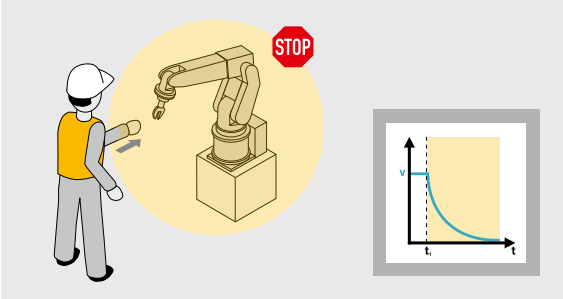
Die EN ISO 10218-2 streift das Thema der Mensch-Roboter-Kollaboration nur. Aus diesem Grund wurde die Technische Spezifikation ISO/TS 15066 geschaffen. Diese ist seit Februar 2016 verfügbar und geht detailliert auf das Thema MRK ein.

In der TS 15066 werden die vier Kollaborationsarten als Schutzprinzipien beschrieben. Diese vier Methoden können einzeln zur Absicherung von MRK-Applikationen angewendet werden. Jede einzelne – oder in Kombination.

Methode 1: Sicherheitsbewerteter überwachter Stillstand (Safeguarded Stop)

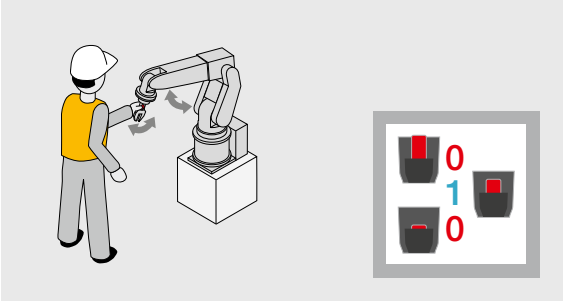
Der Mensch hat nur Zugang zum stillstehenden Roboter („sicherheitsbewerteter überwachter Halt“). Auf Aspekte der Sensortechnik wird hier nicht eingegangen.

Das Robotersystem darf nicht selbstständig und unerwartet wieder anlaufen. Dies könnte z. B. durch Fehler in nicht sicherheitsgerichteten Teilen von Steuerungen geschehen.



Methode 2: Handführung (Handguiding)

Der Mensch hat auch hier nur Zugang zum stillstehenden Roboter. Erst durch die manuelle Bestätigung einer Zustimmeinrichtung darf die Handführung des Robotersystems ermöglicht werden.

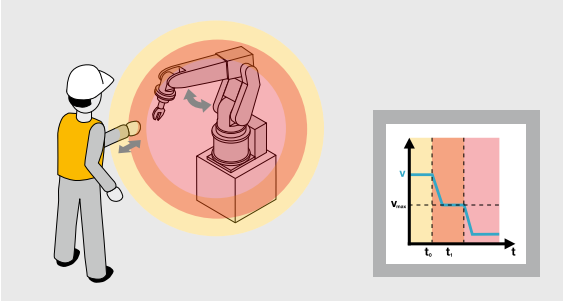


3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

Methode 3: Geschwindigkeits- und Abstandsüberwachung (Speed and Separation Monitoring)

Bei dieser Methode wird durch einen Sensor permanent der Abstand zwischen Mensch und Roboter sicherheitsgerichtet überwacht. Das Robotersystem bewegt sich mit entsprechend sicher reduzierter Geschwindigkeit.

Je näher der Mensch dem Roboter kommt, desto langsamer wird der Roboter. Ist der Abstand zu gering, wird ein Sicherheitshalt ausgelöst.



Derzeit gibt es keine Sensorik am Markt, die die Methode 3 sicherheitsgerichtet komplett abbilden kann.

In einer statischen Variante ist dies derzeit mit Scanner oder SafetyEYE möglich.

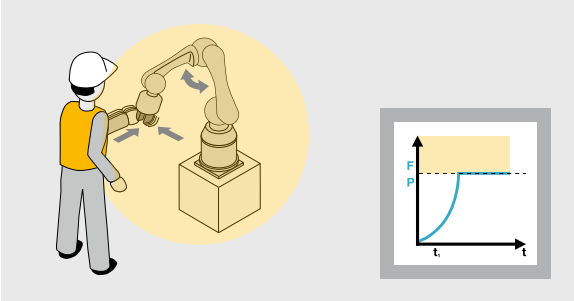
Die Sicherheit wird in den ersten drei Methoden durch den Abstand zwischen Mensch und Maschine gewährleistet. Eine Kollision zwischen Mensch und Roboter ist hier nicht zulässig. Bei der Umsetzung einer dieser drei Methoden werden keine speziellen MRK-Roboter benötigt. Es können Standard-Industrieroboter zur Anwendung kommen, die mit entsprechenden Sicherheitspaketen zur Geschwindigkeitsüberwachung oder Arbeitsraumüberwachung vom Hersteller ausgerüstet sind.

Methode 4: Leistungs- und Kraftbegrenzung (Power and Force Limitation)

Im Gegensatz zu den Methoden 1 bis 3 ist bei Methode 4 der Kontakt zwischen Mensch und Roboter „unter bestimmten Umständen“ möglich. Es muss jedoch durch den Hersteller der Applikation garantiert werden, dass die Kollision zwischen Mensch und Roboter keine Gefahr für den Menschen darstellt.

Dies bestätigt der Hersteller der Applikation mit seiner Unterschrift auf der Konformitätserklärung.

Eine sichere MRK-Applikation erfordert zum einen Robotersysteme, die speziell für die jeweilige Kollaborationsart konzipiert sind. Die Risikominderung kann neben der Anwendung der Kollaborationsarten auch durch eine inhärent sichere Konstruktion des Roboters und des Arbeitsraums umgesetzt werden. Inhärent bedeutet in diesem Falle, dass das Robotersystem aufgrund seiner konstruktiven Merkmale keine gefahrbringende Kollision erzeugen kann.



3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

Kraft-leistungsreduzierter Roboter

Ein Robotersystem, das aufgrund seiner Sensorik die Kollision „spürt“ und daraufhin seine Bewegung stoppt. Diese Kollisionserkennung wird durch Teile der Robotersteuerung realisiert. Bezüglich der Anforderungen, die für sicherheitsgerichtete Teile von Steuerungen gelten, verweist die TS 15066 wieder auf das zuvor angesprochene Kapitel 5.2 der EN ISO 10218-2 (PL d, Kat. 3).

Kollisionen können also auf verschiedene Arten abgemildert werden: Durch konstruktive Maßnahmen wie Abrunden der Kanten und Ecken, Polsterungen oder möglichst große Kontaktflächen, um die Kraft auf der Fläche zu verteilen. Oder aber durch technische Schutzmaßnahmen (z. B. die Reduzierung der Dynamik der Roboterbewegungen sowie Anpassungen der Roboterbahn, um Kollisionen mit besonders sensiblen Köperregionen zu vermeiden). Auch Schulungen der Mitarbeiter können helfen, das Verletzungsrisiko zu verringern.

Letztlich muss aber zwingend durch ein Messverfahren ermittelt werden, ob die möglichen Kollisionen sicherheitstechnisch unbedenklich sind. Im Anhang A der Technischen Spezifikation ISO/TS 15066 wird ein Körpermodell mit 29 spezifischen, in zwölf Körperregionen eingeteilte Köperbereiche aufgeführt.

Das Körperzonenmodell macht zu jedem Körperteil (z. B. am Kopf, an der Hand, am Arm oder am Bein) eine Angabe zu den jeweiligen Belastungsgrenzwerten mit Blick auf Kraft und Druck. Die Grenzwerte kennzeichnen das Eintreten des Schmerzes.

Diese Grenzwerte definieren dafür die maximale Kraft und den maximalen Druck, die bei einer Kollision auf die entsprechende Körperregion einwirken dürfen. Der sensibelste Bereich ist der Kopf. Eine Kollision mit dem Kopf bei bestimmungsgemäßer Verwendung sollte weitgehend ausgeschlossen werden können. Bleibt die Anwendung während einer Begegnung zwischen Mensch und Roboter innerhalb dieser Grenzen, so ist sie normenkonform.

Die ISO unterscheidet auch ganz klar zwischen der Art der Kollision. Es gibt zwei verschiedene Kollisionsarten:

- **Der transiente Kontakt** zwischen Mensch und Roboter. Das entspricht einem Stoß durch den Roboter. Der Mensch wird von dem Roboter getroffen, hat aber die Möglichkeit, zurückzuweichen. Er ist nicht eingeklemmt.
  Diese Kollisionsart wird von der TS 15066 als weniger gefährlich als der quasi-statische Kontakt gesehen. Aus diesem Grund lässt die TS eine Doppelung der Grenzwerte für eine Kollision zu, bei der der Mensch nicht gequetscht wird. Eine Ausnahme ist der Kopf. Hier ist keine Doppelung der Grenzwerte zulässig.
- **Der quasi-statische Kontakt** zwischen Mensch und Maschine. Diese Kontaktart entspricht einer Quetschung des Menschen. Es befindet sich ein Gegenlager (Applikations- oder Gebäudestrukturen) unmittelbar bei dem Menschen. Ein Ausweichen ist nicht möglich, die entsprechende Körperregion wird gequetscht und der Mensch ggf. eingeklemmt und kann sich nicht selbst befreien. Hier lässt die TS eine Doppelung der Grenzwerte lediglich für die ersten 0,5 s der Kollision zu. Dies gilt jedoch nicht für Körperregionen, die den Kopf betreffen.

3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

3.6.4 Validierung

Validierung bedeutet das Überprüfen der realen Applikation. Hier werden nochmals alle risikomindernden Maßnahmen aus der Risikobeurteilung auf deren Umsetzung und Vollständigkeit geprüft.

Die Applikation sollte fertig aufgebaut sein und sich in „auslieferungsfertigem“ Zustand befinden.

Die Validierungsphase einer Roboterzelle besteht aus folgenden Stufen:

Stufe 1: Berechnung des Performance Levels

In der Konstruktionsphase wurden bereits die erforderlichen PL_r ermittelt. Nun wird für jede Sicherheitsfunktion überprüft, ob mit den ausgewählten Komponenten das geforderte PL auch tatsächlich erreicht wird.

Dies kann mit unterstützenden Tools wie z. B. Safety Calculator PAScal erfolgen.

Stufe 2: Sicherheitstechnische Überprüfung

An der fertigen Roboterzelle werden alle Komponenten auf die richtige Implementierung geprüft. Es gilt, etwaige Fehler bei der Installation, Programmierung und Inbetriebnahme aufzudecken. Gerade die Überprüfung von Roboter-Systemen stellt aufgrund ihrer großen Freiheitsgrade eine ganz besondere Herausforderung dar. Es sind jedoch nicht nur der Roboter, sondern auch jede andere Peripherie in der Applikation zu validieren.

Stufe 3: Nachlaufwegmessung

Wenn optische Schutzeinrichtungen in der Anlage verbaut werden, ist zu prüfen, ob sie konform zur EN ISO 13855 installiert wurden. Dies wird mit einem kalibrierten und zertifizieren Nachlaufwegmessgerät durchgeführt und bei bestandener Prüfung mit einem Prüfsiegel auf der optischen Schutzeinrichtung bestätigt. Auf dem Prüfsiegel sollte auch der Zeitpunkt der nächsten Inspektion klar lesbar sein.

Stufe 4: Kollisionsuntersuchung

MRK-Applikationen, die der bereits vorgestellten Methode 4 folgen, womit eine Kollision zwischen Mensch und Roboter möglich ist, müssen die biomechanischen Grenzwerte der ISO/TS 15066 einhalten.

Die Einhaltung der biomechanischen Grenzwerte ist zwingend notwendig, unabhängig davon, ob es ein inhärent sicheres Robotersystem oder ein kraft-/leistungsreduziertes Robotersystem ist.

Die ISO/TS 15066 gibt Anleitung zur rechnerischen Auslegung eines kollaborierenden Robotersystems. Dies ist aber nur ein theoretischer Ansatz. Dieser Ansatz befasst sich jedoch nur mit dem transienten Kontakt. Für den quasi-statischen Kontakt gibt es keine rechnerische Lösung. Somit ist auf jeden Fall ein praktischer Nachweis der real auftretenden Kollisionswerte notwendig.

Bei der Kollisionsuntersuchung werden alle möglichen Kollisionsszenarien real überprüft. Hierbei wird mithilfe der in der ISO/TS 15066 stehenden Informationen jede Körperstelle simuliert. Mit einem speziell dafür entwickelten Kollisionsmessgerät werden die Kennwerte der Kollision aufgezeichnet.

3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

3.6.5 Sinn der Messung

Prinzipiell kann von allen Bewegungen des Roboters Gefahr ausgehen! Deshalb muss der Mensch vor dem Roboter geschützt werden. Um den Schutz des Werkers zu gewährleisten, setzte man früher auf eine strikte Trennung von Mensch und Maschine. Der Roboter blieb für die Erledigung seiner Aufgaben eingehaust in einer Zelle.

Dank einer neuen Generation von Robotern und Technologien kann ein Schutzzaun heute nicht mehr notwendig sein, wenn die Kollision keine Gefahr mehr birgt.

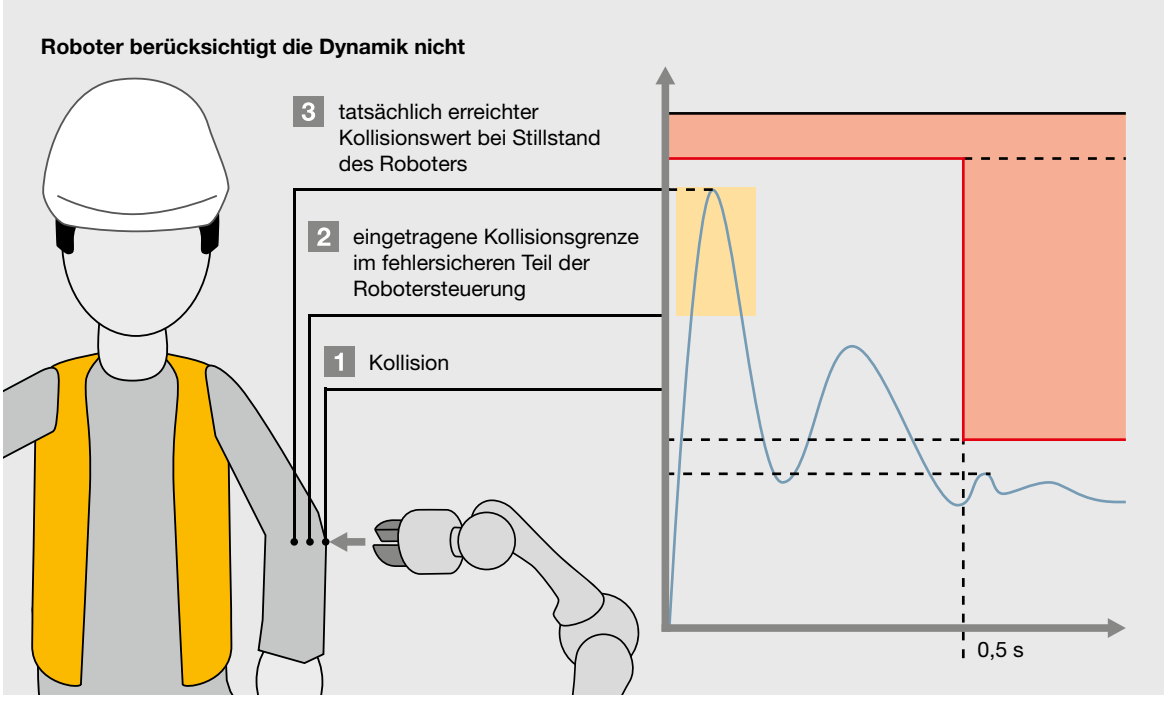
Wer heute die CE-Verantwortung für eine Roboterapplikation übernimmt, in der sich Mensch und Maschine den Arbeitsraum teilen und kein Schutzzaun die Sicherheit gewährleistet, muss für die Einhaltung der Grenzwerte sorgen.

Das Roboter-System alleine kann das nicht! Es berücksichtigt keine Dynamik.

In kraft-leistungsreduzierten Robotersystemen sind im sicherheitsgerichteten Teil der Steuerung Grenzwerte einzutragen, welche die Kollision absichern sollen. Diese Werte sind jedoch keinesfalls als absolut zu sehen.

Was geschieht in der Realität?

1. Wenn die Kollision stattfindet, „spürt“ der Roboter zunächst einen Widerstand. Die Kraft des Roboters liegt zunächst unterhalb der vorgegebenen Kraftgrenze. Der Roboter versucht nun seine Bahn beizubehalten und wird die Leistung der Antriebe erhöhen.
2. Die Gegenkraft steigt und der Roboter erreicht die eingestellte Kraftgrenze für die Kollision.
3. Erst jetzt beginnt der Roboter seine Bewegung zu stoppen. Der Anhalteweg findet nach der Kollision und damit im Inneren des menschlichen Körper statt.



Achtung bei MRK-Methode 4

3.6 Industrieroboter, Mensch-Roboter-Kollaboration (MRK)

MRK Kollisionsmess-Set für normenkonforme Mensch-Roboter-Kollaboration

Auch bei Leichtbaurobotern sind die Themen Nachlaufweg und Reaktionszeiten zu berücksichtigen. Denn in der Realität wird oft das Vielfache der eingestellten Kollisionswerte erreicht.

Abhilfe schafft dann oft nur die Reduzierung der Dynamik des Roboters.

Um deshalb mit gutem Gewissen die Konformitätserklärung abgeben zu können, ist die messtechnische Überprüfung der Kollisionswerte unumgänglich.

Für diese Art von Messungen gilt wie für alle anderen Messmethoden, dass sie verständlich und nachvollziehbar sowie reproduzierbar sein müssen.

Für diese spezielle Kraft- und Druckmessung hat Pilz daher das Kollisionsmessgerät PROBmdf entwickelt. Das mit Federn und entsprechenden Sensoren ausgestattete Gerät misst die auf den menschlichen Körper einwirkenden Kräfte exakt und vergleicht sie mit den Grenzwerten. Das Messgerät wird dafür an den bei der Risikobeurteilung ermittelten Positionen installiert, zwischen Roboterarm und einem steifen, unnachgiebigen Untergrund. Damit wird ein quasi-statischer Kontakt, z. B. das Einquetschen des Werkers zwischen Roboter und Anlage, simuliert. Über eine Software wird die Messung gestartet und werden die Daten anschließend verarbeitet sowie dokumentiert.

Je nach Messpunkt ist es empfehlenswert, den Test bis zu zehnmal durchzuführen. Der höchste Wert, also „worst case“, wird für die Validierung herangezogen. Wenn die Grenzwerte überschritten werden, müssen zusätzliche Sicherheitsmaßnahmen wie z. B. Lichtgitter oder eine trennende Schutzeinrichtung installiert werden.

Das Kollisionsmessgerät ist Bestandteil eines Komplettsets von Pilz für die Validierung gemäß ISO/TS 15066. Das Set beinhaltet neben dem Messgerät mit Folien und Scanner auch verschiedene Federn, mit denen die verschiedenen Körperbereiche simuliert werden können. Pilz bietet das Set, in dem auch Schulung, Wartung, Kalibrierung und regelmäßige Updates enthalten sind, auf Mietbasis an.

3.7 Sicheres Programmieren nach EN ISO 13849-1

Gerne werden die Sicherheitstechnik und die Anforderungen an sie hauptsächlich auf die eingesetzte Hardware bezogen.

Hierbei gehen Anwender entsprechend der EN ISO 13849-1 vor und bestimmen durch die von den Herstellern angegebenen $B10_D$ Werten, den $MTTF_D$- oder den PFH_D Werten den Performance Level der Sicherheitsfunktion. (Anmerkung: Die Architektur, Diagnosedeckungsgrad usw. sind ebenfalls erforderlich.) Hierbei wird oft gerne vergessen, dass zur Realisierung von Sicherheitsfunktionen immer mehr programmierbare Systeme (Steuerungen) zum Einsatz kommen. Da nun auch die Applikationsprogramme (SRASW) dieser Steuerungen einen Einfluss auf die Qualität der Sicherheitsfunktion haben, müssen auch für die Softwareprojektierung entsprechende Methoden und Vorgehensweisen definiert und angewendet werden. Projektierung deshalb, weil neben dem eigentlichen Programmieren (Codieren) mehr zu tun ist.

Eine bekannte Redensart lautet: „Es gibt keine fehlerfreie Software!“ Egal wie sorgfältig und gewissenhaft man programmiert, Fehler im Programmcode lassen sich nicht vermeiden. Man schätzt, dass in ca. 1 000 Zeilen Code durchschnittlich etwa zwei Fehler enthalten sind.

Ein tödliches Beispiel für Softwarefehler ist „Therac-25“. Hierbei führte ein Softwarefehler dazu, dass es bei einem Gerät zur Bestrahlung von Krebstumoren zu einer Überdosis Strahlen kam, die innerhalb von drei Jahren drei Todesopfer forderte (https://de.wikipedia.org/wiki/Therac-25).

Was sind typische Softwarefehler? Softwarefehler, auch Programmierfehler oder Bugs genannt, sind zum Beispiel:

- Syntaxfehler: Verstoß gegen grammatikalische Regeln
- semantische Fehler: z. B. Verwechslung des Befehlscodes
- Laufzeitfehler: z. B. Endlosschleifen
- logische Fehler: z. B. falscher Lösungsansatz
- Designfehler: z. B. Fehler in der Anforderungsdefinition
- Bedienfehler: z. B. unübersichtliches Bedienkonzept.

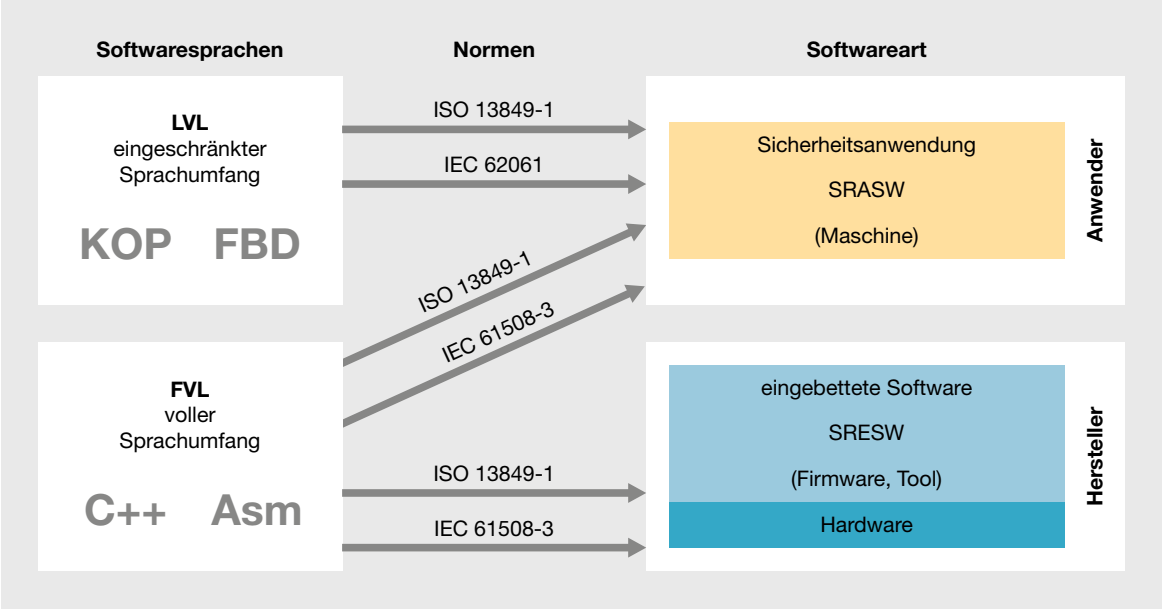
3.7.1 Safety Related Software

In Sicherheitssteuerungen wie zum Beispiel der PSS 4000 sind zwei Arten von Software enthalten. Im Englischen wird diese Software als Safety Related Software bezeichnet. Unterschieden wird dabei, ob es sich um die durch den Hersteller zur Funktion der Sicherheitssteuerung entwickelte oder ob es sich um anwenderentwickelte Software handelt. So wird die durch den Hersteller entwickelte Software auch als Firmware oder Betriebssystem bezeichnet. Im normativen Sprachgebrauch der EN ISO 13849-1 wird dies als Safety Related Embedded Software, kurz SRESW, bezeichnet. Bei der durch den Anwender der Sicherheitssteuerung entwickelten Software, die gerne als Applikationsprogramm bezeichnet wird, sprechen wir von einer Safety Related Application Software (SRASW).

Für die Erstellung dieser Applikationssoftware (SRASW) wird wiederum in der EN ISO 13849-1 in zwei Arten von Programmiersprachen unterschieden.

Programmiersprachen mit nicht eingeschränktem oder auch vollem Sprachumfang werden als FVL (Full Variability Language) bezeichnet. Typische Beispiele für diese FVL-Sprachen sind zum Beispiel C oder C++. Das Einsatzgebiet dieser Sprachen ist z. B. im Bereich der Erstellung von SRESW.

3.7 Sicheres Programmieren nach EN ISO 13849-1



Programmiersprachen mit einem eingeschränkten Sprach- oder Funktionsumfang werden dagegen als LVL (Limited Variability Language) bezeichnet. Diese Sprachen kommen hauptsächlich bei der Erstellung von SRASW zum Einsatz. Diese Sprachen zeichnen sich durch die Fähigkeit aus, bereits vorentwickelte Bibliothekselemente mit neuem Applikations-Code zu kombinieren und damit die geforderte Spezifikation an die Sicherheitsfunktion einzuhalten. Klassische Beispiele für LVL-Sprachen sind SPS-Sprachen wie Kontaktplan oder Funktionsbaustein. Bei dem Automatisierungssystem PSS 4000 ist es auch möglich, die Programmiersprache Strukturierter Text als LVL-Sprache einzusetzen. Immer mehr Steuerungshersteller schränken Hochsprachen wie C oder C++ in ihrer Funktionalität so weit ein, dass auch diese zu den LVL-Sprachen gezählt werden können.

Darüber hinaus wird nicht auf die Erstellung von sicherheitsbezogener Embedded Software eingegangen. Auch wird vom dem Einsatz von FVL- Sprachen bei der Entwicklung von SRASW abgeraten, da bei dem Einsatz dieser Programmiersprachen die Wahrscheinlichkeit eines systematischen Programmierfehlers erhöht ist.

3.7.2 Software in Bezug auf die Risikobeurteilung

Wenn im Rahmen der Risikobeurteilung basierend auf der EN ISO 12100 eine steuerungstechnische Schutzmaßnahme definiert worden ist, kommen verstärkt Sicherheitssteuerungen oder Automatisierungssysteme mit integrierten Sicherheitsfunktionen zum Einsatz. Wie schon erwähnt, ist dabei nicht nur die Einstufung der Sicherheitssteuerung als Hardwarekomponente in einen Performance Level ausschlaggebend, sondern auch die Projektierung der sicherheitsbezogenen Anwendersoftware hat Einfluss auf die Qualität der Sicherheitsfunktion. Basierend auf dem geforderten Performance Level nach der EN ISO 13849-1 muss auch die sicherheitsbezogene Anwendersoftware dem Performance Level standhalten.

Wenn zum Beispiel die Sicherheitsfunktion einen Performance Level von PL d benötigt, dann muss die SRASW mindestens den Maßnahmen zur Erreichung des Performance Levels PL d entsprechen. Im umgekehrten Sinne ist es möglich, dass trotz einer Entwicklung einer SRASW nach Anforderungen des Performance Levels PL e bei der Verwendung einer Hardware mit einem PL c die gesamte Sicherheitssteuerung schlussendlich nur einen Performance Level c erreicht.

3.7 Sicheres Programmieren nach EN ISO 13849-1

3.7.3 Basisanforderungen an die Softwareentwicklung

Im Abschnitt 4.6.3 der EN ISO 1384-1 wird genauer auf Anforderungen an die Erstellung einer SRASW eingegangen. Hier werden neben Anforderungen an die zu entwickelnde Software auch Anforderungen an die Entwicklungswerkzeuge sowie den Entwicklungsprozess gestellt.

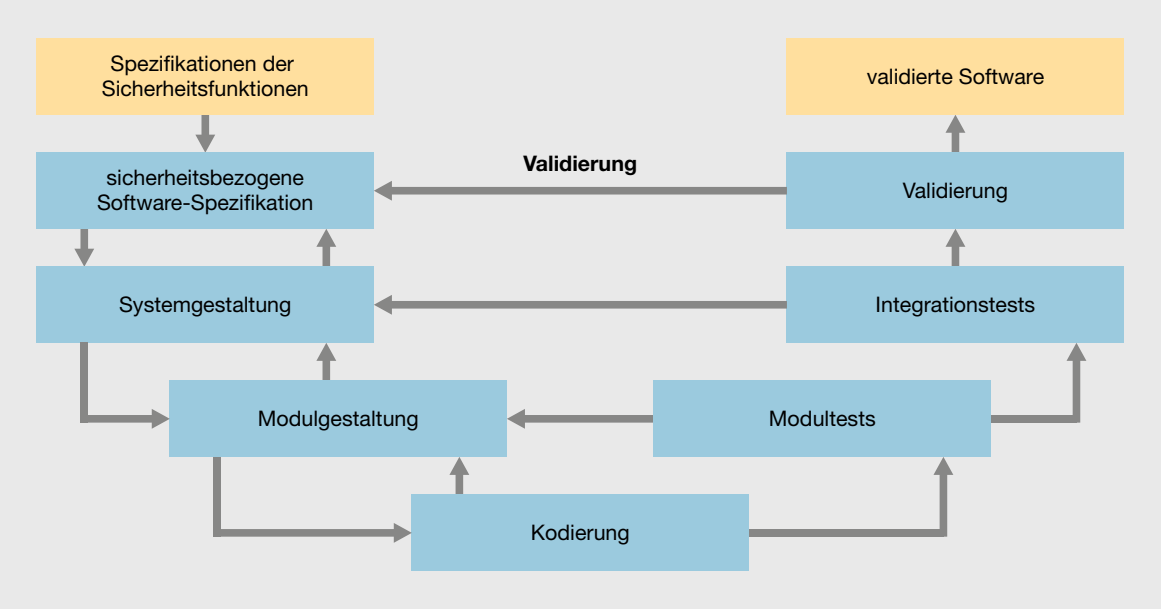
Allgemeine Anforderungen an die SRASW, die in einer Sicherheitsfunktion mit einem Performance Level von a bis e zum Einsatz kommt, sind:

- Entwicklungslebenszyklus mit Verifikation und Validierung
- Dokumentation von Spezifikation und Entwurf
- modulare und strukturierte Programmierung
- funktionale Tests
- geeignete Entwicklungsaktivitäten nach Änderungen

Der Entwicklungslebenszyklus von sicherheitsrelevanter Software wird gerne auch durch das vereinfachte V-Modell beschrieben. Der linke Ast des V-Modells beschreibt dabei die konstruktiven Entwicklungsschritte zur Erstellung der Software. Hier wird jeder Entwicklungsschritt gegenüber dem Ergebnis des vorangegangenen Arbeitsschrittes verifiziert (überprüft). Der rechte Ast des V-Modells beschreibt die überprüfenden Tätigkeiten, auch als Verifikation und Validierung bezeichnet. Auch beschreibt das Modell, dass jedem konstruktiven Entwicklungsschritt ein Verifikations- oder Validierungsschritt gegenübersteht, wobei der für den Test erforderliche Testplan bereits parallel und unabhängig zur Entwicklungsphase entstehen sollte.

Durch die konsequente Anwendung des V-Modells soll durch fehlervermeidende Maßnahmen eine möglichst fehlerfreie Software projektiert/entwickelt werden und sich durch Eigenschaften wie lesbar, verständlich, testbar und wartbar auszeichnen – übergeordnete Anforderung an sicherheitsrelevante Software der EN ISO 13849-1. Weiterhin soll dadurch natürlich eine modulare, strukturierte Programmerstellung gewährleistet sein. Hierbei bietet es sich für die Programmierung von SRASW an, auf bereits durch den Hersteller zertifizierte Softwaremodule/Bausteine zurückzugreifen.

In der Realität wird die Entwicklung natürlich oftmals von Änderungen gestört. Diese müssen bei der Entwicklung laufend berücksichtigt und ihre Auswirkungen abgeschätzt werden (Einflussanalyse). Auch hierzu sollten alle Aktivitäten nach dem V-Modell durchgeführt und mittels einer Änderungshistorie festgehalten werden. Sowieso ist es natürlich Pflicht, die Aktivitäten im Entwicklungsprozess zu dokumentieren.



3.7 Sicheres Programmieren nach EN ISO 13849-1

3.7.4 Weitere fehlervermeidende Maßnahmen für steigende Performance Level

Wie bereits beschrieben, sind Basismaßnahmen für das Erreichen eines Performance Levels PL a bis e notwendig. Mit steigendem Performance Level PL c bis e müssen weitere fehlervermeidende Maßnahmen zusätzlich eingeführt werden. So müssen die Spezifikationen der SRASW überprüft werden und die im Lebenszyklus beteiligten Personen müssen exakte Informationen zu den Sicherheitsfunktionen, den Leistungskriterien sowie der Steuerungsarchitektur und der Erkennung und Beherrschung von externen Ausfällen erhalten.

Weitergehend muss ein Augenmerk auf die Auswahl der Werkzeuge gelegt werden.

3.7.5 Programmierwerkzeuge, Sprachen und Bibliotheken

Unter Werkzeuge versteht man in diesem Sinne die Auswahl der Programmierwerkzeuge, Bibliotheken und Sprachen.

So sollen Programmierwerkzeuge Fähigkeiten zur Vermeidung von systematischen Fehlern wie zum Beispiel:

- Datentypunverträglichkeit
- unvollständiger Aufruf von Schnittstellen
- Rekursionen
- …

enthalten. Die Prüfung sollte bereits während der Kompilierung erfolgen und nicht erst zur Laufzeit der Software.

Im Weiteren sollten die Programmierwerkzeuge für die Anwendung eines modularen Programmierverfahrens geeignet sein und auch eine anerkannte Teilmenge der IEC-61131-3-Sprachen verwenden. Grafische Sprachen wie Kontaktplan oder Funktionsbaustein sind oft besser lesbar und verständlicher als rein textbasierende Sprachen. Daher wird der Einsatz von grafischen Programmiersprachen empfohlen.

Das zum Automatisierungssystem PSS 4000 gehörende Programmiertool PAS4000 bietet neben den textlichen Programmiersprachen wie Instruction List und strukturiertem Text die grafischen Programmiersprache Kontaktplan sowie die Pilz eigene grafische Programmiersprache PASmulti an.

In der Systemfamilie PNOZmulti findet sich die grafische Programmierung PNOZmulti.

Wann immer möglich, sollte auf bereits validierte Funktionsblock-Bibliotheken zurückgegriffen werden. Die Hersteller von Sicherheitssteuerungen bieten eine Vielzahl von bereits validierten und zertifizierten Funktionsbausteine in den Bibliotheken ihrer Programmierwerkzeuge an. Auch bietet sich die Möglichkeit, auf anwendungsspezifische Funktionsbaustein-Bibliotheken zurückzugreifen, die im Rahmen von Projekten auf den Anforderungen zur SRASW-Entwicklung nach EN ISO 13849-1 basierend entwickelt und dokumentiert worden sind.

3.7.6 Strukturierung und Modularität der Software

Eine saubere Strukturierung sowie eine modular aufgebaute Software ist Basis einer Fehlervermeidung sowie Grundlage zur Beherrschung von Änderungen. Es ist daher bereits bei der Spezifikation und dem Design der Software darauf zu achten und diese Vorgehensweise durch die Verwendung von bereits validierten Bibliotheks-Funktionsbausteinen zu unterstützen. Für eigens entwickelte Bausteine sollten auch semiformale Verfahren (grafische Methoden) angewendet werden, um die Daten bzw. den Kontrollfluss zu beschreiben. Hierzu eignen sich besonders Verfahren wie Zustandsdiagramme und Programmflussdiagramme. Auch sollten die zu entwickelnden Funktionsbausteine mit einer minimierten Codelänge programmiert werden und die Ausführung mit Einsprung und Aussprung erfolgen.

3.7 Sicheres Programmieren nach EN ISO 13849-1

Besonders bewährt hat sich eine Architektur in drei Stufen:

- Eingänge: Erfassung der Informationen, und Signale der Sicherheitssensoren durch Sicherheitseingänge
- Bearbeitung: Verarbeitung der Informationen, um die Sicherheitsfunktion zu realisieren, die zu einem sicheren Zustand führt
- Ausgänge: Ansteuerung der Betätigungselemente durch Sicherheitsausgänge

Bei der Ansteuerung von Sicherheitsausgängen ist es unabdingbar, dass diese nur in einem Programmteil verwendet werden. Gerade hier kann die Nichteinhaltung dieser normativen Anforderungen zu gefährlichen Zuständen an Maschinen und Anlagen führen. Generell sollten die Programmierer von SRASW einen defensiven Programmierstil pflegen. Defensive Programmierung zielt auf die Erzeugung von Software, die anormale Abläufe, Daten, Werte (im Programm) zur Laufzeit erkennt und in einer vorbestimmten Weise darauf reagiert.

Dies kann zum Beispiel erreicht werden durch:

- Bereichsprüfung von Variablen
- die Plausibilitätsprüfung von Werten
- Vermeidung von Setze- und Rücksetze-Befehlen
- Gruppierung und Strukturierung der Software

3.7.7 SRASW und Nicht-SRASW in einer Komponente

Moderne Automatisierungssysteme wie die PSS 4000 vermischen die sicherheitsgerichtete Programmierung mit der nicht sicherheitsgerichteten Programmierung. Gerade in solchen Steuerungen bzw. bei der Erstellung von Software für solche Automatisierungssysteme müssen diese Softwareteile in unterschiedlichen Funktionsblöcken und mit einer definierten Schnittstelle realisiert werden. Besonders ist darauf zu achten, dass keine logische Verknüpfung von sicherheitsbezogenen und nicht sicherheitsbezogenen Daten zustande kommt, die eine Reduzierung der Integrität der sicherheitsbezogenen Signale bewirkt, zum Beispiel durch eine Oder-Verknüpfung dieser Signale.

3.7.8 Softwareimplementierung und Codierung

Die Anforderung aus der EN ISO 13849-1 ist, dass der Code lesbar, verständlich und testbar sein muss. Daher ist es wichtig, in der Organisation eindeutige Programmierrichtlinien definiert zu haben. Diese Richtlinien sollte jeder Programmierer verstehen und anwenden können. Programmierrichtlinien (Coding Rules) können z. B. die Syntax von Variablen enthalten, da eine der normativen Forderungen lautet, dass auf eine Verwendung von Hardwareadressen (z. B. E1.0) verzichtet und stattdessen eine symbolische Variable (z. B. Eingang_NotHalt_Kanal 1) verwendet wird.

Wenn möglich, sollte der erzeugte Code (Applikationsprogramm) durch eine Simulation sowie mittels einer Kontroll- und Datenflussanalyse (bei PL d und e) verifiziert werden.

3.7 Sicheres Programmieren nach EN ISO 13849-1

3.7.9 Testen

Nach der Codierung der Software kommt eine oftmals zeitintensive Testphase. Wie schon beleuchtet, kann es trotz aller Maßnahmen zur Fehlervermeidung bei der Erstellung von SRASW zu Fehlern kommen. Diese Fehler sollten in den Testphasen möglichst aufgedeckt werden. Um diese Testphase angemessen durchführen zu können, sollte eine detaillierte Testplanung bereits parallel zu den Spezifikationsphasen aufgesetzt werden. Hierin sollten alle Testfälle mit Abschlussbedingungen sowie die zum Test verwendeten Werkzeuge aufgeführt sein.

Ein angemessenes Validierungsverfahren ist der sogenannte Black-Box-Test des funktionellen Verhaltens sowie der Leistungskriterien. Der Black-Box-Test bezeichnet eine Methode, bei der ohne Kenntnisse der inneren Funktionsweise des Testobjekts die Testkriterien entwickelt und abschließend durchgeführt werden. Für PL d und PL e Software wird eine Testfallausführung auf Basis von Grenzwertanalysen empfohlen, bei der das System bewusst über seinen geplanten Einsatz hinaus getestet wird. Als Beispiel könnte hier ein Parameter mit einem höheren Wert als seinem spezifizierten Grenzwert beaufschlagt werden. Vor dem Start der Black-Box-Tests sollte jedoch noch ein sogenannter I/O-Test sicherstellen, dass die verwendeten sicherheitsbezogenen Signale auch in der SRASW richtig und korrekt verwendet werden.

PL/Kategorie	Prüfmaßnahmen nach DIN EN ISO 13849-2
alle PL_r	Black-Box-Test des funktionellen Verhaltens und der Leistungsfähigkeit, z. B. Zeitverhalten
empfohlen für PL_r d oder e	zusätzlich erweiterte Testfälle, die auf Grenzwertanalysen beruhen
alle PL_r	I/O-Tests, um sicherzustellen, dass die sicherheitsbezogenen Eingangs- und Ausgangssignale richtig verwendet werden
PL_r und Kategorien mit Fehlererkennung	Testfälle, die Fehler simulieren, die vorher analytisch bestimmt werden, zusammen mit der erwarteten Reaktion, um die Eignung der auf der Software beruhenden Maßnahmen zur Fehlerbeherrschung zu bewerten

3.7 Sicheres Programmieren nach EN ISO 13849-1

3.7.10 Dokumentation

Neben dem Resultat eines ausführbaren Codes müssen sämtliche Aktivitäten während des Entwicklungs-Lebenszyklus dokumentiert werden. Werden nachfolgend Änderungen an der SRASW vorgenommen, müssen diese ebenfalls dokumentiert werden. Auch im Bereich der Dokumentation gilt der Grundsatz, dass diese vollständig, verfügbar, lesbar sowie verständlich sein muss. Funktionsbausteine müssen innerhalb des Codes ebenso entsprechend diesen Anforderungen dokumentiert sein. Auch wird gefordert, dass jeder Funktionsbaustein einen Modulkopf enthält, der Informationen wie Funktionsbeschreibung, I/O-Beschreibung, Versionsangabe sowie Angabe einer juristischen Person enthalten muss. Weiterhin ist eine ausreichende Kommentierung des Codes sowie der Deklarationszeilen vorzusehen.

3.7.11 Verifikation

Bei der Verifikation kommt oftmals ein Codereview durch das sogenannte Vier-Augen-Prinzip zum Tragen. Das Vier-Augen-Prinzip bedeutet, dass die Person, die Dokumente oder Code erstellt hat, diesen nicht selbst überprüft, sondern dies durch eine andere kompetente Person durchgeführt wird.

3.7.12 Konfigurationsmanagement

Firmen, die SRASW erstellen, wird ein sogenanntes Konfigurationsmanagement empfohlen. Dabei müssen alle relevanten Dokumente, Softwaremodule, Testergebnisse sowie Werkzeugkonfigurationen die in Bezug auf die Erstellung der SRASW entstanden sind, identifiziert und archiviert werden.

3.7.13 Änderungen

Mit jeder Änderung an der SRASW muss geprüft werden, inwieweit diese Änderung Einfluss auf die Sicherheit und die Anforderungen der EN ISO 13849-1 für die Erstellung von Software hat. Dies bedeutet, dass selbst bei einer Änderung einer SRASW das V-Modell sowie die normativen Vorgaben und Methoden angewendet werden müssen. Weiterhin müssen die Änderungen eindeutig und sauber dokumentiert werden.

3.7.14 Zusammenfassung

Alle Konstrukteure, Entwickler, Programmierer von sicherheitsrelevanter Software sollten einen systematischen Ansatz zur Entwicklung von SRASW verfolgen und sich nicht nur auf die Auswahl der passenden Komponenten (Hardware) beschränken. Software und die darin enthaltenen möglichen Fehler haben einen hohen Anteil an der Qualität der Sicherheit und sollten daher genauso stark berücksichtigt werden wie die richtige Auswahl der Hardwarekomponenten.

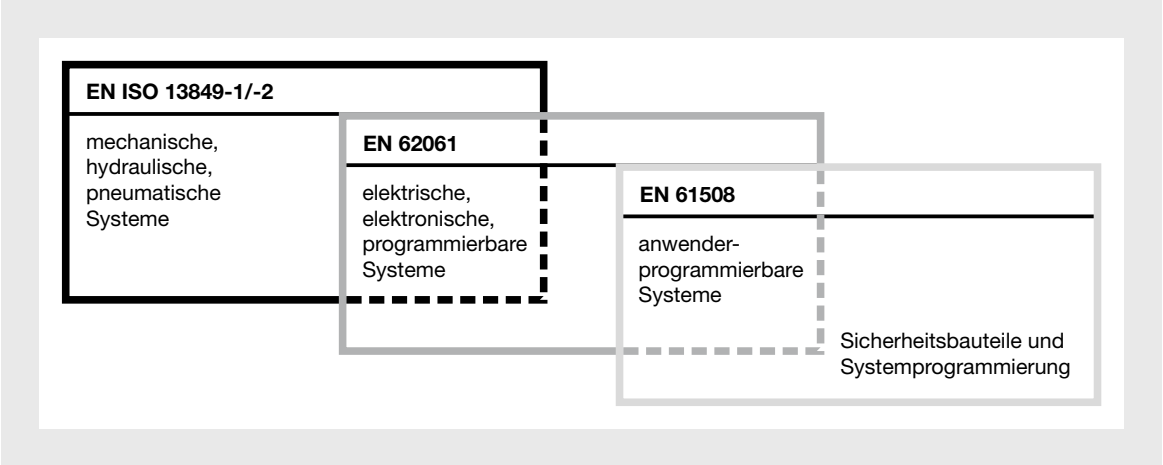
Auch muss das Bewusstsein entstehen, dass die hier beschriebenen Maßnahmen nicht ohne Aufwand herzustellen und anzuwenden sind.

3.8 Validierung

Validierung (von lat. validus: stark, wirksam, gesund) bezeichnet die Prüfung eines Vorhabens oder eines Lösungsansatzes im Hinblick auf eine Aufgabenstellung sowie auf die damit verbundene Lösung eines Problems. Verifizierung beschreibt den Vorgang der Prüfung eines Vorhabens oder eines Lösungsansatzes im Hinblick auf eine zugehörige Spezifikation. Beide Verfahren dienen zusammengefasst dazu, den Eignungsnachweis für einen konkreten Lösungsansatz zu erbringen.

Im Maschinen- und Anlagenbau muss ein Validierungsverfahren den Nachweis führen, dass die Maschine oder Anlage baulich den Anforderungen an ihre bestimmungsgemäße Verwendung entspricht. Im Zuge der Verifizierung werden ferner die Funktionalität der technischen Ausrüstung sowie die sicherheitsbezogenen Teile von Steuerungen geprüft und somit bestätigt, dass diese ihre Funktionen gemäß ihrer Spezifikation sicher erfüllen. Die Dokumentation von Ergebnissen und Lösungen im Rahmen eines Verifizierungs- und Validierungsprozesses stellt sicher, dass das gesteckte Ziel tatsächlich erreicht wurde.

Die harmonisierte Norm EN ISO 12100 mit ihren Grundbegriffen, allgemeinen Gestaltungsleitsätzen, Verfahren zur Beurteilung der Risiken (Analyse und Einschätzung) sowie den Leitsätzen zur Risikobeurteilung und Risikominimierung definiert wichtige Vorgehensweisen sicherheitsrelevanter Systeme bzw. sicherheitsbezogener Teile von Maschinen- und Anlagensteuerungen. Auf Basis dieser grundlegenden Norm beschreiben weitere harmonisierte Normen wie EN ISO 13849-1/-2 sowie EN 61508 mit ihrer Sektornorm EN 62061 (dort hat die Validierung ihren Ursprung) Gestaltung, Aufbau und Integration sicherheitsbezogener Teile von Steuerungen und Schutzeinrichtungen. Im Gegensatz zur EN 62061 beschränkt sich die EN ISO 13849-1/-2 dabei nicht nur auf elektrische Systeme, sondern ist darüber hinaus auch auf mechanische, pneumatische und hydraulische Systeme anwendbar. Beide Normen (EN ISO 13849-1/-2 und EN 62061) legen grundsätzliche Anforderungen für Entwurf und Implementierung sicherheitsbezogener Steuerungssysteme von Maschinen fest und gelten als Nachfolger der nicht mehr relevanten EN 954-1. Bei Verwendung der EN ISO 13849-1 bzw. der EN 62061 ergeben sich Unterschiede bei Konstruktion und Realisierung sicherheitsbezogener Teile von Steuerungen und ihrer anschließenden Bewertung innerhalb des Validierungsprozesses.



Gliederung und Überlappung von Grund- und Sektornormen

3.8 Validierung

3.8.1 Verifikation von Sicherheitsfunktionen nach EN ISO 13849-1/2

Erforderliche Kenndaten: PL, (Steuerungs-)Kategorie, $MTTF_d$, DC, CCF, $B10_d$

Die gestellten Anforderungen bilden die Grundlage des Entwurfs zur Realisierung der Sicherheitsfunktion (Auswahl von Komponenten und Architektur). Die geplanten beteiligten Komponenten werden zu Teil- bzw. Subsystemen zusammengefasst und der damit erreichbare Performance Level (PL) bestimmt. Verifikation der geplanten Sicherheitsfunktion: Erreichter PL ≥ PL_r. Der Validierungsprozess weist die konforme Beschaffenheit und Funktion sicherheitsbezogener Teile von Steuerungen innerhalb der Gesamtspezifikation sowie an Maschinen oder Anlagen nach. Anmerkung: Hilfe bei der Durchführung eines Validierungsverfahrens sowie Möglichkeiten zur Validierung verschiedener technischer Systeme finden sich in der EN ISO 13849-2.

3.8.2 Verifikation von Sicherheitsfunktionen nach EN 62061

Erforderliche Kenndaten: PFH, SIL, $MTTF_d$, DC, CCF, $B10_d$. Auf Basis der formulierten Anforderungen erfolgt der Entwurf zur Realisierung der Sicherheitsfunktion. Diese besteht aus der Auswahl geeigneter Komponenten und dem Aufbau einer schlüssigen Architektur. Die geplanten Komponenten werden zu Teil- oder Subsystemen zusammengefasst und sind Grundlage zur Bestimmung des Safety Integrity Levels (SIL). Verifikation der geplanten Sicherheitsfunktion: Erreichter SIL ≥ erforderlicher SIL.

PL (EN ISO 13849-1)	SIL (EN 62061)
a	-
b	1
c	1
d	2
e	3
-	4

Vergleichstabelle Performance Level (PL) und Safety Integrity Level (SIL)

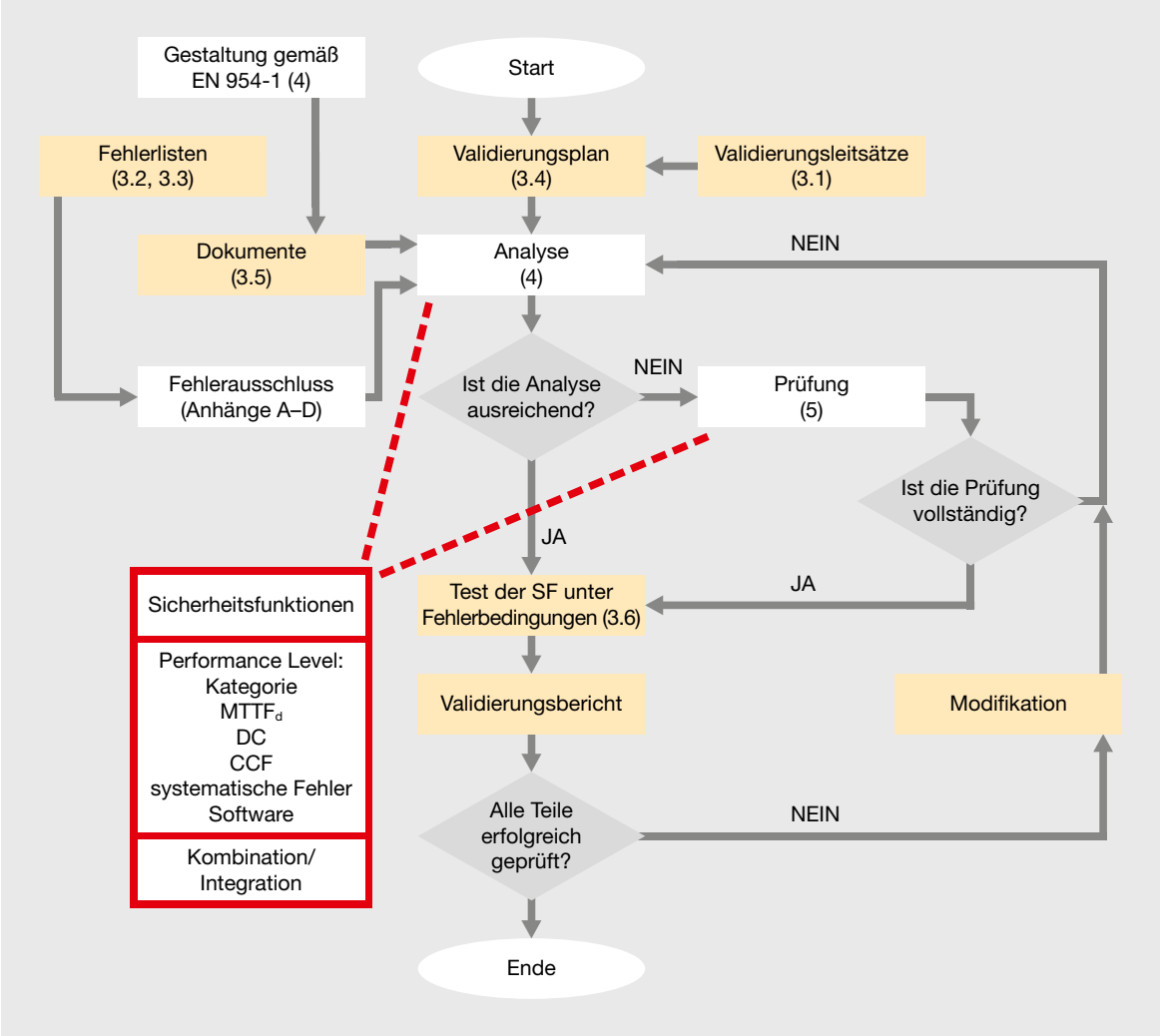
Die Verifikation sicherheitsbezogener Teile von Steuerungen muss aufzeigen, dass die Anforderungen und Vorgaben entsprechend der verwendeten Norm und der sicherheitstechnischen Spezifikation eingehalten werden. Diese Anforderungen beziehen sich konkret auf

- die gemäß Risikobeurteilung und Sicherheitskonzept/-Design festgelegten Eigenschaften einer Sicherheitsfunktion,
- die normenkonforme Architektur der für die Sicherheitsfunktion festgelegten Steuerungskategorie.

Die Verifikation sicherheitsbezogener Teile von Steuerungen besteht aus der Durchführung einer gründlichen Analyse und, falls erforderlich, der Durchführung weiterführender (Funktions-)Prüfungen sowie ggf. Fehlersimulationen. Es empfiehlt sich, mit der Analyse bereits beim Start des Gestaltungsprozesses zu beginnen, um etwaige Fehler und/oder Probleme frühzeitig erkennen und entsprechend handeln zu können.

Die Durchführung von Analyse und Prüfungen ist abhängig von der Größe und Komplexität der Steuerung sowie deren Integration innerhalb der Maschine oder Anlage. Sinnvoll ist es daher, gewisse Analysen oder Prüfungen erst dann vorzunehmen, wenn die Steuerung bereits ein hohes Maß an Gestaltung erreicht hat. Damit eine Analyse neutral verläuft, ist damit eine unabhängige Person oder Stelle zu beauftragen. Zur Durchführung der Validierung ist zunächst ein Validierungsplan zu erstellen, der den Umfang von Analyse und Prüfungen festlegt. Der genaue Umfang sowie die Abwägung zwischen beiden Verfahren hängt stets von der verwendeten Technologie und deren Komplexität ab. Einen schematischen Überblick über das Validierungsverfahren gibt die nachfolgende Abbildung.

3.8 Validierung



Validierungsplan gemäß EN ISO 13849-2

3.8.3 Allgemeines zum Validierungsplan

Der Validierungsplan muss sämtliche Anforderungen beschreiben, die für die Durchführung der Validierung der festgelegten Sicherheitsfunktionen sowie deren Kategorien notwendig sind. Darüber hinaus muss der Validierungsplan Aufschluss über die zur Durchführung der Validierung benutzten Mittel geben. Je nach Komplexität der zu prüfenden Steuerung oder Maschine muss der Validierungsplan Auskunft geben über:

- die Anforderungen zur Durchführung der Validierung
- die Betriebs- und Umgebungsbedingungen
- die grundlegenden und bewährten Sicherheitsprinzipien
- die bewährten Bauteile
- die Fehlerannahmen und Fehlerausschlüsse
- die angewandten Analysen und Prüfungen

Der Validierungsplan enthält darüber hinaus sämtliche Dokumente der Validierung.

3.8 Validierung

3.8.4 Validieren durch Analyse

In erster Linie sind es Analysen, die die sicherheitsbezogenen Teile von Steuerungen validieren. Dabei ist der Beweis zu führen, dass alle von einer Sicherheitsfunktion (SRCF) geforderten Eigenschaften] tatsächlich gegeben sind. Folgende Faktoren fließen in die Analyse mit ein:

- die mit der Maschine in Verbindung stehenden identifizierten Gefährdungen
- die Zuverlässigkeit
- die Systemstruktur
- qualitative, nicht quantifizierbare Aspekte mit Auswirkungen auf das Systemverhalten
- deterministische Argumente wie z. B. Erfahrungswerte, Qualitätsmerkmale und Fehlerraten

Analysetechniken „Top-down“/„Bottom-up“

Bei der Auswahl der Analysetechnik stehen zwei verschiedene Techniken zur Auswahl: die deduktive „Top-down“- und die induktive „Bottom-up“-Methode. Die deduktive „Top-down“-Methode lässt sich in Form einer Fehlerbaumanalyse oder als Ereignisbaumanalyse anwenden. Beispiele für die induktive „Bottom-up“-Methode sind die Fehlerarten- und Auswirkungsanalyse (FMEA) sowie die Fehlerarten-, Auswirkungs- und kritischen Zustandsanalysen (FMECA).

3.8.5 Validieren durch Prüfung

Wenn Validierung durch Analyse nicht ausreichend erscheint, sind weiterführende Prüfungen erforderlich, um die Validierung zu vervollständigen. Weil viele Steuerungen und deren Anforderungen äußerst komplex sind, ist die Durchführung weiterer Prüfungen in den meisten Fällen erforderlich.

Die praktische Prüfung erfordert zunächst einen Prüfplan, der Folgendes umfassen muss:

- die Prüfspezifikationen
- die erwarteten Prüfergebnisse
- die Reihenfolge der einzelnen Prüfungen

Die Prüfungsergebnisse sind anschließend nachvollziehbar zu dokumentieren, das Ergebnisprotokoll muss dabei folgende Mindestangaben enthalten:

- den Namen der prüfenden Person und/oder Stelle
- die zum Zeitpunkt der Prüfung herrschenden Umgebungsbedingungen
- die Vorgehensweise während der Prüfung mit Angabe der Prüf- oder Messmittel

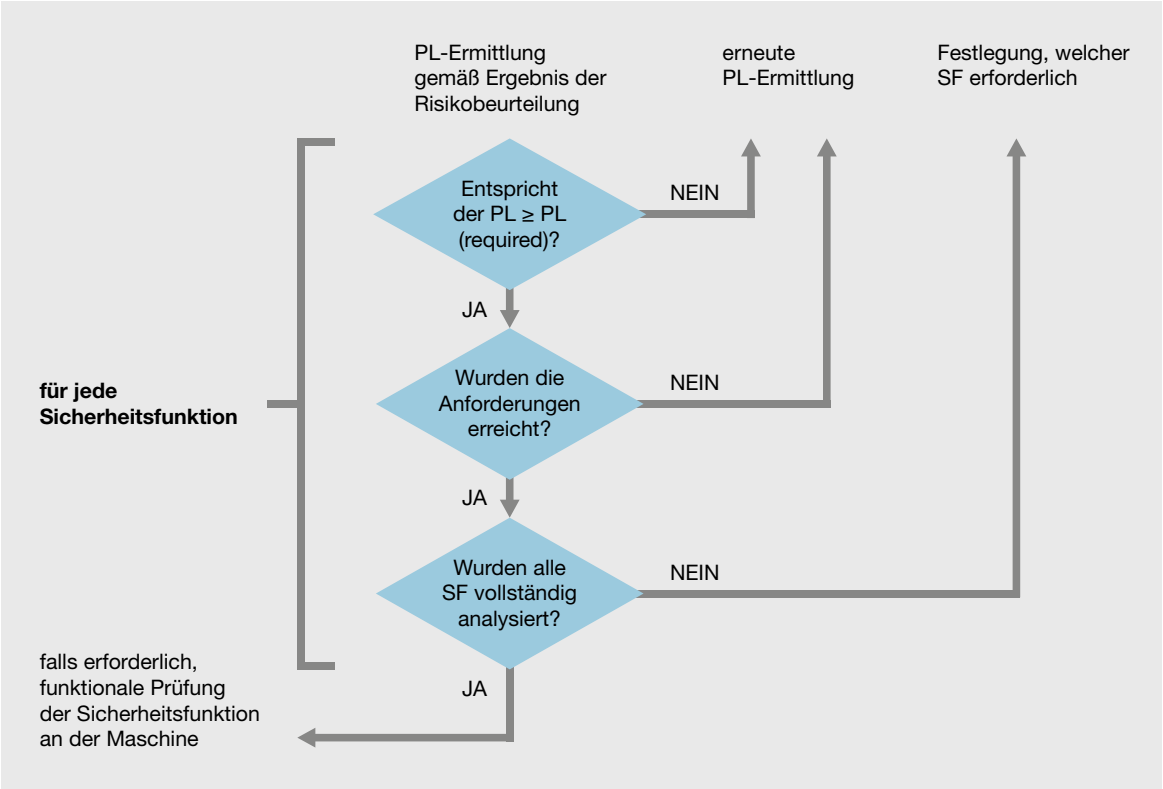
Um nachzuweisen, dass man das angestrebte und festgelegte Schutzziel tatsächlich erreicht hat, werden abschließend die Prüfergebnisse mit den Vorgaben des Prüfplans verglichen.

3.8.6 Verifikation von Sicherheitsfunktionen

Maßgeblicher Bestandteil der Validierung ist die Verifikation der Sicherheitsfunktionen auf ihre Übereinstimmung mit den vorgesehenen Spezifikationen, Funktionen sowie mit den Steuerungskategorien und Architekturen. Von Bedeutung ist dabei, die festgelegten SRCFs in allen Betriebsarten der Maschine/Anlage zu validieren. Neben der grundlegenden Validierung einer jeden Sicherheitsfunktion spielt auch die Validierung des PL und/oder des SIL-Wertes innerhalb der Sicherheitsfunktion eine wichtige Rolle. Folgende Schritte sind bei der Verifikation des erreichten PL einer Sicherheitsfunktion erforderlich:

- Validieren der Steuerungskategorie
- Validieren der $MTTF_d$-Werte
- Validieren der DC-Werte
- Validieren der Maßnahmen gegen Fehler gemeinsamer Ursache/CCF
- Validieren der Maßnahmen gegen systematische Ausfälle

3.8 Validierung



Ablaufschema Verifikation und Validierung (Quelle: Schulungsmaterialien Pilz)

Da es sich bei der Validierung von Sicherheitsfunktionen um ein recht aufwendiges Verfahren handelt, empfiehlt sich in diesem Fall die Zuhilfenahme eines Software-Tools (z. B. PAScal), das bei der Berechnung geplanter und/oder realisierter Sicherheitsfunktionen unterstützt. Auf der Grundlage sicherheitsrelevanter Kennwerte der geplanten bzw. verwendeten Komponenten validieren diese Berechnungs-Tools die tatsächlich erreichten Werte einschließlich der geforderten oder verlangten Vorgabewerte PL_r bzw. SIL. Der Vorteil softwarebasierter Tools ist die schrittweise Führung durch die einzelnen Teilschritte der Validierung von Sicherheitsfunktionen. Die Möglichkeit der grafischen Modellierung von Sicherheitsfunktionen innerhalb des Tools gibt dem Prüfer zusätzliche Sicherheit bei der Berechnung und trägt zur besseren Nachvollziehbarkeit der Ergebnisse bei.

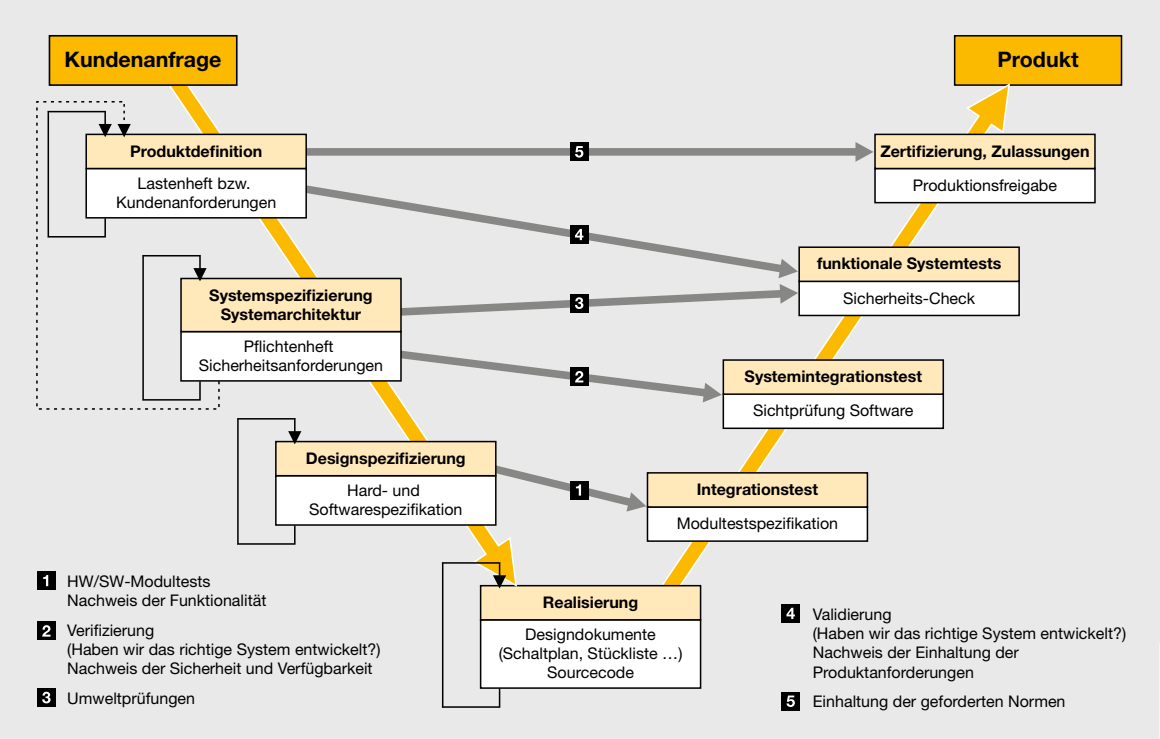
3.8 Validierung

3.8.7 Validierung von Software

Die Bestimmungen in den Normen EN 62061 und EN ISO 13849-1/-2 erlauben, sicherheitsbezogene Software im Maschinensektor für alle Performance Level bzw. Safety Integrity Level zu entwickeln. Software übernimmt damit eine hohe Verantwortung und bestimmt zu einem wesentlichen Teil die Qualität der zu realisierenden Sicherheitsfunktion. Es ist daher überaus wichtig, lesbare, verständliche, test- und wartbare Software zu erstellen. Um die Qualität der Software sicherzustellen, unterliegt auch diese einem Validierungsprozess, der die Entwicklung begleitet. Grundlagen hierfür sind:

- Arbeiten nach dem V-Modell (Entwicklungslebenszyklus inkl. Verifikation und Validierung)
- Dokumentation von Spezifikation und Entwurf
- modulare und strukturierte Programmierung
- Durchführung funktionaler Tests
- geeignete Entwicklungsaktivitäten nach Änderungen oder Anpassungen

Um zu bestätigen, dass die Software der Spezifikation der Sicherheitsanforderungen entspricht, wird auch in diesem Fall ein entsprechender Bericht verfasst, der Bestandteil des Validierungsberichts der Maschine oder Anlage wird. Wie auch bei der Validierung von Sicherheitsfunktionen sollte die Validierung der Software nicht der Programmierer selbst, sondern eine neutrale Person durchführen.



V-Modell Pilz GmbH & Co. KG für Engineering-Projekte

3.8 Validierung

Zum Entwickeln und Programmieren sicherheitsgerichteter Software sind heute sehr gute bereits zertifizierte Software-Tools zur jeweiligen Sicherheitssteuerung erhältlich. Die Verwendung der Software-Tools vereinfacht zudem den gesamten Validierungsprozess, da die in der Software enthaltenen Bausteine grundsätzlich bereits zertifiziert und gleichzeitig validiert sind. Je mehr dieser Software-Bausteine in einer Applikation Verwendung finden, desto geringer ist der zu leistende Validierungsaufwand. Ebenso verhält es sich bei der Verwendung parametrierbarer Anwender-Software, auch hier sind die enthaltenen Bausteine bereits validiert. Ob die Sicherheitsfunktionen dann auch gemäß ihrer Spezifikation funktionieren, müssen die anschließenden funktionalen Testreihen nachweisen. Diese beinhalten auch die Simulation anzunehmender Fehler.

3.8.8 Validieren der Widerstandsfähigkeit gegenüber Umgebungsanforderungen

Bei der Festlegung der Leistungsfähigkeit von sicherheitsbezogenen Teilen von Steuerungen spielen die Umgebungsbedingungen, d. h. der Umgebungsort, die Art und Weise der späteren Verwendung der Steuerung bzw. des Systems eine erhebliche Rolle. Relevante Stichworte hier sind u. a. Wasserdichtigkeit und Vibrationsschutz. Die Validierung des Systems muss deshalb über die Analyse erfolgen. Konkret muss die Analyse darstellen, dass die Steuerung bzw. das System über eine mechanische Haltbarkeit verfügen, die den vielfältigen Beanspruchungen durch Umgebungseinflüsse wie Schock, Vibration und dem Eindringen von Stäuben und Flüssigkeiten standhalten kann. Dabei müssen die sicherheitsbezogenen Teile von Steuerungen ihren sicheren Zustand unter allen Umständen beibehalten. Daher sind im Zuge der Analyse auch Faktoren wie Temperatur, Feuchte sowie die elektromagnetische Verträglichkeit zu berücksichtigen.

3.8.9 Erstellen des Validierungsberichts

Abschließend und nach der Durchführung aller Verifikations- und Validierungsschritte steht die Erstellung des Validierungsberichts. Dieser enthält in nachvollziehbarer Form alle Angaben zu den durchgeführten Analysen und Prüfungen – und zwar hard- wie softwareseitig. Dabei sind Querverweise auf andere Dokumente zulässig, sofern sie nachvollziehbar und identifizierbar sind. Auch jene sicherheitsbezogenen Teile von Steuerungen, die das Validierungsverfahren nicht bestanden haben, sind unter Hinzufügung derjenigen Faktoren, die zum Ausschluss geführt haben, zu benennen.

3.8.10 Fazit

Wartung und Instandhaltung/periodische Tests

Der Zahn der Zeit nagt selbstverständlich auch an der Leistungsfähigkeit sicherheitsbezogener Steuerungen. Verschleiß, Korrosion und dauerhafte (mechanische) Beanspruchungen führen zu einer Verringerung der Sicherheit, im Extremfall sogar zu gefahrbringenden Ausfällen von Steuerungsteilen oder gar der gesamten Steuerung. Deshalb ist es notwendig, die sicherheitsbezogenen Teile von Steuerungen in regelmäßigen Abständen zu warten und periodische Tests zur Prüfung der funktionalen Sicherheit durchzuführen. Ein Wartungs- und Instandhaltungsplan wie auch Prüfprotokolle der periodischen Tests sollten in Schriftform vorliegen. Die Durchführung der Funktionsprüfungen muss eine fachkundige Person vornehmen. Art, Umfang und Frequenz der periodischen Tests sind, basierend auf der Gefährdungsbeurteilung gemäß §3 der Betriebssicherheitsverordnung, durch den Betreiber einer Maschine oder Anlage festzulegen. Details zum Thema „Betriebssicherheitsverordnung“ und nähere Informationen zu unseren Dienstleistungen finden Sie auf www.pilz.com.

3.8 Validierung

3.8.11 Anhang

In der Folge ist von grundlegenden und bewährten Sicherheitsprinzipien sowie von Sicherheitsbauteilen und Fehlerausschlüssen die Rede. Die folgenden Tabellen entsprechen den normativen Vorgaben der EN ISO 13849-1 und EN ISO 13849-2 und bieten einen kurzen Überblick über die sicherheitstechnischen Aspekte.

Grundlegende Sicherheitsprinzipien nach EN ISO 13849-1/EN ISO 13849-2

Eigenschaften grundlegender Sicherheitsprinzipien können sein:

- die Anwendung geeigneter Werkstoffe und Herstellungsverfahren unter Berücksichtigung von Haltbarkeit, Festigkeit, Elastizität und Verschleiß
- die richtige Dimensionierung und Formgebung, unter Berücksichtigung von Spannungen und Dehnungen
- druckbegrenzende Maßnahmen, wie z. B. Druckregelventile und Drosseln
- geschwindigkeitsbegrenzende Maßnahmen

Eine Auflistung der grundlegenden Sicherheitsprinzipien, die mechanische, hydraulische, pneumatische und elektrische bzw. elektronische Systeme betreffen, findet sich in den Anhängen A–D der EN ISO 13849-2.

Bewährte Sicherheitsprinzipien nach EN ISO 13849-1/EN ISO 13849-2

Eigenschaften bewährter Sicherheitsprinzipien sind zum Beispiel:

- die Vermeidung von Fehlern, z. B. durch die gesicherte Position beweglicher Elemente von Bauteilen
- die Verringerung der Fehlerwahrscheinlichkeit, z. B. durch Überdimensionierung von Bauteilen
- die Festlegung der Ausfallrichtung, z. B. durch elektrische Zwangstrennung/ zwangsöffnende Kontakte
- die Verringerung der Fehlerwirkung, z. B. durch Vervielfachung von Bauteilen

Eine Auflistung bewährter Sicherheitsprinzipien für mechanische, hydraulische, pneumatische und elektrische/elektronische Systeme findet sich in den Anhängen A–D der EN ISO 13849-2.

Bewährte Bauteile nach EN ISO 13849-1/EN ISO 13849-2

Ein Bauteil kann als bewährtes Bauteil angesehen werden, wenn es

- in einer Vielzahl von Applikationen und Anwendungen erfolgreich eingesetzt wurde,
- nach Prinzipien hergestellt wurde, die die Eignung und Zuverlässigkeit des Bauteils dokumentieren.

Eine Auflistung von vornherein bewährten Bauteilen für mechanische Systeme, so z. B. Schrauben, Federn und Nocken sowie Bauteile für elektrische Systeme wie z. B. Schütze und Relais findet sich in den Anhängen A–D der EN ISO 13849-2. Für pneumatische und hydraulische Systeme sind derzeit keine bewährten Bauteile gelistet.

Fehlerausschlüsse nach EN ISO 13849-2

Die Erfordernisse bei der Verwendung eines Fehlerausschlusses sind grundsätzlich im Validierungsplan anzugeben. Wichtig ist, dass jeder Fehlerausschluss mit einer sinnvollen nachvollziehbaren Erklärung zu rechtfertigen ist. Die Anhänge A–D der EN ISO 13849-2 geben einen Überblick über mögliche Fehlerausschlüsse, bezogen auf ihre Fehlerannahme. Diese können z. B. sein:

- Bruch durch Überdimensionierung bei mechanischen Systemen
- selbsttätige Verstellung durch Sicherung bei pneumatischen Systemen
- Veränderung von Schaltzeiten durch Zwangsbetätigung bei hydraulischen Systemen
- Kurzschlüsse zwischen Leitern durch Isolation und Verlegung bei elektrischen/elektronischen Systemen

3.8 Validierung

Was kann Pilz für Sie tun?

Pilz GmbH & Co. KG bietet ein breites Spektrum an Dienstleistungen, darunter u. a. die Validierung im Maschinen- und Anlagenlebenszyklus. Eine Spiegelung der Risikobeurteilung und des Sicherheitskonzepts passt die erarbeiteten Lösungen den tatsächlichen Anforderungen in der Systemintegration an. Auf die Validierung durch Pilz folgt eine objektive und systematische Nachbetrachtung der umgesetzten Maßnahmen, Nachberechnung der technischen Schutzmaßnahmen und die Durchführung von Funktionstests. Selbstverständlich werden dabei sämtliche gültigen Sicherheitsnormen und -richtlinien eingehalten. Mit ihrer umfassenden Erfahrung in der Validierung von Maschinen haben die Ingenieure von Pilz strukturierte Methoden für die Inspektion sicherheitskritischer Elemente von Maschinen und Anlagen entwickelt. Das Berechnungstool PAScal unterstützt bei der Verifikation des erreichten Performance Levels der jeweiligen Sicherheitsfunktion.

Validierung durch Pilz umfasst:

- Spiegelung der Anforderungen aus Risikobeurteilung und Sicherheitskonzept
- Verifikation des erreichten Performance Levels nach EN ISO 13849-1/EN IEC 62061 anhand des Berechnungstools PAScal, Sistema etc.
- Verifikation der Betriebsanleitung
- Durchführung einer Funktionsprüfung und Fehlersimulation (Safety Check)
- Test der sicherheitsrelevanten Soft- und Hardwarefunktionen
- Prüfung der Sensor- und Aktortechnologie sowie ihrer Verdrahtung
- Durchführung von Messungen (Schutzleiter, Schallpegel etc.)
- Erstellung eines Prüfberichts mit ausführlichen Angaben zu den Ergebnissen
- Übernahme der Verantwortung als „Bevollmächtigter“ durch Unterzeichnung der EG-Konformitätserklärung

Ihre Vorteile bei einer Validierung durch Pilz

- qualifizierte Methoden beim Konformitätsbewertungsverfahren
- Berücksichtigung aller relevanten Aspekte bei der Validierung und CE-Kennzeichnung
- Unterstützung durch die Sicherheitsexperten der Firma Pilz

Vervollständigen Sie mit der CE-Kennzeichnung Ihren gesamten Sicherheitsprozess

Um den Sicherheits-Lebenszyklus Ihrer Maschine zu vervollständigen, bietet Pilz die CE-Kennzeichnung als abschließende Dienstleistung an. Dabei übernimmt Pilz den kompletten Konformitätsbewertungsprozess für Sie und gleichzeitig die Verantwortung für das gesamte Verfahren. Per Unterschrift bestätigt Pilz als Bevollmächtigter auf der EG-Konformitätserklärung, dass die Anforderungen den Richtlinien entsprechend eingehalten wurden. Sie erhalten damit den für Ihre Maschine erforderlichen „Reisepass“ für den gesamten europäischen Binnenmarkt.

Wer seine Maschine oder Anlage dauerhaft sicher betreiben will, muss regelmäßige Überprüfungen bzw. Wissens-Updates bezüglich Normen, Richtlinien und Produktentwicklungen vornehmen. Die ordnungsgemäße Beschaffenheit und Montage sowie die regelmäßige Überprüfung von berührungslos wirkenden Schutzeinrichtungen (zum Beispiel Lichtgitter, Lichtschranken, Scanner etc.) sind aufgrund der Betriebssicherheitsverordnung (BetrSichV) unerlässlich. Die Verantwortung hierfür liegt in vollem Umfang beim Betreiber.

Durch regelmäßige Inspektionen sind Sie auf der sicheren Seite

Eine unabhängige Inspektionsstelle, akkreditiert durch die DAkkS (Deutsche Akkreditierungsstelle) gemäß DIN EN ISO 17020, garantiert Objektivität, hohe Verfügbarkeit Ihrer Maschinen und Anlagen sowie größtmögliche Sicherheit für Ihre Mitarbeiter.

Am Ende des Verfahrens händigt Pilz den Inspektionsbericht aus und bespricht sämtliche Ergebnisse mit Ihnen. Nach bestandener Prüfung erhält die Anlage die Prüfplakette von Pilz.

3.9 Zertifizierung und Akkreditierung

Immer mehr Kunden betrachten Zertifikate oder Dienstleister, die durch Dritte zertifiziert wurden, als Garanten für Qualität. Grundsätzlich jedoch sind Zertifikate rechtlich unverbindlich und können praktisch von jedermann ausgestellt werden. Sie sind nur ein Hinweis darauf, dass ein Dritter geprüft hat, dass bestimmte Arbeitsabläufe nach entsprechenden Vorgaben ausgeführt werden. Die Zertifikate sagen dabei noch nichts über die Qualität dieser Prüfung durch Dritte aus. Es ist daher wichtig, die Kompetenz des zertifizierenden Unternehmens genau zu kennen oder ggf. zu hinterfragen.

Anders verhält es sich bei akkreditierten Unternehmen: Akkreditierungen sind rechtsverbindlich und können nur von staatlichen Stellen ausgestellt werden. Durch eine Akkreditierung bestätigt die staatliche Akkreditierungsstelle dem Unternehmen oder der Institution die Kompetenz, bestimmte Konformitätsbewertungsaufgaben durchzuführen. Eine Konformitätsbewertung ist ein Verfahren, bei dem überprüft wird, ob bestimmte Vorgaben definitions- oder zielgemäß erfüllt werden. Stellen akkreditierte Unternehmen oder Institutionen Zertifikate aus, darf man als Kunde davon ausgehen, dass sie die entsprechende Kompetenz dazu besitzen.

3.9.1 Akkreditierung: Qualitätssiegel für Kunden

Akkreditierte Konformitätsbewertungsstellen, auch kurz akkreditierte Stellen genannt, sind in der Regel Institutionen wie Prüf-, Kalibrierlaboratorien, Inspektions- oder Zertifizierungsstellen. Diese stellen Dienstleistungen wie Prüfungen, Inspektionen, Zertifizierungen z. B. von Managementsystemen, Personen und Produkten bereit, um die Konformität von Produkten, Anlagen oder Managementsystemen zu bewerten. Die Bewertung erfolgt dabei üblicherweise im Rahmen eines Prüfungsverfahrens, das nachweisen muss, dass bestimmte Anforderungen, wie sie in Normen gelistet sind, erfüllt werden.

In Europa ist die Akkreditierung rechtlich einheitlich durch die Akkreditierungsrichtlinie 765/2008/EG geregelt. Alle Mitgliedstaaten sind seit 01.01.2010 verpflichtet, genau eine staatliche Akkreditierungsstelle zu unterhalten. Diese akkreditiert die Konformitätsbewertungsstellen und bewertet sie in regelmäßigen Abständen durch Audits, um die kontinuierliche Einhaltung der Anforderungen sicherzustellen. Bei der Akkreditierung werden u. a. die Unabhängigkeit der Organisation, das Qualitätsmanagement, die Ausbildung der Mitarbeiter, die Verwaltung kalibrierter Messgeräte, die Durchführungsanweisungen sowie die Handhabung von Aufzeichnungen und Prüfberichten auf ihre Konformität mit der jeweiligen EN/ISO-Norm geprüft. Die staatlichen Akkreditierungsstellen überprüfen und bewerten darüber hinaus die praktische Umsetzung der Zertifizierungsaufgaben vor Ort. Die Akkreditierung ist für die akkreditierte Institution und deren Kunden gleichermaßen von Vorteil: Gegenüber den Kunden macht sie deutlich, dass die Institution ihre Arbeit korrekt und den Normen entsprechend ausführt. Gleichzeitig erhalten die Kunden einen Bewertungsmaßstab für die Kompetenz der prüfenden Organisation.

In aller Regel arbeiten die Organisationen getrennt von anderen und erhalten selten, wenn überhaupt, eine unabhängige technische Bewertung ihrer Leistungen. Eine regelmäßige Begutachtung durch eine Akkreditierungsstelle überprüft sämtliche Tätigkeitsaspekte einer Einrichtung in Bezug auf die fortlaufende Erstellung präziser und verlässlicher Daten. Die Akkreditierungsstelle identifiziert und erörtert verbesserungswürdige Bereiche, am Ende der Begutachtung steht ein ausführlicher Bericht. Sofern erforderlich, überwacht die Akkreditierungsstelle die nachfolgenden Tätigkeiten. Das Unternehmen kann also sicher sein, angemessene Korrekturmaßnahmen getroffen zu haben.

3.9 Zertifizierung und Akkreditierung

Einige Beispiele für Akkreditierungsstellen in Europa

3.9 Zertifizierung und Akkreditierung

Für Deutschland zuständig ist die Deutsche Akkreditierungsstelle GmbH* (DAkkS), die vom Bundesministerium für Wirtschaft gegründet wurde. Alle vorherigen Akkreditierungsstellen (DACH, DAP, TGA/DATECH und DKD) gingen Anfang 2010 in der DAkkS auf.

* Für Österreich: bmwfi, für die Schweiz: Schweizerische Akkreditierungsstelle SAS

Zusammenführung der deutschen Akkreditierungsstellen zur DAkkS

Weiterhin genießt die Akkreditierung aufgrund der Vereinbarungen der DAkkS mit der International Laboratory Accreditation Cooperation (ILAC), des International Accreditation Forum (IAF) und der European Co-operation for Accreditation (EA) weltweite Anerkennung.

Internationale Anerkennung der DAkkS

MRA = Mutual Recognition Agreement
MLA = Multilateral Recognition Arrangement

3.9 Zertifizierung und Akkreditierung

Diese Vereinbarungen stellen sicher, dass weltweit alle akkreditierten Stellen über ein einheitliches Kompetenzniveau verfügen und die durchgeführten Dienstleistungen höchsten Qualitätsansprüchen gerecht werden. Die Akkreditierung wird sowohl national als auch international als ein hoch anerkannter Indikator für technische Kompetenz angesehen. Viele Industriebereiche fordern routinemäßig eine Akkreditierung für Anbieter von Prüfdienstleistungen.

Im Gegensatz zur Zertifizierung z. B. nach ISO 9001 verwendet die Akkreditierung Kriterien und Verfahren, die speziell entwickelt wurden, um die technische Kompetenz festzustellen. Sie garantiert Kunden somit, dass die durch Laboratoriums- oder Inspektionsdienstleister bereitgestellten Prüf-, Kalibrier- oder Messdaten präzise und zuverlässig sind. Erkennbar sind akkreditierte Stellen am Symbol der entsprechenden Akkreditierungsstelle, das sich üblicherweise auf Prüf- oder Kalibrierberichten wiederfindet. Eine Liste der in Deutschland akkreditierten Stellen findet man unter www.dakks.de.

Beispiel DAkkS-Logo der Pilz Inspektionsstelle

3.9.2 Akkreditierung oder Zertifizierung

Die Akkreditierung verwendet Kriterien und Verfahren, die speziell entwickelt wurden, um die technische Kompetenz zu bestimmen. Technische Fachbegutachter führen eine gründliche Bewertung aller Faktoren in einer Organisation durch, die einen Einfluss auf die Erzeugung von Prüf- oder Kalibrierdaten haben. Die Kriterien basieren auf den internationalen Normen wie ISO/IEC 17020, ISO/IEC 17025 oder ISO 15189, die weltweit bei der Bewertung von akkreditierten Organisationen Verwendung finden. Akkreditierungsstellen verwenden diese Norm insbesondere, um jene Faktoren zu begutachten, die für die technische Kompetenz maßgeblich sind, wie beispielsweise:

- technische Kompetenz der Mitarbeiter
- Gültigkeit und Angemessenheit von Prüfmethoden
- Rückführung von Messungen und Kalibrierungen auf nationale Normen
- Eignung, Kalibrierung und Wartung der Prüfeinrichtung
- Prüfumgebung
- Probenahme, Handhabung und Transport von Prüfgegenständen
- Qualitätssicherung von Prüf- und Kalibrierdaten

Mit diesem Vorgang versichert die Akkreditierung den Organisationen und deren Kunden, dass die Prüf- und Kalibrierdaten ihrer akkreditierten Stelle präzise und zuverlässig sind.

Eine Zertifizierung beispielsweise nach dem ISO-9001-Standard ist bei Hersteller- und Serviceorganisationen weit verbreitet. Sie drücken damit aus, dass ihre Produkte, Dienstleistungen und Abläufe den geforderten Qualitätsstandards entsprechen. So zielt z. B. die Zertifizierung des Qualitätsmanagementsystems einer Organisation nach ISO 9001 darauf ab, die Übereinstimmung des Managementsystems mit dieser Norm zu bestätigen. Obwohl auch Laboratorien und Inspektionsstellen nach ISO 9001 zertifiziert werden können, liefert eine solche Zertifizierung im Gegensatz zur Akkreditierung keine Aussage zu deren technischer Kompetenz.

3.9 Zertifizierung und Akkreditierung

3.9.3 Prüfungen gemäß BetrSichV und Akkreditierung

Alle Arbeitgeber in Europa sind rechtlich verpflichtet, ihren Arbeitnehmern ausschließlich sichere Arbeitsmittel zur Verfügung zu stellen. In Deutschland ist dies spätestens seit Oktober 2002 durch die Betriebssicherheitsverordnung* geregelt. Diese Verordnung ist eine verpflichtende Umsetzung der von der EU bereits im Jahr 1989 erlassenen und mittlerweile neu gefassten Arbeitsmittelbenutzungsrichtlinie 2009/104/EG.

* in Österreich: Arbeitsmittelverordnung;
in der Schweiz: UVG-Bundesgesetz

Der Arbeitgeber ist verpflichtet, diese Forderung beim erstmaligen Gebrauch des jeweiligen Arbeitsmittels und anschließend regelmäßig durch Prüfungen sicherzustellen. Hierbei muss er die Prüfabstände unter Berücksichtigung der gesetzlichen Vorgaben selbst festlegen. Er muss daneben sicherstellen, dass diese Prüfungen nur von „befähigten Personen“ durchgeführt werden. Welche Anforderungen eine „befähigte Person“ erfüllen muss, regelt die TRBS 1203. Grundsätzlich müssen eine Berufsausbildung sowie eine gewisse Berufserfahrung, eine zeitnahe berufliche Tätigkeit und entsprechende regelmäßige Weiterbildungen auf dem zu prüfenden Gebiet vorliegen. Ein Arbeitgeber ist in seiner Entscheidung frei, welchen Mitarbeiter er zur „befähigten Person“ ernennt. Er muss sich lediglich von dessen Kompetenz überzeugen und diese im Rechtsfalle nachweisen können.

Alternativ kann ein Unternehmen diese Prüfungen auch bei einem externen Dienstleister einkaufen. Dies entbindet ihn jedoch nicht von der Pflicht, die Kompetenz des ausführenden Unternehmens zu prüfen. Im Gegensatz zu zertifizierten Unternehmen erweisen sich hierbei akkreditierte Stellen als besonders hilfreich, da nur die Akkreditierung eine rechtlich verbindliche Kompetenzaussage solcher Stellen trifft und der Nachweispflicht damit Genüge getan ist.

So verfügt Pilz GmbH & Co. KG über eine solche akkreditierte Inspektionsstelle, die im Auftrag von Unternehmen Prüfungen von Schutzeinrichtungen an Maschinen und Anlagen übernimmt. Aufgrund der Akkreditierung sind die Dienstleistungen weltweit anerkannt. Die Inspektionsstelle greift dabei auf qualifizierte Inspekteure in Deutschland sowie in anderen EU-Mitgliedsstaaten zurück. Pilz kann diese Dienstleistungen somit innerhalb der EU, aber auch weltweit anbieten. Im Jahr 2015 hat die Deutsche Akkreditierungsstelle (DAkkS) diese Akkreditierung erneuert. Dies bringt zum Ausdruck, dass Pilz sämtliche Anforderungen der EN ISO/IEC 17020:2012 für eine Inspektionsstelle Typ C im Bereich Maschinen und Anlagen erfüllt und die Kompetenz besitzt, die vordefinierten Konformitätsbewertungsaufgaben durchzuführen. Pilz kann selbst sehr aufwendige Überprüfungen übernehmen. Die Inspektionsstelle bietet hier insbesondere folgende Leistungen an:

Beispiel Umsetzung der EU-Arbeitsmittelbenutzerrichtlinie

3.9 Zertifizierung und Akkreditierung

- Inspektionen von berührungslos wirkenden Schutzeinrichtungen (Lichtvorhänge, Scanner, sichere Kamerasysteme)
- Nachlaufmessung zur Bestätigung der vorgegebenen Sicherheitsabstände
- Inspektionen von weiteren Sicherheits-einrichtungen (Not-Halt, Schutztüren, 2-Hand)
- Verifizierung der Einhaltung der Mindest-vorschriften der Betriebssicherheitsverordnung
- Verifizierung der Einhaltung der Mindest-anforderungen der Maschinenrichtlinie (CE)

Wählt der Kunde eine akkreditierte Inspektionsstelle, die seinen Prüf-, oder Messbedarf erfüllt, so kann er sicher sein, dass die Inspektionsstelle präzise und zuverlässige Ergebnisse anbieten kann.
Die technische Kompetenz einer Inspektionsstelle hängt von Faktoren ab wie:

- Qualifikation, Schulung, Erfahrung des Personals
- richtige Ausrüstung, korrekt kalibriert und gewartet
- angemessene Qualitätssicherungsverfahren
- entsprechende Prüfverfahren
- validierte Prüfmethoden
- Rückführung der Inspektionen auf nationale Normen
- genaue Verfahren zur Aufzeichnung und Berichterstattung
- geeignete Prüfeinrichtungen

Alle diese Faktoren tragen dazu bei, dass eine akkreditierte Inspektionsstelle technisch kompetent und in der Lage ist, die angebotenen Prüfungen auszuführen.

3.9.4 Fazit

Grundsätzlich steht es jedem Unternehmen frei, seine Arbeitsmittel durch eigene Mitarbeiter prüfen zu lassen oder ein externes Unternehmen damit zu beauftragen. In jedem Fall aber muss die prüfende Person dazu befähigt sein. Fällt die Wahl auf einen eigenen Mitarbeiter, kann der Unternehmer dessen Kompetenz in aller Regel beurteilen. Entscheidet er sich für einen externen Dienstleister, muss er sich auf schriftliche Nachweise verlassen. Zertifikate sind dabei in aller Regel nicht hinreichend aussage-kräftig, bei Rechtsstreitigkeiten halten sie den formellen Anforderungen meist nicht stand. Hingegen bieten Akkreditierungen für die ent-sprechenden Dienstleistungen eine zuverlässige rechtliche Sicherheit.

Informative Links:

- DAkkS: http://www.dakks.de
- EA: http://www.european-accreditation.org
- ILAC: http://www.ilac.org

4

Schutz-einrichtungen

4 Schutzeinrichtungen

4 Schutzeinrichtungen

4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen 4-3

4.1.1 Normen für trennende Schutzeinrichtungen 4-7

4.1.2 Normen für die Dimensionierung trennender Schutzeinrichtungen 4-7

4.1.3 Normen zur Gestaltung nicht trennender oder berührungslos wirkender Schutzeinrichtungen 4-7

4.2 Trennende Schutzeinrichtungen 4-8

4.2.1 Feststehende trennende Schutzeinrichtungen 4-8

4.2.2 Beweglich trennende Schutzeinrichtungen 4-9

4.2.3 Weitere Aspekte zur Gestaltung von Schutzeinrichtungen 4-11

4.3 Nicht trennende Schutzeinrichtungen 4-16

4.3.1 Aktive optoelektronische Schutzeinrichtungen 4-16

4.3.2 Weitere wichtige Aspekte im Zusammenhang mit berührungslos wirkenden Schutzeinrichtungen 4-18

4.3.3 Andere sensorisch wirkende Schutzeinrichtungen 4-19

4.4 Manipulation von Schutzeinrichtungen 4-22

4.4.1 Zur Rechtslage 4-22

4.4.2 Sicherheitswidriges Verhalten – was steckt dahinter? 4-24

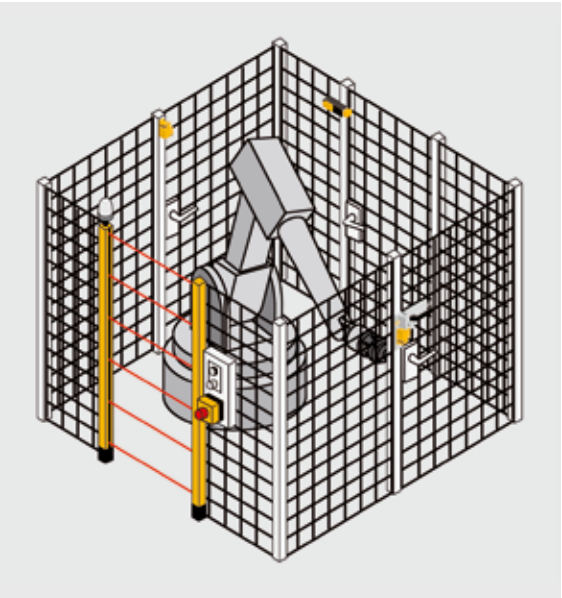
4.4.3 Was können Konstrukteure tun? 4-26

4.4.4 Benutzerfreundliche trennende Schutzeinrichtungen 4-27

4.4.5 Schlussbetrachtung 4-29

4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen

Schutzeinrichtungen sind erforderlich, um Menschen so weit als möglich vor Gefahren zu schützen, die eine Maschine im Betrieb hervorrufen kann. In erster Linie sind dies Zäune oder Barrieren, die den Zugang zur Maschine physikalisch erschweren. Doch mitunter ist es nicht möglich oder auch nicht sinnvoll, solche festen Schutzeinrichtungen zu wählen. Dann fällt die Wahl auf steuerungstechnische Lösungen, die bei Annäherung eines Menschen an eine Gefahrenquelle die Maschine oder einen Teil der Maschine abschalten oder auf andere Weise in einen sicheren Zustand versetzen. Scheidet auch diese Art des Schutzes vor Gefahren aus oder verbleiben trotz Anwendung der genannten Maßnahmen dennoch Gefahrenpotenziale, bleibt als letzte Möglichkeit die hinweisende Sicherheitstechnik: Dabei wird zum Beispiel in der Betriebsanleitung oder an der Maschine auf Restgefahren hingewiesen.



Trennende Barrieren und Sicherheitseinrichtungen schützen vor Gefahren.

4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen

Zum Thema Schutzeinrichtungen an Maschinen existieren umfangreiche Vorschriften. Nachfolgend zunächst die gesetzlichen Vorschriften der europäischen Richtlinie 2006/42/EG.

Maschinenrichtlinie (2006/42/EG)

1.4. Anforderungen an Schutzeinrichtungen

1.4.1. Allgemeine Anforderungen

Trennende und nichttrennende Schutzeinrichtungen

- *müssen stabil gebaut sein,*
- *müssen sicher in Position gehalten werden*
- *dürfen keine zusätzlichen Gefährdungen verursachen,*
- *dürfen nicht auf einfache Weise umgangen oder unwirksam gemacht werden können,*
- *müssen ausreichend Abstand zum Gefahrenbereich haben,*
- *dürfen die Beobachtung des Arbeitsvorgangs nicht mehr als unvermeidbar einschränken und*
- *müssen die für das Einsetzen und/oder den Wechsel der Werkzeuge und zu Wartungszwecken erforderlichen Eingriffe möglichst ohne Abnahme oder Außerbetriebnahme der Schutzeinrichtungen zulassen, wobei der Zugang ausschließlich auf den für die Arbeit notwendigen Bereich beschränkt sein muss,*
- *müssen trennende Schutzeinrichtungen nach Möglichkeit vor einem Herausschleudern oder Herabfallen von Werkstoffen und Gegenständen sowie vor den von der Maschine verursachten Emissionen schützen.*

1.4.2. Besondere Anforderungen an trennende Schutzeinrichtungen

1.4.2.1 Feststehende trennende Schutzeinrichtungen

Die Befestigungen feststehender trennender Schutzeinrichtungen dürfen sich nur mit Werkzeugen lösen oder abnehmen lassen. Die Befestigungsmittel müssen nach dem Abnehmen der Schutzeinrichtungen mit den Schutzeinrichtungen oder mit der Maschine verbunden bleiben. Soweit möglich dürfen trennende Schutzeinrichtungen nach Lösen der Befestigungsmittel nicht in der Schutzstellung verbleiben.

1.4.2.2. Bewegliche trennende Schutzeinrichtungen mit Verriegelung

Bewegliche trennende Schutzeinrichtungen mit Verriegelung müssen

- *soweit möglich mit der Maschine verbunden bleiben, wenn sie geöffnet sind,*
- *so konstruiert und gebaut sein, dass sie nur durch eine absichtliche Handlung eingestellt werden können.*

4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen

Bewegliche trennende Schutzeinrichtungen mit Verriegelung müssen mit einer Verriegelungseinrichtung verbunden sein,

- *die das Ingangsetzen der gefährlichen Maschinenfunktionen verhindert, bis die Schutzeinrichtung geschlossen ist, und die einen Befehl zum Stillsetzen auslöst, wenn die Schutzeinrichtungen nicht mehr geschlossen sind.*

Besteht die Möglichkeit, dass das Bedienungspersonal den Gefahrenbereich erreicht, bevor die durch die gefährlichen Maschinenfunktionen verursachten Risiken nicht mehr bestehen, so müssen bewegliche trennende Schutzeinrichtungen zusätzlich zu der Verriegelungseinrichtung mit einer Zuhaltung ausgerüstet sein,

- *die das Ingangsetzen der gefährlichen Maschinenfunktionen verhindert, bis die Schutzeinrichtung geschlossen und verriegelt ist, und*
- *die die Schutzeinrichtung in geschlossener und verriegelter Stellung hält, bis das Risiko von Verletzungen aufgrund gefährlicher Funktionen der Maschine nicht mehr besteht.*

Bewegliche trennende Schutzeinrichtungen mit Verriegelung müssen so konstruiert sein, dass bei Fehlen oder Störung eines ihrer Bestandteile das Ingangsetzen gefährlicher Maschinenfunktionen verhindert wird oder diese stillgesetzt werden.

1.4.2.3. Zugangsbeschränkende verstellbare Schutzeinrichtungen

Verstellbare Schutzeinrichtungen, die den Zugang auf die für die Arbeit unbedingt notwendigen beweglichen Teile beschränken, müssen

- *je nach Art der Arbeit manuell oder automatisch verstellbar sein und*
- *leicht und ohne Werkzeug verstellt werden können.*

1.4.3. Besondere Anforderungen an nicht trennende Schutzeinrichtungen

Nicht trennende Schutzeinrichtungen müssen so konstruiert und in die Steuerung der Maschine integriert sein, dass

- *die beweglichen Teile nicht in Gang gesetzt werden können, solange sie vom Bedienungspersonal erreicht werden können,*
- *Personen die beweglichen Teile nicht erreichen können, solange diese Teile in Bewegung sind, und*
- *bei Fehlen oder Störung eines ihrer Bestandteile das Ingangsetzen der beweglichen Teile verhindert wird oder die beweglichen Teile stillgesetzt werden. Ihre Einstellung darf nur durch eine absichtliche Handlung möglich sein.*

4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen

Einige Punkte der zuvor genannten Forderungen seien hier gesondert betrachtet:

Trennende Schutzeinrichtungen müssen nach Möglichkeit vor einem Herausschleudern oder Herabfallen von Werkstoffen und Gegenständen sowie vor den von der Maschine verursachten Emissionen schützen. Hier wird die Wirkrichtung des Schutzes beschrieben: Nicht nur Gefährdungen beim Annähern des Menschen an Gefahrenorte sind zu beachten, manche Gefährdungen können auch von der Maschine selbst ausgehen, nach außen wirken und bedürfen daher einer Absicherung.

Schutzeinrichtungen dürfen die Beobachtungsmöglichkeit eines Arbeitsvorgangs nicht mehr als unvermeidbar einschränken.

Ferner wird gefordert, dass die Befestigungsmittel einer feststehenden trennenden Schutzeinrichtung nach dem Lösen der Einrichtung entweder an der Maschine oder an der Schutzeinrichtung selbst verbleiben. Demnach müssen z. B. Schrauben an Schutzabdeckungen künftig auch nach dem Lösen so fixiert sein, dass sie nicht verloren gehen können.

Diese sehr strikte Forderung wirft einige Fragen nach der Durchführbarkeit auf. Sind hiervon beispielsweise alle Schrauben eines Schutzzaunes betroffen? Im Extremfall würden sogar die Bodenbefestigungen des Schutzzaunes unter diese Bestimmung fallen.

Im Kommentar „Leitfaden zur Anwendung der Richtlinie 2006/42/EG – 2. Ausgabe – Juni 2010“ der Europäischen Kommission findet sich dazu eine Interpretation: Die Forderung ist für feststehende trennende Schutzeinrichtungen anzuwenden, bei denen damit zu rechnen ist, dass der Maschinenbenutzer sie entfernt. Ein praktisches Beispiel wäre eine monatlich zu nutzende Reinigungsöffnung. Im Gegensatz dazu kann bei Schutzeinrichtungen, die ausschließlich zu Generalüberholungen oder für größere Reparaturen entfernt werden, auf diese Forderung verzichtet werden. Für Maschinenhersteller empfiehlt sich daher, eine Einstufung in diesem Sinne vorzunehmen.

Nicht trennende Schutzeinrichtungen dürfen nur durch eine absichtliche Handlung verstellbar sein. Diese Forderung ist insbesondere im Zusammenhang mit Lichtschranken oder Lichtvorhängen sinnvoll. Diese Einrichtungen werden im Zuge der Maschineninbetriebnahme justiert und sollen ab diesem Zeitpunkt nicht ohne triftigen Grund verstellt werden können, da sonst der erforderliche Sicherheitsabstand möglicherweise nicht mehr gewährleistet ist.

4.1 Normen, Richtlinien und Gesetze in der Europäischen Union zum Thema Schutzeinrichtungen

4.1.1 Normen für trennende Schutzeinrichtungen

Neben den gesetzlichen Vorschriften der Maschinenrichtlinie existieren zurzeit folgende europäische Normen zum Thema Schutzeinrichtungen:

Norm	Titel
EN ISO 14120:2015	Sicherheit von Maschinen Trennende Schutzeinrichtungen – Allgemeine Anforderungen an Gestaltung und Bau von feststehenden und beweglichen trennenden Schutzeinrichtungen
EN ISO 14119:2013	Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl

4.1.2 Normen für die Dimensionierung trennender Schutzeinrichtungen

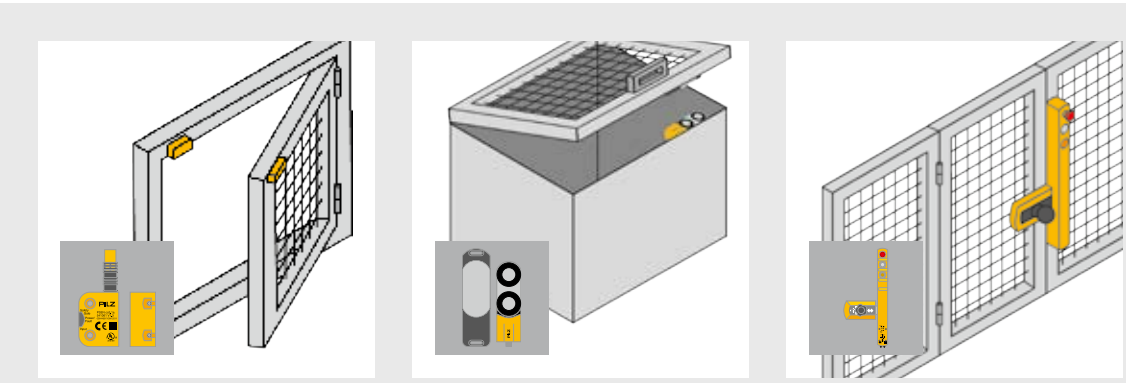
Norm	Titel
EN ISO 13857:2008	Sicherheit von Maschinen Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen (ISO 13857:2008)
EN 349:1993+A1:2008	Sicherheit von Maschinen Mindestabstände zur Vermeidung des Quetschens von Körperteilen

4.1.3 Normen zur Gestaltung nicht trennender oder berührungslos wirkender Schutzeinrichtungen

Norm	Titel
EN 61496-1:2013	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen
EN 61496-2:2013	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven optoelektronischen Prinzip arbeiten
CLC/TS 61496-3:2008	Sicherheit von Maschinen Berührungslos wirkende Schutzeinrichtungen – Teil 3: Besondere Anforderungen an aktive, optoelektronische diffuse Reflektion nutzende Schutzeinrichtungen (AOPDDR)
EN ISO 13855:2010	Sicherheit von Maschinen Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen

4.2 Trennende Schutzeinrichtungen

Eine trennende Schutzeinrichtung ist der Teil einer Maschine, der speziell als eine Art körperliche Sperre zum Schutz des Menschen vor den Gefahren der Maschine notwendig ist. In anderen Fällen bewirken dieselben Schutzeinrichtungen gleichzeitig den Schutz der Maschine vor dem Menschen, wenn beispielsweise zeitkritische Prozesse nicht von sich zufällig annähernden Menschen unterbrochen werden dürfen. Die hier vorliegende Betrachtung beschäftigt sich nur mit dem ersten Fall.



Beispiele für trennende Schutzeinrichtungen

Der Begriff „trennend“ bezieht sich auf die körperliche Trennung zwischen Maschinenbediener und Gefährdung, im Gegensatz zu den später behandelten „nicht trennenden“ oder „berührungslos wirkenden“ Schutzeinrichtungen wie z. B. Lichtvorhängen und Lichtschranken. Derartige Schutzeinrichtungen verhindern nicht den Zugang zu einer Gefährdung, sie erkennen vielmehr einen Menschen oder einen Körperteil des Menschen bei Annäherung an eine Gefahr. In diesem Fall wird über eine nachfolgende Steuerung die Gefährdung so rechtzeitig abgeschaltet, dass diese bei Erreichen des Gefährdungsortes bereits beseitigt ist. Je nach Bauform kann eine trennende Schutzeinrichtung als Gehäuse, Abdeckung, Schirm, Tür, Verkleidung oder auf andere Art und Weise ausgeführt werden. Trennende Schutzeinrichtungen existieren daher in vielfältigen Formen und Varianten.

4.2.1 Feststehende trennende Schutzeinrichtungen

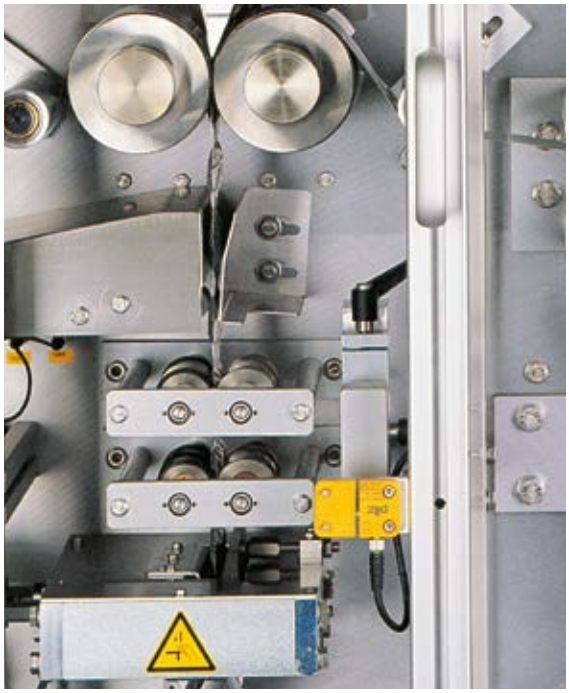
Feststehende trennende Schutzeinrichtungen sind fest mit der Maschine verbunden. Diese Ausführung setzt voraus, dass keine betriebsmäßige Notwendigkeit zur Entfernung dieser Schutzeinrichtung besteht bzw. während des Arbeitsvorganges ein Zugang nicht erforderlich ist. Beispiele dazu sind Kettenabdeckungen oder Gitter vor Motorlüftern.

4.2 Trennende Schutzeinrichtungen

4.2.2 Beweglich trennende Schutzeinrichtungen

Ist es erforderlich, Zugriff zu der Gefahrenstelle zu haben, kann die trennende Schutzeinrichtung beweglich ausgeführt werden, z. B. als Schutztür.

Ob eine trennende Schutzeinrichtung in fester oder beweglicher Form auszuführen ist, hängt von der Häufigkeit des erforderlichen Zugriffs ab. Dazu geben die Normen Entscheidungshilfen.



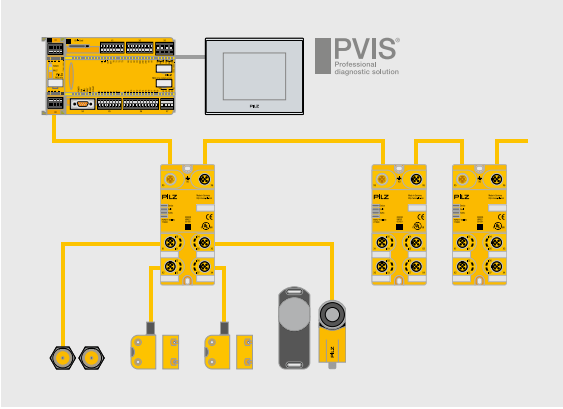
EN 14120

Fälle, in denen der Zugang nur bei Maschineneinstellung, Verfahrenskorrektur oder Instandhaltung erforderlich ist, erlauben die nachstehenden trennenden Schutzeinrichtungen wie folgt:

a) Bewegliche trennende Schutzeinrichtung, wenn die Häufigkeit des Zugangs vorhersehbar hoch ist (z. B. mehr als einmal je Woche) oder wenn das Entfernen oder Wiederanbringen einer feststehenden trennenden Schutzeinrichtung schwierig sein würde. Bewegliche trennende Schutzeinrichtungen müssen mit einer Verriegelung bzw. einer Verriegelung mit Zuhaltung versehen sein (siehe ISO 14119).

b) Feststehende trennende Schutzeinrichtung nur dann, wenn die Häufigkeit des Zugangs gering ist, ihr Wiederanbringen einfach ist, und außerdem das Entfernen und Wiederanbringen in einem sicheren Arbeitssystem ausgeführt werden kann.

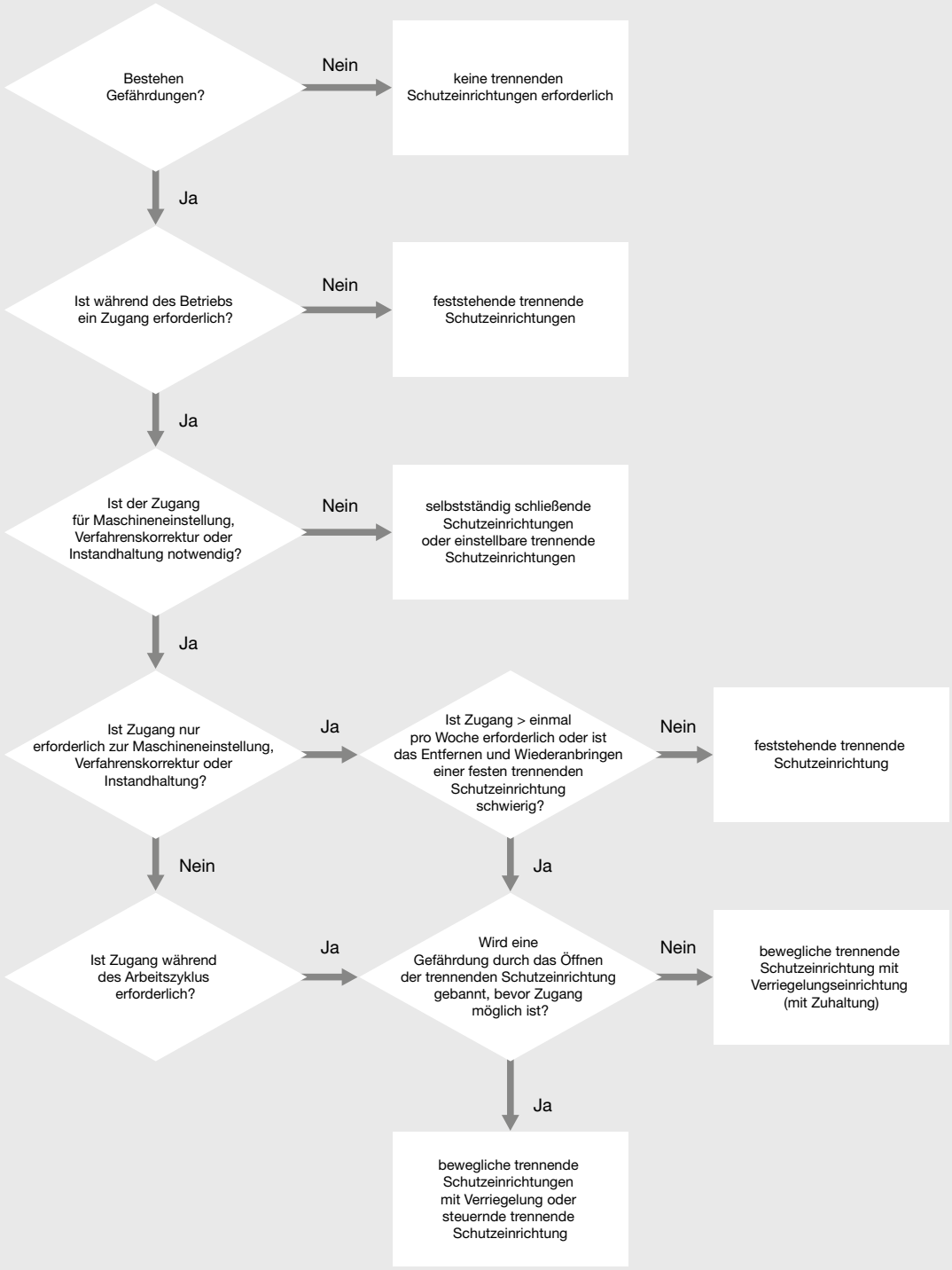
Anmerkung: Mit dem Begriff „Verriegelung“ ist hier die elektrische Verknüpfung der Stellung der Schutzeinrichtung mit den abzuschaltenden Antrieben gemeint. Die umgangssprachlich verstandene mechanische „Verriegelung“ im Sinne eines Schlosses wird in der Sicherheitstechnik „Zuhaltung“ genannt.



Überwachung mehrerer Schutztüren mit einem Auswertegerät dank Einzeldiagnose

4.2 Trennende Schutzeinrichtungen

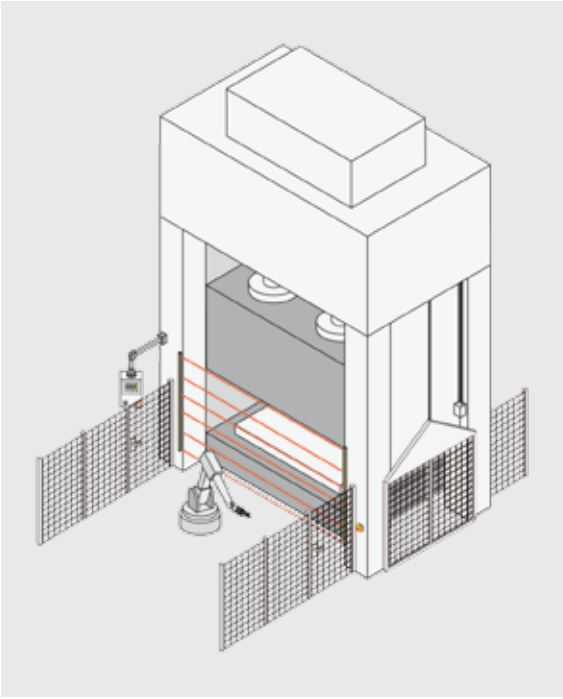
Auswahlhilfe zur Art der trennenden Schutzeinrichtung



Nach EN 14120

4.2 Trennende Schutzeinrichtungen

Zusammenfassung
Trennende Schutzeinrichtungen, die während des Produktionsbetriebs einer Maschine geöffnet werden müssen, sind im Allgemeinen als bewegliche trennende Schutzeinrichtungen ausgeführt, im Gegensatz zu feststehenden trennenden Schutzeinrichtungen, die nur selten benutzt werden, wie beispielsweise Wartungs- und Reparaturöffnungen. Auch weil mit der Art oder Wahl der trennenden Schutzeinrichtung unterschiedliche Kosten verbunden sind, ist es von Bedeutung, diese Einstufung fundiert vorzunehmen.



Feststehende trennende Schutzeinrichtungen für Wartungs- oder Reparaturarbeiten

4.2.3 Weitere Aspekte zur Gestaltung von Schutzeinrichtungen

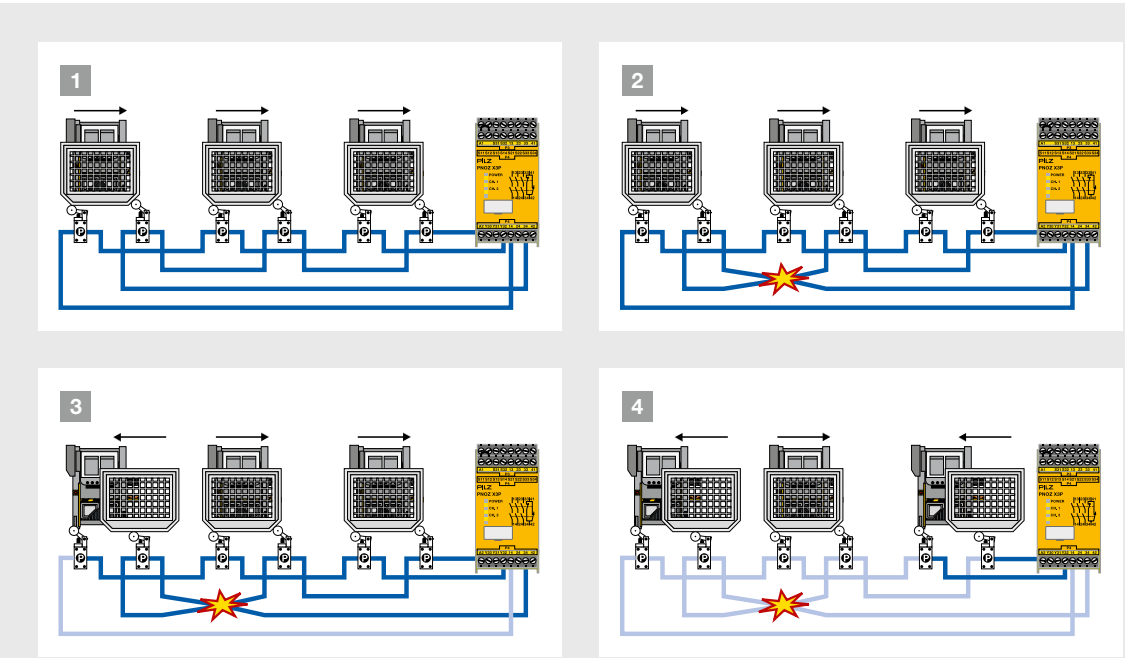
Hat man sich auf eine bewegliche trennende Schutzeinrichtung festgelegt, ist in einem weiteren Schritt nach EN 62061 oder EN ISO 13849-1 das Schutzniveau der zugehörigen Verriegelung (Safety Integrity Level SIL oder Performance Level PL) festzulegen. Im Anschluss daran folgen Entwurf und Validierung des zugehörigen Steuerungssystems.

Zu diesem Steuerungssystem gehören als Sensoren Schalter, die die Position der Schutzeinrichtung erkennen. Über diese Erkennung kann beim Öffnen der Schutzeinrichtung das Stillsetzen der gefährlichen Bewegungen erfolgen. Eine weitere Sicherheitsfunktion kann die Verhinderung eines unerwarteten Anlaufs von Antrieben bei geöffneter Schutztür sein. Es ist die Nachlaufzeit gefährlicher Bewegungen zu berücksichtigen: Ist anzunehmen, dass nach Öffnen einer Schutztür eine gefahrbringende Bewegung durch einen Antrieb mit großer Nachlaufzeit entsteht, benötigt man für diese Tür eine Zuhaltung. Das Freigeben dieser Zuhaltung muss durch aktives Einschalten einer Entriegelung geschehen. Nur dadurch wird sichergestellt, dass sich die Schutztür nicht etwa bei einem Stromausfall unabsichtlich entriegelt. Zu beachten ist in diesem Fall auch, dass eine Person, die sich zum Zeitpunkt des Stromausfalls im Gefahrenbereich aufhält und die Schutztür hinter sich geschlossen hat, nicht durch einen Entriegelungsbefehl an der Maschinensteuerung befreit werden kann. Für diesen als selten anzunehmenden, aber denkbaren Fall existieren Varianten der Zuhaltungen, die eine mechanische Entriegelungsfunktion besitzen. Allerdings muss das Bedienpersonal darauf achten, das passende Betätigungswerkzeug verfügbar zu haben bzw. Kenntnis über die Bedienung der Notentriegelung zu besitzen.

4.2 Trennende Schutzeinrichtungen

Reihenschaltung von Schutztürschaltern

Bei der Auswahl der Sensoren zur Abfrage beweglicher trennender Schutzeinrichtungen stellt sich die Frage, ob und, falls ja, wie viele solcher Sensoren man in Serie an ein Auswertegerät anschließen kann. Die Beantwortung dieser Frage hängt mit den anzunehmenden Fehlern bzw. mit der Verdeckung der Erkennbarkeit dieser Fehler zusammen. Zur Erklärung dient das Beispiel einer Reihenschaltung von Schutztürsensoren:



Beispiel Reihenschaltung von Schutztüren

1 Im Beispiel wird eine Reihenschaltung von drei Schutztüren an einem Auswertegerät gezeigt. Die Schutztüren sind zunächst alle geschlossen, die Ausgänge des Schaltgerätes sind „an“, d. h. die Maschine kann betrieben werden.

2 Nun entsteht ein Kurzschluss in der Zuleitung zum Schalter mit dem Öffnerkontakt an der linken Schutztür: Der Fehler wird zunächst nicht bemerkt, die Maschine kann weiter betrieben werden.

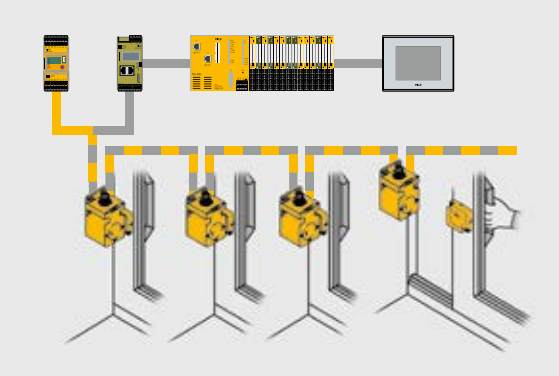
3 Danach wird die linke Schutztür geöffnet, der linke Schalter signalisiert diese Öffnung an das Schaltgerät. Dieses entdeckt über den Plausibilitätsvergleich der beiden Schalter eine Inkonsistenz und geht in den Fehlerzustand, d. h. die Maschine ließe sich nach Schließen dieser Schutztür nicht wieder starten.

4 Nun wird zusätzlich die rechte Schutztür geöffnet. Das Schaltgerät erkennt anhand der Signale wieder den Normalzustand. Der Fehlerzustand wird zurückgesetzt, jetzt können die Schutztüren wieder von links nach rechts geschlossen werden, die Maschine ist wieder startbereit.

Das Beispiel zeigt einen unentdeckten Fehler in der Sicherheitsschaltung. Durch einen weiteren Fehler könnte die gesamte Schutztürabsicherung gefährlich ausfallen. Diese und ähnliche Fehler werden als Maskierung von Fehlern bezeichnet. Je nach Wahrscheinlichkeit der Maskierung wird in der aktuellen Normung der maximal erreichbare Diagnosedeckungsgrad (DC) der Schalter eingeschränkt.

4.2 Trennende Schutzeinrichtungen

Ein Auftreten derartiger Fehlermaskierungen ist gleichermaßen für mechanische Schalter wie für magnetische Näherungsschalter zu beachten. Lediglich Schalter mit interner Diagnose und OSSD-Ausgang, wie sie bei RFID-basierten Schaltern üblich sind, sind hiervon nicht betroffen.



Sicherheitsschalter mit integrierter Fehlererkennung

In der Praxis ist bei einem einzelnen Schalterpaar, das über ein Sicherheitsschaltgerät ausgewertet wird, ein DC = 99 % erreichbar. Im ISO/TR 24119 wird basierend auf dieser Grundvoraussetzung der maximale DC einer Verkettung von Schaltern in Abhängigkeit der Anzahl in Serie geschalteter Schalter und deren Betätigungshäufigkeit angegeben.

Wie in der Tabelle auf der nächsten Seite zu sehen, ist durch die Maskierung der erreichbare DC und in direkter Folge der erreichbare PL eingeschränkt. Wird eine Verkettung von Schaltern gemäß einem PL e gefordert, so existiert eine technische Lösung im Einsatz von Schaltern mit integrierter Fehlererkennung. Weil hierbei keine Maskierung auftreten kann, ist eine Verkettung ohne Einschränkung des DC oder des PL möglich.

Mechanische Schalter

In diesem Zusammenhang stellt sich auch die Frage nach der Notwendigkeit von mechanischer Redundanz bzw. der Anzahl von unabhängigen Schaltern an einer Schutztür. Während magnetisch betätigte Näherungsschalter und RFID-Näherungsschalter bei korrekter Montage häufig so konzipiert sind, dass ein einzelner mechanischer Fehler nicht zum Verlust der Sicherheit führt, ist bei mechanisch betätigten Schaltern (Zungen- oder Rollenschalter) der einkanalige mechanische Betätiger besonders zu betrachten. Die Dokumentation der Schalter ist in jedem Fall sorgfältig zu prüfen, ob und wenn ja welche zugesicherten Produkteigenschaften der Schalter selbst hat. Dies gilt vor allem dann, wenn ein elektrisch zweikanaliges Schaltelement vorliegt. Fehlerausschlüsse für den mechanischen Teil dieser Schalter sind, sofern nicht explizit vom Schalterhersteller im Rahmen der bestimmungsgemäßen Verwendung bestätigt, vom Anwender zu begründen. Das ist häufig nicht oder nur sehr schwer leistbar, da Effekte wie Verschleiß, Vibration, Korrosion oder mechanische Fehlbelastung kaum abschätzbar sind. In diesen Fällen müssen für PL d oder PL e entweder zwei mechanische Türschalter je Tür oder ein zweikanaliger magnetischer Schalter oder ein RFID-Schalter mit OSSD-Ausgang verwendet werden.

4.2 Trennende Schutzeinrichtungen

Anzahl häufig benutzter beweglicher trennender Schutzeinrichtungen [1) 2)]		Anzahl zusätzlicher beweglicher trennender Schutzeinrichtungen [3)]	Maximal erreichbarer Diagnosedeckungsgrad (DC) [4)]
0	+	2 bis 4	mittel
		5 bis 30	niedrig
		> 30	kein
1	+	1	mittel
		2 bis 4	niedrig
		≥ 5	kein
> 1	+	≥ 0	kein

1) Wenn die Frequenz höher ist als 1 Mal pro Stunde.

2) Wenn die Anzahl der Bediener, die separate Schutzeinrichtungen öffnen können, höher als 1 ist, dann wird die Zahl der häufig benutzten beweglichen trennenden Schutzeinrichtungen um 1 erhöht.

3) Die Anzahl zusätzlicher beweglicher trennender Schutzeinrichtungen kann um 1 verringert werden, wenn eine der folgenden Bedingungen erfüllt ist:
- wenn der Mindestabstand zwischen den Schutzeinrichtungen höher ist als 5 m oder
- wenn keine der zusätzlichen beweglichen trennenden Schutzeinrichtungen direkt erreichbar ist.

4) Wenn in jedem Fall vorhersehbar ist, dass Fehlerverdeckung auftritt (z. B. mehrere bewegliche trennende Schutzeinrichtungen sind gleichzeitig geöffnet als Teil des normalen Betriebs oder Service), dann ist der Diagnosedeckungsgrad auf „Kein“ begrenzt

Maximal erreichbarer Diagnosedeckungsgrad (DC) (vereinfacht)

Bei der Berücksichtigung zusätzlicher Parameter wie Verkabelungsart, Testimpulse und Schaltertyp sind über die Werte der Tabelle hinaus komplexere Betrachtungen vorgesehen. Diese führen in Einzelfällen zu besseren Ergebnissen, sind aber immer auf ein Maximum DC = mittel beschränkt.

Ferner besteht die Frage, wie bei einer Serienschaltung von Sensoren mit eigenem PL vorzugehen ist. In diesem Fall ist die Diagnose integraler Bestandteil des Sensors und wird durch eine Serienschaltung nicht beeinflusst bzw. reduziert. Trotzdem muss das Schaltsignal des ersten Sensors in der Kette durch alle weiteren Sensoren geleitet werden, bevor es von einem Auswertegerät verarbeitet werden kann. Ein sicherheitsrelevanter Ausfall eines weiteren Sensors in der Kette könnte diese Weiterleitung verhindern. Daher sind in diesem Fall die Ausfallwahrscheinlichkeiten aller Sensoren in der Kette zu addieren – auch wenn nur der erste Sensor zu der gerade betrachteten Sicherheitsfunktion gehört.

4.2 Trennende Schutzeinrichtungen

Bemessung von Magnetschaltern

Bei der Verwendung von magnetisch betätigten Türschaltern (mit Reed-Kontakten) hat sich ein Problem als kritisch erwiesen. Werden Paarungen von Schaltern und Sicherheitsschaltgeräten eingesetzt, die nicht herstellerseitig als füreinander geeignet geprüft wurden, so ist durch den Maschinenbauer sicherzustellen, dass Spitzenströme im Schalter nicht zu vorzeitigem Verschleiß führen. Betroffen sind hauptsächlich Paarungen von Reed-Schaltern mit Sicherheitsschaltgeräten auf Relais-Basis.

Zur Bemessung ist der maximal auftretende Spitzenstrom I_S zu bestimmen (siehe Formel 1) und mit dem zulässigen Spitzenstrom der Schalter I_{Smax} zu vergleichen. Bei Serienschaltungen müssen alle Schalter berücksichtigt werden, weshalb der kleinste aller zulässigen Spitzenströme größer oder gleich dem maximalen Schaltstrom sein muss (siehe Formel 2).

$R_{Smin}(i)$	Mindest-Innenwiderstand Schalter i
$I_{Smax}(i)$	Maximaler zulässiger Spitzenstrom Schalter i
U_{Pmax}	Maximale Spannung
R_{Pmin}	Mindest-Innenwiderstand Sicherheitsschaltgerät
I_S	Maximaler Schaltstrom

$$I_S = \frac{U_{max}}{R_{Pmin} + \sum_i R_{Smin}(i)}$$

Formel 1

$$I_S \leq \underset{i}{MIN}\,(I_{Smax}(i))$$

Formel 2

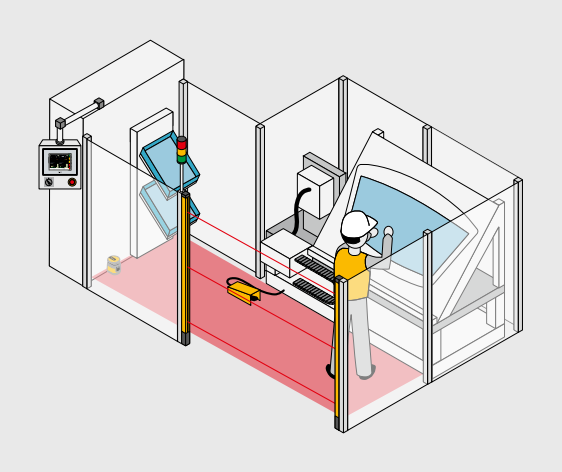
Bei mechanisch betätigten Schaltern und Schaltern mit OSSD-Ausgang tritt das Problem des vorzeitigen Verschleißes normalerweise nicht auf, weil deren Verschleiß in erster Linie über den durchschnittlichen Strom und das thermische Verhalten bestimmt ist.

Aus der EN ISO 13855 ergibt sich eine weitere Neuerung für die Betrachtung von Schaltern an beweglichen trennenden Schutzeinrichtungen. Es geht um eine mögliche Gefährdung, die dann entsteht, wenn eine Tür in einem Schutzzaun so weit geöffnet werden kann, dass eine Person durch den geöffneten Spalt in die Gefahrenzone greifen kann, ohne dass der entsprechende Türschalter einen Signalwechsel erfahren hat. Diese eher theoretisch anmutende Gefährdung kann durch eine Vergrößerung des Sicherheitsabstands abgesichert werden, die sich nach der Größe des unerkannt geöffneten Türspalts bemisst. In der Praxis sollte sich das Problem durch den Einsatz eines situationsgerecht ausgewählten und angebrachten Türschalters gar nicht erst stellen.

Mehr Praxisbezug hat in diesem Zusammenhang der eigentliche Sicherheitsabstand zwischen Tür und Gefahrenort. In diesem Fall lautet die Frage, was passiert, wenn die Schutztür in einem Schutzzaun geöffnet wird, eine Person den Gefahrenbereich betritt, die Maschine aber noch ausläuft bzw. bremst. Hier lassen sich bei ausreichend schneller Annäherung und entsprechend langer Bremszeit der Maschine relevante Gefahrstellen noch erreichen. Gemäß der Norm kann für diesen Fall auf die Berechnung für die Benutzung von Lichtvorhängen zurückgegriffen werden. Der Sicherheitsabstand S berechnet sich als S = (K x T). K ist die Schreitgeschwindigkeit des Menschen von 1 600 mm/sec und T die Zeit vom Auslösen des Türschalters bis zum Anhalten der Maschine (Herstellung des sicheren Zustandes). Abgezogen werden kann die Zeit, die das Öffnen der Tür in Anspruch nimmt. Sie kann entweder durch theoretische Überlegungen oder praktische Versuche ermittelt werden, da keine Standardwerte angegeben sind.

4.3 Nicht trennende Schutzeinrichtungen

4.3.1 Aktive optoelektronische Schutzeinrichtungen



Überwachung von Produktionsbereichen, in die aktiv eingegriffen werden muss

Sichere Kamerasysteme zur dreidimensionalen Raumüberwachung

Nicht trennende Schutzeinrichtungen (berührungslos wirkende Schutzeinrichtungen, im Folgenden BWS genannt) kommen immer dann zum Einsatz, wenn der Zugang zu dem dahinter liegenden Gefährdungsort besonders leicht möglich sein soll und man nicht mit gefährlichen Auswirkungen von der Maschine selbst zu rechnen hat (Beispiel: Schweiß- oder Schleifprozesse). Um eine mögliche Gefährdung schnell genug abschalten zu können, ist es erforderlich, die Schutzeinrichtung in einem geeigneten Abstand zu montieren. Dieser Abstand oder Sicherheitsabstand (S) wird in der EN ISO 13855 definiert und hängt insbesondere von folgenden Faktoren ab:

- t_1 = Reaktionszeit der Schutzeinrichtung selbst
- t_2 = Reaktionszeit der Maschine, d. h. Anhaltezeit der Maschine als Reaktion auf das Signal der Schutzeinrichtung
- C = mögliche Annäherung an einen Gefahrenort, ohne von der Schutzeinrichtung erkannt zu werden, wie z. B. das unerkannte Durchgreifen durch zwei Strahlen eines Lichtvorhangs, abhängig vom Abstand dieser Strahlen
- K = anzunehmende Annäherungsgeschwindigkeit des menschlichen Körpers oder von Körperteilen. Dieser Faktor wird in der EN ISO 13855 mit 1 600 mm/sec für die Schreitgeschwindigkeit und 2 000 mm/sec für die Greifgeschwindigkeit definiert.

Der zu realisierende Abstand beträgt dann
$S = K \times (t_1 + t_2) + C$

4.3 Nicht trennende Schutzeinrichtungen

Nach EN ISO 13855 sind folgende Vorzugsabstände definiert:

Auflösung	Berechnungsformel (Abstand S [mm])	Bemerkungen
d ≤ 40 mm	S = 2000 x T + 8 (d –14)	Wenn das Ergebnis < 100 mm, müssen mindestens 100 mm eingehalten werden.
	Wenn das Ergebnis > 500 mm, darf mit S = 1600 x T + 8 (d –14) gerechnet werden.	In diesem Fall darf S nicht < 500 mm gewählt werden.
40 < d ≤ 70 mm	S = 1600 x T + 850	Höhe des untersten Strahls ≤ 300 mm
		Höhe des obersten Strahls ≥ 900 mm

Mehrere Einzelstrahlen		Strahlzahl	Strahlhöhen in mm
Mehrstrahlig	S = 1600 x T + 850	4	300, 600, 900, 1200
		3	300, 700, 1100
		2	400, 900
Einstrahlig	S = 1600 x T + 1200	1	750
	Sofern die Risikobewertung eine einstrahlige Anordnung zulässt		

Bilden die BWS horizontale oder geneigte Schutzfelder über einer abzusichernden begehbaren Fläche, so sind diese in einer durch Anwendung und BWS vorbestimmten Mindesthöhe anzubringen. Der Sicherheitsabstand zwischen dem äußeren Schutzfeldrand und der abzusichernden Gefahrenstelle ist auch hier so zu bemessen, dass unter Berücksichtigung der Maschinennachlaufzeit Verletzungen durch die gefährliche Bewegung im Gefahrenbereich auszuschließen sind.

- Auch nach sorgfältiger Auslegung einer Schutzeinrichtung müssen eventuelle Umgehungsmöglichkeiten berücksichtigt werden. Ein Herüber- oder Herumreichen um das Detektionsfeld einer Schutzeinrichtung muss ausgeschlossen werden. Da das Verdecken eventueller Lücken neben dem Detektionsfeld und einem angrenzenden Schutzzaun nicht immer möglich ist, sind auch hier Sicherheitsabstände zwischen Mensch und Gefahrstelle einzuhalten. Die Berechnung dieser Abstände ähnelt sehr stark denjenigen der Sicherheitsabstände, die für das Erreichen von Gefahrstellen durch ein Detektionsfeld hindurch gelten. Diesen wichtigen Unterschied gilt es besonders zu beachten. In der Praxis kann es z. B. vorkommen, dass der Zugang zu einem Gefahrenbereich durch ein vertikal aufgestelltes Lichtgitter abgesichert wird. Dieses Lichtgitter ist aber oftmals nicht so hoch, wie eine Person greifen könnte, sondern z. B. in Anlehnung an ein Geländer nur 1100 mm hoch. In diesem Fall kann also eine Person knapp vor dem Lichtgitter stehen, ohne das Detektionsfeld zu unterbrechen. Weiterhin kann sie sich dabei noch vorbeugen und bei ausgestrecktem Arm mit der Hand in den Bereich hinter dem Lichtgitter eingreifen. Um in dieser Situation Gefährdungen zu vermeiden, sind Mindestabstände zwischen Gefahrstelle und Lichtvorhang beschrieben. Diese Mindestabstände setzen sich aus zwei Teilen zusammen: der Schreit- bzw. Greifgeschwindigkeit multipliziert mit der Reaktionszeit des Systems und einem Zuschlag, der von der Höhe des Gefahrenortes und der Höhe der Schutzeinrichtung abhängt. Dieser Zuschlag kann bis zu 1200 mm betragen. Wenn Platznot herrscht, lohnt es sich, eine feste Abdeckung aller Umgehungsmöglichkeiten ins Auge zu fassen.
- Angaben zur Größenauslegung von Schaltmatten finden sich in Kapitel 7 der EN ISO 13855. Auch hier wird mit der bekannten Formel S = (K x T) + C gerechnet. K beträgt hier 1600 mm/sec, abgeleitet aus der normalen Schreitgeschwindigkeit. Um ausgestreckte Arme/Hände zu schützen, die von der Schaltmatte nicht erfasst werden, ist ein minimaler Abstand von C = 1200 mm gefordert.
- Die Auslegung des Sicherheitsabstandes S für die Anbringung von Zweihandschaltungen folgt der Formel S = (K x T) + C. C ist hier 250 mm, K ist 1600 mm/sec.

4.3 Nicht trennende Schutzeinrichtungen

4.3.2 Weitere wichtige Aspekte im Zusammenhang mit berührungslos wirkenden Schutzeinrichtungen

4.3.2.1 Wiederanlauf

Der Wiederanlauf einer Maschine nach Auslösen einer Schutzeinrichtung darf nicht automatisch nach Verlassen des Schutzfeldes erfolgen. Er darf nur durch das Quittieren an einem Befehlsgerät außerhalb des Gefahrenbereiches und mit Sichtkontakt auf diesen möglich sein.

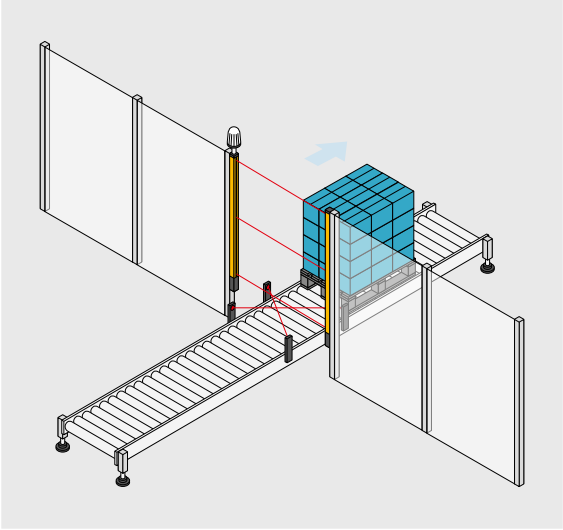
4.3.2.2 Hintertretschutz

Neben der offensichtlichen Gefahrenstellenabsicherung ist zusätzlich die Möglichkeit des Über-, Unter- oder Umgreifens sowie des Hintertretens zu berücksichtigen. Als Hintertretschutz kann eine rein mechanische Absicherung oder ein weiterer Lichtvorhang eingesetzt werden. Sind solche Umgehungsmöglichkeiten vorhanden, müssen zu deren Absicherung weitere Maßnahmen getroffen werden.

4.3.2.3 Muting

Muting ist das automatische und vorübergehende Überbrücken einer berührungslos wirkenden Schutzeinrichtung, um z. B. Material in einen Gefahrenbereich oder aus ihm heraus zu transportieren. Über spezielle Sensoren wird der Mutingzyklus von der Mutingsteuerung nur dann gestartet, wenn das Material durch das Schutzfeld transportiert wird. Die Anordnung der Sensoren muss so erfolgen, dass Personen nicht in der Lage sind, die Mutingsensoren zu aktivieren. Diese lösen beim Zugang in den Schutzbereich sofort das Abschalten der gefahrbringenden Bewegung aus.

Speziell für diesen Fall hat die Industrie besondere Sicherheitsschaltgeräte mit Muting-Funktion entwickelt. Einige Lichtvorhänge bieten auch die Möglichkeit, das Schutzfeld nur teilweise zu überbrücken (Blanking). Damit setzt man z. B. exakt jenen Teil passiv, durch den ein Gut gefördert wird. Über diesen deaktivierten Teil des Schutzfeldes dürfen aber keinesfalls Personen unerkannt in den Gefahrenbereich gelangen. Per konstruktiver Absicherung (z. B. mit einer Abdeckung des verbleibenden Freiraumes) ist dafür zu sorgen, dass seitlich zwischen Gut und Schutzvorrichtung niemand in den Gefahrenbereich gelangen kann.



Muting mit vier Mutingsensoren

4.3 Nicht trennende Schutzeinrichtungen

4.3.3 Andere sensorisch wirkende Schutzeinrichtungen

4.3.3.1 Laserscanner

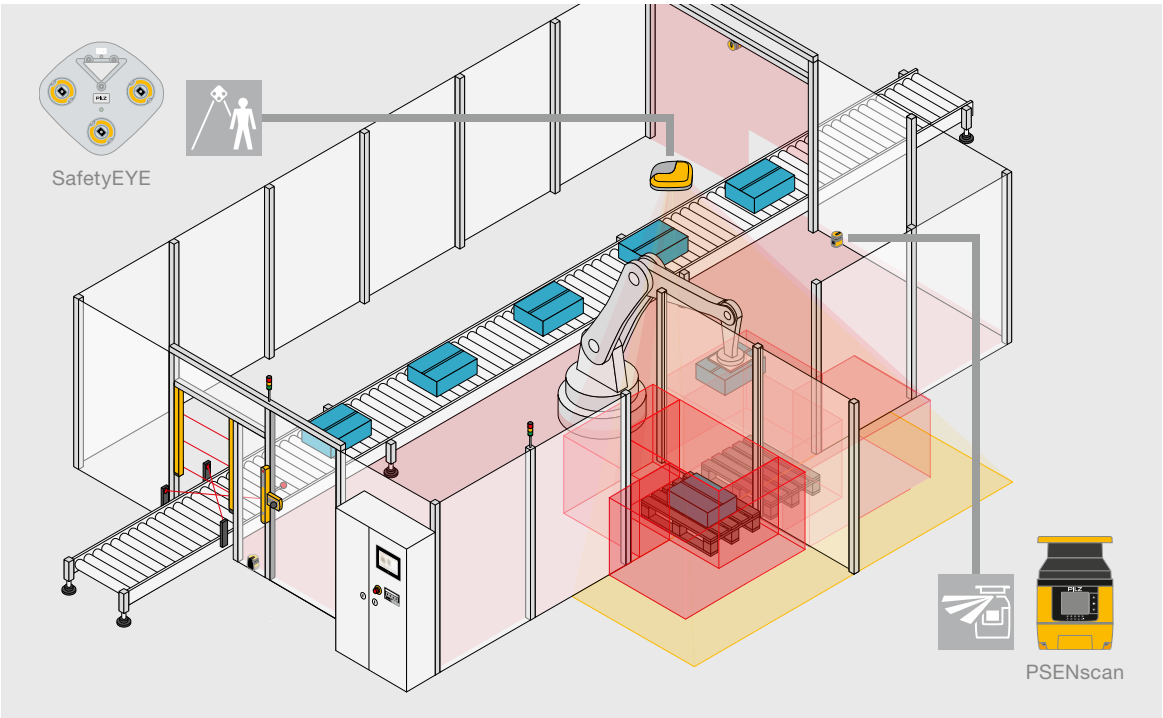
Häufig wird als Hintertretschutz einer BWS eine zweite, waagerecht oder schräg montierte BWS eingesetzt. Diese kann oftmals nur einen kleinen Bereich abdecken. Bei größeren abzusichernden Bereichen kann als weitere optische Hintertretkontrolle ein Scanner eingesetzt werden. Ein Laserstrahl tastet die zu überwachende Fläche ab. Wird er durch einen Fremdkörper reflektiert, wird dieser erkannt und die gefahrbringende Bewegung sicher abgeschaltet.

4.3.3.2 Sichere Kamerasysteme

Neuere Entwicklungen am Markt sind sichere Kamerasysteme zur Überwachung frei konfigurierbarer Bereiche. Im Unterschied zu einfachen Sensoren können sie detaillierte Informationen über den gesamten Überwachungsbereich erfassen und auswerten. Damit werden gefahrbringende Arbeitsprozesse zum Schutz von Mensch und Maschine sicher überwacht.

4.3.3.3 Schaltmatten

Viele Schaltmatten funktionieren nach dem Schließerprinzip: Zu ihrem Einsatz sind spezielle Auswertegeräte erforderlich, die diesem Betätigungsprinzip Rechnung tragen und eine entsprechende Fehlererkennung gewährleisten. Ebenso sind aber auch Schaltmatten im Öffnerprinzip erhältlich, die in niedrigen Sicherheitsstufen und bei niedrigen elektrischen Beanspruchungen auch direkt Schütze ansteuern können.



Gefahrenbereichsabsicherung mit Sicherheits-Laserscanner und sicherem Kamerasystem

4.3 Nicht trennende Schutzeinrichtungen

4.3.3.4 Zweihandsteuerungen

Zweihandsteuerungen dienen dazu, an einem Arbeitsplatz beide Hände des Bedieners örtlich zu binden und damit während der Betätigung vom Gefahrenbereich fernzuhalten. Dazu sind verschiedene Typen von Zweihandschaltungen definiert, die je nach erforderlichem Absicherungsniveau zum Einsatz kommen können. Anforderungsstufen an Zweihandsteuerungen:

Anforderungen		**Typen**				
	EN 574 Abs.	I	II	III		
				A	B	C
Benutzung beider Hände	5.1	◆	◆	◆	◆	◆
Loslassen eines der beiden Stellteile beendet das Ausgangssignal	5.2	◆	◆	◆	◆	◆
Versehentliches Betätigen weitestgehend verhindern	5.4	◆	◆	◆	◆	◆
Kein einfaches Umgehen der Schutzwirkung möglich	5.5	◆	◆	◆	◆	◆
Erneutes Ausgangssignal nur nach Loslassen beider Stellteile	5.6	◆	◆	◆	◆	◆
Ausgangssignal nur nach synchroner Betätigung innerhalb max. 500 ms	5.7			◆	◆	◆
Anwendungen der Sicherheitskategorie 1 nach EN 954-1	6.2	◆		◆		
Anwendungen der Sicherheitskategorie 3 nach EN 954-1	6.3		◆		◆	
Anwendungen der Sicherheitskategorie 4 nach EN 954-1	6.4					◆

Auswertung von Zweihandschaltungen

Die EN 574 bezieht sich in der aktuellen Fassung noch auf die zurückgezogene EN 954-1. Die EN 574 befindet sich u. a. deswegen derzeit in Überarbeitung.

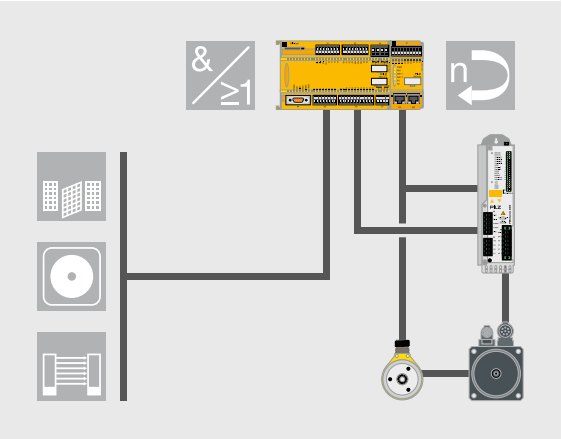
4.3 Nicht trennende Schutzeinrichtungen

4.3.3.5 Funktionale Schutzeinrichtungen

Vermeidung von unerwartetem Anlauf nach EN 1037 bzw. demnächst DIN EN ISO 14118:

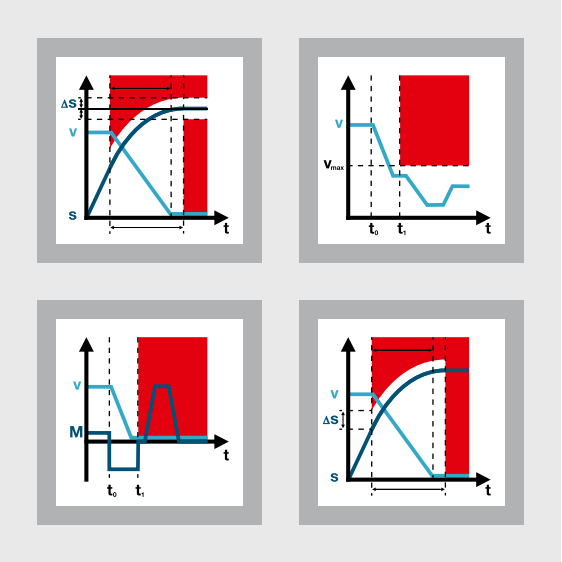
Bei Arbeiten im laufenden Betrieb stellt sich stets die Frage, wie sicher der ungewollte Wiederanlauf von Maschinen verhindert ist, die über einen betriebsmäßigen Stopp-Befehl stillgesetzt wurden: Was passiert, wenn in dieser Situation ein Fehler in der Steuerung auftritt und daraufhin ein Antrieb unerwartet anfährt? Eine Frage, die ebenso wichtig ist wie die Betrachtung der funktionalen Sicherheit in Verbindung mit „auffälligeren“ Schutzeinrichtungen. Ein wesentlicher Faktor sind dabei die mit Umrichtern gesteuerten Antriebe. Diese Antriebe erden oft durch Signale wie „Geschwindigkeit Null“ oder „Reglersperre“ angehalten. Das Abschalten der Leistungsversorgung ist oft unerwünscht, um nicht Daten über den momentanen Antriebszustand zu verlieren. In einigen Fällen ist das spontane Abschalten der Verbindung zwischen Netz und Umrichter oder sogar zwischen Umrichter und Antrieb mit Gerätedefekten verbunden und kann daher nicht in Betracht gezogen werden.

In diesen Fällen hat der Maschinenkonstrukteur zwei Möglichkeiten: Wenn eine Trennung von der Energieversorgung ohne Gerätedefekte und ohne Auslösen anderer gefährlicher Bewegungen möglich ist, kann eine Stillstandsüberwachung eingesetzt werden. Hierbei wird der stehende, aber immer noch aktiv vom Umrichter angesteuerte Antrieb darauf überwacht, dass er sich nicht bewegt. Erfolgt aufgrund eines Fehlers trotzdem eine Bewegung, wird sofort die Versorgung des gesamten Zweiges per Schütz abgeschaltet. Diese Lösung setzt außerdem voraus, dass die im Fehlerfall auftretende geringe Antriebsbewegung keine Gefährdung hervorruft. Denn die Bewegung setzt sich aus zwei Teilen zusammen: aus dem Teil, der die Sensorik der Überwachung ansteuert, und jenem, der entsteht, bis die Reaktion der Schutzschaltung eingetreten und ein Schütz geschaltet ist. Diese Einflüsse sind in einer Risikobetrachtung zu untersuchen.



Externe Antriebsüberwachung durch das Sicherheitssystem PNOZmulti mit Drehzahlüberwachung

Ist eine solche ungewollte Bewegung nicht akzeptabel, muss sichere Antriebstechnik eingesetzt werden, die ein solches fehlerhaftes Verhalten von Anfang an verhindert (siehe auch Kapitel 7: Sichere Bewegungssteuerung).



Beispiele antriebsintegrierter Sicherheit

4.4 Manipulation von Schutzeinrichtungen

Der Umgang mit Schutzeinrichtungen und deren Manipulation stellt einen Sachverhalt dar, dessen wahre Ursachen lange Zeit weitgehend tabuisiert wurden. Eigentlich unverständlich, denn ohne negative Rückmeldungen gibt es kaum Ansatzpunkte für positive Veränderungen bei der Konstruktion von Maschinen und Anlagen.

Dies hat sich inzwischen geändert: So veröffentlichte der Hauptverband der gewerblichen Berufsgenossenschaften eine Untersuchung, aus der hervorgeht, dass bei knapp 37 % der untersuchten metallverarbeitenden Maschinen Sicherheitseinrichtungen manipuliert waren. Im Klartext: Bei gut einem Drittel wurden Manipulationen entdeckt und untersucht, doch darf man davon ausgehen, dass die Dunkelziffer um einiges höher liegt.

Unverändert ist leider die Tatsache, dass sich an Maschinen mit manipulierten Schutzeinrichtungen immer wieder Unfälle ereignen, wie den Mitteilungsblättern der Berufsgenossenschaften regelmäßig zu entnehmen ist.

4.4.1 Zur Rechtslage

Die Rechtslage ist eindeutig: Hersteller von Maschinen sind aufgrund des europäischen und nationalen Rechts (z. B. EG-Maschinenrichtlinie und Produktsicherheitsgesetz) verpflichtet, nur Produkte mit ausreichender Sicherheit in den Verkehr zu bringen. Hersteller müssen bei allen Maschinen vorab sämtliche Gefährdungspotenziale ermitteln und die mit ihnen verbundenen Risiken bewerten. Den Ergebnissen der Risikoanalyse und Risikobewertung entsprechend sind sie verpflichtet, für die jeweiligen Produkte ein Sicherheitskonzept zu entwickeln, umzusetzen und zu dokumentieren. Potenzielle Gefahren dürfen sich weder schädigend auf spätere Benutzer und Dritte noch auf die Umwelt auswirken. Dabei müssen sie auch die vernünftigerweise vorhersehbare Fehlanwendung mit einbeziehen. Darüber hinaus sind in Betriebsanleitungen der bestimmungsgemäße Gebrauch von Produkten eindeutig festzulegen und bekannte sachwidrige Verwendungen zu verbieten.

Niemals dürfen Konstrukteure die technische Intelligenz und Kreativität von Maschinenbenutzern unterschätzen, wie einschlägige Praktiken zum Umgehen von Schutzeinrichtungen offenbaren: Dies beginnt mit plumpen, aber wirkungsvollen Eingriffen in den mechanischen Aufbau der Signalflusskette und reicht bis zu kunstvoll nachgefeilten Schaltzungen von Sicherheitsschaltern der Bauart 2. Nur schwer erkennbare, gelöste formschlüssige Welle/Naben-Verbindungen an Schaltnocken zählen ebenso dazu wie raffiniert herbeigeführte Leitungs- und Querschlüsse, getarnte und sorgfältig versteckte, aber schnell zugängliche Überbrückungsschalter in Öffner-Schließer-Kombinationen in der Verbindungsleitung zwischen Steuerung und Sicherheitsschalter. Dies ist nur eine kleine Kostprobe entdeckter Manipulationen ohne Anspruch auf Vollständigkeit.

4.4 Manipulation von Schutzeinrichtungen

Konstrukteure sollten darüber hinaus bedenken, dass Maschinenbediener, in der Regel mit technischem Verständnis und handwerklichem Geschick ausgestattet, vielfach wesentlich mehr Zeit haben, sich über nicht zu Ende gedachte Bedienungs- und Sicherheitskonzepte zu ärgern und über wirksame „Verbesserungen“ nachzudenken, als den Konstrukteuren Zeit zur Verfügung stand, eben diese Konzepte zu entwickeln und zu realisieren. Dabei waren sie nicht selten nur auf normative Vorgaben angewiesen – ohne tiefgehende Kenntnisse realistischer Praxisbedürfnisse.

Die Aufgabe, mögliche Manipulationen im Voraus zu berücksichtigen, ist daher widersprüchlich: Diesbezüglich sollten Konstrukteure Fantasie und Tatendrang der zwar häufig unter Druck stehenden, dennoch aber mit ausreichend Zeit und Energie zum Erarbeiten alternativer Lösungen ausgestatteten Bediener nachvollziehen. Sie sollen gewonnene Erkenntnisse in ihre Konstruktionen einbeziehen und unter den heute üblichen kurzen Zeitvorgaben in manipulationsfeste Sicherheitsmaßnahmen umsetzen. Eine Aufgabe, die nicht immer einfach zu lösen ist.

Um mögliche Manipulationen vorherzusehen, leistet die in der EN ISO 14119 enthaltene Checkliste zur Beurteilung der Anreize zum Umgehen von Verriegelungseinrichtungen wertvolle Dienste. Wünschenswert wäre es jedoch auch, würden sich Konstrukteure künftig verstärkt in die Lage des Benutzers versetzen und ehrlich und redlich die Frage beantworten, was sie wohl selbst mit dem vorgefundenen Bedienungs- und Sicherheitskonzept anstellen würden.

4.4 Manipulation von Schutzeinrichtungen

4.4.2 Sicherheitswidriges Verhalten – was steckt dahinter?

Begriffsbestimmung

Umgehen auf einfache Weise
Unwirksam machen von Hand oder mit leicht verfügbaren Gegenständen (wie z. B. mit Bleistiften, Drahtstücken, Flaschenöffnern, Kabelbindern, Klebestreifen, metallisierten Folien, Münzen, Nägeln, Schraubendrehern, Taschenmessern, Türschlüsseln, Zangen; aber auch mit Werkzeugen, die für die bestimmungsgemäße Verwendung der Maschine benötigt werden) ohne größere intellektuelle Anstrengungen oder handwerkliches Geschick (siehe auch EN ISO 14119).

Manipulation (lat. für Hand-, Kunstgriff)
Im Sinne der Sicherheitstechnik ein absichtlicher, eigenmächtiger, zielgerichteter und verdeckter Eingriff mit Werkzeug in das Sicherheitskonzept einer Maschine zum eigenen Vorteil (siehe auch EN ISO 14119).

Sabotage
Heimlich, absichtlich und böswillig herbeigeführter Eingriff in ein technisches System, um Arbeitgeber oder Kollegen zu schädigen. Wortursprung:
Ein in die Dreschmaschine geworfener Holzschuh (frz.: sabot) eines Landarbeiters resp. Maschinenstürmers im 19. Jahrhundert.

Mit der Konstruktion und Gestaltung von Maschinen legen Hersteller fest, was die Maschinen leisten können und sollen, gleichzeitig aber auch, wie die Benutzer mit ihnen umgehen werden. Zu einer erfolgreichen Konstruktion gehört nicht nur, dass die Maschine ihre technologische Funktion hinsichtlich der im Pflichtenheft dokumentierten Ausstoßmenge, Qualität und Toleranzen der zu erzeugenden Produkte erfüllt. Sie muss gleichzeitig ein schlüssiges Sicherheits- und Bedienungskonzept aufweisen, damit die Benutzer die Maschinenfunktionen überhaupt erst realisieren können. Beide Gestaltungsbereiche greifen ineinander, sie sollten daher auch gemeinsam und synchron entwickelt und verwirklicht werden.

Hier bieten inzwischen zahlreiche Produktsicherheitsnormen (z. B. die EN 1010 oder EN 12 717) praktikable Lösungen an. Trotzdem findet man, selbst an neuen Maschinen, immer wieder planerische und konstruktive Unzulänglichkeiten, wie z. B.

- wiederkehrende Störungen im Arbeitsablauf, hervorgerufen z. B. durch Mängel in der technologischen Konzeption oder in der Teilegenauigkeit (Originalton eines Betriebsingenieurs: „Den größten Beitrag zur aktiven Arbeitssicherheit können Konstrukteure leisten, wenn sie Maschinen so konstruieren, dass sie genau so funktionieren, wie es beim Kauf versprochen wurde.“),
- fehlende oder erschwerende Eingriffs- oder Zugriffsmöglichkeiten, um z. B. notwendige Stichproben gefahrlos entnehmen zu können,
- fehlende Segmentabschaltungen mit Materialpuffern, um bei Störungen gefahrlos in Teilbereiche eingreifen zu können, ohne dass die Gesamtanlage abgeschaltet und dann wieder zeitraubend hochgefahren werden muss.

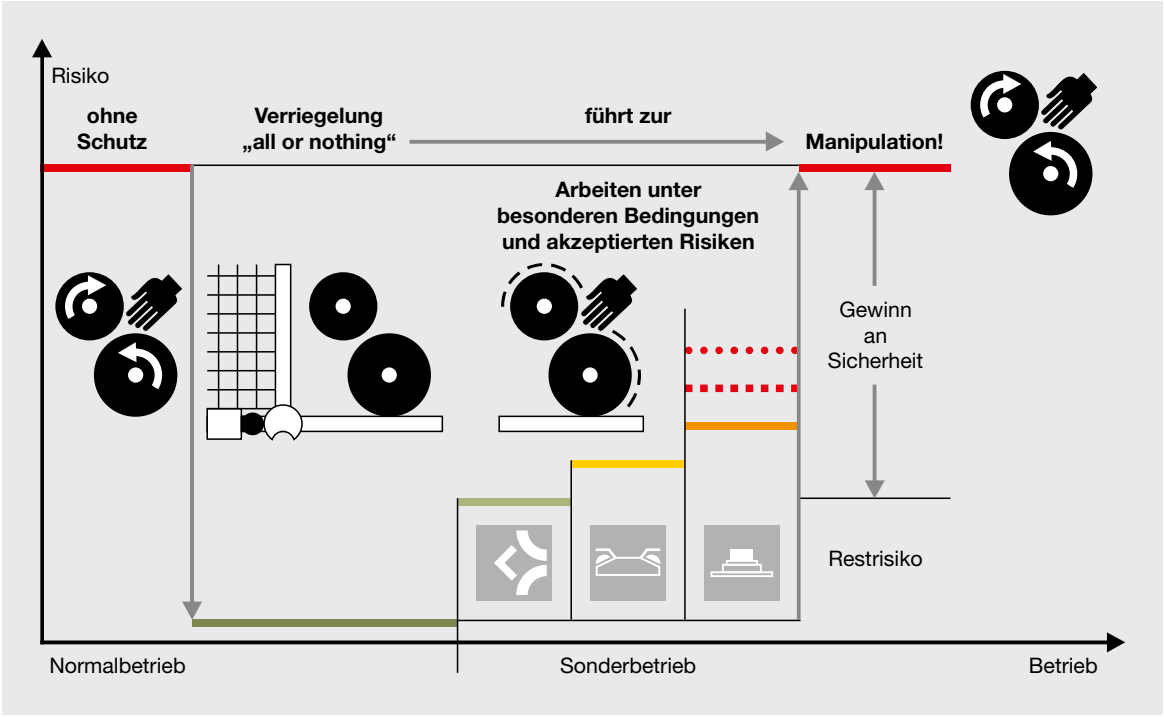
Aber auch auf nicht zu Ende gedachte Sicherheitskonzepte stößt man in der Praxis immer wieder. Viele Fehler werden bei verriegelten Schutzeinrichtungen begangen, so z. B. wenn

- ungefährliche oder häufig zu betätigende Funktionselemente, z. B. Stellteile, Vorratsbehälter, Einfüllöffnungen hinter (verriegelten) Schutzeinrichtungen untergebracht sind,
- die Verriegelung beim Öffnen einer Schutzeinrichtung die gefahrbringende Situation zwar schnell und zwangsläufig unterbricht, die Maschine oder der Prozess sich aber nachher überhaupt nicht mehr fortführen lässt oder neu gestartet werden muss.

4.4 Manipulation von Schutzeinrichtungen

Niemand zweifelt daran, dass Konstrukteure beim Konzipieren und Realisieren technologischer wie der auf den Menschen resp. Bediener bezogenen Funktionen nach bestem Wissen und Gewissen vorgehen. Man kann ihnen noch nicht einmal verübeln, dass sie dabei annehmen, dass sich spätere Benutzer beim Umgang mit den Maschinen vernünftig und korrekt verhalten werden. Genau hier ist Vorsicht geboten: Menschen verhalten sich, wie im täglichen Leben, so auch beim Lösen von Arbeitsaufgaben vor allem vorteilsorientiert. Sie streben an, die ihnen übertragenen oder selbstgestellten Aufgaben so schnell und so gut wie nötig zu erledigen, sich dabei gleichzeitig aber so wenig wie möglich zu beanspruchen.

Menschen versuchen auch aktiv und unterstützend in einen Prozess einzugreifen, wenn dieser nicht so verläuft, wie er soll. Sie bemühen sich, lästige Störungen auf schnellstem und einfachstem Wege zu beseitigen. Lässt das die Konzeption (und das in der Betriebsanleitung niedergeschriebene Entstörverfahren) nicht zu, suchen sie einen Ausweg, indem sie z. B. Verriegelungen umgehen. Oft fassen sie dabei den Mehraufwand als persönlichen Misserfolg bei der reibungslosen Erfüllung ihrer Arbeitsaufgabe auf. Die unter Umgehung der vorgesehenen Sicherheitsmaßnahmen weniger aufwendige Entstörungsprozedur wird als Erfolg erlebt. Erfolgreiches Verhalten tendiert dazu, wiederholt zu werden, bis es sich zu einer in diesem Fall leider sicherheitswidrigen und gefährlichen Gewohnheit verfestigt.



Verriegelungskonzept für Sonderbetriebsarten

4.4 Manipulation von Schutzeinrichtungen

Je häufiger solch ein Regelverstoß von der Führungsebene toleriert und nicht sanktioniert wird, umso größer ist die Wahrscheinlichkeit, weiterhin straflos gegen die Regel verstoßen zu können. Das unkorrekte Verhalten wird zur neuen informellen Regel. Denn im Laufe der Zeit stumpft das Bewusstsein gegenüber den eingegangenen Risiken ab, die Handelnden sind davon überzeugt, mögliche Gefahren durch umsichtiges Verhalten zu beherrschen. Dennoch ist die Gefahr objektiv vorhanden, sie wartet geradezu auf ihre Chance, irgendwann einmal zuzuschlagen.

Es steht außer Frage, dass die den Unfall auslösenden Faktoren vordergründig im Verhalten der Betroffenen liegen. Konzeptionelle Fehler der Maschine begünstigen jedoch das für die Betroffenen (lebens-)gefährliche Fehlverhalten. Solche Maschinen sind nicht konform mit der EG-Maschinenrichtlinie. Mit anderen Worten: Hersteller sind verpflichtet, Schutzmaßnahmen so zu konzipieren, dass bei ausreichender, d. h. dem ermittelten Risiko entsprechender Sicherheit die Funktionsfähigkeit und Benutzerfreundlichkeit der Maschine gewährleistet ist. Letztlich ist es in jedem Fall besser, mit einem sorgfältig durchdachten und mit der Praxis abgestimmten Sicherheitskonzept ein kalkulier- und akzeptierbares Restrisiko einzugehen, anstatt die Maschinenbediener nach erfolgreicher Manipulation dem vollen Risiko ungesicherter Abläufe auszusetzen.

4.4.3 Was können Konstrukteure tun?

Konstruieren sicherheitsgerechter Maschinen bedeutet mehr als das Einhalten von Vorschriften und anderen rechtlichen Vorgaben. Das Nachschlagen in den einschlägigen Regel- und Normenwerken sowie die latent abwehrende Frage „Wo steht das?!“ – um nur die allernötigsten Sicherheitsmaßnahmen umsetzen zu müssen – können intensives Nachdenken über sicherheits- und menschengerechte, aber dennoch betriebstaugliche Lösungen nicht ersetzen.

Vor allem müssen Konstrukteure sensibler auf die aus der Praxis kommenden Forderungen der Betreiber an die Bedienbarkeit von Maschinen und deren Sicherheitseinrichtungen reagieren und auf diese ernsthaft eingehen. Das erschwert nicht das sicherheitsgerechte Konstruieren, sondern ist die Grundlage, um benutzerfreundliche und zugleich sicherheitsgerechte Maschinen zu bauen. Das setzt voraus, dass dem eigentlichen Entwickeln und Konstruieren eine ausführliche und redliche Analyse betrieblicher Anforderungen vorausgeht, deren Ergebnisse in einer verbindlichen Anforderungsliste festgehalten werden. Andernfalls kann es passieren, dass Maschinen bzw. die dort getroffenen Sicherheitsmaßnahmen nicht akzeptiert werden. Vielmehr bringen sie ihre Benutzer auf „neue Ideen“, die meistens nicht im Sinne der Arbeitssicherheit sind. Diese können wiederum völlig neue Gefährdungen heraufbeschwören, an die während des Konstruierens niemand gedacht hatte.

Dennoch: Manipulation geschieht selten aus freien Stücken, sondern deutet auf nicht optimale Maschinen- bzw. Bedienungskonzepte hin. Mit sicherheitswidrigen Handlungen ist immer dann zu rechnen, wenn

- Arbeitsabläufe Handlungen abverlangen, die sich nicht unmittelbar positiv auf Arbeitsergebnisse auswirken,
- Arbeitsabläufe zu ständigen Wiederholungen immer gleicher Arbeitsschritte zwingen oder das Erreichen angestrebter Arbeitsziele immer wieder neuer Anläufe bedarf,
- Schutzeinrichtungen die für die Tätigkeit notwendigen Seh- und Bewegungsräume einschränken,
- Schutzeinrichtungen die zum erfolgreichen Arbeiten notwendige visuelle oder auditive Rückkopplung erschweren oder gar unterbinden,
- Fehlersuche und Entstören bei geöffneten Schutzeinrichtungen unmöglich sind.

4.4 Manipulation von Schutzeinrichtungen

Mit anderen Worten: Mit Manipulationen muss man immer dann rechnen, wenn eingeschränkte Maschinenfunktionen oder unzumutbare Erschwernisse die Maschinenbenutzer zum Nachbessern von Schutzkonzepten verleiten oder gar zwingen. Hersteller müssen demnach Schutzmaßnahmen so gestalten, dass bei tolerier- und akzeptierbaren Restrisiken sowohl Funktionsfähigkeit als auch Benutzerfreundlichkeit der Maschine gewährleistet bleiben: zukünftige Manipulationsversuche vorausdenken, ihnen mit Konstruktionsmaßnahmen entgegenwirken und zugleich die Handhabung der Maschinen verbessern.

Hersteller von Maschinen stehen demnach dreifach in der Pflicht:

1. Gründe und Anreize für Manipulationen vorwegnehmen, Umgehen von Verriegelungen präventiv verhindern durch zu Ende gedachte Bedienungs- und Sicherheitskonzepte von Maschinen.
2. Manipulationen konstruktiv erschweren, z. B. durch unzugänglichen Einbau von Sicherheitsschaltern, Verwendung von Scharnierschaltern, Befestigung der Sicherheitsschalter und deren Betätiger mit Schrauben, die sich zwar einschrauben, aber nicht mehr lösen lassen usw.
3. Unzulänglichkeiten im Rahmen der im Produktsicherheitsgesetz festgelegten Beobachtungspflicht systematisch aufdecken und beseitigen durch konsequente Produktbeobachtung bei allen Betreibern (Berichte der Kundendienstmonteure und Ersatzteillieferungen sind da manchmal sehr aufschlussreich!).

Aber auch der Auftraggeber einer Maschine kann Manipulationen entgegenwirken, indem er ein für beide Seiten verbindliches Pflichtenheft mit redlichen Anforderungen zusammen mit dem Maschinenhersteller diskutiert, erstellt und offen über Störungen und Unzulänglichkeiten des Prozesses spricht und diese Sachverhalte dokumentiert.

4.4.4 Benutzerfreundliche trennende Schutzeinrichtungen

Es ist wichtig zu wissen, dass Schutzeinrichtungen – selbst verriegelte – immer dann bereitwillig angenommen und nicht manipuliert werden, wenn sie Arbeitsabläufe nicht behindern, sondern unterstützen oder gar vereinfachen. Fehler im Sicherheitskonzept, die zu Manipulationen an Schutzeinrichtungen zwingen, sind dagegen veritable Konstruktionsfehler, für die Maschinenhersteller u. U. haften müssen. Sicherheitstechnische Lösungen mit toleriertem Restrisiko müssen nicht nur für den störungsfreien Normalbetrieb, sondern auch für das Rüsten, Testen, Entstören und für die Fehlersuche verwirklicht sein.

Manipulationsversuche nur technisch zu erschweren, löst das Problem nur scheinbar (siehe auch EN ISO 14119). Denn ist der Druck groß genug, findet man auch eine „Lösung“. Es muss vielmehr die Ursache für Manipulation behoben werden. Nicht Überfunktionalität (auch nicht sicherheitstechnische), sondern Benutzerfreundlichkeit ist gefragt. Sofern Zweifel bestehen, ob das Sicherheitskonzept ausreichend ist, empfiehlt es sich, sachkundigen Rat bei der zuständigen Berufsgenossenschaft oder beim Hersteller von Sicherheitskomponenten einzuholen.

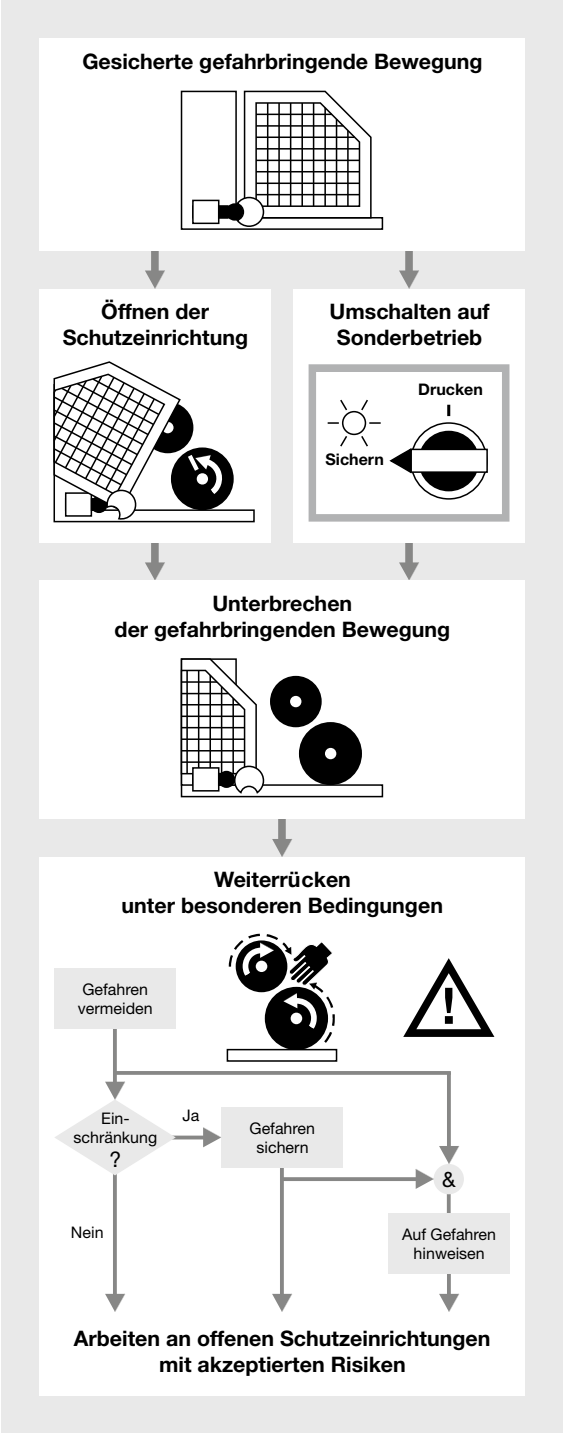
4.4 Manipulation von Schutzeinrichtungen

Trennende Schutzeinrichtungen unterbinden durch materielle Barrieren das räumliche und zeitliche Zusammentreffen von Menschen mit gefährlichen Situationen. Grundlegende Anforderungen an deren Gestaltung enthalten die EN 14120 und EN ISO 14119. Neben den zu lösenden Fragen zur Werkstoffwahl und der Berücksichtigung mechanischer Gesichtspunkte wie z. B. Festigkeit müssen sicherheitstechnische und ergonomische Aspekte in Betracht gezogen werden. Sie entscheiden nicht nur über die Qualität der Schutzfunktion, sondern auch darüber, ob die mit erheblichem Aufwand konstruierten und gefertigten Schutzeinrichtungen von den Beschäftigten bereitwillig genutzt, eher abgelehnt oder gar manipuliert werden.

Die Erfahrung zeigt, dass trotz aller Beteuerungen nahezu jede Schutzeinrichtung im Laufe der Zeit einmal abgenommen oder geöffnet werden muss. Grundsätzlich gilt, dass auch bei geöffneten Schutzeinrichtungen Gefährdungen möglichst vermieden und Beschäftigte vor Gefahren geschützt werden sollen. Über die Befestigungs- und Überwachungsmodalitäten der Schutzeinrichtungen entscheiden der Öffnungsgrund, die Öffnungshäufigkeit sowie das konkrete Risiko bei Tätigkeiten, die hinter geöffneten Schutzeinrichtungen durchzuführen sind (vgl. nachfolgende Abbildungen).

Öffnungsmodalitäten an Schutzeinrichtungen

4.4 Manipulation von Schutzeinrichtungen



Verriegelungskonzept für Schutzeinrichtungen.

Sind Schutzeinrichtungen betriebsbedingt häufiger zu öffnen, muss dies ohne Werkzeug möglich sein. Dann ist allerdings zu gewährleisten, dass gefahrbringende Situationen verriegelt oder gar zugehalten werden. Damit nun die erforderlichen Tätigkeiten bei geöffneten Schutzeinrichtungen mit akzeptablem Risiko durchgeführt werden können, müssen weitergehende Schutzmaßnahmen mit dem sich jetzt ergebenden Risiko sowie mit den (antriebs-) technischen und technologischen Gegebenheiten abgestimmt sein.

4.4.5 Schlussbetrachtung

Zum Schluss noch einige Merksätze für alle Konstrukteure: Verriegelungen so zu konzipieren, dass nach dem Öffnen der Schutzeinrichtung überhaupt keine Bewegung der Maschine oder von Teilbereichen mehr möglich ist, provoziert geradezu sicherheitswidriges Verhalten und in letzter Konsequenz Unfälle. Nichtsdestotrotz sind nicht die Menschen, sondern die Ursachen zu bekämpfen. Funktioniert eine Maschine nicht wie vorgesehen, helfen die Benutzer hier notgedrungen nach. Mit großer Wahrscheinlichkeit wird die Maschine sich dafür irgendwann einmal mit einem Unfall „revanchieren“. Dafür wurde sie eigentlich nicht konstruiert!


PASvisu Project
PILZ

5

Sichere Steuerungs-technik

5 Sichere Steuerungstechnik

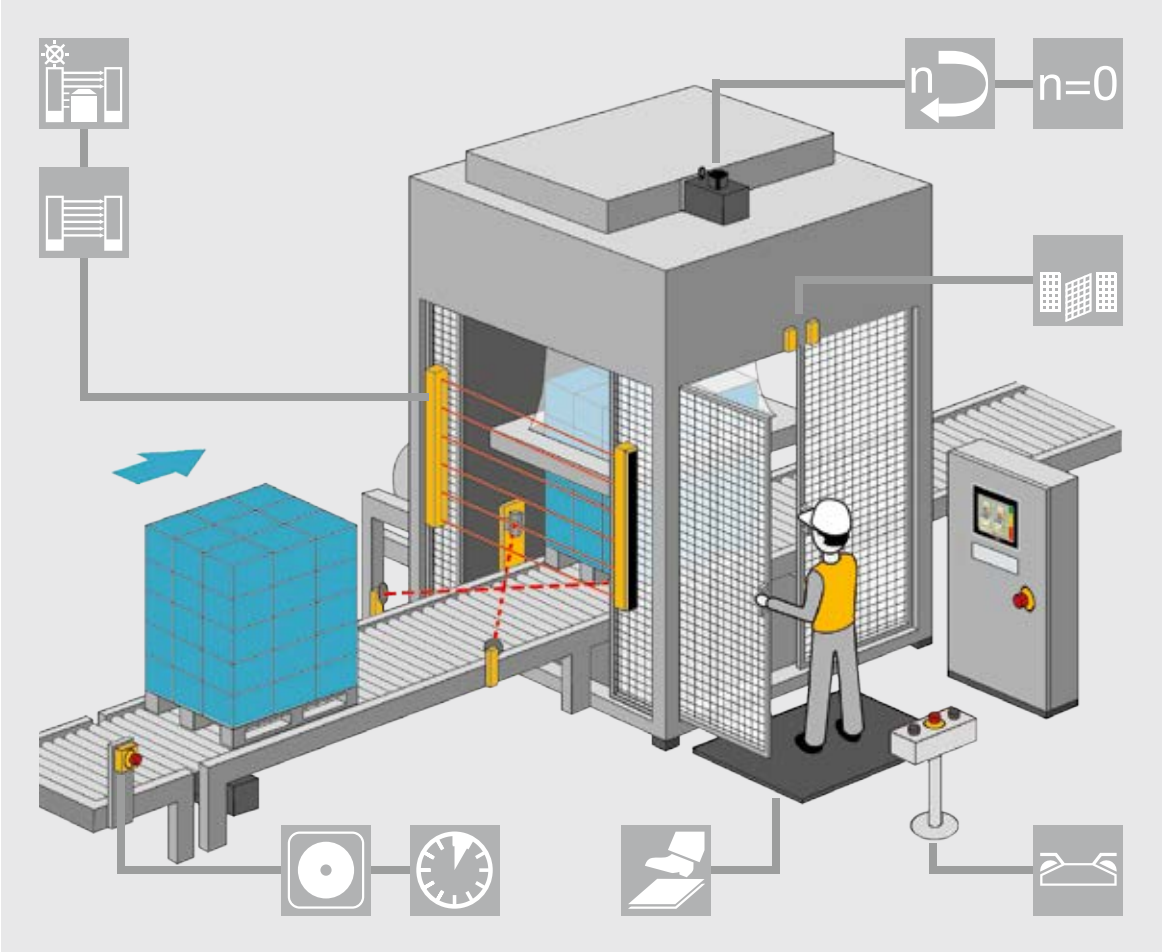
5 Sichere Steuerungstechnik

5.1 Sicherheitsschaltgeräte 5-4
5.1.1 Sicherheitsschaltgeräte im Überblick 5-4
5.1.2 Aufbau und Funktion von Sicherheitsschaltgeräten 5-4
5.1.3 Relais und Elektronik 5-6
5.1.4 Mehr Flexibilität bei der Installation 5-7
5.1.5 Spezielle Eigenschaften und Funktionen 5-10
5.2 Konfigurierbare sichere Kleinsteuerungen 5-11
5.2.1 Sichere und nicht sichere Kommunikation 5-13
5.2.2 Kundennutzen durch Funktions- und Logikelemente 5-16
5.3 Sicherheit und Automation 5-21
5.3.1 Sicherheitssteuerungen im Überblick 5-21
5.3.2 Integration in das Automatisierungsumfeld 5-22
5.3.3 Sichere Dezentralisierung und Zustimmprinzip 5-24
5.3.4 Funktionsbausteine in sicheren Steuerungen 5-25
5.3.5 Gebrauchsdauer bei Sicherheitsfunktionen 5-26
5.3.6 Einsatz gebrauchter Komponenten 5-26
5.4 Mit Sicherheitssteuerungen zur sicheren Steuerungstechnik 5-27
5.4.1 Übersicht 5-27
5.4.2 Strukturen der sicheren Steuerungstechnik 5-28
5.4.3 Modularisierung der Automatisierungsaufgabe 5-29
5.5 Sichere Steuerungstechnik im Wandel 5-30
5.5.1 Neue Anforderungen an die sichere Steuerungstechnik 5-30
5.5.2 Komplex und dennoch einfach – kein Widerspruch 5-32
5.5.3 Von statischer zu dynamischer Sicherheit 5-37
5.5.4 Über Industrie 4.0 5-38

5 Sichere Steuerungstechnik

In den Anfängen der Steuerungstechnik standen die Funktion und damit die Abbildung des Prozesses in einer Steuerung im Vordergrund. Relais und Schütze steuerten Maschinen und Anlagen. Sofern Einrichtungen zum Abschalten oder zum Schutz von Personen existierten, trennte man im Bedarfsfall einfach den Aktor von der Energieversorgung. Nach und nach reifte allerdings die Erkenntnis, dass diese Art von Sicherungssystem im Fehlerfall außer Kraft gesetzt werden könnte, die Schutzfunktion somit nicht mehr gegeben wäre. Dies gab den Anstoß, über Möglichkeiten der Sicherstellung derartiger Trennfunktionen nachzudenken. Spezielle Relaisverschaltungen wie z. B. die 3-Schütz-Kombination waren ein erstes Ergebnis solcher Überlegungen. Diese Gerätekombinationen führten letztlich zur Entwicklung des ersten Sicherheitsschaltgeräts, dem PNOZ.

Sicherheitsschaltgeräte sind somit Geräte, die in der Regel Sicherheitsfunktionen realisieren.
Eine derartige Sicherheitsfunktion hat die Aufgabe, das im Rahmen einer Gefährdung bestehende Risiko durch geeignete Maßnahmen auf ein akzeptables Maß zu mindern. Dies können Sicherheitsfunktionen wie Not-Halt, Schutztürfunktion oder auch die Stillstandsüberwachung eines Antriebs sein. Sicherheitsschaltgeräte überwachen also eine spezifische Funktion; durch Verschaltung mit weiteren Sicherheitsschaltgeräten stellen sie die Gesamtüberwachung einer Maschine oder Anlage sicher.
Die erste sicherheitsgerichtete Steuerung entstand letztlich aus dem Wunsch, ähnlich wie bei einer speicherprogrammierbaren Steuerung (SPS) Funktionen flexibel durch Programmierung verschalten zu können.



Sicherheitsfunktionen für alle Anforderungen

5.1 Sicherheitsschaltgeräte

Konfigurierbare sichere Kleinsteuerungen wie das PNOZmulti entstanden aus der Kombination von Sicherheitsschaltgerät und Sicherheitsteuerung. Unter Berücksichtigung der Vor- und Nachteile beider Systeme vereinen sie die Einfachheit eines Schaltgerätes mit der Flexibilität einer Sicherheitssteuerung. Zwar sind Sicherheitsschaltgeräte und Sicherheitssteuerungen primär auf die Überwachung von Sicherheitsfunktionen ausgerichtet, doch geht der aktuelle Trend in Richtung intelligente Verzahnung von Sicherheits- und Automatisierungsfunktionen in einem System.

5.1.1 Sicherheitsschaltgeräte im Überblick

Sicherheitsschaltgeräte führen definierte Sicherheitsfunktionen aus. Sie sorgen z. B. für

- ein gesteuertes und damit sicheres Stillsetzen einer Bewegung,
- die Positionsüberwachung von beweglichen Schutzeinrichtungen,
- die Unterbrechung einer Schließbewegung bei einem Eingriff.

Sicherheitsschaltgeräte dienen der Risikominderung: Sie leiten im Fehlerfall und bei Verletzung von Schutzbereichen eine sichere und zuverlässig erfolgende Reaktion ein. Sicherheitsschaltgeräte sind in nahezu allen Bereichen des Maschinen- und Anlagenbaus anzutreffen, vorrangig dort, wo die Anzahl der Sicherheitsfunktionen überschaubar ist. Allerdings gibt es zunehmend Bestrebungen, Diagnoseinformationen in Steuerungs- und Gesamtkonzepte zu integrieren. Daher wird man künftig in Maschinen und Anlagen immer häufiger Sicherheitsschaltgeräte, aber auch sichere Kleinsteuerungen mit Kommunikationsschnittstellen vorfinden.

Es liegt an ihrem klaren Aufbau und ihrer einfachen Handhabung, dass der Einsatz von Sicherheitsschaltgeräten keine besonderen Schulungsmaßnahmen erfordert. Normale Fachkenntnisse der Elektrotechnik und das Wissen über aktuell gültige Normen der Maschinensicherheit genügen in der Regel, um diese Geräte mit Erfolg zu nutzen. Die kompakte Bauform, ihre hohe Zuverlässigkeit und nicht zuletzt der Sachverhalt, dass die Sicherheitsschaltgeräte sämtliche geforderten Normen erfüllen, haben zu ihrer Verbreitung beigetragen. Inzwischen sind sie integrierter Bestandteil jeder Maschine oder Anlage geworden, bei denen Sicherheitsfunktionen eine Rolle spielen.

Seit der Entwicklung der ersten Sicherheitsschaltgeräte – zunächst nur für die Überwachung der Not-Halt-Funktion gedacht – hat sich eine Vielzahl von Geräten etabliert, die neben einfachen Überwachungsfunktionen sehr spezielle Aufgaben übernehmen können: so z. B. die Überwachung von Drehzahlen oder die Kontrolle von Spannungsfreiheit an einem Leistungsschütz. Die Geräte sind so konzipiert, dass sie mit den am Markt angebotenen Sensoren und Aktoren optimal und problemlos zusammenarbeiten. Heute ist praktisch für jede Anforderung ein Sicherheitsschaltgerät verfügbar. Mit ihrer Funktionsvielfalt können Sicherheitsschaltgeräte fast jede Sicherheitsfunktion realisieren, so z. B. die Überwachung der gesamten Sicherheitskette vom Sensor über die Auswertelogik bis zur Ansteuerung des Aktors.

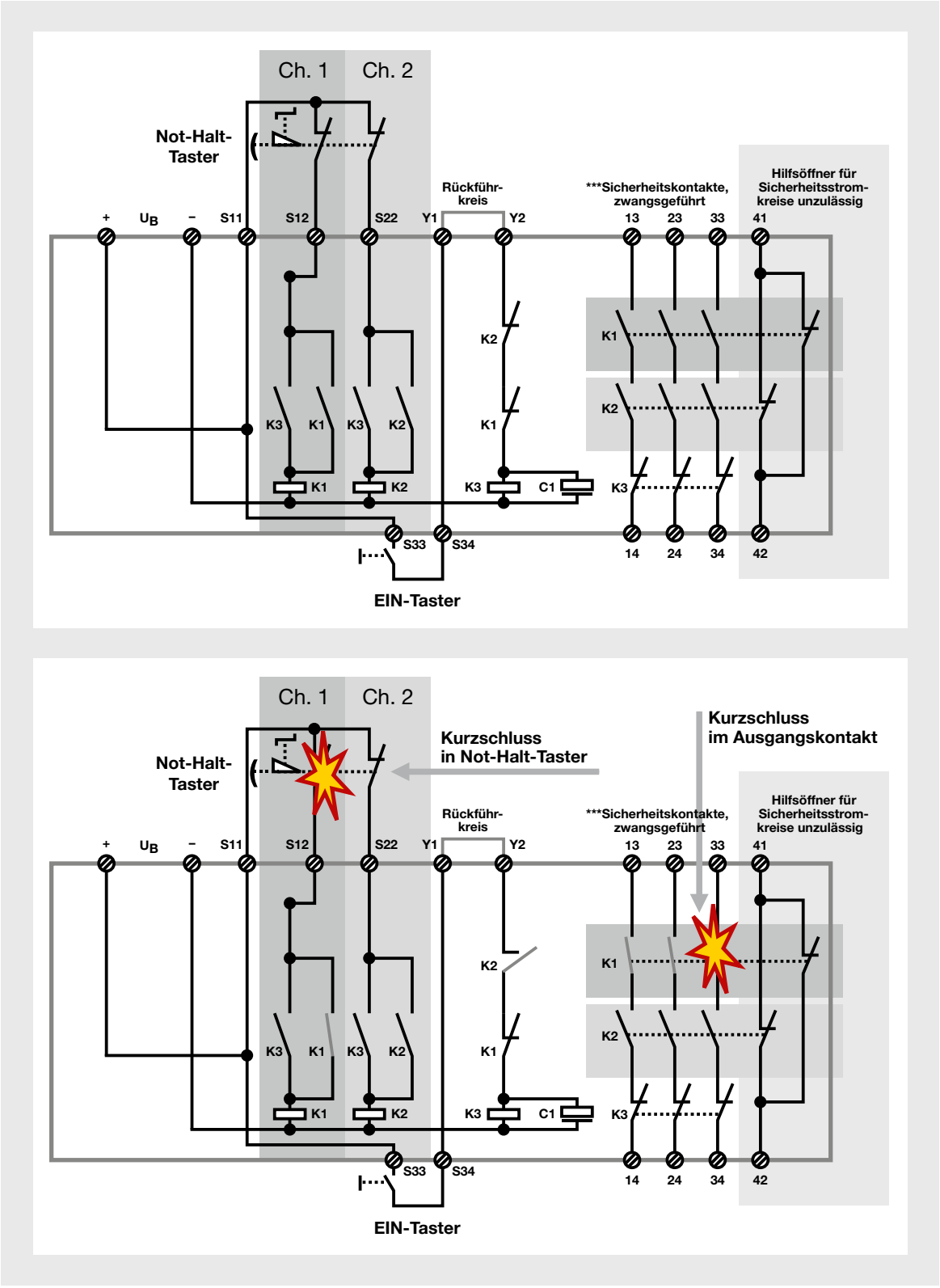
5.1.2 Aufbau und Funktion von Sicherheitsschaltgeräten

Heute unterscheiden sich Sicherheitsschaltgeräte primär im technologischen Aufbau:

- klassisch auf Basis kontaktbehafteter Relaistechnik
- mit elektronischer Auswertung und kontaktbehafteten potenzialfreien Ausgängen
- bis zu vollelektronische Geräte mit Halbleiterausgängen

Nichts geändert hat sich an der grundsätzlichen Anforderung, dass Sicherheitsschaltgeräte stets so aufgebaut sein müssen, dass – bei richtiger Beschaltung – weder ein Fehler im Gerät noch ein extern durch Sensor oder Aktor verursachter Fehler zum Verlust der Sicherheitsfunktion führen darf. Der technologische Wandel hat die Entwicklung elektronischer Sicherheitsschaltgeräte vorangetrieben, die einen deutlich höheren Kundennutzen bieten: Die elektronischen Geräte sind verschleißfrei, diagnosefähig und lassen sich auf einfachste Weise in gängige Bussysteme zu Steuerungs- und Diagnosezwecken einbinden.

5.1 Sicherheitsschaltgeräte



Aufbau und Funktion eines Sicherheitsschaltgeräts

5.1 Sicherheitsschaltgeräte

Der typische Aufbau eines Sicherheitsschaltgeräts der ersten Generation in Relaistechnik ist der klassischen 3-Schütz-Kombination nachempfunden. Der redundante Aufbau stellt sicher, dass Fehler in der Beschaltung nicht zu einem Verlust der Sicherheitsfunktion führen. Zwei Relais (K1, K2) mit zwangsgeführten Kontakten stellen die sicheren Schaltkontakte zur Verfügung. Die beiden Eingangskreise CH1 und CH2 steuern jeweils eines der beiden internen Relais an. Über das Startrelais K3 wird die Schaltung gestartet. Ein weiterer Überwachungskreis liegt zwischen den Anschlusspunkten Y1 und Y2 (Rückführkreis). Dieser Anschluss dient der Kontrolle und Stellungsüberwachung von Aktoren, die über die Sicherheitskontakte angesteuert oder abgeschaltet werden. Das Gerät ist so aufgebaut, dass es Fehler im Eingangskreis wie z. B. das „Verschweißen“ eines Kontakts des Not-Halt-Tasters oder eines der Sicherheitskontakte des Ausgangsrelais erkennt. Die Sicherheitseinrichtung verhindert das Wiedereinschalten des Geräts und damit das Aktivieren von Relais K1 und K2.

5.1.3 Relais und Elektronik

Sicherheitsschaltgeräte der neuesten Generation arbeiten mit Mikroprozessortechnologie. Diese Technik, wie z. B. in der Produktgruppe PNOZsigma umgesetzt, bietet gegenüber herkömmlichen Schaltgeräten weiteren Zusatznutzen. Neben einem geringeren Verschleiß durch Einsatz elektronischer Auswertungsverfahren und Diagnosefähigkeit reduzieren die Sicherheitsschaltgeräte die Variantenvielfalt: Ein Gerät kann nun für verschiedene Sicherheitsfunktionen und Sensoren eingesetzt werden, z. B. für kontaktbehaftete Sensoren wie Not-Halt-Taster oder mechanische Schutztürschalter, aber auch für Sensoren mit Halbleiterausgängen wie berührungslos wirkende Schutztürschalter, Lichtgitter sowie Zweihandbedienungen. Weil elektronische Sicherheitsschaltgeräte kompakter aufgebaut sind, beanspruchen sie deutlich weniger Platz.

Aufgrund der reduzierten Baugröße lassen sich auf gleicher Nutzfläche mehr Funktionen realisieren. Einstellbarer Anlauftest und optionales Rücksetzen zum Wiedereinschalten erlauben einen flexiblen Einsatz der Geräte. Da ein einziger Gerätetyp gleich mehrere und unterschiedliche Sicherheitsfunktionen umsetzen kann, sind Einsparungen bei Lagerhaltung, Projektierung, Konstruktion und letztlich auch bei der Inbetriebnahme von Maschinen und Anlagen die Folge. Dies verringert gleichzeitig den Engineering-Aufwand in jeder Lebenszyklusphase und vereinfacht notwendige Erweiterungen oder Anpassungen.

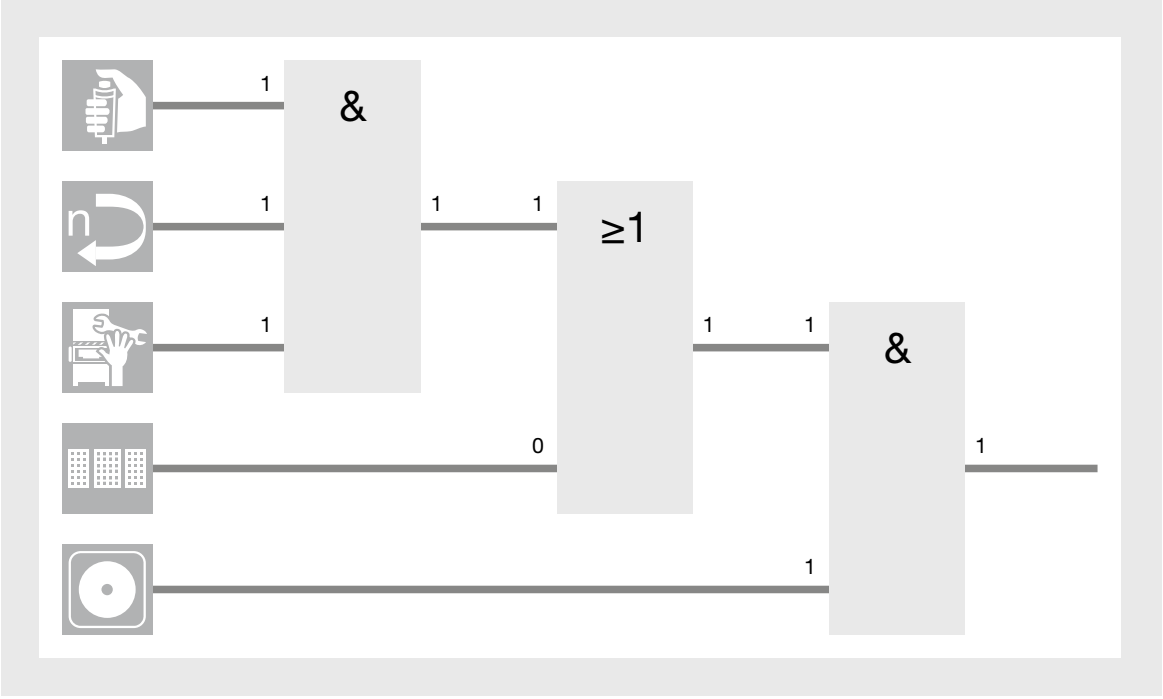
Elektronische Sicherheitsschaltgeräte und Kleinsteuerungen sind auf einfachste Art und Weise erweiterbar. Ob mit zusätzlichen Kontaktblöcken oder Funktionsmodulen: Eine Anpassung an die spezifischen Anforderungen der jeweiligen Maschine oder Anlage ist mit Kontakterweiterungen über Verbindungsstecker einfach und problemlos möglich. Der Anwender kann mit einem einzigen Grundgerät und, bedarfsabhängig, zusätzlichen Erweiterungen sämtliche klassischen Funktionen komplett umsetzen.

5.1 Sicherheitsschaltgeräte

5.1.4 Mehr Flexibilität bei der Installation

Lange Zeit war die Verschaltung der einzelnen Funktionen bei Sicherheitsschaltgeräten aufwendig und problematisch und wirkte sich nachteilig auf den Installationsprozess aus. Man stelle sich folgende Situation an einer Maschine vor: Eine Schutztür soll das zufällige oder unbedachte Betreten eines Gefährdungsbereichs verhindern. Ein Zutritt ist nur dann möglich, wenn die gefährliche Bewegung zuvor gestoppt wurde und sich die Maschine, zumindest im Gefährdungsbereich, in einem sicheren Zustand befindet. Man will jedoch, dass verschiedene Antriebe z. B. im Rahmen der Installation und Wartung mit reduzierter Geschwindigkeit betrieben werden können, selbst wenn die Tür geöffnet ist. Für diesen Zweck ist ein Zustimmschalter installiert, der gleichzeitig betätigt werden muss.

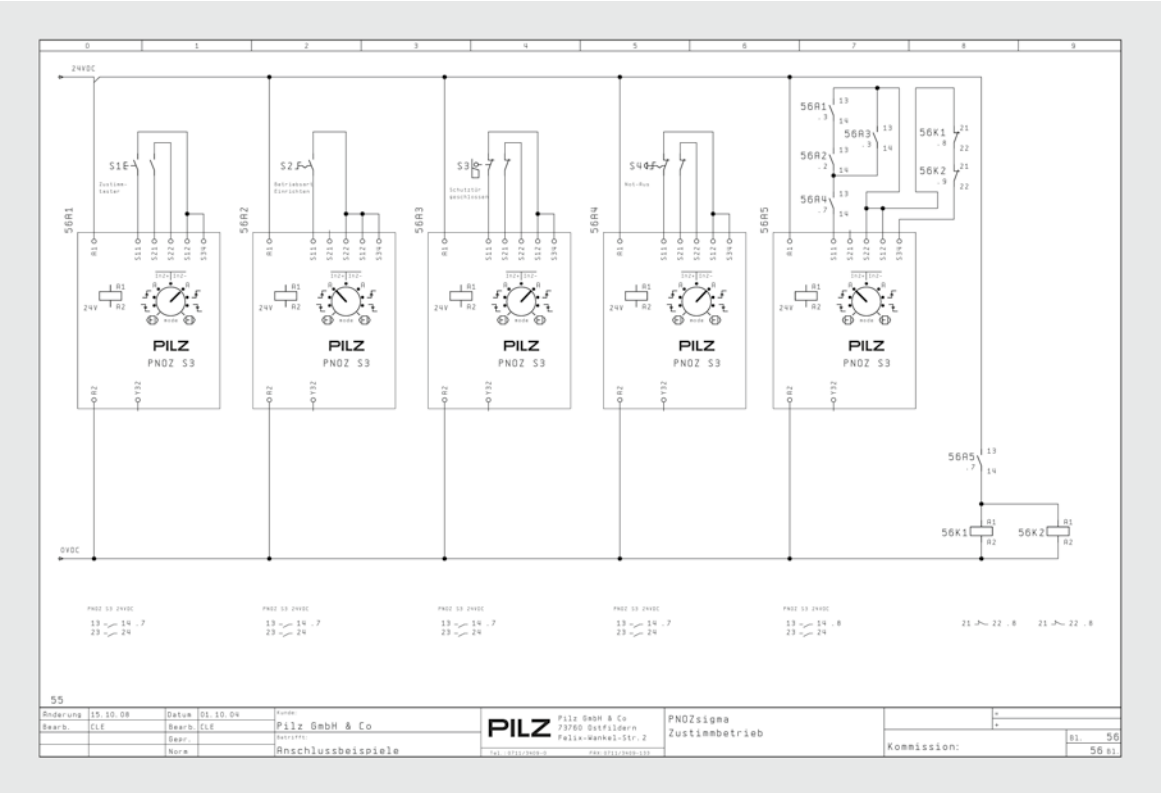
Möchte man diese Anforderungen in der Praxis so umsetzen, dass der Betreiber vor potenziellen Gefahren geschützt ist, hat dies einen erheblichen Verdrahtungsaufwand durch die Verschaltung der einzelnen Sicherheitsschaltgeräte zur Folge. Denn neben der eigentlichen Absicherung der Schutztür sind Sicherheitsschaltgeräte für den Zustimmschalter, für die Abfrage der Betriebsart „Einrichten“ sowie für die übergeordnete Not-Halt-Funktion notwendig. Rein auf die logischen Zusammenhänge reduziert könnte die Verschaltung wie nachfolgend aussehen:



Verschaltungsbeispiel

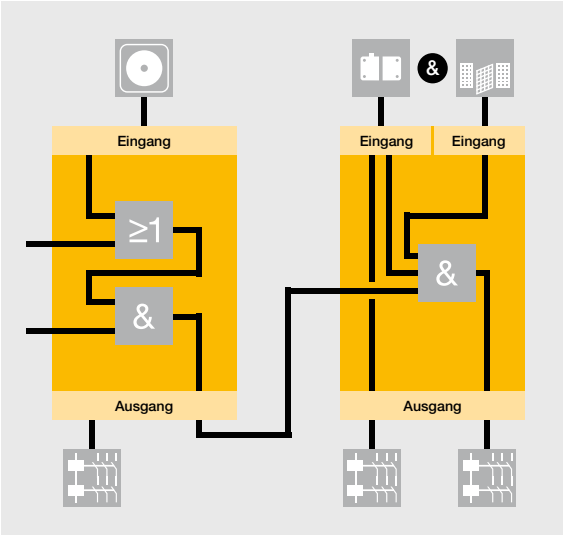
5.1 Sicherheitsschaltgeräte

Wird diese Applikation mit klassischen kontaktbehafteten Geräten umgesetzt, so entspricht dies in etwa der Ausführung in nachfolgender Darstellung:



Schaltungsbeispiel mit kontaktbehafteten Sicherheitsschaltgeräten

Anhand der Darstellung ist nachvollziehbar, dass eine Realisation mit kontaktbehafteten Geräten nicht gerade zu übersichtlichen Ergebnissen führt und aufgrund des immensen Verdrahtungsaufwands sehr kostenintensiv ist. Aus dieser Erkenntnis folgte fast zwangsläufig die Überlegung, logische Verknüpfungen zwischen den Sicherheitsschaltgeräten auf einfachere Art und Weise zu realisieren. Man begann also damit, neue Gerätetypen mit integrierter Verknüpfungslogik zu entwickeln.

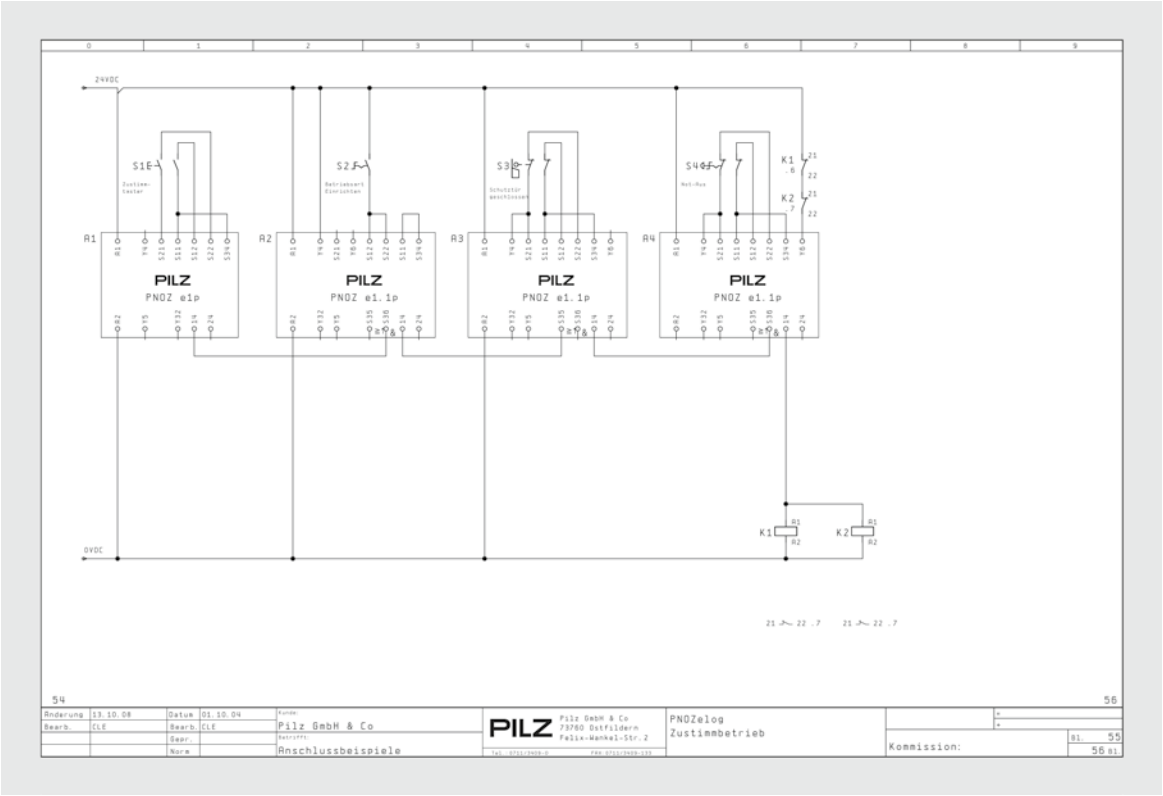


Weniger Verdrahtung durch verknüpfbare Ausgänge

5.1 Sicherheitsschaltgeräte

Die Mikroprozessortechnologie eröffnete hier völlig neue Möglichkeiten, was beispielsweise an den überwiegend elektronisch aufgebauten Geräten der Produktgruppe PNOZelog zum Ausdruck kommt. Dies schuf die Voraussetzungen für eine bis dahin ungeahnte Flexibilität: Ein Gerät ist nun für verschiedene Einsatzgebiete parametrierbar, ein weiteres Gerät für unterschiedliche Sicherheitsfunktionen. Anders als herkömmliche Sicherheitsschaltgeräte verfügen die Schaltgeräte über elektronische Sicherheits- und Hilfsausgänge in Halbleitertechnik. Sie sind dadurch wartungsarm und verschleißfrei und eignen sich deshalb besonders für Anwendungen mit häufigen Schaltvorgängen oder zyklischen Funktionen. Neben der eigentlichen Grundfunktion, wie z. B. der Überwachung einer Schutztür oder einer Not-Halt-Funktion, beinhalten diese Geräte einen Logikblock, der über spezielle Eingänge verfügt und logische UND- sowie ODER-Verknüpfungen zwischen den Geräten möglich macht. Ein Ausgangsblock mit Hilfs- und Sicherheitsausgängen komplettiert das Sicherheitsschaltgerät.

Das nachfolgende Applikationsbeispiel zeigt die Umsetzung des oben genannten Beispiels mit den elektronischen Sicherheitsschaltgeräten der genannten Produktgruppe. Im Vergleich zu einer Ausführung mit kontaktbehafteter Technologie ist die Darstellung wesentlich übersichtlicher, der Verdrahtungsaufwand sinkt drastisch.



Schaltungsbeispiel mit elektronischen Sicherheitsschaltgeräten

5.1 Sicherheitsschaltgeräte

5.1.5 Spezielle Eigenschaften und Funktionen

Ein wesentlicher Vorteil von Sicherheitsschaltgeräten ist deren Spezialisierung. Aufgrund der abgeschlossenen und klaren Aufgabe, die sie zu erfüllen haben, führten spezifische Kundenanforderungen zu einer Vielzahl von Sicherheitsschaltgeräten mit besonderen Funktionen und Eigenschaften: Dazu zählen beispielsweise Geräte mit Muting-Funktion, mit sicherer Überwachung von Drehzahl, Stillstand, Spannungsfreiheit oder Sicherheitsschaltgeräte im Ex-Bereich mit speziellen Eigenschaften. Nachfolgend einige Beispiele für derartige Funktionen.

5.1.5.1 Muting-Funktion

Die Muting-Funktion dient dazu, eine mittels Lichtvorhang oder Laserscanner realisierte Schutzfunktion zweckgerichtet – automatisch und zeitlich begrenzt – zu überbrücken. Eine Muting-Funktion wird häufig dazu verwendet, um Material in einen oder aus einem Gefahrenbereich zu transportieren.

5.1.5.2 Sicherheitsschaltgeräte für den Ex-Bereich

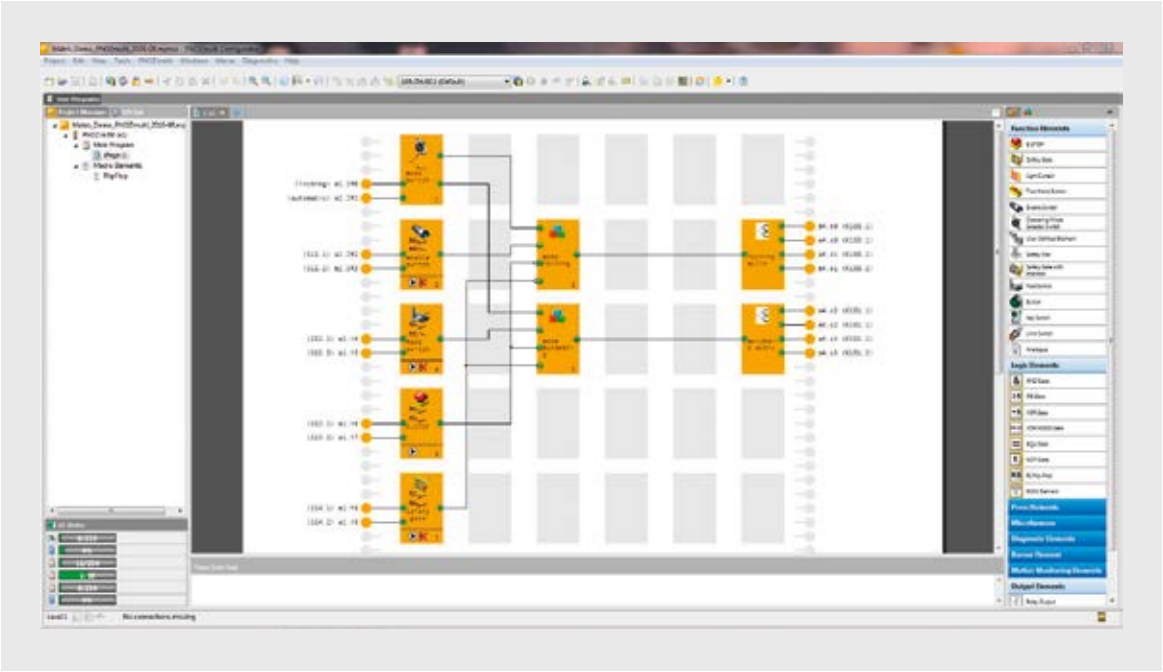
Zu den gefährlichsten Maschinen und Anlagen gehören solche, die Stäube, brennbare Gase oder Flüssigkeiten herstellen, transportieren, lagern oder verarbeiten. Bei diesen Prozessen können explosive Gemische entstehen, die bei Zündung eine Gefahr über das engere Bedienumfeld hinaus darstellen. In solchen explosionsgefährdeten Bereichen bedarf es spezieller Geräte, bei denen elektrische Funkenbildung an Kontakten sowie unzulässig hohe Temperaturen verhindert werden müssen. Solche Sicherheitsschaltgeräte müssen einen sogenannten eigensicheren Ausgangsstromkreis und potenzialfreie Kontakte für explosionsgefährdete Bereiche zur Verfügung stellen. Es stehen je nach Einsatzgebiet verschiedene Varianten an Sicherheitsschaltgeräten zur Verfügung, die für den Einsatz in explosionsgefährdeten Bereichen zugelassen sind.

Zertifiziertes Sicherheitsschaltgerät für den Ex-Bereich

5.2 Konfigurierbare sichere Kleinsteuerungen

Analog zum Fortschritt im Bereich der Automatisierungstechnik hat sich die sichere Steuerungstechnik von der verdrahteten Schütztechnik über kontaktbehaftete Sicherheitsschaltgeräte sowie Geräte mit integrierter Logikfunktion sukzessive in Richtung flexibel konfigurierbarer Kleinsteuerungen entwickelt. Dahinter steckte der Wunsch, sichere Steuerungstechnik für den Anwender transparenter und handhabbarer zu gestalten. Dies hat die Entwicklung der Geräte maßgeblich vorangetrieben und führte letztlich auch zur Entwicklung neuartiger Konfigurationstools, die Funktion und Logik grafisch darstellen und die konfigurierte Einstellung dann per Chipcard oder USB-Stick an das Basisgerät weitergeben. Dies ermöglicht dem verantwortlichen Elektrokonstrukteur ein Höchstmaß an Flexibilität, er muss nur die erforderlichen digitalen und analogen Ein-/Ausgänge planerisch berücksichtigen. Die Funktionen kann er zu einem späteren Zeitpunkt beliebig einbinden und ggf. an die veränderte Situationen anpassen. Ganz nebenbei entfällt jeglicher Aufwand für die Verdrahtung der Logikfunktionen.

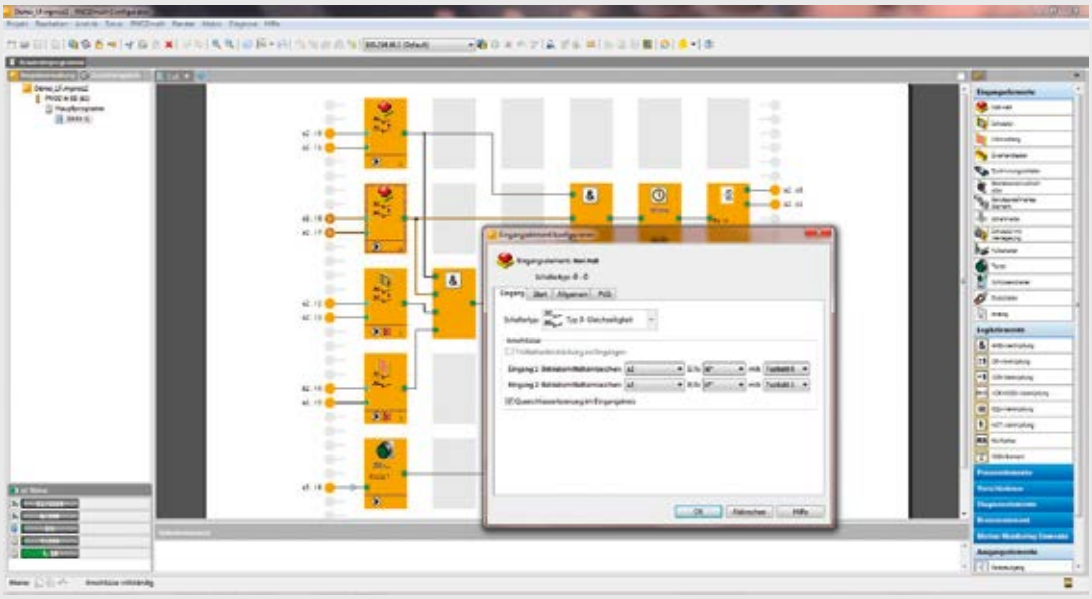
Die Sicherheitsfunktionen sowie deren logische Verknüpfung werden bei dieser Gerätegeneration ausschließlich über das Softwaretool konfiguriert. Der Hersteller stellt die Sicherheitsfunktionen als Funktionselemente bereit, die von benannten Stellen wie BG oder TÜV vorab sicherheitstechnisch geprüft wurden. Mithilfe der sicheren Funktionselemente und Logikverknüpfung der Elemente untereinander erstellt der Maschinen- oder Anlagenbauer die geforderte sicherheitsgerichtete Applikation, die er früher umständlich und zeitaufwendig über die Verdrahtung von Schützen und Schaltgeräten realisiert hätte. Linien zwischen den vorgefertigten Elementen ersetzen Kontakte und Drähte. Die Erstellung eines elektrischen Schaltplans mit der Abbildung der Logikfunktionalitäten entfällt.



Einfache Konfiguration durch logische Verknüpfung der Elemente

5.2 Konfigurierbare sichere Kleinsteuerungen

Neben der einfachen Verknüpfung von Funktionselementen untereinander lassen sich diese durch einen einfachen Mausklick auch noch optimal an die Anforderungen der Applikation anpassen. Einstellbare Eigenschaften bestimmen das Verhalten der einzelnen Elemente in der Applikation, ob ein- oder mehrkanalig, ob mit oder ohne automatischen Wiederanlauf z. B. beim Schließen einer Schutztür. Das Verhalten eines Elements lässt sich so, je nach Sicherheitsanforderung der Applikation, auf einfachste Weise parametrieren.



Eingangselemente konfigurieren

Die im Fenster „Eingangselement konfigurieren“ (siehe Abbildung) angebotenen Parameter spiegeln im Kern die von den Sicherheitsschaltgeräten bekannten Funktionen wider. Diese müssen nicht mehr umständlich am Gerät eingestellt oder durch Drahtbrücken gewählt werden, das funktioniert mit dem Parametriertool nun auf einfachste Weise. Der Anwender findet sämtliche nützlichen und bewährten Elemente aus der Welt der klassischen Sicherheitsschaltgeräte, nur eben in anderer Form dargestellt. Die neue Art der Konfiguration hat noch einen weiteren, ganz simplen sicherheitstechnischen Vorteil: Eine gewählte Konfiguration kann nicht einfach per Schraubendreher oder Gerätewahlschalter von Unbefugten verändert werden.

Die einfache Konfiguration der benötigten Eingangs- und Ausgangselemente sowie spezielle Elemente für Drehzahl oder Analogverarbeitung erlauben es dem Anwender, eine Sicherheitssteuerung nach seinen individuellen Bedürfnissen zu kreieren. Ohne großen Aufwand können Funktionen später hinzugefügt bzw. angepasst werden. Aus einer Liste kann der Bediener diese Elemente auswählen und die benötigten Logikfunktionen erstellen.

5.2 Konfigurierbare sichere Kleinsteuerungen

5.2.1 Sichere und nicht sichere Kommunikation

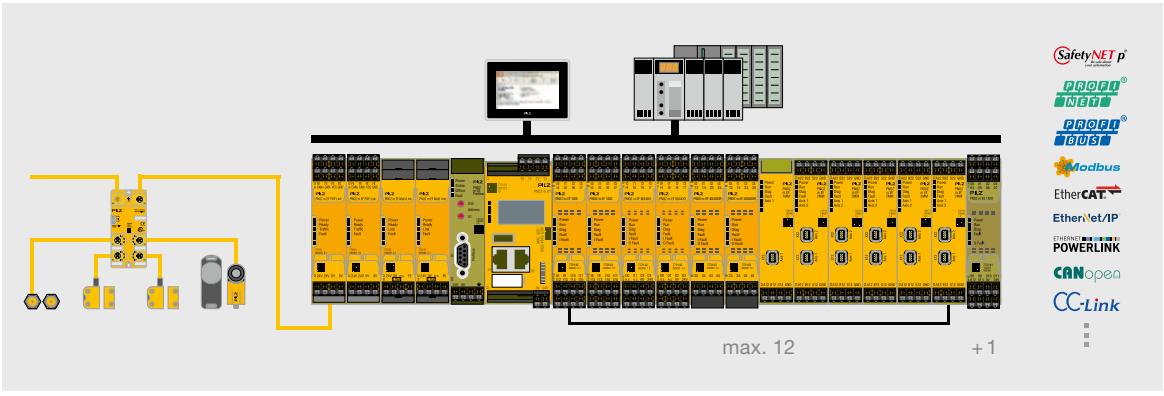
5.2.1.1 Nicht sichere Kommunikation von Standardsignalen und Diagnosedaten

Klassische Sicherheitsschaltgeräte in kontaktbehafteter Technologie können nur sehr eingeschränkt kommunizieren. Schon die Anzeige von Fehlerzuständen gestaltet sich teilweise schwierig. Wechselt man zu elektronischen Varianten, wird die Kommunikation bereits etwas komfortabler: Leuchtdioden blinken, teilweise mit wechselnden Frequenzen, zur Differenzierung spezifischer Fehlfunktionen. LCD-Anzeigen zeigen Fehler und/oder Betriebszustände im Klartext.

Konfigurierbare Kleinsteuerungen bieten hier ganz andere Möglichkeiten: Sie lassen sich über Feldbusmodule an annähernd jeden Feldbus koppeln. Hierdurch wird ein bidirektionaler Austausch von Signalen und Informationen auf einfache Weise ermöglicht. Dies bewirkt eine engere Verzahnung von Automation und Sicherheit und somit der gesamten Automationsstruktur. Die Feldbusmodule der konfigurierbaren Kleinsteuerungen verhalten sich in diesem Fall wie jeder andere Feldbusteilnehmer im Feldbussystem. Über diese Anbindungen lassen sich Diagnosedaten zu jedem Automatisierungssystem übertragen, was erheblich zur Reduzierung von Anlagen- und Maschinenstillständen führt.

Integrierte komfortable Diagnosekonzepte ermöglichen eine gezielte Fehlererkennung und Abhilfe. Über den von Pilz bereitgestellten OPC bzw. OPC UA Server ist mithilfe von Active-X-Elementen eine direkte Darstellung auf Bedienterminals möglich.

Über eine OPC UA Server-Anbindung kann PNOZmulti auch mit der webbasierten Visualisierungssoftware PASvisu verknüpft werden. Dabei werden alle Variablen der sicheren Kleinsteuerung übernommen. So kann lokal und über Fernzugriff ein umfassender und komfortabler Überblick über Maschinen und Anlagen geschaffen werden!



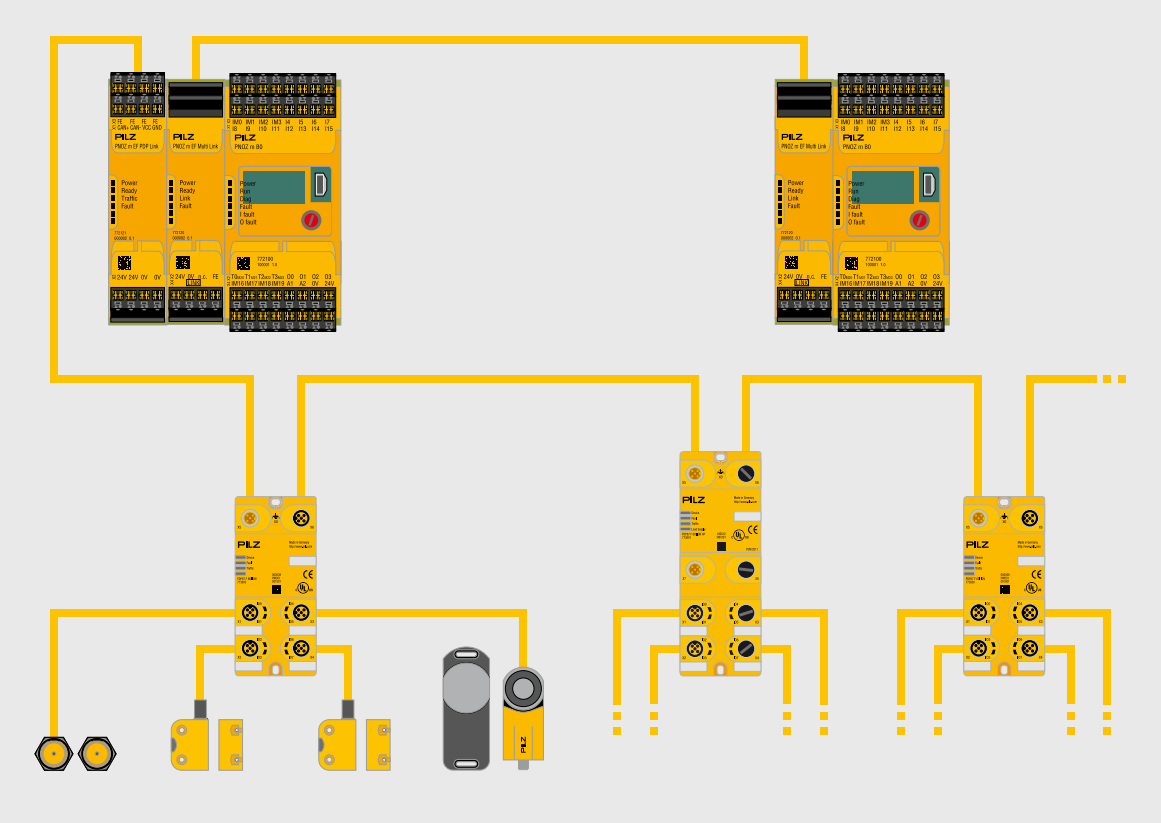
PNOZmulti 2 – für große Automatisierungsprojekte in Verbindung mit der Diagnoselösung PVIS, den Bedienterminals PMI, sicherer Sensorik PSEN und dezentraler Peripherie PDP67

5.2 Konfigurierbare sichere Kleinsteuerungen

5.2.1.2 Sichere Kommunikation mit konfigurierbaren Kleinsteuerungen

Der fortschreitende Vernetzungsgedanke ist bis auf die Ebene der konfigurierbaren Kleinsteuerung vorgedrungen. Über spezielle Linkmodule beziehungsweise Protokolle sind diese in der Lage, sicherheitsrelevante Daten bis zu Performance Level e nach EN ISO 13849-1 untereinander auszutauschen. Die sichere Datenübertragung mit dieser Technik bietet neue Perspektiven im Bereich der konfigurierbaren Kleinsteuerungen. Sollen beispielsweise mehrere Maschinen in einem engen Verbund zusammenarbeiten, verlangen die Sicherheitsanforderungen darüber hinaus den Austausch von Sicherheitssignalen zwischen den Steuerungen.

Dies konnte bisher nur mittels Austausch zwischen Hardware-Signalen bewerkstelligt werden. Das ist umständlich und aufgrund der hohen Kosten pro übertragener Information äußerst ineffizient. Benutzt man statt der bisherigen hart verdrahteten Lösung Linkmodule, so reduzieren sich Verdrahtungsaufwand und Kosten, gleichzeitig erhöht sich die Anzahl der Informationsdaten.



Verknüpfung von konfigurierbaren sicheren Kleinsteuerungen

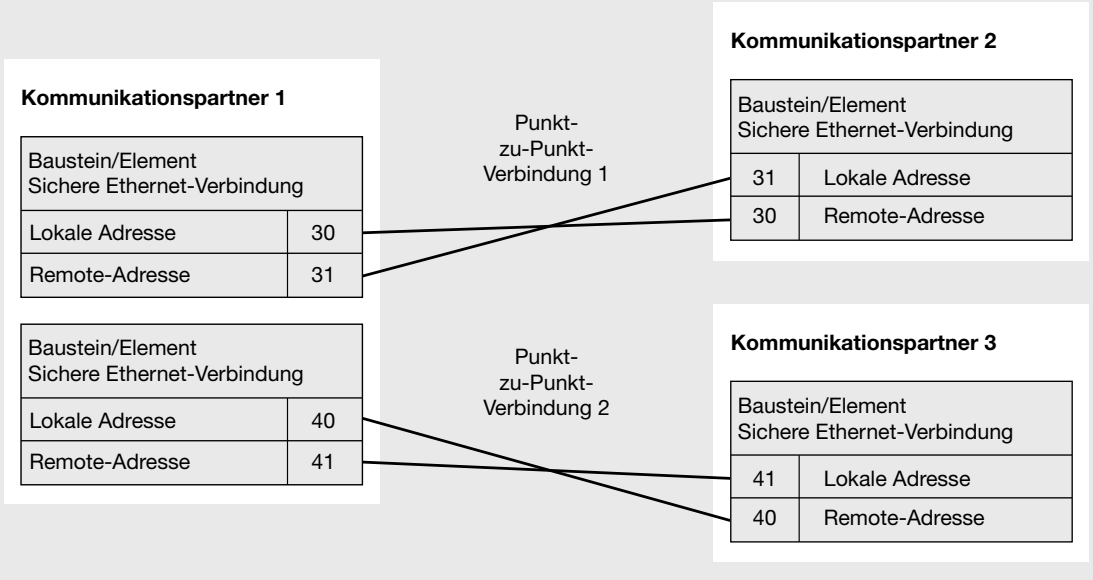
5.2 Konfigurierbare sichere Kleinsteuerungen

Neben den speziellen Linkmodulen kommen auch im Bereich der Sicherheitssteuerungen immer mehr Sicherheitsprotokolle auf Ethernetbasis zum Einsatz. Hierbei ermöglicht das Black-Channel-Prinzip, die parallele Nutzung des Ethernet-Netzwerks mit Automations- und Sicherheitsprotokollen.

Zur Übertragung von Sicherheitsinformationen wurde ein Funktions- und Logikelement entwickelt, das dem Anwender einfach ermöglicht, die Daten mit dem Automatisierungssystem PSS 4000 in komplexen Netzwerken auszutauschen.

Die Verlagerung dieser sicheren Kommunikation in Software-basierte Elemente oder spezielle Hardware ist die wohl effizienteste Lösung, die derzeit in der Vernetzung möglich ist.

Die sichere Ethernet-Verbindung (Safe Ethernet Connection) ermöglicht eine Punkt-zu-Punkt-Verbindung zwischen einem PNOZmulti Basisgerät und einem PSS 4000 Gerät. Über diese Verbindung können bis zu 48 sichere virtuelle Ein- und Ausgänge übertragen werden.



Verbindungsadressen bei zwei Punkt-zu-Punkt-Verbindungen

5.2 Konfigurierbare sichere Kleinsteuerungen

5.2.2 Kundennutzen durch Funktions- und Logikelemente

Konfigurierbare sichere Kleinsteuerungen bieten eine Vielzahl an vordefinierten Funktionselementen. Diese Elemente bilden die Basis für die Umsetzung der Anforderungen an die Sicherheitstechnik von Maschinen und Anlagen. Stehen Elemente für möglichst viele Anwendungsfälle und Funktionen zur Verfügung, kann der Anwender auf effektive, schnelle Art und Weise seine Anforderungen umsetzen.

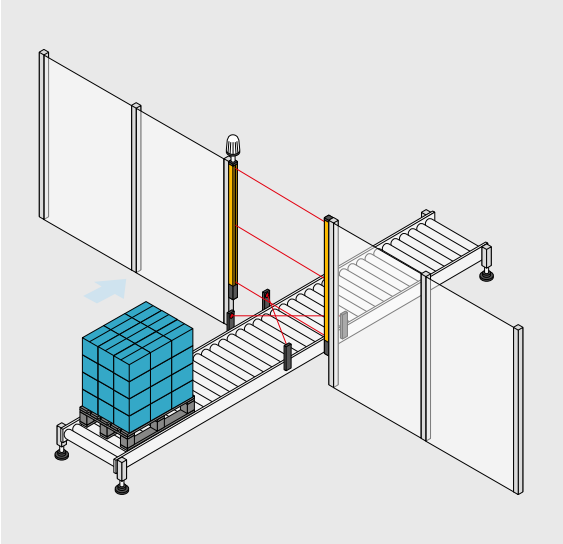
5.2.2.1 Funktionselemente für Muting-Funktion

Aufwendige Funktionen wie z. B. die „Muting-Funktion“, die bislang nur mit speziellen Schaltgeräten umsetzbar war, ist mit konfigurierbaren Kleinsteuerungen auf einfachste Weise realisierbar. Die Funktion dient dazu, eine Schutzfunktion wie Lichtvorhang oder Laserscanner zeitlich begrenzt und automatisch zu überbrücken. Anwendung findet sie beispielsweise, um Material in einen oder aus einem Gefahrenbereich zu transportieren. Man unterscheidet zwischen sequenziellem und Kreuz-Muting. Typische Anwendungsgebiete sind in der Automobilindustrie, bei Palettieranlagen von Getränkeabfüllern oder im Bereich der Herstellung von Steinerzeugnissen (Betonsteine, Dachziegel etc.) zu finden. Dabei nutzt man zusätzliche Sensorik, um Personen von Gegenständen unterscheiden zu können.

Beispiel: Sequenzielles Muting

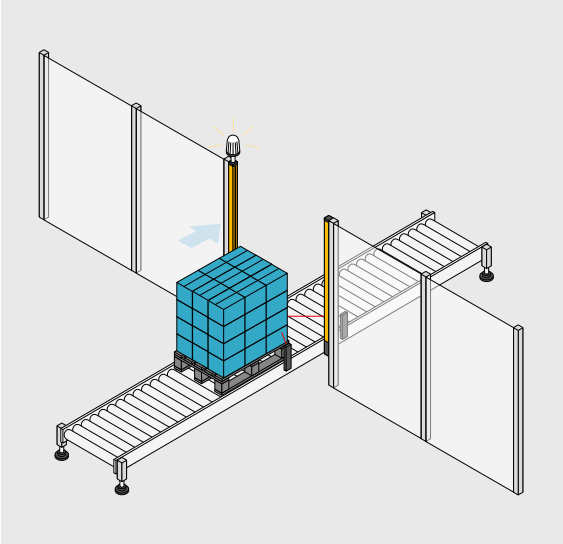
Muting-Phase 1:

- Material vor dem Gefahrenbereich
- Lichtvorhang aktiv
- Muting-Lampe aus



Muting-Phase 2:

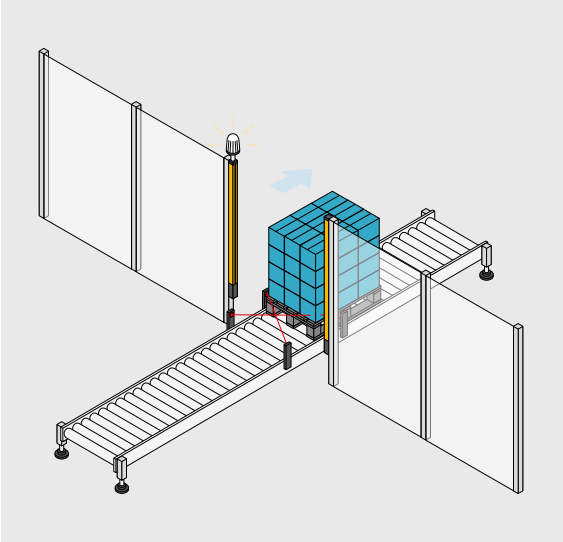
- Muting-Sensoren 1 und 2 betätigt
- Lichtvorhang überbrückt
- Muting-Lampe an



5.2 Konfigurierbare sichere Kleinsteuerungen

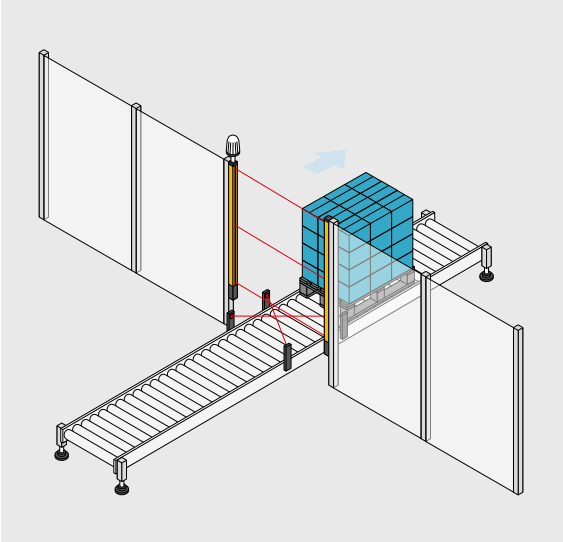
Muting-Phase 3:

- Muting-Sensoren 3 und 4 betätigt
- Lichtvorhang überbrückt
- Muting-Lampe an



Muting-Phase 4:

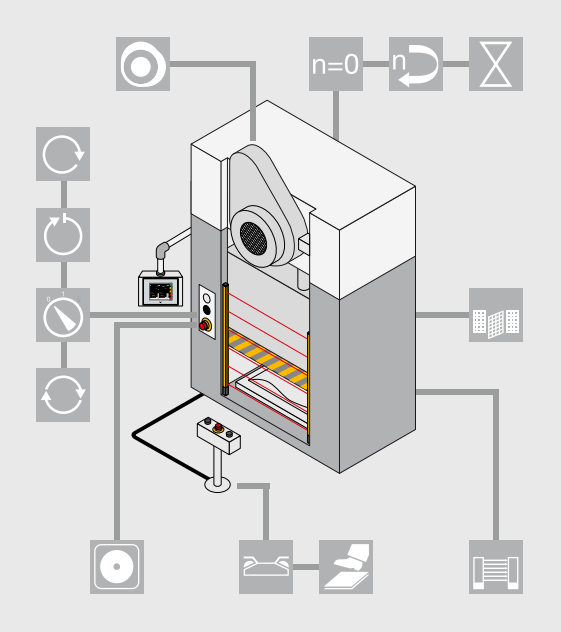
- Muting-Vorgang beendet
- Lichtvorhang wieder aktiv
- Muting-Lampe aus



5.2 Konfigurierbare sichere Kleinsteuerungen

5.2.2.2 Logikelemente für Pressenanwendungen

Neben den Logikelementen für einzelne Funktionen stehen auch komplette Anwendungspakete für konkrete abgeschlossene Anwendungen zur Verfügung, wie z. B. für mechanische und hydraulische Pressen. Solche Pakete sind derart ausgelegt, dass sie neben den sicherheitstechnischen Anforderungen auch Steuerungsaufgaben übernehmen können. Das Paket beinhaltet sämtliche Grundfunktionen, die eine Presse benötigt: z. B. Elemente für die Betriebsarten Einrichtbetrieb, Einzelhub, Automatik; Überwachung eines mechanischen Nockenschaltwerks; Laufwächterkontrolle zur Überwachung der mechanischen Kraftübertragung auf Wellenbruch; Überwachung von berührungslos wirkenden Schutzeinrichtungen im Schutz- und/oder Taktbetrieb; Ansteuerung und Überwachung des Pressensicherheitsventils sowie Hubauslösung mittels einer Zweihandansteuerung.

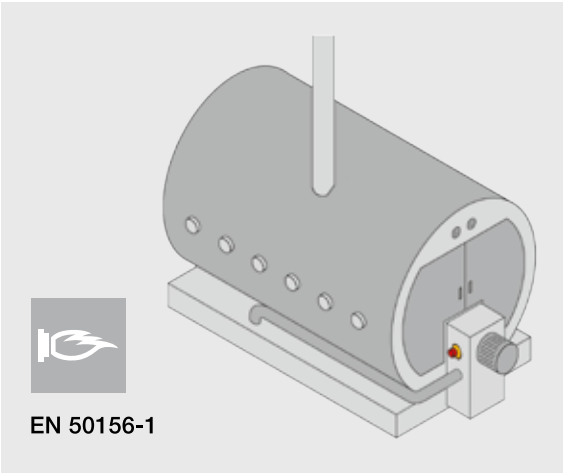


Sichere Steuerung und Überwachung von Pressen

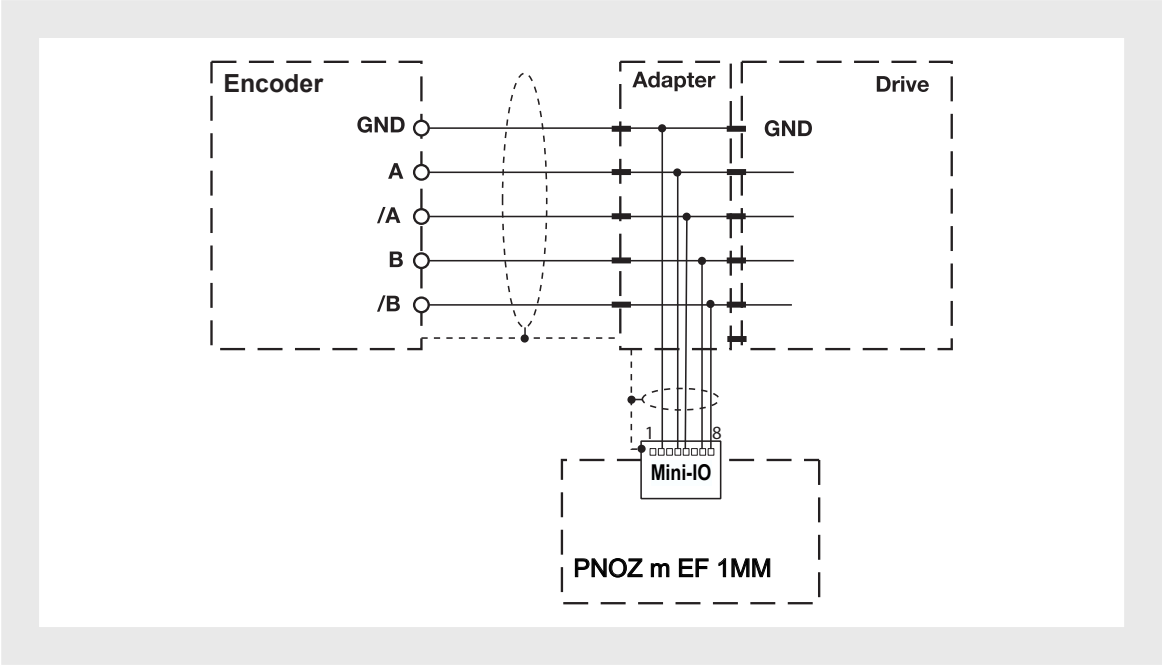
5.2.2.3 Logikelemente für Brenneranwendungen

Eine weiteres abgeschlossenes Anwendungspaket ist für Brenneranwendungen verfügbar. Das Logikelement Brenner ist ausgelegt für die Steuerung und Überwachung von Brennern (Feuerungsautomat) gemäß den meisten hierfür notwendigen Normen wie zum Beispiel EN 50156-1, EN 298 oder EN 676.

Durch das Element werden Sicherheitsketten, Verbrennungsluftdruck, Zündung, Flammenüberwachung, externe Verbundregelung oder Dichtheitskontrolle überwacht. Weiterhin können Funktionen wie Sicherheitsventile, Zündventile, Zündung oder auch externe Verbundregelung gesteuert werden. Durch die Parametrierung des Logikelements können diese Steuer- und Überwachungsfunktionen flexibel für den jeweils eingesetzten Brennertyp angepasst werden. Der Brennerablauf erfolgt dann in mehreren Phasen, bei denen je nach Brennertyp unterschiedliche Schritte durchlaufen werden. Sind die Eingangssignale für den Schritt korrekt, wird der nächste Ablaufschritt durchgeführt. Anderenfalls wird je nach Konfiguration eine Sicherheits- oder Störabschaltung durchgeführt.



5.2 Konfigurierbare sichere Kleinsteuerungen



„Mithören“ eines Standard-Encoders durch die Sicherheitssteuerung

5.2.2.4 Logikelemente im Antriebsumfeld

Neben allgemeinen Sicherheitsfunktionen wie der Überwachung von Schutztüren, der Not-Halt-Funktion oder der Auswertung von Lichtgittern bieten konfigurierbare Kleinsteuerungen erweiterte Möglichkeiten wie z. B. die sichere Erfassung von Bewegung und Stillstand an Antrieben mittels spezieller Erweiterungsmodule und spezifischer Logikelemente. Mit den Drehzahlwächtermodulen der PNOZmulti Geräte sind bis zu zwei Achsen pro Erweiterungsmodul mit jeweils acht Grenzwerten für Geschwindigkeits- und Stillstandsüberwachung sowie Rechts- und Linkslauferkennung möglich. Unabhängig vom eingesetzten Antriebssystem lassen sich so Bewegungsinformationen direkt in die Sicherheitskleinsteuerung integrieren.

Die Überwachung ist bis zum Performance Level d nach EN ISO 13849-1 mit regulären Standarddrehgebern möglich. Es werden keine teuren sicheren Geber benötigt. Durch einfaches „Mithören“ der Gebersignale – mittels „Anzapfen“ der Geberleitung über einen T-Verteiler – ist keine umständliche Verkabelung notwendig. Der direkte Signalabgriff am Motorgeber minimiert die Aufwendungen im mechanischen wie im elektrischen Aufbau durch passende Adapterkabel für verschiedenste Antriebe. Plug and play zur Drehzahl- und Stillstandserfassung einschließlich deren Auswertung mittels angepasster Logikelemente ist damit auf einfache Weise möglich.

5.2 Konfigurierbare sichere Kleinsteuerungen

5.2.2.5 Logikelemente für sichere Analogverarbeitung

Die sichere Verarbeitung von Analogsignalen war in der Vergangenheit mit Sicherheitskleinsteuerungen so gut wie nicht möglich. Erst die Integration spezieller Erweiterungsmodule und die Bereitstellung entsprechend angepasster Logikelemente hat die sichere Analogverarbeitung möglich gemacht. Ähnlich wie bei der Vorgehensweise im Antriebsumfeld lassen sich mit konfigurierbaren Kleinsteuerungen Sensorinformationen aus dem analogen Prozessumfeld auswerten. Dies können z. B. Prozesszustände wie Füllstand, Position, Temperatur oder Druck sein, die erweiterten Einsatzmöglichkeiten sind praktisch unbegrenzt. Mittels Konfiguration des Moduls bzw. Parametrierung des Logikelements sind auch für analoge Signale Grenz- und Schwellenwerte oder Wertebereiche definierbar, innerhalb derer sich ein Messwert bewegen darf. Damit wird zuverlässige Überwachung Realität, sämtliche Werte sind auswert- und weiterverarbeitbar.

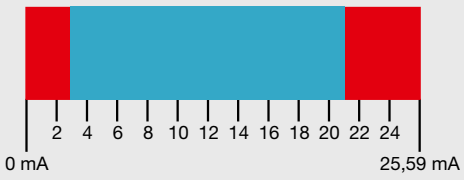
Beispiel: Bereichsüberwachung 4 … 20 mA Stromschleife

Bei einer Bereichsüberwachung definiert man zunächst den zulässigen Wertebereich. Je nach eingestellter Bedingung („größer als“ oder „kleiner als“) wird bei Über- oder Unterschreiten einer Bereichsgrenze der Ausgang für die Schwellenwertüberwachung auf „0“ gesetzt.

Im Beispiel sollen zwei Bereichsgrenzen definiert werden:

- I < 3 mA überwacht auf Drahtbruch und
- I > 21 mA überwacht auf Geberfehler

	Fehler wenn		Kommentar
	Bedingung	Wert	
R1	<	3 mA	Drahtbruch
R2	>	21 mA	Geberfehler



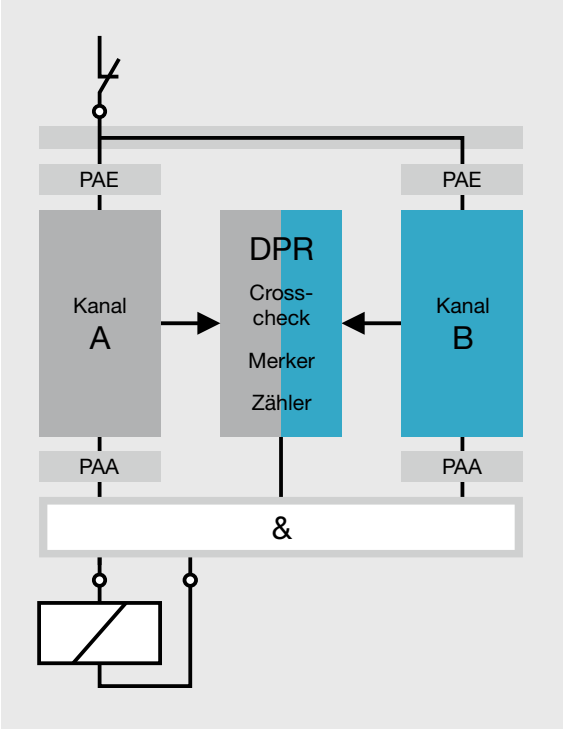
Beispiel: Positionsüberwachung eines Stellventils durch Bereichsüberwachung

Stellventile in der Prozesstechnik, z. B. für die Regelung von Durchflüssen, steuert man in der Regel analog an, gleichzeitig verfügen sie über eine analoge Rückmeldung der Ventilposition. Ohne sichere Analogverarbeitung konnten bisher nur spezielle Schalter die Stellungssignale von Ventilen digital auswerten. PNOZmulti erlaubt nun die Einstellung beliebig vieler Ventilstellungen und überwacht deren Einhaltung sicher und zuverlässig.

5.3 Sicherheit und Automation

5.3.1 Sicherheitssteuerungen im Überblick

Sicherheitssteuerungen entstanden vor allem aus dem Wunsch heraus, Sicherheit ähnlich wie bei einer SPS-Steuerung per Programmierung verschalten zu können. Es ist daher nicht verwunderlich, dass Sicherheitssteuerungen dem Muster der SPS-Welt folgen. Am Anfang standen zentrale, später folgten dezentrale Systeme in Verbindung mit sicheren Bussystemen. Die Programmierung folgte demselben Schema, nur den Befehlssatz reduzierte man von Beginn an drastisch. Zudem wurden einfache Sprachen wie IL (Instruction List) oder LD (Ladder Logic/Kontaktplan) verwendet. Diese Maßnahmen dienten der Sicherheit, denn man war der Ansicht, durch eine Einschränkung der Programmiermöglichkeiten Fehler bei der Programmerstellung minimieren zu können. Die ersten Systeme legten den Fokus eindeutig auf die Bearbeitung der Sicherheitsfunktionen. Obwohl von Anfang an eine Programmierung der Sicherheitssteuerung für Standard-Automatisierung möglich war, fand dies nur sehr eingeschränkt Anwendung in der Praxis. Mittlerweile halten jedoch immer mehr eingeschränkte Hochsprachen wie Strukturierter Text in der Programmierung Einzug.



Prinzipaufbau eines sicheren Steuerungssystems

Abgesehen von den sicherheitstechnischen Besonderheiten unterscheiden sich Sicherheitssteuerungen in ihrer eigentlichen Funktion nur unwesentlich von Steuerungen für die Standard-Automatisierung. Im Kern besteht eine Sicherheitssteuerung quasi aus zwei SPS-Steuerungen, die ein Anwendungsprogramm parallel abarbeiten, dasselbe Prozessabbild der Ein-/Ausgänge nutzen und sich ständig abgleichen. Was hier so einfach klingt, ist im Detail allerdings recht komplex: Quervergleiche, Tests der Ein-/Ausgangsebene, Ermittlung eines gemeinsamen gültigen Ergebnisses usw. sind allesamt vielschichtige Vorgänge, die solche Systeme intern aufwendig darstellen. Natürlich bemerkt der Anwender davon letztlich wenig, bis auf spezifische Besonderheiten wie z. B. die Nutzung von Taktsignalen zur Querschlusserkennung verhalten sich moderne Systeme wie andere SPS-Steuerungen auch.

Aufbau eines sicheren Steuerungssystems:

- zwei getrennte Kanäle
- diversitärer Aufbau mit unterschiedlicher Hardware
- ständiger Test der Ein- und Ausgänge
- ständiger Vergleich der Anwenderdaten
- Spannungs- und Zeitüberwachungen
- sichere Abschaltung im Fehler-/Gefahrenfall

5.3 Sicherheit und Automation

5.3.2 Integration in das Automatisierungsumfeld

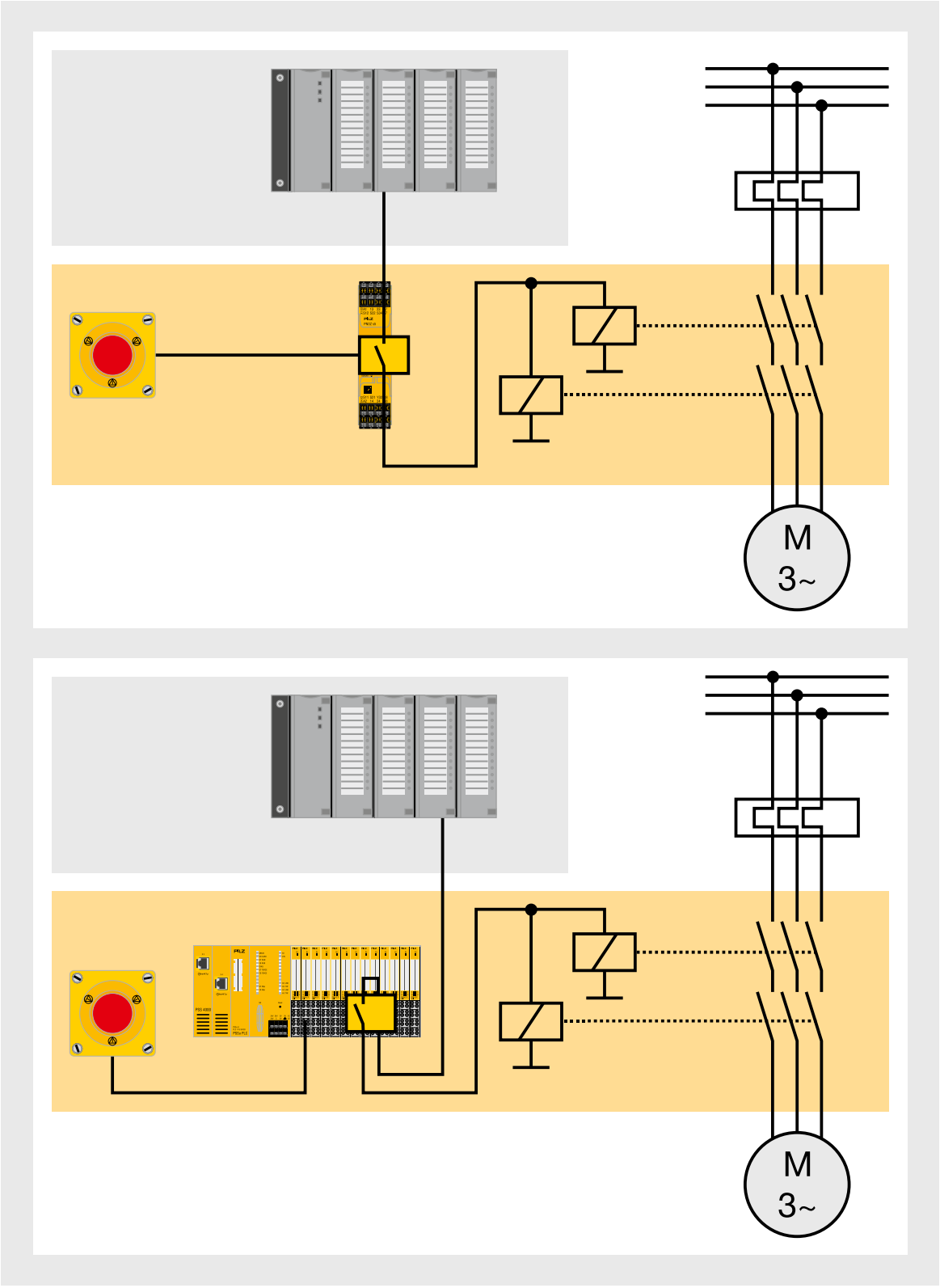
Taktzeiten werden immer kürzer, die Produktivität wie auch die Anforderungen an die Steuerungssysteme von Maschinen und Anlagen nehmen zu. Neben den steuerungstechnischen Anforderungen steigt mit Blick auf die Prozess- und Maschinendaten der Informationsbedarf ständig. Dies hat zur Folge, dass Kommunikationstechniken aus der Bürowelt Einzug in die Steuerungstechnik gehalten haben. Eine Auswirkung dieses Trends ist z. B. die Verbreitung von auf Ethernet basierenden Bussystemen in der Automatisierungstechnik bis auf die Feld- und Prozessebene.

Die Sicherheitstechnik fungierte früher mehr oder weniger ausgeprägt als sogenannte Überwachungsfunktion und gliederte sich als solche in die Automatisierungskette ein. Die Prozesssteuerung dominierte und bestimmte damit die eigentlichen Prozessschritte. Die Sicherheitssteuerung als „Überwachungsorgan“ stimmte den Entscheidungen der Prozesssteuerung entweder zu oder eben nicht. Die Abbildung auf der folgenden Seite veranschaulicht das Prinzip.

Die Überwachung und damit die Zustimmung ist auf sicherheitstechnisch relevante Steuerungsfunktionen begrenzt. Prozessausgänge ohne Sicherheitsanforderung sind nicht betroffen. Klarer Vorteil einer solchen Vorgehensweise ist die saubere Trennung der Aufgaben und somit der Verantwortlichkeiten. Ein getrenntes System ist für die Ausführung und Überwachung der Sicherheitstechnik verantwortlich, eine davon getrennte, separate Steuerung lenkt die Maschine und den Prozess. Damit ist die sogenannte Rückwirkungsfreiheit sichergestellt: Veränderungen vorrangig im Standard-Steuerungssystem bleiben ohne Auswirkung auf die Sicherheitssteuerung. Dies ist eine wesentliche Sicherheitsanforderung an ein Sicherheitssystem.

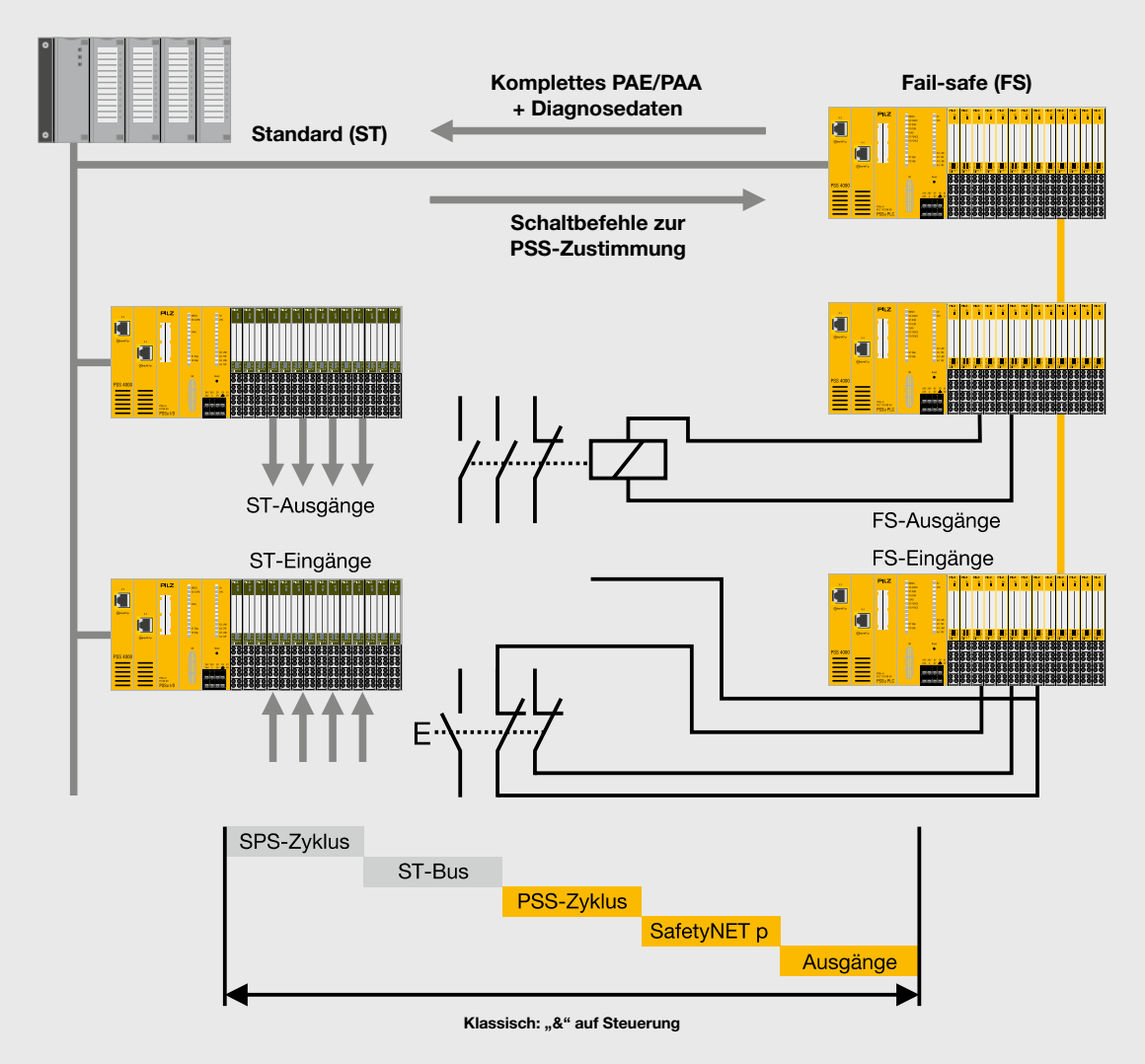
Die Aufgabenteilung hat mehrere positive Aspekte: Zum einen steigert sie die Gesamtperformance, weil sich jede Einheit nur um jene Dinge kümmert, für die sie ausgelegt und konzipiert wurde. Produktivitätssteigerungen wirken sich dabei nicht nur positiv auf die Ausbringung der Maschine oder Anlage aus: Sie können auch für die Handhabung förderlich sein, wenn beispielsweise schnellere Reaktionszeiten die Minimierung von Sicherheitsabständen erlauben. Zum anderen kann die Trennung dazu genutzt werden, die Verantwortlichkeit für die einzelnen Systeme unterschiedlichen Personen zu übertragen. Dies hilft beiden, weil sich so jeder auf seine Aufgabe konzentrieren kann.

5.3 Sicherheit und Automation



Funktionsprinzip Zustimmung mit Sicherheitsschaltgerät oder -steuerung

5.3 Sicherheit und Automation



Schaltbeispiel für das Zustimmprinzip

5.3.3 Sichere Dezentralisierung und Zustimmprinzip

Wie bereits mehrfach erläutert, folgt die Sicherheitstechnik in vielen Fällen den Entwicklungen der Standard-Steuerungstechnik. Die Vorteile der Verlagerung der Ein-/Ausgabeebene ins Feld mittels Dezentralisierung führten dazu, dasselbe nun auch auf die sicherheitsrelevanten Ein- und Ausgänge zu übertragen. Daraus folgte die Entwicklung eines Sicherheitsbussystems, das neben Ein- und Ausgängen im Feld auch die sicherheitsgerichtete Kopplung von Sicherheitssteuerungen untereinander erlaubt.

Die obere Abbildung zeigt eine typische Applikation, bei der das Zustimmprinzip umgesetzt ist. Die Sicherheitssteuerung schaltet die sicherheitstechnisch relevanten Ausgänge, die Standard-SPS überträgt den Schaltbefehl für den entsprechenden Ausgang via Feldbus an die Sicherheitssteuerung. Diese holt den Schaltbefehl dort ab und fügt ihn als UND-Funktion in das Ansteuerprogramm für den Ausgang ein. Modernere Steuerungen vereinen die Bearbeitung von Sicherheits- und Standardfunktion in einem Gerät. Die Datenübertragung findet somit innerhalb der Gesamtsteuerung zwischen dem Sicherheits- und Standardbereich statt. Die Datenlaufzeit über den Feldbus entfällt, wodurch die Reaktionszeiten sich deutlich verkürzen. Der Feldbus überträgt nun in einem Medium sichere und nicht sichere Daten an dezentrale Module.

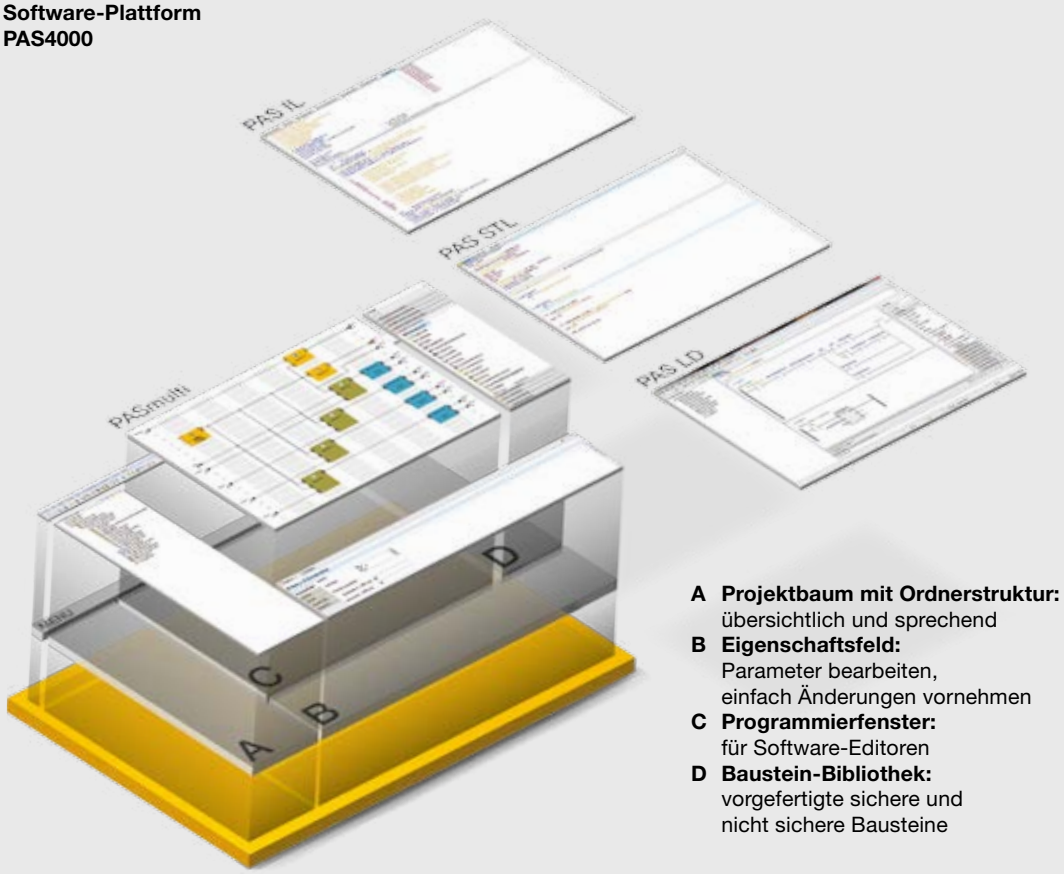
5.3 Sicherheit und Automation

5.3.4 Funktionsbausteine in sicheren Steuerungen

Funktionsbausteine für sicherheitstechnische Funktionen sind der Schlüssel zum Erfolg von Sicherheitssteuerungen. Waren sie anfangs mehr oder weniger nur ein Abbild der Funktionen und Eigenschaften von Sicherheitsschaltgeräten, kamen Zug um Zug neu entwickelte Elemente für spezifische Spezialanwendungen wie z. B. Pressenapplikationen oder Brennermanagement hinzu. Heute stehen Funktionselemente für fast alle denkbaren sicherheitstechnischen Anwendungen zur Verfügung. Diese sind alle durch benannte Stellen geprüft und bieten dem Anwender damit optimale Sicherheit im Alltagseinsatz.

Das Konzept der Funktionselemente war ursprünglich für die Sicherheitssteuerung gedacht und wurde dann wie beschrieben für die konfigurierbaren Kleinsteuerungen zu konfigurierbaren Logikelementen weiterentwickelt, um so die Anwendungen noch kundenfreundlicher zu gestalten. Auch bei Sicherheitssteuerungen ist das Prinzip der konfigurierbaren Logikelemente Teil einer weiterentwickelten Programmierumgebung. Der Anwender kann zwischen klassischer Programmierung z. B. in IEC 61131 und einer Konfiguration wählen, wie man sie von konfigurierbaren Kleinsteuerungen kennt.

Software-Plattform PAS4000



A Projektbaum mit Ordnerstruktur: übersichtlich und sprechend
B Eigenschaftsfeld: Parameter bearbeiten, einfach Änderungen vornehmen
C Programmierfenster: für Software-Editoren
D Baustein-Bibliothek: vorgefertigte sichere und nicht sichere Bausteine

Modulare Software zum Steuern, Programmieren und Überwachen am Beispiel der Software-Plattform PAS4000

5.3 Sicherheit und Automation

5.3.5 Gebrauchsdauer bei Sicherheitsfunktionen

Was geschieht am Ende der Gebrauchsdauer (T_m) mit Komponenten in Sicherheitsfunktionen (ausgelegt nach EN ISO 13849-1 oder IEC 62061)?

Seit Anwendung der EN ISO 13849-1 für Auslegung und Validierung steuerungstechnischer Sicherheitsfunktionen ist die Einsatzdauer der entsprechenden Baugruppen ein Thema. Die Norm gibt als Standardwert einen Zeitraum von 20 Jahren für sicherheitstechnisch relevante Komponenten vor. Es ist allerdings auch möglich, Komponenten mit kürzerer Gebrauchsdauer einzusetzen, sofern in den Begleitunterlagen der Maschine eindeutig auf diese Komponente und die daraus entstehende Austauschnotwendigkeit hingewiesen wird.

Auch wenn das Thema derzeit noch weitgehend ausgeklammert wird: Bei langlebigen Maschinen wird der Zeitpunkt kommen, an dem die projektierte Gebrauchsdauer abläuft, die Maschine aber noch weiter verwendet werden soll. In diesem Fall ist die sicherheitstechnische Integrität nur dann weiter gewährleistet, wenn die betroffenen Komponenten ausgetauscht werden. Da zu diesem Zeitpunkt der ursprüngliche Maschinenhersteller wahrscheinlich keine Verpflichtungen mehr an der Maschine hat, geht die Verantwortung dafür an den Betreiber über. Die betroffenen Komponenten müssen identifiziert und ersetzt werden. Die neuen Komponenten müssen wiederum vergleichbare oder bessere sicherheitstechnische Kenndaten (PL, SIL, $B10_d$, $MTTF_d$ usw.) aufweisen. Dies kann dadurch erleichtert werden, dass der ursprüngliche Maschinenhersteller diese Daten von vornherein mit bekanntgibt (z. B. durch Nachweis der Auslegung mithilfe eines Berechnungsprogrammes wie PAScal). Vorstellbar ist in dieser Situation, dass Komponenten ausgetauscht werden, die äußerlich einwandfrei aussehen und auch ihre steuerungstechnische Aufgabe nach wie vor anstandslos leisten. Dennoch ist ein Austausch erforderlich, da die Wahrscheinlichkeit eines gefahrbringenden Ausfalls über das akzeptable Maß hinaus gestiegen ist.

Theoretisch gibt es die Möglichkeit, eine gebrauchte Komponente z. B. durch den Hersteller überprüfen und evtl. so instandsetzen zu lassen, dass eine neue Gebrauchsdauer (T_m) beginnt. Dieser Ansatz wird jedoch nur selten und nur bei sehr wertvollen Komponenten wirtschaftlich sein.

Auch die IEC 62061 kennt eine ähnliche Größe, nämlich das „Proof-Test-Intervall“. Nach Ablauf eines solchen Intervalls muss das Bauteil einem Proof Test unterzogen werden, um die weitere Verwendbarkeit zu untersuchen. Die Situation ist vergleichbar zu der nach der EN ISO 13849-1, nur das die Gebrauchsdauer nicht auf 20 Jahre fixiert ist, sondern vom Hersteller individuell festgelegt wird und damit schwieriger nachzuvollziehen ist.

5.3.6 Einsatz gebrauchter Komponenten

Grundsätzlich ist auch der Einsatz gebrauchter Komponenten zu betrachten. Sinnvoll ist das nur bei hochwertigen Komponenten, die noch einen erheblichen Restwert haben, der den zusätzlichen Aufwand rechtfertigt. Sollen in neu zu realisierenden Sicherheitsfunktionen gebrauchte Komponenten eingesetzt werden, ist abzuschätzen, welcher Anteil der Gebrauchsdauer (T_m) bereits abgelaufen ist bzw. wie viel davon noch verbleibt. Auch andere Kenndaten, insbesondere der $B10_d$-Wert bei Komponenten, die durch Betätigung verschleißen, können teilweise verbraucht sein. Solche Komponenten sind also nur dann einsetzbar, wenn eine Verfolgung und Dokumentation ihres bisherigen Einsatzes vorhanden ist. In der Validierung der neuen Sicherheitsfunktion muss dann mit diesen (reduzierten) Werten gerechnet werden.

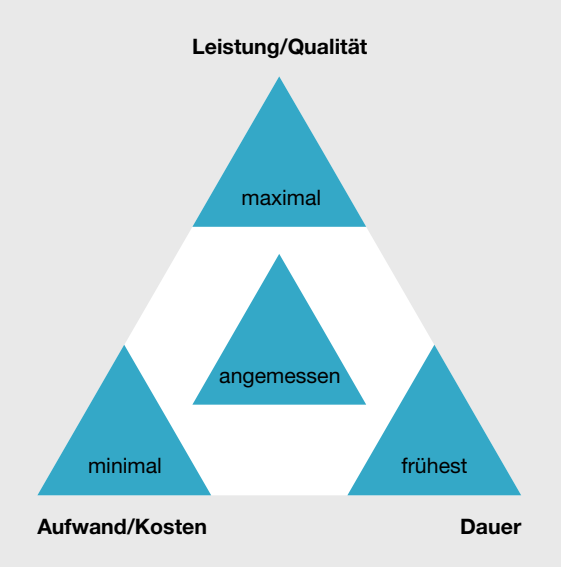
5.4 Mit Sicherheitssteuerungen zur sicheren Steuerungstechnik

5.4.1 Übersicht

In welche Richtung entwickelt sich die Sicherheitstechnik, welche Steuerungssysteme stiften den höchsten Anwendernutzen? Wie werden künftig die verschiedenen Disziplinen Sicherheit, Steuerung, Motion, CNC und Visualisierung zusammenarbeiten? Wird es gelingen, trotz zunehmender Komplexität kostengünstige Lösungen zu realisieren? Auch in Zukunft wird es verschiedene Ansätze zur Erfüllung der Anforderungen geben. Ein möglicher Ansatz ist die Modularisierung der Maschinen und Anlagen in funktionelle Einheiten. Dies findet bereits heute statt, allerdings vorzugsweise für den mechanischen Teil der Maschinen und Anlagen. Steuerungstechnisch wird dieser Ansatz bislang nur partiell genutzt.

Gleichgültig ob im Hinblick auf Sicherheits- oder auf andere Automatisierungsaufgaben: Die Anforderungen an Maschinen und Anlagen werden immer umfangreicher, daher sind zunehmend Methoden gefragt, die dazu dienen, Applikationen gut zu strukturieren und somit beherrschbar zu machen. Im Fokus steht immer mehr die Forderung nach minimalem Aufwand und einer damit verbundenen Reduzierung von Kosten. Ziel ist die weitere Verkürzung von Engineeringzeiten.

Die nachfolgende Grafik beschreibt den bislang gültigen Kompromiss aus minimalen Kosten, maximaler Qualität und schneller Umsetzung:



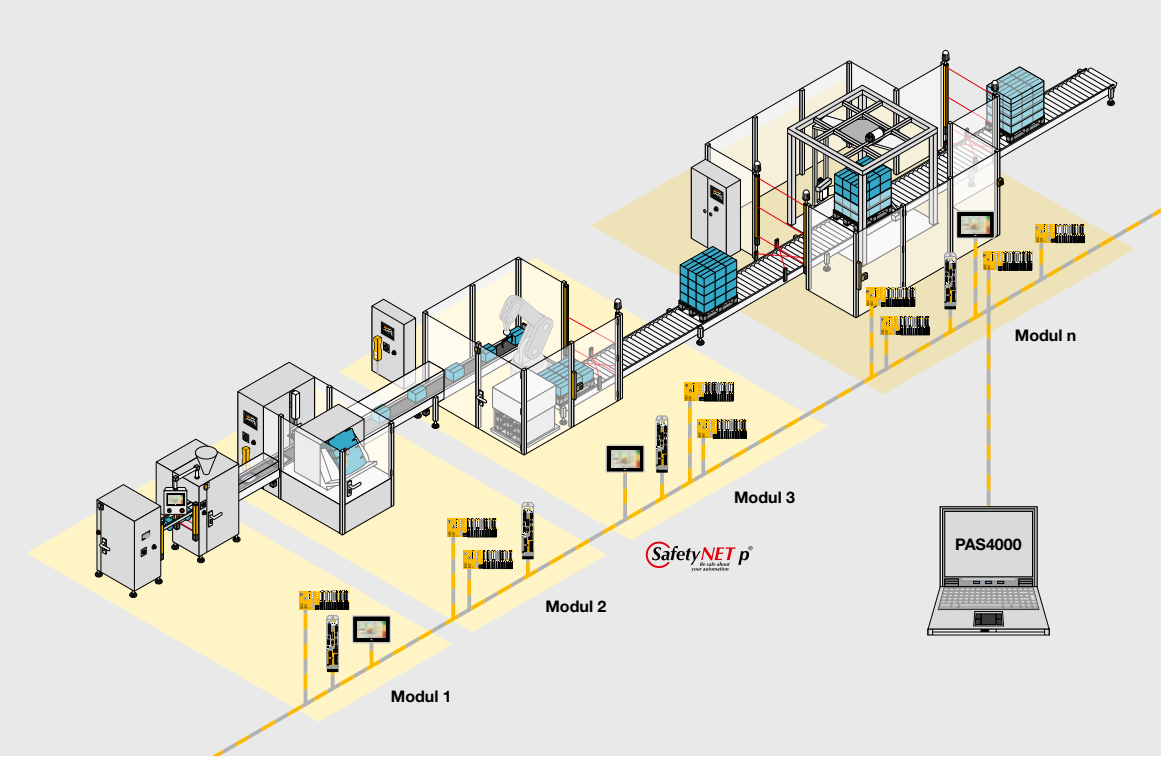
Eine gute Unterstützung im Rahmen der Engineering-Phase durch ein geeignetes Programmiermodell, eine benutzerfreundliche Programmierumgebung sowie eine große Bibliothek führen jedoch zu mehr Qualität in kürzerer Zeit bei insgesamt geringeren Kosten.

5.4 Mit Sicherheitssteuerungen zur sicheren Steuerungstechnik

5.4.2 Strukturen der sicheren Steuerungstechnik

Das Modell der Sicherheitstechnik als reine „Überwachungsfunktion“ wandelt sich drastisch: War Sicherheitstechnik lange Zeit fast ausschließlich verbunden mit Not-Halt, Schutztür, Lichtvorhängen und Verriegelungen, so ist das Thema Sicherheit heute beispielsweise bei Antrieben nicht mehr wegzudenken. Weitere Bereiche werden sichere Pneumatik und Hydraulik sein. Einsatzfelder werden folgen, die derzeit zwar noch nicht im Mittelpunkt stehen, doch wird eines deutlich: Sicherheit ist integraler Bestandteil der Gesamtfunktion von Maschinen und Anlagen, sie muss deshalb von Anfang an entsprechende Berücksichtigung finden. Denn sichere Steuerungstechnik heißt im Klartext: Mach die Steuerungsfunktion sicher! Sichere Steuerungstechnik ist dann Realität, wenn Sicherheit auf allen Ebenen der Automatisierungstechnik so gegenwärtig ist, dass die gleichen Mechanismen, dasselbe Handling und dieselbe Flexibilität wie im Standardbereich gelten.

Das heißt keineswegs, dass Sicherheits- und Automationsfunktionen zwangsläufig in einem Gerät vereint sein müssen. Vielmehr sollen sie als System gemeinsam an der Be- und Abarbeitung von Aufgaben arbeiten, ohne sich zu behindern. Dabei bearbeitet jedes Gerät, jede Steuerung das, was es/sie am besten kann. Rückgrat dieses Systems ist ein extrem leistungsfähiges Bussystem, das den Datenverkehr im Hintergrund managt. Das Ergebnis der technologischen Entwicklung ist somit ein System, das die systemimmanenten Vorteile von Technologiesteuerungen nutzt. Es ergibt also keinen Sinn, wenn z. B. eine Sicherheitssteuerung Motion-Aufgaben abwickeln muss, denn das ist eine spezifische Aufgabe der Technologiesteuerung Motion.



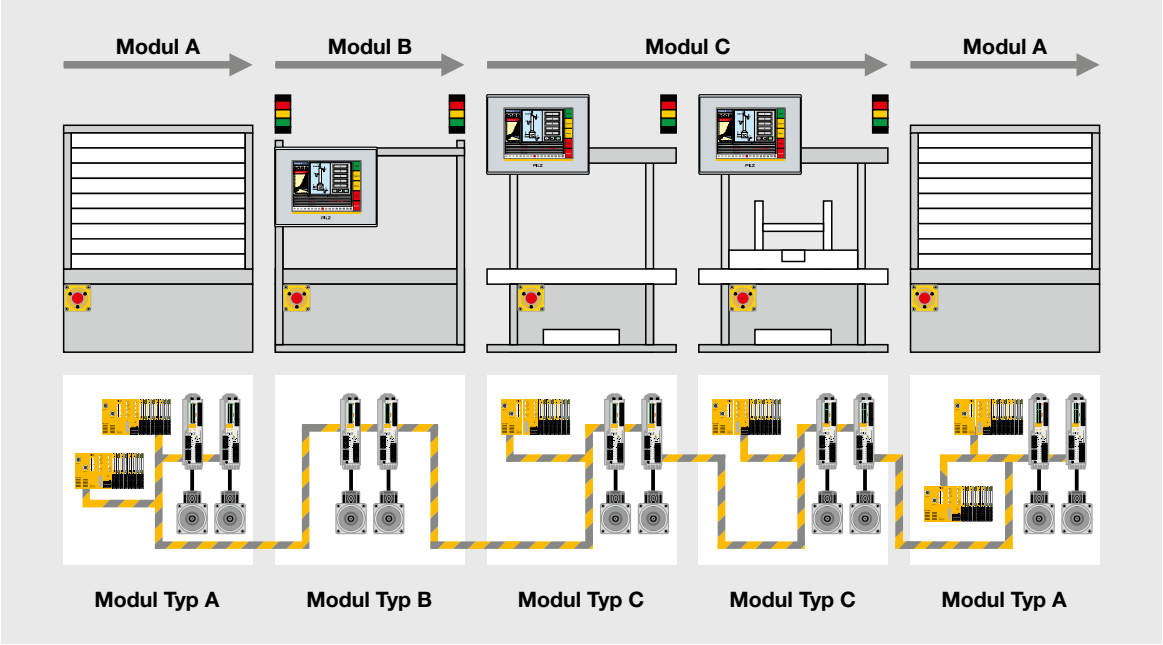
Sicherheits- und Automations-Steuerungsfunktionen in einem System vereint

5.4 Mit Sicherheitssteuerungen zur sicheren Steuerungstechnik

Das bedeutet letztlich aber auch, dass sämtliche Steuerungssysteme gemeinsam auf dieselben Daten zugreifen können müssen, ohne dass der Anwender gefordert wäre, dies zu organisieren. Diese Aufgabe muss das System im Hintergrund selbstständig erledigen. Auch die Tools müssen sich künftig nach Look and Feel sowie Handling einheitlich präsentieren. Egal ob Motion, Steuerung oder Visualisierung: Es dürfen keine Brüche im Handling der verschiedenen Funktionen und Aufgaben entstehen.

5.4.3 Modularisierung der Automatisierungsaufgabe

Modularisierung als Lösungsansatz für die Anforderung an die Steuerungstechnik der Zukunft bedeutet letztlich auch die Teilung der Steuerungstechnik in entsprechende Einheiten bzw. Module und damit ein Zerlegen bis hinunter zu den Technologiefunktionen.



Modularisierung einer Maschine und Verteilung der Aufgaben auf verschiedene Steuerungssysteme

Was sich mechanisch zerlegen lässt, ist auch bezüglich der Automatisierung in Einzelteile oder Komponenten zerlegbar. Dabei darf sich ein auf Komponenten basierender Ansatz nicht auf einzelne Stationen beschränken (wie z. B. in der Abbildung Module A bis C), sondern muss sich vielmehr bis hinunter zu den einzelnen Funktionseinheiten (sogenannte mechatronische Einheiten) fortsetzen. Wenn künftig umfassende Bibliotheken diese Einheiten als wiederverwendbare Komponentenbausteine anbieten, lassen sich Applikationen sehr viel effektiver umsetzen.

Selbst wenn die Teilung in Module und mechatronische Einheiten sinnvoll erscheint, sollte man dabei nicht den Blick für das Ganze verlieren: Programmiermodelle, die sowohl die Einheiten zusammenhalten als auch als Ganzes darstellen, bieten einen weit höheren Kundennutzen als solche, die Komponenten nur mit Schnittstellen versehen und dem Anwender letztlich die Versorgung dieser Schnittstellen zumuten.

5.5 Sichere Steuerungstechnik im Wandel

Mitunter erscheint die sichere Sicherheitstechnik wuchtig und überdimensioniert, dahinter steckt jedoch immer das Streben nach einfachen „Rezepten“: Sicherheit muss einfach, übersichtlich, nachvollziehbar und überprüfbar sein. Deshalb ist in der sicheren Steuerungstechnik kaum Platz für unkonventionelle Lösungsansätze, sie ist quasi per Definition konservativer Bestandteil der Steuerungs- und Automatisierungstechnik. Den dortigen innovativen Trends oder Strömungen folgt sie meist etwas zeitverzögert nach. Diese Denkweise manifestiert sich auch in der gängigen Vorstellung, dass Sicherheitstechnik im Fehlerfall respektive bei Anforderung der Sicherheit (beispielsweise bei Betätigung der Not-Halt-Funktion) immer sicher abschalten muss, nach Möglichkeit elektromechanisch und ohne jegliche elektronische Zusatzkomponente.

Woher rührt diese Vorstellung? Die sichere Steuerungstechnik soll den Mensch vor allen Gefahren schützen, die von Maschinen und Anlagen ausgehen können. Dabei ist sie wie kaum ein anderer Bereich durch Standards und Normen geprägt. Sicherheit wird nicht zuletzt auch dadurch erreicht, dass Regeln und Vorgaben transparent dargestellt werden und so das Verständnis für deren Umsetzung erleichtern.

Auch wenn die üblichen Rezepte und Sichtweisen bis heute gelten und im Kern noch immer sinnvoll sind, unterliegen auch Sicherheitssteuerungen im Zuge des allgemeinen technologischen Fortschritts einem massiven Wandel. Bereits in der Vergangenheit hat sich die sichere Steuerungstechnik kontinuierlich den steuerungstechnischen Gegebenheiten angepasst: Wie sonst gäbe es heute Sicherheitslösungen, die in den achtziger Jahren völlig undenkbar gewesen wären und den damaligen Normen schon deshalb nicht entsprechen konnten, weil zu dieser Zeit ausschließlich elektromechanische Lösungen zugelassen waren? Erst nach aufwendigen Prüfverfahren durch entsprechend notifizierte Stellen (TÜV, BG etc.) kamen nach und nach elektronische Sicherheitslösungen zum Einsatz. Moderne Herstellungsverfahren erfordern neue technische Ansätze, Prozess- und Fertigungsabläufe verändern sich nachhaltig. Klar, dass die sichere Steuerungstechnik mit den Entwicklungen im Bereich der Automatisierungstechnik eng einhergehen muss. Kunden erwarten innovative Produkte und Lösungen mit entsprechend integrierten Sicherheitskonzepten, die die Produktivität steigern, effiziente Arbeitsprozesse unterstützen und zusätzlichen Nutzen stiften.

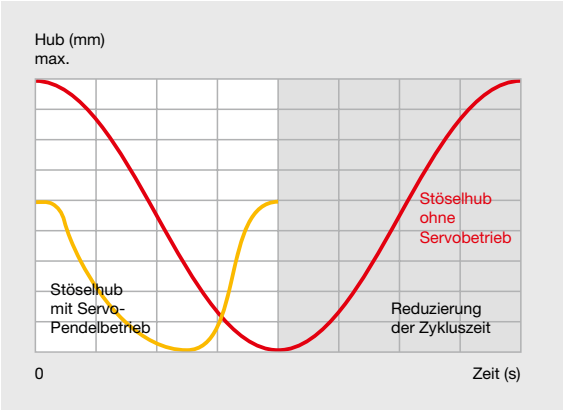
5.5.1 Neue Anforderungen an die sichere Steuerungstechnik

Welchen Herausforderungen steht die sichere Steuerungstechnik heute gegenüber? Aktuellen Anforderungen wie zum Beispiel mehr Flexibilität bei Konfiguration und Programmierung oder einem erhöhten Kommunikationsbedarf wird ja bereits Rechnung getragen. Einige andere Anforderungen sind allerdings weder explizit erkennbar noch offensichtlich benannt. Die von Henry Ford überlieferte Aussage „Hätte ich auf meine Kunden gehört, hätte ich nicht Autos gebaut, sondern stärkere Pferde gezüchtet“ macht deutlich, dass sich erfolgreiche Entwicklungen nicht allein an vordergründigen Bedürfnissen orientieren dürfen, sondern stets den Kern des Bedarfs erfassen müssen. Denn nur mit visionärer Weitsicht entstehen am Ende im echten Wortsinne innovative Produkte und Lösungen. Überträgt man diese Erkenntnis auf die sichere Steuerungstechnik, wird klar, dass sich die Aufgaben der Zukunft mit heute gängigen Rezepten nicht lösen lassen und Unternehmen neue Lösungen anbieten müssen.

Noch heute funktioniert Sicherheit in vielen Unternehmen so, dass beim Betreten eines Schutzbereichs sämtliche Antriebe oder die gesamte Anlage stromlos geschaltet wird. Im Zuge steigender Produktivitätsanforderungen muss es jedoch möglich sein, definierte Schutzräume einer Anlage betreten zu können, ohne dass der gesamte Produktionsprozess zum Erliegen kommt. Gleichzeitig muss die Sicherheit des Bedieners gewährleistet sein. Daher steigt die Nachfrage nach intelligenten, dynamischen Sicherheitslösungen. Das komplette Abschalten als Reaktion auf ein sicherheitstechnisch relevantes Ereignis kann in Zukunft nur noch die letzte aller Möglichkeiten sein.

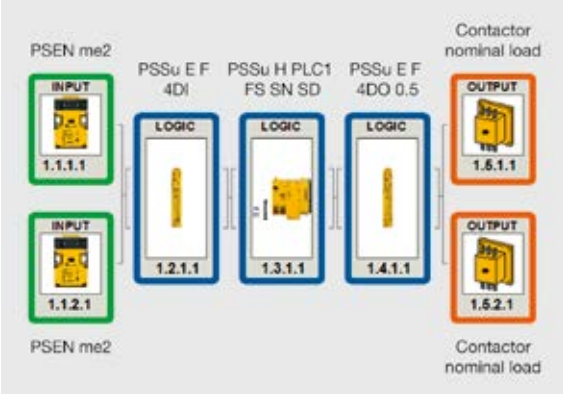
5.5 Sichere Steuerungstechnik im Wandel

Zu Recht wird von den Herstellern für sichere Steuerungstechnik in Zukunft eine völlig neue Generation von Sicherheitssteuerungen erwartet. So, wie im Auto immer häufiger Assistenzfunktionen zum Einsatz kommen, die den Fahrer unterstützen und zusätzliche Sicherheit anbieten (wie beispielsweise die Abstandsüberwachung und selbstständige Reduzierung der Fahrgeschwindigkeit), werden auch im Maschinen- und Anlagenbau zunehmend nützliche und Sicherheit schaffende Zusatzfeatures Einzug halten. Ein Beispiel aus der Umformtechnik, wo heute Servopressen immer mehr an Bedeutung gewinnen, macht die geänderten Anforderungen deutlich: War es bei üblichen Pressen ausreichend, dass ein mechanisches Nockenschaltwerk die Sicherheit der Hubbewegung regelte, so ist der Bewegungsablauf bei Servopressen ein grundlegend anderer. Ein Pressenhub ist jetzt nicht mehr die Umdrehung eines Exzenters um 360°, sondern eine Pendelbewegung zwischen variablen Winkelstellungen. Um bei solchen Applikationen Sicherheit zu gewährleisten, greifen bislang bewährte Vorgehensweisen nicht mehr, die Anforderungen an das Auswertegerät sind deutlich komplexer als bisher.



Stöselhub mit und ohne Servobetrieb

Die skizzierten Beispiele sollen zeigen, dass die sichere Steuerungstechnik künftig umfangreiche Berechnungen durchführen muss, um den gestellten Anforderungen gerecht zu werden. Sicherheitssteuerungen müssen komplexe Messgrößen erfassen, verarbeiten und ausgeben können. Dies erfordert signifikant andere Mittel als jene, die bislang zur Verfügung standen. Dies betrifft nicht nur die eingesetzten Sensoren und Aktoren, sondern vor allem die verarbeitenden Logik-Funktionen, die aufgrund der gestiegenen Anforderungen nicht mehr mit einfachen Befehlssätzen auskommen. Zusammenfassend gilt, dass die Vorgänge in Maschinen und Anlagen aufgrund der an sie gestellten Anforderungen komplexer und dynamischer werden. Die sichere Steuerungstechnik der Zukunft muss den veränderten Anforderungen Rechnung tragen.

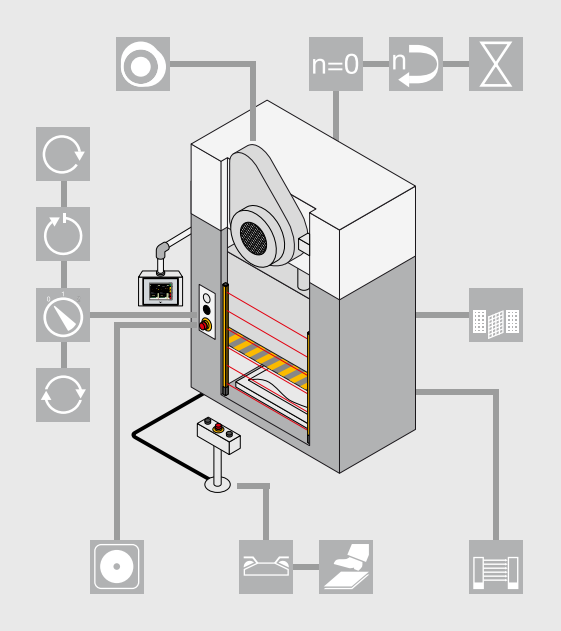


Sicherheitsfunktion nach EN13849-1 mit Sensor, Logik und Aktor

5.5 Sichere Steuerungstechnik im Wandel

5.5.2 Komplex und dennoch einfach – kein Widerspruch

In der klassischen, heute verbreiteten Sicht auf die Sicherheitstechnik geht es meist um Sicherheitsfunktionen wie im nachfolgenden Bild dargestellt. Es sind gängige Funktionen wie Not-Halt, Schutztüren, Zweihandbedienung, Betriebsartenwahl, Ventilansteuerung, Drehrichtungsüberwachung oder Nockenschaltwerk, die einen Großteil der notwendigen Sicherheitsfunktionen abdecken – grundlegende Funktionen, wie sie in dieser oder ähnlicher Form in fast allen Maschinen benötigt werden.



Sicherheitsfunktionen an einer Exzenterpresse

Für Maschinen und Anlagen, bei denen sich Sicherheit auf grundlegende Funktionen beschränkt, wird auch in Zukunft ein Bedarf an einfachen Sicherheitssteuerungen bestehen, mit denen man eine überschaubare Anzahl an Sicherheitsfunktionen auf simple Art und Weise realisieren kann. Das ist eine der Stärken sogenannter konfigurierbarer Kleinsteuerungen wie beispielsweise PNOZmulti: Die Programmierung erfolgt über grafische Symbole per Drag and Drop auf einfache Art und Weise. Dies ist inzwischen Stand der Technik und seit der Jahrtausendwende praktisch Marktstandard. Bis heute ist PNOZmulti innerhalb dieser Geräteklasse Vorbild und technologischer Vorreiter gleichermaßen.

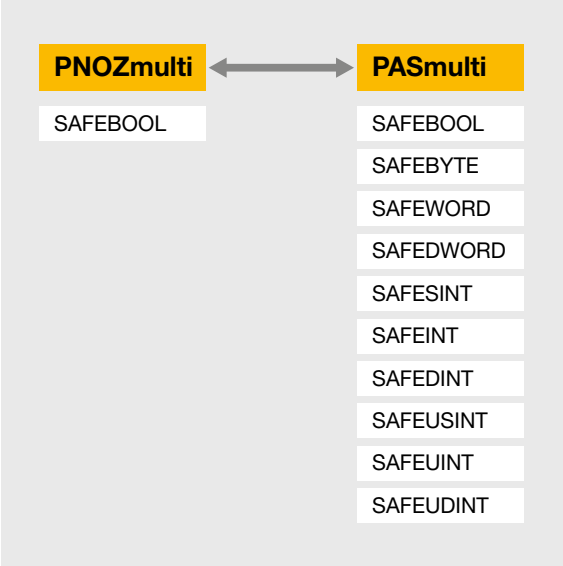
5.5.2.1 Konfigurierbare sichere Kleinsteuerungen entwickeln sich weiter

Die einfache Handhabung von Softwaretool und Hardware hat allerdings dazu geführt, dass Applikationen, die ursprünglich den leistungsfähigen „echten“ Sicherheitssteuerungen vorbehalten waren, sukzessive zu den konfigurierbaren Kleinsteuerungen abgewandert sind. Dies ist grundsätzlich kein Problem, solange die Geräte den Anforderungen gerecht werden. Allerdings sieht sich der Anwender immer häufiger damit konfrontiert, dass die Kleinsteuerung an die Grenze ihrer Leistungsfähigkeit gelangt. Denn mitunter entstehen derart umfangreiche Konfigurationen, dass selbst der Ersteller den Überblick zu verlieren droht. An dieser Stelle gerät man rasch in einen Widerspruch: Je mehr Funktionalitäten in den konfigurierbaren Kleinsteuerungen abgebildet werden sollen, umso mehr verlieren sie an Übersichtlichkeit und einfacher Anwendbarkeit (Usability). Letzteres ist aber genau das, was der Anwender schätzt.

5.5 Sichere Steuerungstechnik im Wandel

5.5.2.2 Konfigurierbare Sicherheitssteuerungen der neuesten Generation

Was unterscheidet die konfigurierbare Steuerung PSSuniversal multi des Automatisierungssystems PSS 4000 von etablierten Geräten wie z. B. dem PNOZmulti? Die Steuerungen PSSuniversal multi sind wesentlich leistungsfähiger als die konfigurierbaren sicheren Kleinsteuerungen und begründen damit eine völlig neue Geräteklasse der „konfigurierbaren Sicherheitssteuerungen“. PSSuniversal multi unterscheidet sich in zwei wesentlichen Punkten von ihren Vorgängern: Von grundlegender Natur ist die Erweiterbarkeit um zusätzliche Datentypen. Die Geräte können jetzt nicht nur mit Boole'schen Variablen umgehen, sondern wie „ausgewachsene“ Steuerungen jegliche Art von Datentyp verarbeiten. Des Weiteren wurden die grafischen Möglichkeiten so erweitert, dass sich zusammengesetzte komplexe Datenstrukturen grafisch in Form einzelner Linien im Editor darstellen lassen. Dies fördert die Übersichtlichkeit, ohne wichtige Informationen zu verlieren.

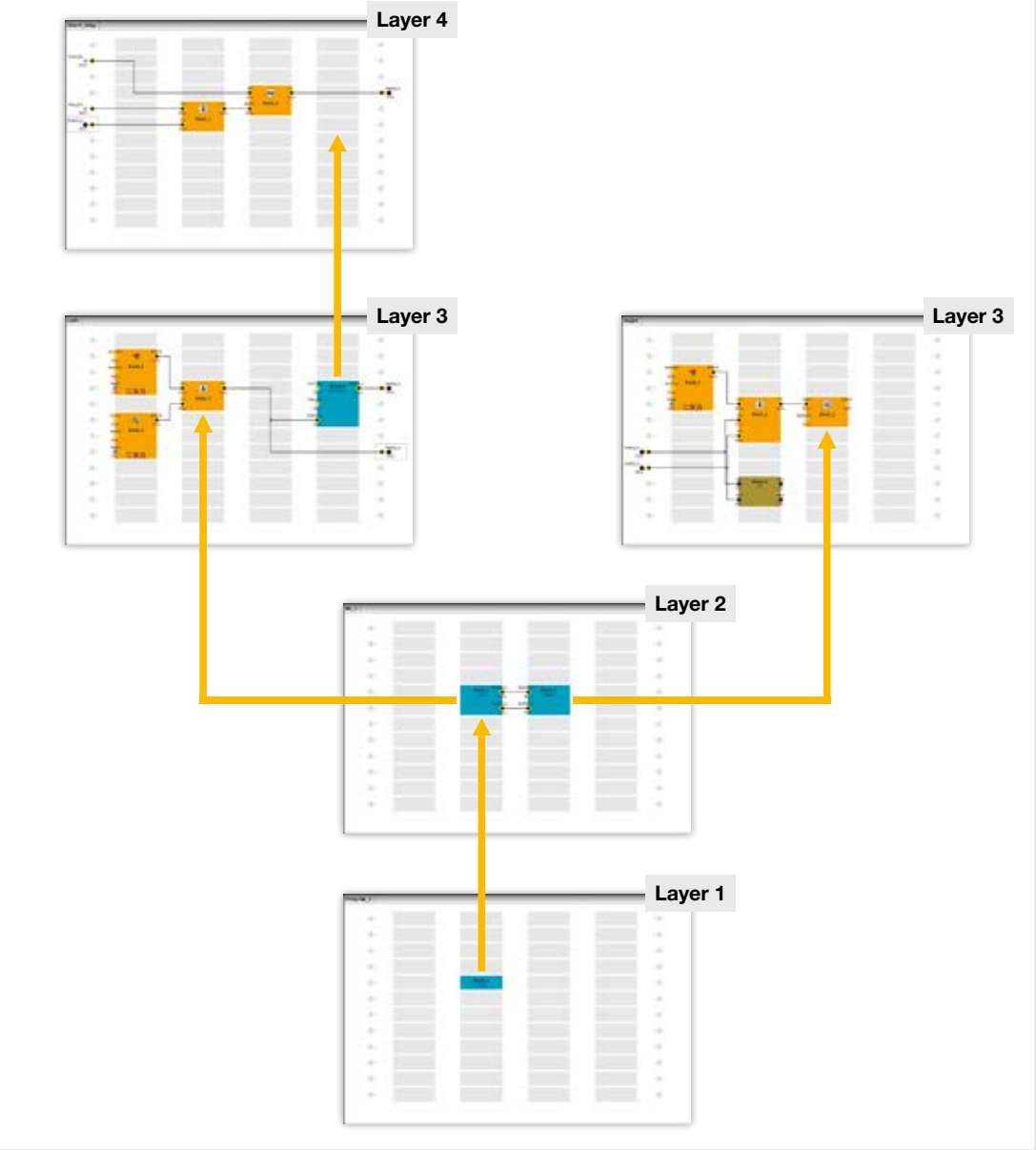


Vergleich PNOZmulti mit PSSuniversal multi Datentypen

Eine weitere Veränderung grundlegender Art betrifft den strukturellen Aufbau eines Programms. Aus Sicht einer SPS-Steuerung ist man gewohnt, Programme hierarchisch zu gliedern. Programme beinhalten Funktionsbausteine, die wiederum Funktionen oder Elemente aufrufen. Ein Merkmal konfigurierbarer Kleinsteuerungen ist die Darstellung des Programms in einer Ebene. Hierarchische Strukturen, wie man sie von SPS-Steuerungen gewohnt ist, konnten bislang nicht abgebildet werden. Für einfache Applikationen ist das durchaus sinnvoll und hat auch zum Erfolg dieser Geräteklasse beigetragen. Komplexere Anwendungen machen diese Art der Programmerstellung aber schnell unübersichtlich.

Nun hat man die konfigurierbare Steuerung PSSuniversal multi um genau diesen Aspekt erweitert: Programmteile lassen sich zu einem Block zusammenfassen und machen dadurch das Programm übersichtlich, ohne den Informationsgehalt des Programmteils zu verlieren. Wird eine Funktion in gewohnter Form „flach“ erstellt, kann sie per Markierung zu einem neuen Block zusammengefasst werden. Das neue Element „erbt“ alle offenen Schnittstellen als seine Schnittstelle nach außen und kann per Doppelklick wieder geöffnet, erweitert oder verändert werden. Ein Einblick in die innere Struktur des Elements ist also jederzeit möglich.

5.5 Sichere Steuerungstechnik im Wandel

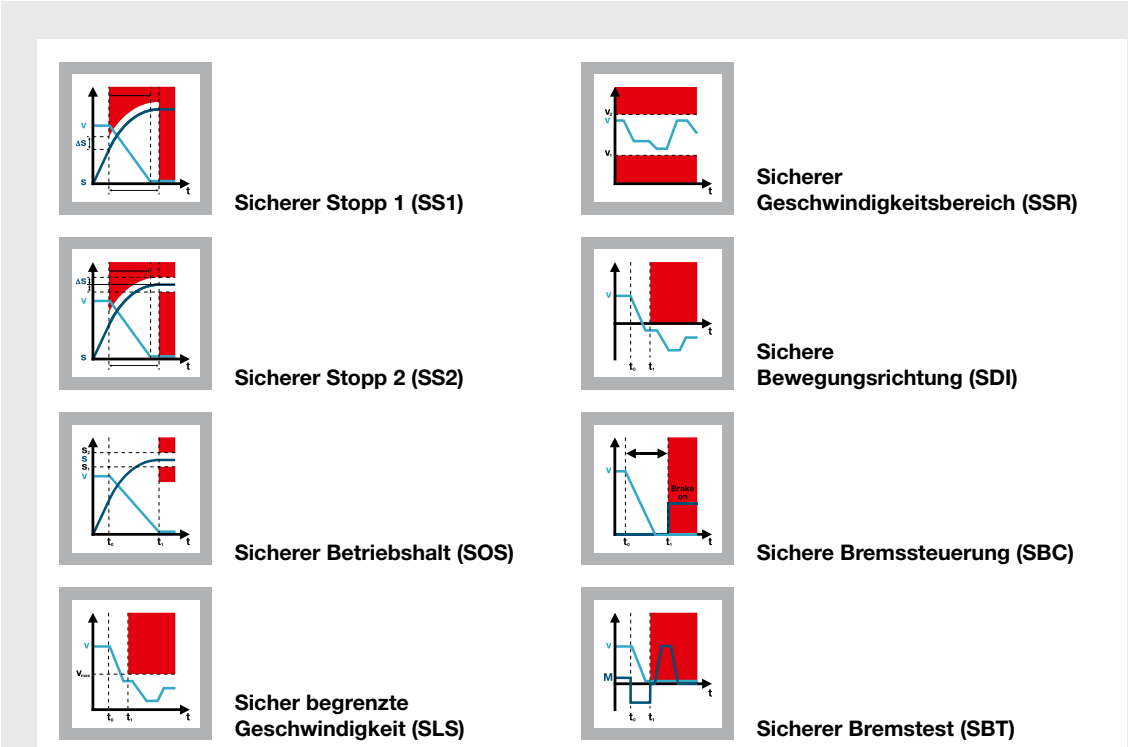


Hierarchische Strukturierung der Steuerung PSSuniversal multi des Automatisierungssystems PSS 4000

5.5 Sichere Steuerungstechnik im Wandel

5.5.2.3 Integration von Automatisierungs- und Sicherheitstechnik

Bisherige Sicherheitssteuerungen zeichnen sich primär durch die Möglichkeit der freien Programmierung ähnlich einer Standard-SPS aus. Allerdings ist dies nicht uneingeschränkt möglich: Um sicherzustellen, dass Programme übersichtlich und verständlich bleiben, hat man bei den meisten Systemen den Befehlssatz und/oder die Anzahl der verfügbaren Editoren begrenzt. Dies war und ist kein Problem, solange Maschinen und Anlagen nur einfache Sicherheitsmaßnahmen erfordern. Doch bezüglich der Anforderungen an sichere Steuerungstechnik vollzieht sich aktuell ein struktureller Wandel: Die Prozesse werden immer dynamischer, der Bedarf an kontrollierten Eingriffen in den Prozess wie die Anforderungen an die Produktivität steigen und verändern somit sukzessive auch die sichere Steuerungstechnik. Die bisherige Strategie des sicheren Abschaltens bei Anforderung der Sicherheit oder im Fehlerfall wird zukünftig nicht mehr akzeptabel sein. Die sichere Steuerungstechnik muss sich den innovativen Prozessen öffnen, wie die Beispiele sicherer Antriebsfunktionen heute schon anschaulich machen.



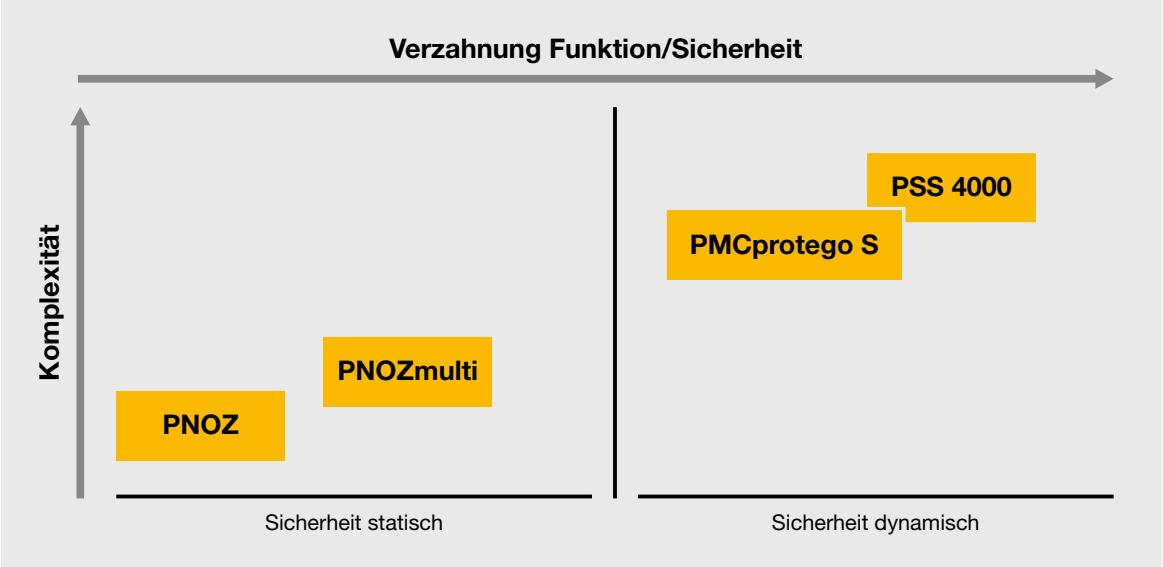
Antriebsintegrierte Sicherheit mit PMCprotego DS

5.5 Sichere Steuerungstechnik im Wandel

Doch das ist erst der Anfang: Schritt für Schritt wird die sichere Steuerungstechnik fester Bestandteil der Automatisierungstechnik werden müssen, wie dies heute bei der Antriebstechnik in Form dynamischer Geschwindigkeits- oder Stillstandsüberwachung bereits der Fall ist. In Zukunft werden noch weit dynamischere Sicherheitskonzepte wie beispielsweise die Drehmomentüberwachung in Abhängigkeit der Position einer oder mehrerer Achsen notwendig sein. Die bislang verfügbaren Sicherheitssteuerungen werden diesen neuen Anforderungen nur teilweise gerecht. Einerseits werden hier Befehlssätze benötigt, die den Ansprüchen an die Dynamisierung der Sicherheitsfunktionen gerecht werden können. Andererseits soll die Programmierung weiterhin auf einfachen überschaubaren Grundelementen aufbauen, die ein sicheres Vorgehen bei der Programmerstellung, wie beispielweise durch die Normen IEC 61508 gefordert, erlauben.

Letztlich vereinen moderne Sicherheitssteuerungen die Vorgehensweise bei der Programmierung einer SPS mit den Vorzügen der Konfiguration der Geräteklasse „Konfigurierbare Kleinsteuerungen“ sinnvoll miteinander. Dies bedeutet im Detail, dass eine heutige Sicherheitssteuerung über eine große Anzahl an Editoren verfügen muss. Die „Klaviatur“, die dem Anwender in die Hand gegeben wird, sollte nicht nur eine Oktave umfassen, sondern nach Möglichkeit das gesamte „hörbare“ Spektrum abdecken. Zu berücksichtigen ist dabei, dass die Editoren auch den Ansprüchen der unterschiedlichen Branchen und Zielgruppen entsprechen müssen. Komplexe Sicherheitsfunktionen sollten in einer Hochsprache erstellt und getestet werden können. Im Anschluss an die Testphase muss eine Konvertierung in eine grafische Darstellung möglich sein.

5.5 Sichere Steuerungstechnik im Wandel



Statische und dynamische Sicherheit

5.5.3 Von statischer zu dynamischer Sicherheit

Neben den Veränderungen auf Geräteebene finden parallel Veränderungen auf Systemebene statt. In Ansätzen erkennbar ist dies im Bereich der Sicheren Antriebstechnik. Bisher war die Sicherheitsfunktion an die Steuerung gebunden, jetzt wird sie verteilt, d. h. die Funktion wandert ab in die lokale Funktionssteuerung, zum Beispiel in den Antrieb. Gleichzeitig wird die Trennung zwischen Sicherheits- und Steuerungsfunktion zunehmend unschärfer, am Ende des Weges könnte die Steuerungsfunktion sicher sein. Betrachtet man heutige Maschinen und Anlagen, stellt man fest, dass sich die Anforderungen an die sichere Automation nicht nur in der Anzahl der Sicherheitsfunktionen und deren Verknüpfung verändert haben, sondern dass der Wunsch nach flexibleren Lösungen immer mehr zunimmt. Was sind die Gründe dafür? Maßgeblich für die teilweise gravierenden Veränderungen im Maschinenbau in den vergangenen Jahren war der Trend, Mechanik durch Elektronik zu ersetzen. Dies hat neben wirtschaftlichen Aspekten auch neue technische Freiheitsgrade mit sich gebracht, die sich nun konsequenterweise in den Anforderungen an die sichere Steuerungstechnik widerspiegeln.

War Sicherheit bislang von vorwiegend statischen Ereignissen wie beispielsweise der Betätigung einer Not-Halt-Einrichtung, dem Öffnen einer Schutztür oder der Unterbrechung eines Lichtvorhanges geprägt, so stehen heute Anforderungen im Vordergrund, die eine angepasste Reaktion der Sicherheit auf dynamische Vorgänge in der Maschine erlauben. Es sind also nicht mehr nur einfache logische Verknüpfungen, die Reaktionen auslösen sollen, sondern mitunter vielschichtige Zustände oder die Ergebnisse komplexer Berechnungen, auf die Sicherheit angemessen reagieren muss.

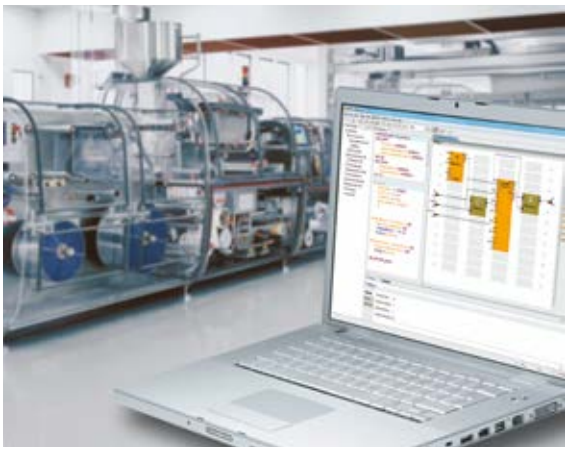
Welche Auswirkungen hat dies auf Entwicklungen in der sicheren Steuerungstechnik? Dynamische Sicherheit erfordert eine enge Verzahnung der Steuerungsfunktion mit der Sicherheit. Daraus folgt die Notwendigkeit, noch stärker in Systemen zu denken. Wenn Teilfunktionen optimal ineinandergreifen sollen, können Funktionen nicht einfach aufgesetzt werden, sondern müssen integraler Bestandteil des Gesamtsystems sein. Vergleichbar mit den Entwicklungen im steuerungstechnischen Bereich, wo heute schon Funktionen über Gerätegrenzen hinweg ausgeführt werden, wird sich dies auch in der sicheren Automation durchsetzen. Die Herausforderung besteht letztlich in der Integration der Funktionen in das Gesamtsystem. Insellösungen werden bei hochkomplexen dynamischen Aufgaben keinen Mehrwert generieren.

5.5 Sichere Steuerungstechnik im Wandel

5.5.4 Über Industrie 4.0

Industrie 4.0 ist mehr als eine Zukunftsvision. Die intelligente Vernetzung ist für die Industrie eine große Chance. Durch eine flexible Produktion kann eine optimale Auslastung der Anlagen erreicht werden. Individualisierte Produkte können zu Bedingungen der Massenproduktion hergestellt werden, wodurch die Produktivität der Anlage steigt. Dennoch sind viele Unternehmen noch zögerlich, was die Umsetzung von Industrie 4.0 in ihrer eigenen Produktion angeht. Laut der Studie „Industry 4.0 – How to navigate digitization of the manufacturing sector, “ [1)] des McKinsey-Instituts fühlen sich nur sechs von zehn Unternehmen in Deutschland auf Industrie 4.0 vorbereitet, obwohl 91 Prozent die Digitalisierung der industriellen Produktion als Chance wahrnehmen. Dem möchten wir gerne entgegensteuern und für Unternehmen weltweit Lösungen und Produkte für Industrie 4.0 anbieten. Denn auch international rückt das Thema Industrie 4.0 immer mehr in den Fokus: Gerade wegen der fortschreitenden Globalisierung ist es notwendig, Voraussetzungen dafür zu schaffen, dass die Vernetzung durch Digitalisierung von Produktionsprozessen entlang der Wertschöpfungskette ermöglicht wird.

[1)] https://www.mckinsey.de/sites/mck_files/files/mck_industry_40_report.pdf



Anlagen lassen sich in übersichtliche, selbstständig arbeitende Einheiten zerlegen.

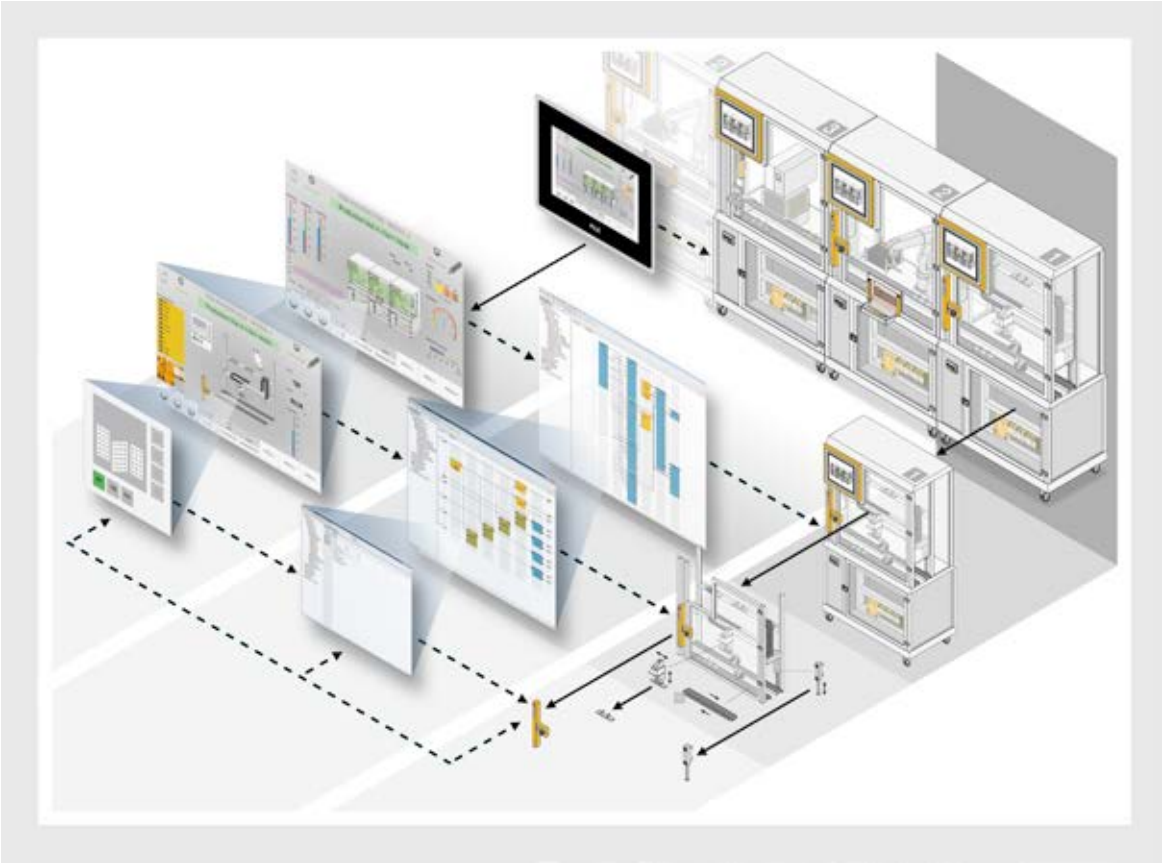
Modulare Maschine und Dezentralisierung

Als ein Schlüssel zu mehr Flexibilität in der Produktion gilt seit mehreren Jahren der modulare Maschinen- und Anlagenbau. Eine Gesamtanlage setzt sich aus mehreren autarken Maschinenmodulen zusammen. Ein Modul bildet dabei jeweils einen oder mehrere standardisierte Produktionsschritte ab und kann mit anderen Modulen zu einem kompletten Prozess kombiniert werden. Dazu werden alle Module an einen Backbone angeschlossen, der die Module sowohl energetisch (400 VAC Drehstrom, Druckluft ...) als auch mit Prozess- und Steuerungsdaten versorgt. Zudem verfügt jedes Produkt/Werkstück über alle relevanten Informationen zu dem jeweiligen Produktionsprozess. Soll sich das Produktionsverfahren ändern oder sich die Produktivität erhöhen, können ein oder mehrere Module ausgetauscht oder gleiche Module hinzugefügt werden.

Auf dem Weg in die Zukunft der Automatisierung sind folglich Modularisierung und Dezentralisierung zwei der wichtigsten Erfolgsfaktoren. Voraussetzung dafür sind Automatisierungssysteme, die in der Lage sind, die in den Maschinenmodulen verteilte Intelligenz anwenderfreundlich zu steuern. Alle Maschinen und Anlagen lassen sich dann in übersichtliche, selbstständig arbeitende Einheiten zerlegen.

Der modulare Aufbau von Maschinen und Anlagen folgt dem mechatronischen Ansatz. Dieser verfolgt die Philosophie, durchgängig alle am Entstehungsprozess einer Maschine beteiligten Disziplinen zusammenzuführen: Mechanik, Elektrik und Automatisierungstechnik. Durchgängig definiert ist dabei das Zusammenspiel diverser automatisierungstechnischer Einzelkomponenten und der zugehörigen Softwaretools zu einer Automatisierungslösung. Diese Durchgängigkeit erstreckt sich über die vier Ebenen der Automatisierungspyramide (Managementebene, Betriebsführungsebene, Steuerungsebene und Feldebene). Der mechatronische Ansatz erfordert, dass auch Steuerungsfunktionalitäten in die einzelnen mechatronischen Module „hineinwandern“ können.

5.5 Sichere Steuerungstechnik im Wandel



Anlagen lassen sich in übersichtliche, selbstständig arbeitende Einheiten zerlegen.

Hier stoßen bisherige Systeme an ihre Grenzen. Zwar können Funktionsmodule erstellt werden, doch wenn die Funktion durch mächtige zentrale Steuerungssysteme ausgeführt werden sollen, wird die Inbetriebnahme einzelner Module durch die Komplexität schnell aufwendig. Ebenso entsteht ein erhöhter Aufwand bei nachträglich notwendigen Änderungen der Konfiguration und der Programmierung der einzelnen Funktionsmodule.

Mithilfe dezentral angelegter Systeme können Module einfach in Betrieb genommen werden. Auch die Erstellung der Konfiguration ist sehr anwenderfreundlich, da sich identische Steuerungsprogramme und -teilfunktionen für verschiedene Module verwenden lassen.

Für die Automatisierung der Zukunft sind also Lösungen gefragt, die zum einen in der Lage sind, Steuerungsintelligenz zu verteilen, und zum anderen gewährleisten, dass die notwendige Vernetzung mehrerer Steuerungen für den Anwender einfach zu handhaben bleibt. Solch eine Lösung bietet Pilz mit dem Automatisierungssystem PSS 4000.

5.5 Sichere Steuerungstechnik im Wandel

Sicherheit – Safety und Security

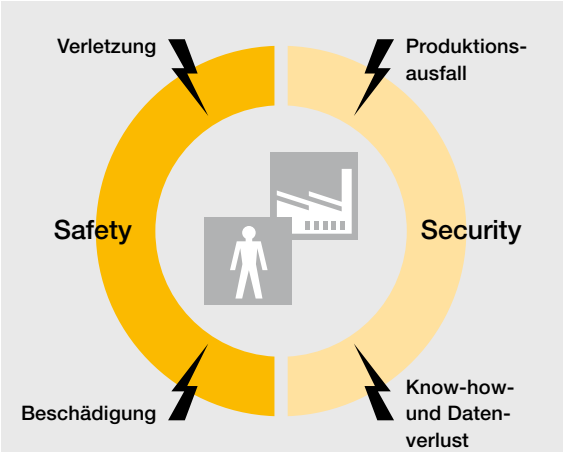
Mit der Weiterentwicklung der Automatisierungslandschaft zur Industrie 4.0 kommen neue Sicherheitsanforderungen auf Unternehmen zu. Die Welt der Automatisierung verschmilzt mit der IT-Welt. Die jeweiligen Sichtweisen auf das Thema Sicherheit unterscheiden sich deutlich: Die international verwendeten Begriffe „Safety“ für Maschinensicherheit und „Security“ für IT-und Datensicherheit helfen zunächst bei der grundlegenden Differenzierung.

Safety verlangt, dass Restrisiken, die von einer Maschine oder Anlage ausgehen, akzeptable Werte nicht übersteigen. Das schließt sowohl Gefährdungen der Umgebung der Anlage (z. B. Umweltschäden) als auch Gefährdungen innerhalb der Anlage (z. B. der Personen, die sich in der Anlage aufhalten) ein.

Security betrifft den Schutz einer Maschine oder Anlage vor unbefugten Zugriffen von außen sowie den Schutz sensibler Daten vor Verfälschung, Verlust und unbefugtem Zugriff im Innenverhältnis. Das schließt sowohl explizite Angriffe als auch unbeabsichtigte Security-Vorfälle ein.

Der umfassende Schutz von produktions- und Safety-relevanten Steuerungsdaten bei der Übertragung, Verarbeitung und Speicherung muss folgende Security-Bereiche adressieren:

- physische Sicherheit und Verfügbarkeit der IT-Systeme
- Netzwerksicherheit
- Software-Anwendungssicherheit
- Datensicherheit
- Betriebssicherheit



Zusammenspiel zwischen Safety und Security

5.5 Sichere Steuerungstechnik im Wandel

Handlungsfelder von Industrie 4.0

Eine der Grundlagen für eine nachhaltige Marktakzeptanz ist die Schaffung von standardisierten Mechanismen in der Kommunikation zwischen den Maschinen und innerhalb der Maschine. Nur wenn die Anforderungen der beiden Welten (Automatisierung und IT) berücksichtigt sind, entstehen praktikable, vom Anwender akzeptierte Lösungen.

Zusammengefasst heißt das, dass Pilz sich für moderne Steuerungsarchitekturen im Umfeld von Industrie 4.0 engagiert.

Dabei bilden die folgenden Themen unsere Schwerpunkte:

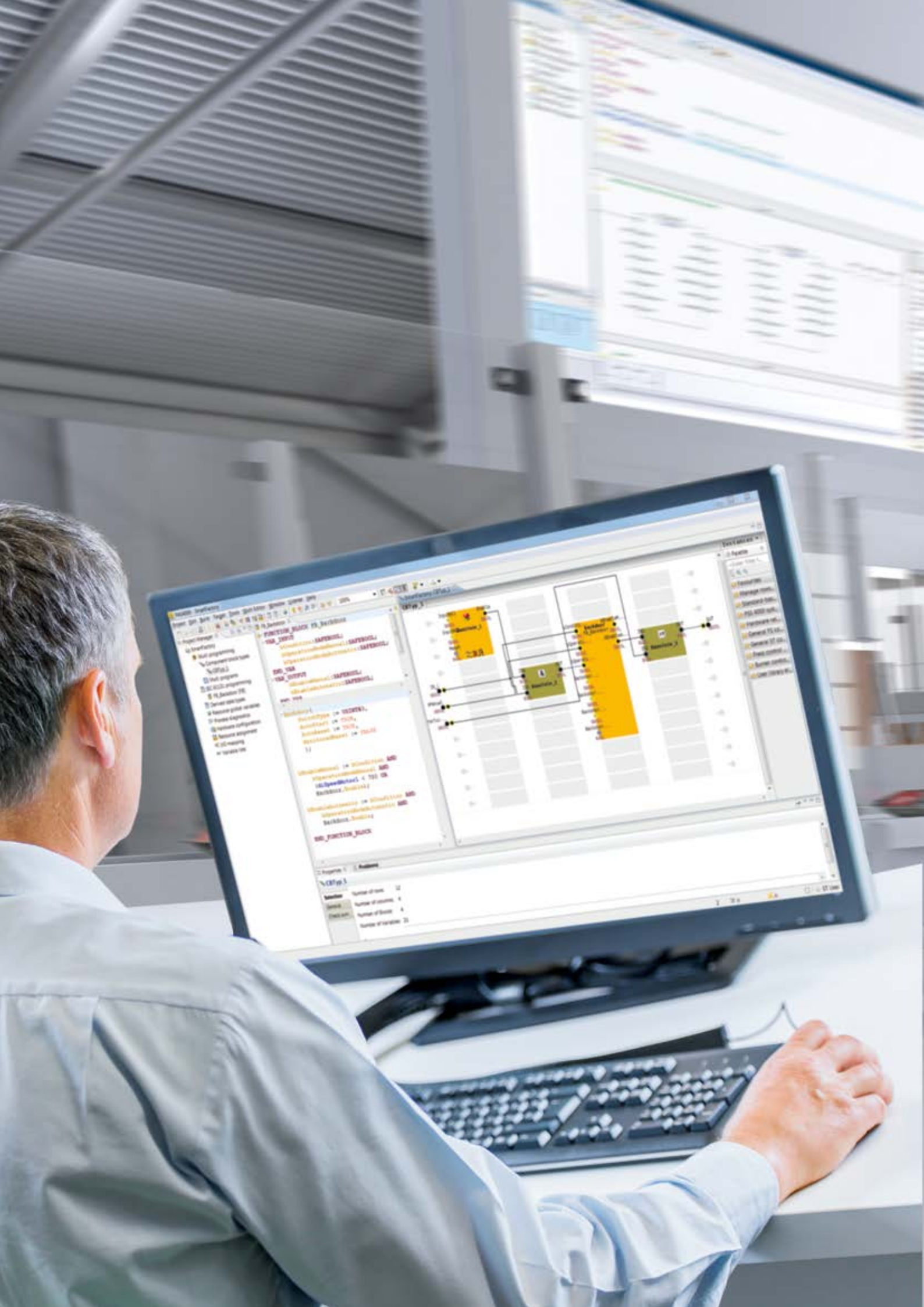
Modularer Ansatz:

Unsere modernen Steuerungsfunktionen sind auf eine Verteilbarkeit und Objektorientierung ausgelegt – Sensoren und Aktoren werden intelligent. Wir bilden damit den Trend zu mechatronischen Steuerungsobjekten (Automatisierungskomponenten) in unseren Produkten und den zugehörigen Engineering-Tools ab.

Safety und Security:

Beide besitzen deutliche Parallelen in der Standardisierung und der Vorgehensweise im Engineering-Prozess. Wir wollen mit unserer Erfahrung aus Maschinensicherheit und Automation diese wichtige Arbeit voranbringen.

Alle für die Steuerungsfunktion erforderlichen Geräte und Automatisierungskomponenten erhalten einen direkten Internetzugang für den Austausch von Prozessdaten und von Parametrierdaten für Diagnose und (Fern-)Wartung. Damit steigen für alle beteiligten Automatisierungsgeräte die Anforderungen in Bezug auf Security und eine einheitliche Diagnoseanbindung und -darstellung.



6 Sichere Kommunikation

6 Sichere Kommunikation

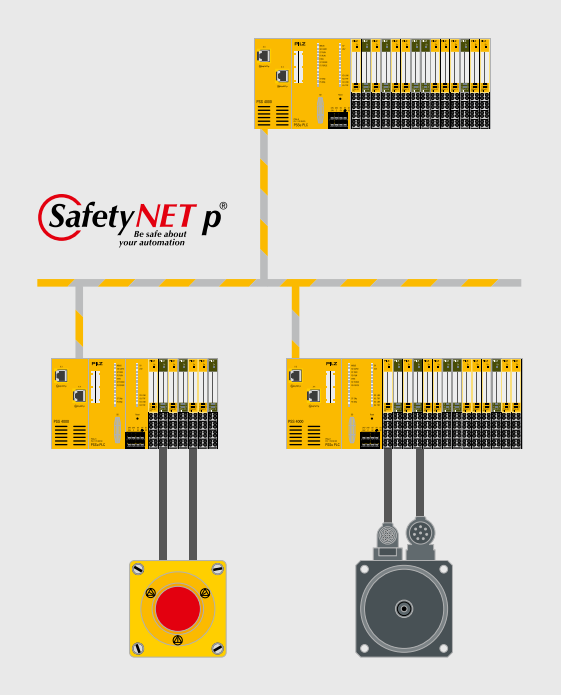
6	**Sichere Kommunikation**	
6.1	Grundprinzipien sicherheitsgerichteter Kommunikation	6-3
6.1.1	Prinzip dezentrale Sicherheitstechnik	6-3
6.1.2	Beherrschung von Kommunikationsfehlern	6-3
6.1.3	Prinzip Redundanz	6-5
6.2	Sichere Ethernet-Kommunikation mit SafetyNET p	6-6
6.2.1	Warum Ethernet in der Automatisierungstechnik?	6-6
6.2.2	Systembeschreibung SafetyNET p	6-7
6.2.3	UDP/IP-basierte Kommunikation mit RTFN	6-9
6.2.4	Harte Echtzeit-Kommunikation mit RTFL	6-10
6.2.5	Applikationsschicht	6-11
6.2.6	Sichere Kommunikation über SafetyNET p	6-11
6.2.7	Sicherer Telegrammaufbau	6-12
6.2.8	Branchen, Applikationen	6-12
6.2.9	Anwendungsbeispiel modularer Maschinenbau	6-14

6.1 Grundprinzipien sicherheitsgerichteter Kommunikation

Im Maschinen- und Anlagenbau hat sicherheitsgerichtete Kommunikation heute bereits in zahlreichen Applikationen die Parallelverdrahtung abgelöst. Die Gründe dafür sind vielfältig: So werden aufwendige Verdrahtungen reduziert, Diagnose und Fehlersuche vereinfacht und die Verfügbarkeit der gesamten Applikation gesteigert. Nachfolgend soll die Funktionsweise sicherer Kommunikation am Beispiel von SafetyNET p erläutert und Anwendungsfälle aufgezeigt werden.

6.1.1 Prinzip dezentrale Sicherheitstechnik

Die Anbindung von Peripherie wie NOT-HALT-Schaltern an eine Sicherheitssteuerung ist, abhängig vom angestrebten Sicherheitslevel, in aller Regel zweikanalig ausgelegt. Aufgrund der Redundanz und zusätzlicher Leitungstests können somit Fehler wie Kurzschlüsse oder Leitungsbrüche aufgedeckt und beherrscht werden. Auf einem Buskabel erfolgt die Übertragung einkanalig seriell, wobei die physikalische Leitungsredundanz nicht gegeben ist. Daher müssen zusätzliche Maßnahmen im Protokoll Fehler wie abgetrennte Buskabel oder Kommunikationsstörungen aufdecken.



Prinzip dezentrale Sicherheitstechnik

6.1.2 Beherrschung von Kommunikationsfehlern

Nachfolgend werden mögliche typische Fehler und Maßnahmen sowie deren Beherrschung beschrieben, wie sie bei der Kommunikation von sicheren Daten über ein industrielles Kommunikationssystem auftreten können.

6.1.2.1 Wiederholung von Nachrichten

Fehlfunktionen innerhalb des Busteilnehmers oder einer Netzwerkkomponente können zur Wiederholung von Telegrammen führen. Um wiederholte Nachrichten zu erkennen, erhält jede Nachricht eine laufende Nummer. Aufgrund der „Erwartungshaltung“ des Empfängers an die laufende Nummer erkennt dieser wiederholte Telegramme und leitet geeignete Maßnahmen ein.

6.1 Grundprinzipien sicherheitsgerichteter Kommunikation

6.1.2.2 Verlust von Nachrichten

Aufgrund einer Fehlfunktion bei einem Busteilnehmer oder einer Netzwerkkomponente können Nachrichten gelöscht werden bzw. keine Telegramme mehr beim Empfänger ankommen. Der Empfänger erkennt den Verlust von Datenpaketen anhand einer laufenden Nummer. Zusätzlich überwacht ein Timeout beim Empfänger, wann eine neue Nachricht spätestens eingetroffen sein muss. Nach Ablauf des Timeouts kann der Empfänger die Applikation in den sicheren Zustand bringen.

6.1.2.3 Einfügung von Nachrichten

Aufgrund einer Fehlfunktion bei einem Busteilnehmer oder einer Netzwerkkomponente können sich zusätzliche Nachrichten einschleichen. Anhand der laufenden Nummer lassen sich diese – wie die Wiederholung von Nachrichten – entdecken und entsprechend behandeln.

6.1.2.4 Falsche Abfolge von Nachrichten

Fehler bei einem Busteilnehmer oder Telegramme speichernde Netzwerkkomponenten wie Ethernet Switches und Router können die Reihenfolge von Telegrammen verfälschen. Dies wird jedoch anhand der laufenden Nummern bemerkt.

6.1.2.5 Verfälschung von Nachrichten

Fehlfunktionen eines Busteilnehmers bzw. einer Netzwerkkomponente oder Störungen auf dem Übertragungsmedium, z. B. EMV-verursacht, können Nachrichten verfälschen: Ein über den sicheren Telegramminhalt gelegter Datensicherungsmechanismus (Checksumme) erkennt dies und entdeckt die verfälschte Nachricht.

6.1.2.6 Verzögerung von Nachrichten

Eine Fehlfunktion beim Busteilnehmer oder ein nicht kalkulierbares Datenaufkommen im Netzwerk kann zu Verzögerungen führen: Eine Zeiterwartung (Timeout) beim Empfänger erkennt die Verzögerungen und leitet geeignete Maßnahmen ein.

6.1.2.7 Kopplung sicherheitsrelevanter und nicht sicherheitsrelevanter Übertragungsfunktionen

In gemischten Systemen mit sicheren und nicht sicheren Teilnehmern interpretieren Empfänger das Telegramm eines Standardteilnehmers mitunter als sicheres Telegramm. Mit Maßnahmen wie netzwerkweit eindeutigen Kennungen sowie einer unterschiedlichen Datensicherung für sichere und nicht sichere Nachrichten lassen sich derartige Verwechslungen beim Empfänger vermeiden.

	Maßnahmen pro Nachricht				
Fehler	Laufende Nummer	Zeiterwartung	Kennung für Sender und Empfänger	Daten-sicherung	Unterschiedliche Daten-sicherung für sichere und nicht sichere Nachrichten
Wiederholung	◆				
Verlust	◆	◆			
Einfügung	◆		◆		
falsche Abfolge	◆				
Nachrichten-verfälschung				◆	
Verzögerung		◆			
Kopplung von sicheren und nicht sicheren Nachrichten			◆		◆

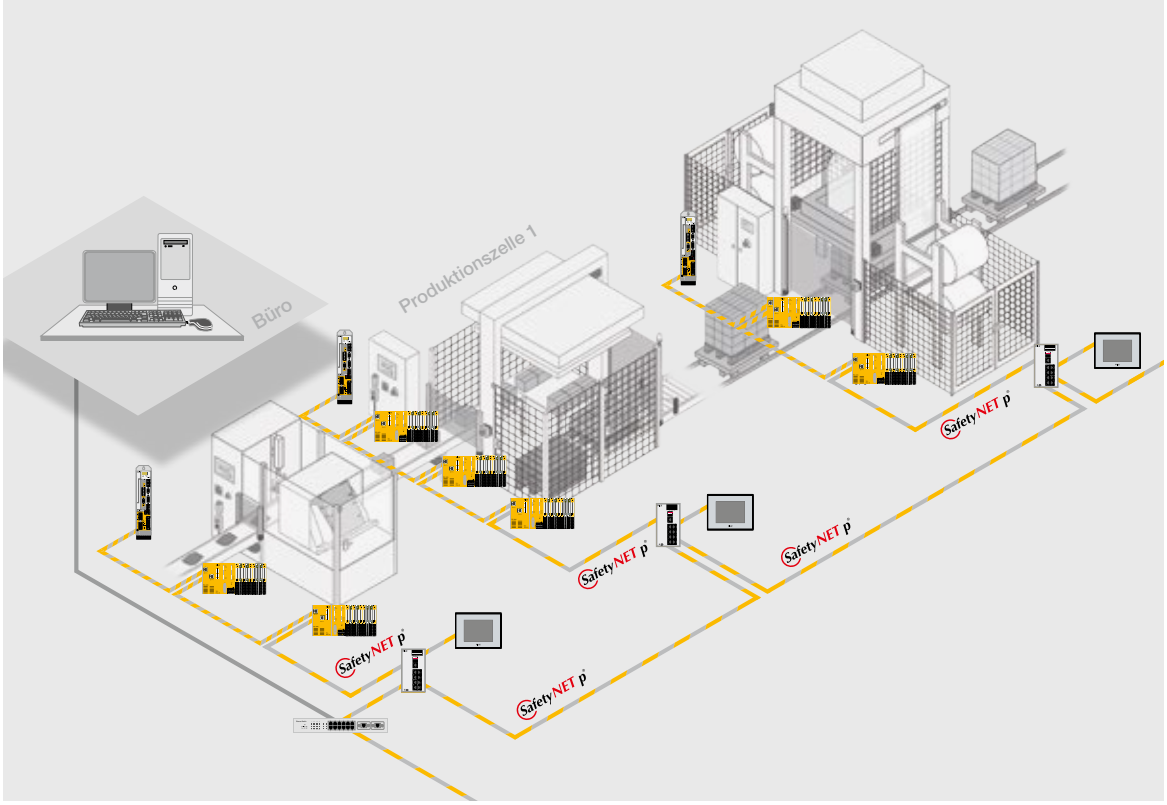
Fehler und Maßnahmen am Beispiel SafetyNET p, entnommen aus BIA GS-ET 26

6.1 Grundprinzipien sicherheitsgerichteter Kommunikation

6.1.3 Prinzip Redundanz

Um mögliche Fehler bei der Erfassung und Verarbeitung von sicheren Signalen in den Busteilnehmern zu beherrschen, wird jede Funktion von mindestens zwei unterschiedlichen Komponenten oder Methoden bearbeitet, die sich gegenseitig überwachen. Beim Erkennen eines Fehlers gelingt es mittels der Komponenten oder Methoden, den sicheren Zustand herbeizuführen. So arbeiten zum Beispiel beim sicheren Bussystem SafetyNET p redundante Mikroprozessoren die Applikationssoftware ab, die ihre jeweiligen Ergebnisse vergleichen und dem redundanten Controller übergeben. Dieser erzeugt dann die eigentliche sichere Nachricht.

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®



Am Beispiel des weit verbreiteten sicherheitsgerichteten Bussystems SafetyNET p werden nachfolgend Funktionsweise und Anwendung eines sicheren, auf Ethernet basierenden Bussystems erläutert.

6.2.1 Warum Ethernet in der Automatisierungstechnik?

Die Automatisierungstechnik entwickelt sich derzeit weg von zentralisierten Steuerungssystemen mit einfachen binären Sensoren und Aktoren hin zu komplexen und intelligenten Systemen. Dabei wächst der Anteil an Steuerungs- und Prozessleistung innerhalb der Sensoren und Aktoren stetig. Dieser Trend ändert die Anforderungen an die Kommunikation dramatisch: Statt des heute noch üblichen Master-Slave-Systems werden künftig immer mehr Daten direkt zwischen den Teilnehmern ausgetauscht. Die einzelnen, heute noch weitgehend einfachen Teilnehmer übernehmen dabei immer mehr die Funktion von Teilnehmern mit eigener Rechenleistung.

Die moderne IT-Technologie bietet – wie in der Bürokommunikation mit Personalcomputern und Netzwerkkomponenten – eine Vielzahl an Systemkomponenten zu günstigen Preisen. Das Innovationspotenzial ist enorm. Deshalb wollen Anwender diese Technologie zunehmend in abgeänderter Form auch für dieindustrielle Automatisierungstechnik nutzbar machen. Eine herausragende Rolle spielt dabei das Ethernet, das sich in der Bürokommunikation schon vor Jahren als Standard etabliert hat.

Parallel zu diesem Trend steigen die Anforderungen an die einzelnen Elemente einer Produktionsanlage stetig. Dies betrifft unter anderem Zykluszeiten, Genauigkeit oder Häufigkeit von Messungen, Datenmenge oder Prozessorleistungen. Für das Automatisierungssystem bedeutet dies, dass die Leistungsfähigkeit der Steuerungen und der Kommunikationssysteme den steigenden Anforderungen genügen müssen. Als modernes ethernetbasiertes Feldbussystem entspricht SafetyNET p diesen Anforderungen. Gleichzeitig ist SafetyNET p so einfach zu installieren und so zuverlässig wie Feldbussysteme.

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.2 Systembeschreibung SafetyNET p

SafetyNET p ist ein Bussystem, bei dem alle Geräte im Netzwerk die gleichen Rechte haben. Die Buszykluszeit von SafetyNET p kann den Applikationsanforderungen angepasst werden. Dabei werden die Daten nach dem Publisher/Subscriber-Prinzip ausgetauscht. Jedes Gerät kann als Publisher (Veröffentlicher) anderen Geräten (Subscriber) Daten via SafetyNET p zur Verfügung stellen. Diese Subscriber wiederum können die veröffentlichten Daten von einzelnen oder allen Teilnehmern lesen. Auf diese Art und Weise ist es möglich, Daten effizient zwischen allen Teilnehmern auszutauschen.

6.2.2.1 Sicherheit

Das Protokoll verfügt über einen sicheren Datenkanal, der für die Übertragung nach SIL 3 der IEC 61508 zertifiziert ist. Die Übertragung der sicheren und nicht sicheren Daten erfolgt über das gleiche Ethernetkabel. Nicht sichere Teilnehmer können auf die sicheren Daten direkt zugreifen und sie zur weiteren nicht sicheren Verarbeitung verwenden.

Kommunikationsmedien

Um den unterschiedlichen Applikationsanforderungen gerecht zu werden, stehen SafetyNET p eine Vielzahl an Kommunikationsmedien zur Verfügung. So lassen sich Kupferkabel, Funkstrecken und Lichtwellenleiter einsetzen.

Fiberoptische Kommunikation

Anstelle von Kupferleitungen kommen bei der Lichtwellenleiter-Kommunikation (LWL) fiberoptische Leitungen sowie optische Sender und Empfänger zum Einsatz. Bei SafetyNET p stehen unterschiedliche Geräte zum Aufbau von fiberoptischen Strecken zur Verfügung. Typischerweise wird diese Aufgabe von Ethernet Switches übernommen, die je nach Anwendung fiberoptische Wandler für Lichtwellenleiterstrecken von bis zu 40 Kilometern Länge bieten.

LWL-Übertragung ist in vielfältigen Applikationen zu finden. Sie ist dann von Bedeutung, wenn eine hohe EMV-Belastung die Kommunikation stören würde, wie dies z. B. bei Schweißrobotern in der Automobilindustrie der Fall sein kann. Auch für die sicherheitsgerichtete Kommunikation zwischen Berg- und Talstation von Seilbahnen, wo hohe Distanzen im freien Feld überbrückt werden müssen, sind fiberoptische Strecken sehr häufig zu finden.

Sichere Funkkommunikation

Durch den Einsatz von Access Points können SafetyNET p-Daten über Funk übertragen werden. Die Access Points sind aus Sicht der Sicherheitssteuerungen transparent, d. h. sie sind nicht als Teilnehmer im Netzwerk sichtbar. Der Sicherheitslevel von SafetyNET p wird durch die Funkübertragung nicht beeinflusst.

Sichere Funkkommunikation kommt dort zum Einsatz, wo das Verlegen von Kabeln zu aufwendig und damit nicht kosteneffizient wäre. Ein weiterer Anwendungsfall sind Teilnehmer auf bewegten Einrichtungen. Das können rotierende oder linear bewegte Anlagenteile sein, wie sie bei Krananlagen zu finden sind, oder fahrerlose Transportsysteme. Beim Einsatz von sicherer Funktechnologie werden vor allem hohe Anforderungen an die Qualität der Funkverbindung gestellt, da diese die Anzahl von Telegrammverlusten, falscher Abfolge sowie Verzögerungen beeinflusst und zu sicherheitsgerichteten Abschaltungen der Applikation führen kann. Dies hat wiederum Auswirkungen auf die Verfügbarkeit der Applikation.

Um die Qualität der Funkverbindung sicherzustellen, ist auf die Auswahl der für die Applikation geeigneten Funk- und Antennentechnologie sowie Redundanzkonzepte besonderes Augenmerk zu richten und ggf. durch Feldversuche zu verifizieren.

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.2.2 Flexible Wahl von Topologie und Buszykluszeit

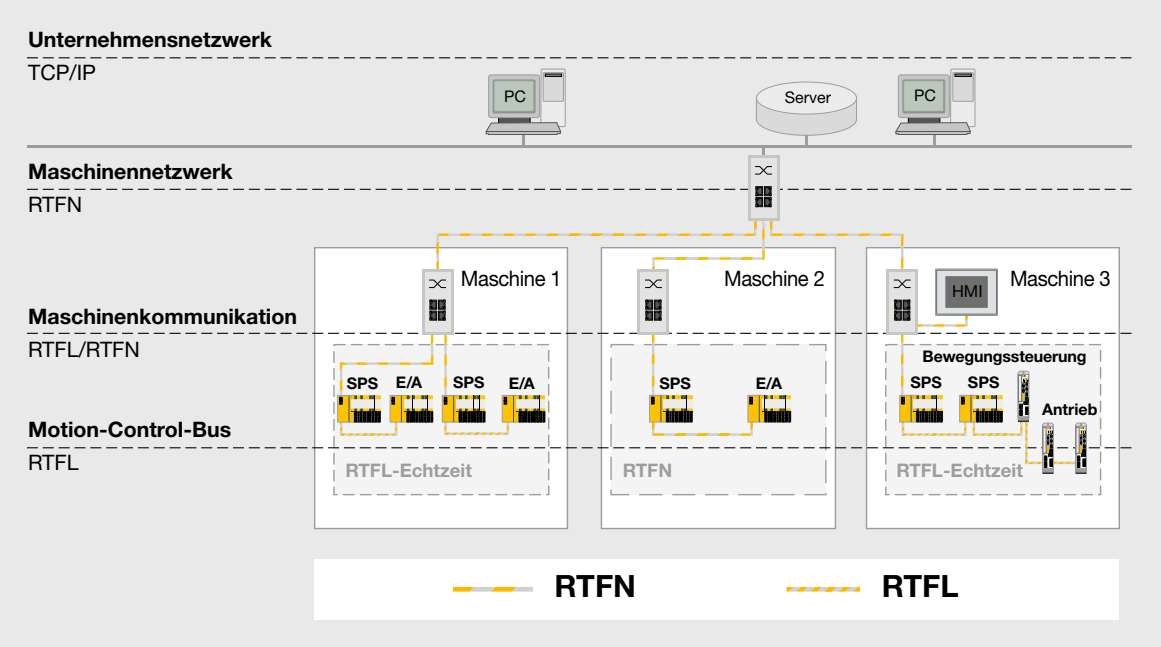
SafetyNET p ist nicht nur in Bezug auf die Wahl eines geeigneten Kommunikationsmediums äußerst flexibel, sondern auch bei der Frage nach der passenden Topologie: Das System unterstützt Linien-, Stern-, Baum- sowie Ringtopologien. Für die Kommunikation innerhalb einer Zelle eignet sich das RTFL (Real Time Frame Line)-Kommunikationsprinzip, das schnellste Zykluszeiten gestattet. Aufträge und Ereignisse können quer über das gesamte Netz mit hoher Präzision erfasst und ausgeführt werden. Unabdingbar für Echtzeitanwendungen: Ein Jitter von etwa 100 ns ist in Echtzeitregelschleifen erreichbar. Damit ist es möglich, SafetyNET p selbst im Regelkreis eines Umrichters zwischen Drehgeber und Geschwindigkeitsregler einzusetzen. Natürlich sind auch andere hochdynamische Anwendungen realisierbar.
Auf übergeordneten Ebenen wird üblicherweise das RTFN-(Real-Time-Frame-Network-)Verfahren eingesetzt, das maximale Koexistenzfähigkeit zu vorhandenen Diensten bietet.

6.2.2.3 Applikationsschicht

Die Schnittstelle zur Applikation basiert auf der weit verbreiteten CANopen-Technologie.

6.2.2.4 Standard-Ethernet-Technologie

SafetyNET p verwendet für die Kommunikation von Zelle zu Zelle oder in allgemeine Netze die weit verbreitete UDP/IP-Kommunikation. Für den Aufbau der Netzwerkinfrastruktur kommen herkömmliche handelsübliche Netzwerkkomponenten zum Einsatz. Dies beinhaltet insbesondere Stecker, Kabel, Switches, Router und Gateways.

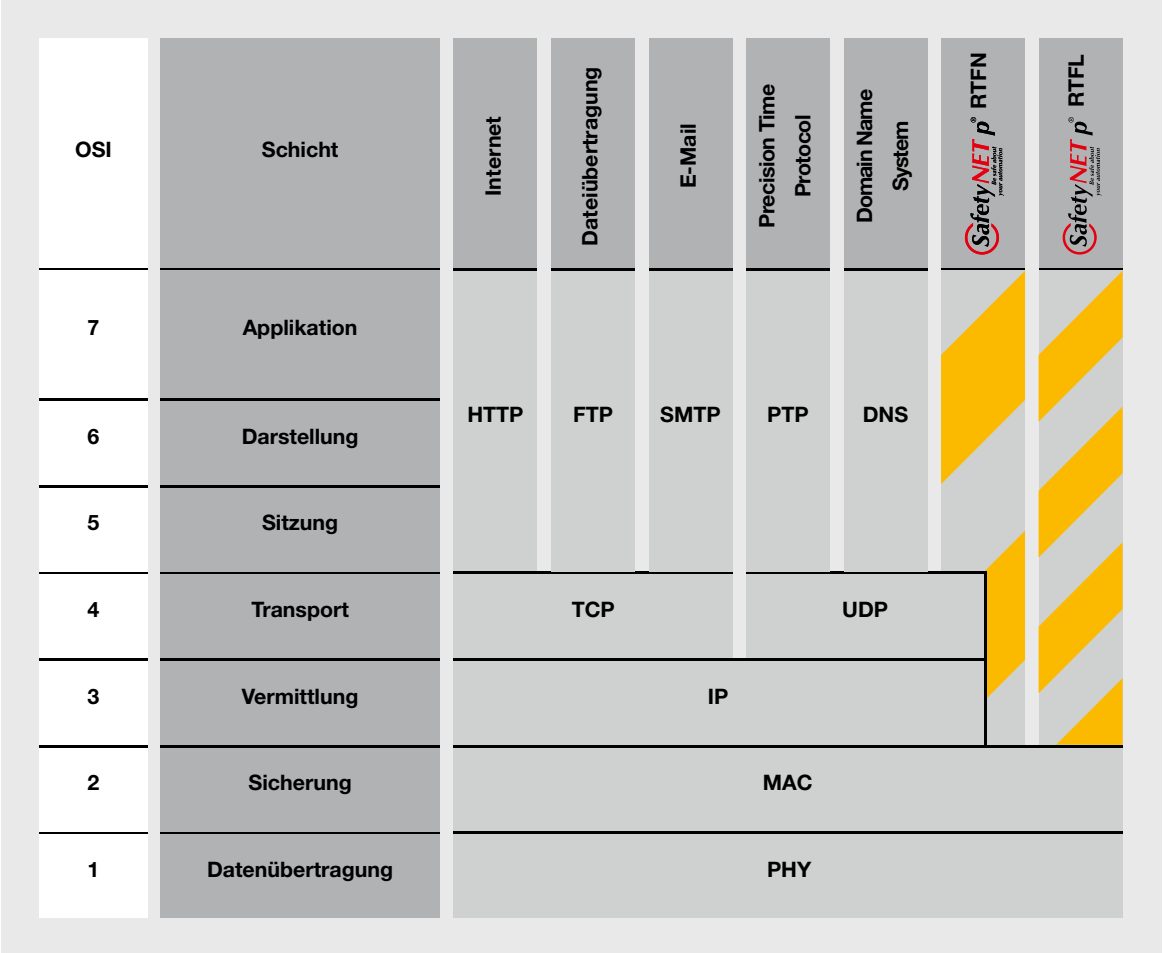


SafetyNET p in der Kommunikationshierarchie

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.3 UDP/IP-basierte Kommunikation mit RTFN

Auf Anlagen- und Fertigungszellenebene, wo Standard-Ethernetprotokolle gefordert und die Anforderungen an Echtzeit geringer sind, kommt die RTFN-Transportschicht von SafetyNET p zum Einsatz. RTFN dient dazu, die RTFL-Echtzeitzellen miteinander zu vernetzen und Teilnehmer wie Visualisierungsgeräte oder Service-PCs anzubinden. Typisch für die RTFN-Ebene ist die Baumtopologie, wie sie auch in der Bürowelt verwendet wird. Ausgehend von Ethernet-Switches werden die Netzwerkteilnehmer in individuellen Punkt-zu-Punkt-Verbindungen angeschlossen.

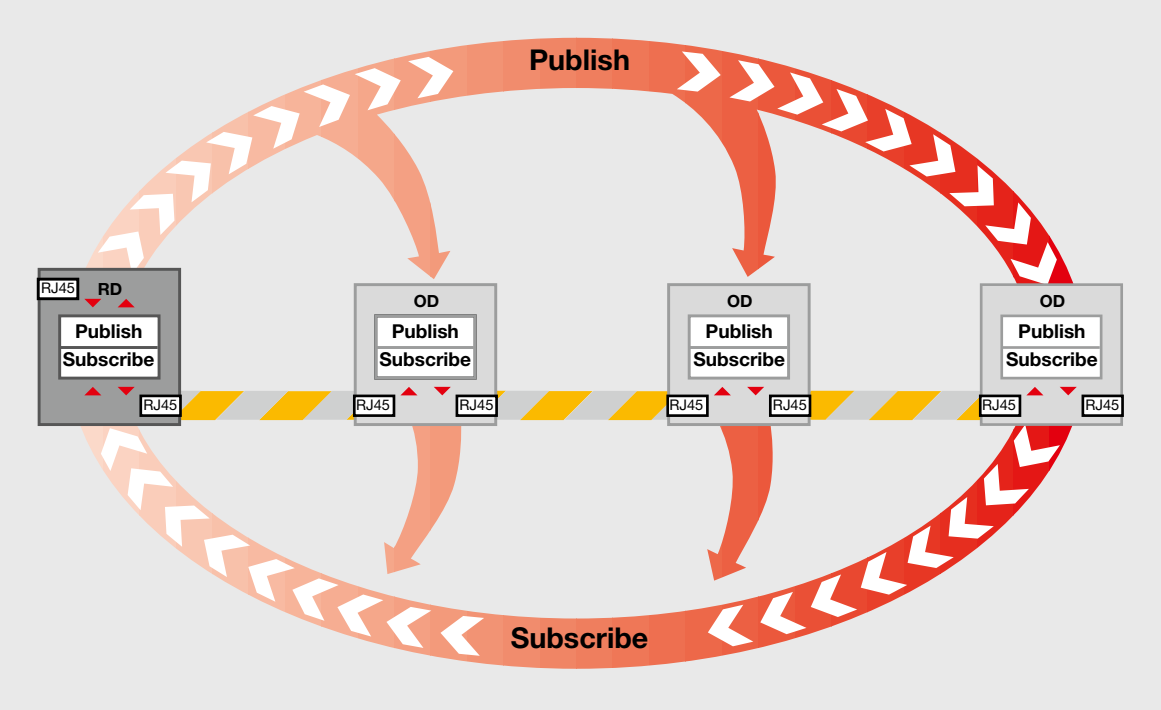


SafetyNET p im ISO/OSI-Referenzmodell

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.4 Harte Echtzeit-Kommunikation mit RTFL

Die RTFL-Transportschicht von SafetyNET p ist für schnellste Echtzeitanwendungen optimiert. Typischerweise sind dabei die Geräte, wie bei den traditionellen Feldbussen üblich, in Linienstruktur miteinander verbunden. Daten werden nach dem Publisher/Subscriber-Prinzip ausgetauscht. Jedes Gerät kann als Publisher (Veröffentlicher) anderen Geräten (Subscriber) Daten via SafetyNET p zur Verfügung stellen. Diese Subscriber wiederum können die veröffentlichten Daten von einzelnen oder allen Teilnehmern lesen. Auf diese Art und Weise ist es möglich, Daten effizient zwischen allen Teilnehmern auszutauschen. Als Kommunikationsmechanismus verwendet RTFL eine sehr schnelle zyklische Datenübertragung. Die Kommunikation wird dabei von einem Root Device (RD) initiiert. Der im Root Device erzeugte Ethernetrahmen wird dann an die übrigen Geräte (OD – Ordinary Device) übertragen. Die ODs befüllen nacheinander den Ethernetrahmen mit zu publizierenden Daten und entnehmen dem Ethernetrahmen die zu lesenden Daten. Jedes RTFL-Segment benötigt genau ein Root Device. RTFL-Geräte besitzen zwei Ethernet-Schnittstellen, wodurch die von den Feldbussen gewohnte Daisy Chain-Verkabelung zur Anwendung kommt.



SafetyNET p RTFL-Kommunikation

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.5 Applikationsschicht

Die Applikationsschicht von SafetyNET p adaptiert die Mechanismen von CANopen an die Gegebenheiten von SafetyNET p. CANopen ist ein herstellerunabhängiger offener Feldbusstandard, der von der CiA (CAN in Automation)-Organisation spezifiziert bzw. standardisiert wurde. Für SafetyNET p ist somit eine einheitliche Anwendungsschicht für industrielle Applikationen verfügbar.

Die SafetyNET p-Applikationsschicht orientiert sich weitgehend an dem CANopen-Standard. Anpassungen wurden vor allem im Kommunikationsbereich sowie für die Behandlung sicherer Anwendungsdaten getroffen. Zentrales Element von CANopen ist das Objektverzeichnis, das als Schnittstelle zwischen der Anwendung und dem Kommunikationssubsystem agiert. Es ist im Wesentlichen eine Gruppierung von Objekten und Funktionen, die dann als Applikationsobjekte gespeichert und abgerufen werden können.

Für die Kommunikation zwischen Geräten stehen in der Regel zwei Möglichkeiten zur Verfügung: Applikationsdaten können zu Prozessdatenobjekten (PDOs) zusammengefasst (sog. Mapping) und über das Kommunikationssystem veröffentlicht werden. Dies geschieht über den zyklischen Datenkanal in SafetyNET p. Die zweite Möglichkeit ist das sogenannte SDO (Service-Daten-Objekte), das man für azyklische Daten nutzt und das beispielsweise bei der Parametrierung von Steuerungen Verwendung findet.

6.2.6 Sichere Kommunikation über SafetyNET p

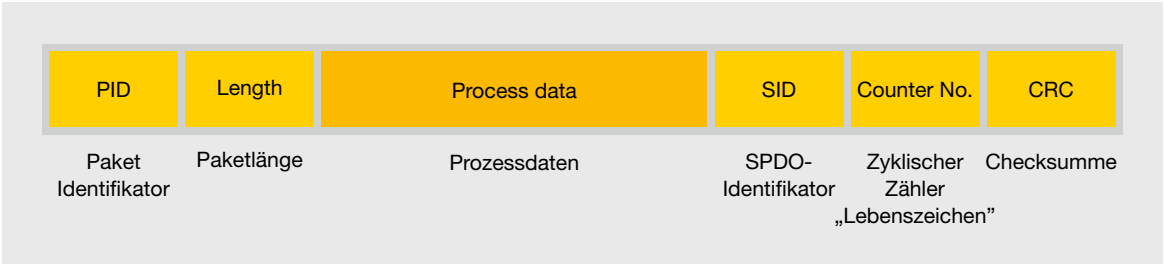
Durch eine integrierte sichere Kommunikationsschicht können mit SafetyNET p auch sicherheitsgerichtete Daten kommuniziert werden. Die Sicherungsmechanismen sind bis SIL 3 nach IEC 61508 ausgelegt. Die sicheren Daten werden gekapselt in SafetyNET p-Telegrammen verschickt. Dadurch können alle anderen Netzwerkkomponenten wie Switches oder Kabel Standard-Ethernetkomponenten sein, die keinen Einfluss auf die Sicherheit nehmen. Auch nicht sichere Netzwerkteilnehmer, wie zum Beispiel PCs oder Standard-Steuerungen, sind ohne Einfluss auf die sicherheitsgerichtete Kommunikation. Somit ist ein gemischter Betrieb von sicheren und nicht sicheren Geräten in einem Netzwerk möglich.

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.7 Sicherer Telegrammaufbau

Zyklische Daten werden in SafetyNET p als sichere PDOs (SPDOs) kommuniziert und haben folgendes Format:

- PID (Packet Identifier):
  dient zusammen mit der SID der eindeutigen Identifizierung des Datenpakets
- Length: komplette Länge des Pakets in Byte
- Process data: sichere Prozessdaten
- SID (Safe ID): 16 Bit netzweit eindeutige ID, durch die der Sender sowie das SPDO eindeutig identifizierbar sind
- Counter No.: 8 Bit zyklischer Zähler für die Lebenszeichen-Überwachung von Teilnehmern
- CRC: 32 Bit Prüfsumme über das gesamte sichere Datenpaket



Sichere PDO-Nachricht

6.2.8 Branchen, Applikationen

SafetyNET p kommt weltweit in einer Vielzahl von Branchen und Applikationen zum Einsatz. Die folgende Auflistung stellt lediglich einen Auszug dar.

6.2.8.1 Flughafen

In Flughäfen sind Gepäck- und Fördertechnik-Applikationen zu finden, mit denen weite Distanzen überbrückt werden müssen. Dabei sind über die gesamte Strecke sicherheitstechnische Einrichtungen wie beispielsweise NOT-HALT-Taster und -Reißleinen verteilt. SafetyNET p sammelt die sicherheitsgerichteten Signale ein und stellt sie den Sicherheitssteuerungen zur Verfügung, die bei Bedarf die Antriebe sicherheitsgerichtet anhalten oder abschalten.

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.8.2 Personentransport

Auch in Seilbahnen dient SafetyNET p der Kommunikation: Hier werden sicherheitsgerichtete Signale zwischen Berg- und Talstation ausgetauscht sowie Signale auf der Strecke eingesammelt.
Um große Distanzen zu überbrücken, dienen häufig Lichtwellenleiter als Kommunikationsmedium.

6.2.8.3 Krananwendungen

Moderne Steuerungskonzepte basieren auf leistungsfähiger Ethernet-Technologie. Alle Informationen sind somit überall verfügbar. Das Echtzeit-Ethernet SafetyNET p wird zum Beispiel in weit verzweigten Krananlagen für den zuverlässigen Austausch und die Synchronisation von Steuerungs-, Fail-safe-Daten und Zuständen genutzt.

6.2.8.4 Fahrerlose Transportfahrzeuge (FTF/AGV)

Das Echtzeit-Ethernet SafetyNET p wird auch bei fahrerlosen Transportsystemen eingesetzt. Übertragen werden sowohl Daten für Automatisierungsaufgaben wie die Beladung und Entladung als auch für sicherheitsgerichtete Steuerungsaufgaben wie etwa Geschwindigkeit und Richtung einer einzelnen Transporteinheit.

6.2 Sichere Ethernet-Kommunikation mit SafetyNET p®

6.2.9 Anwendungsbeispiel modularer Maschinenbau

Maschinen und Anlagen werden zunehmend modularisiert. Das bedeutet, sie werden in funktional gegliederte mechatronische Einheiten zerlegt. In einem solchen Konzept folgt die Elektrotechnik dem mechanischen Aufbau der Maschine, was zu vielfältigen Vorteilen führt. Einmal entwickelte Maschinenmodule können in verschiedenen Maschinen verwendet werden, was letztlich den Entwicklungsaufwand reduziert. Zudem werden Module getrennt gefertigt und erst im Rahmen der Endmontage zusammengefügt. Darüber hinaus können Module getrennt voneinander entwickelt werden, was durch die Parallelisierung der Aufgaben Zeitersparnis bei der Entwicklung bringt.

Diese Art von Maschinenbau nach dem Baukastenprinzip ermöglicht die Realisierung von kundenindividuellen Lösungen mit geringerem Aufwand. Feldbussysteme verhindern diesen modularen Ansatz, da sie meist auf einem zentralen Master-Slave-Ansatz beruhen. Insbesondere in der Sicherheitstechnik ist häufig eine zentrale Instanz vorhanden: der Master. Mit dem bei SafetyNET p durchgängig angewendeten Publisher/Subscriber-Kommunikationsprinzip wird auf eine zentrale Instanz verzichtet und dadurch modularer Maschinenbau ermöglicht.

Modularer Maschinenbau

7

Sichere Bewegungs-steuerung/ Safe Motion

7 Sichere Bewegungssteuerung/Safe Motion

7 Sichere Bewegungssteuerung/Safe Motion

7.1 Definition von Safe Motion 7-3
7.2 Grundprinzip 7-4
7.2.1 Sichere Trennung der krafterzeugenden Energiezufuhr 7-4
7.2.2 Sichere Überwachung der Bewegung 7-6
7.2.3 Sichere Grenzwertvorgabe 7-9
7.3 Norm EN 61800-5-2 7-10
7.4 Sicherheitsfunktionen 7-12
7.4.1 Stopp-Funktionen und deren Normenbezug 7-12
7.4.2 Sicherheitsfunktionen nach EN 61800-5-2 7-12
7.5 Systembetrachtung 7-22
7.5.1 Antriebselektronik 7-23
7.5.2 Motor 7-24
7.5.3 Sichere Logik 7-24
7.5.4 Sichere Bremse 7-25
7.5.5 Bewegungsüberwachung 7-25
7.5.6 Bewegungssteuerung 7-26
7.5.7 Realisierungsbeispiele 7-26
7.6 Beispiele für Safe Motion 7-28
7.6.1 Performance Level von Sicherheitsfunktionen 7-28
7.6.2 Reaktionszeiten von Sicherheitsfunktionen 7-42

7.1 Definition von Safe Motion

Sichere Antriebsfunktionen haben mittlerweile in Normen, Produkten und Applikationen Einzug gehalten und können heute als Stand der Technik bezeichnet werden. Sie sind Teil der funktionalen Sicherheit von Maschinen und Anlagen und finden als produktivitätssteigernde Maßnahmen zunehmend Verbreitung am Markt. Neben dem Personenschutz erhält auch der Schutz von Maschinen und Einrichtungen immer größere Bedeutung.

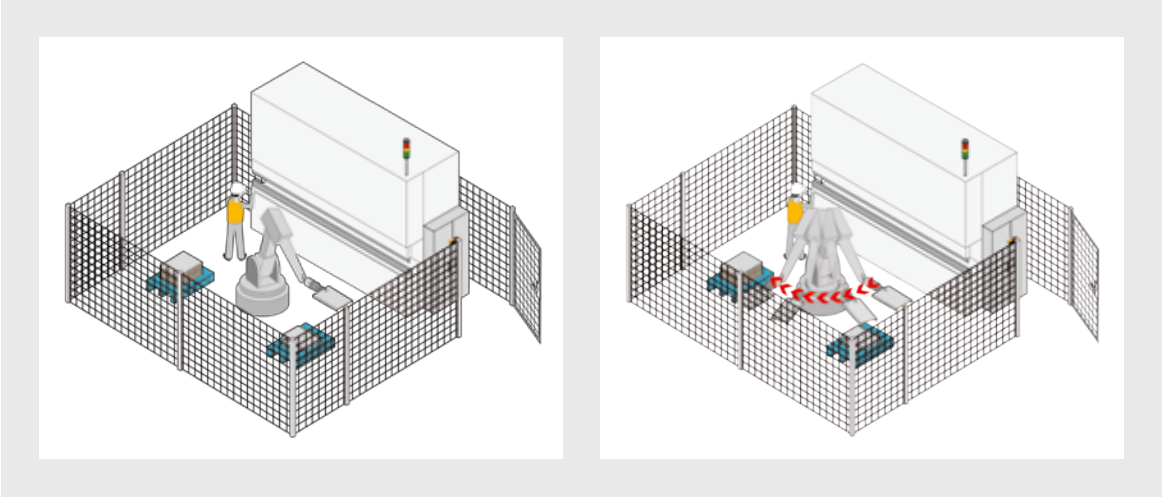
Betrachtet man die Anwendung des Fail-safe-Prinzips innerhalb der klassischen Sicherheitsfunktionen, so führt das Auslösen der Sicherheitsfunktion zu einem Abschalten der Ausgänge, was als „sicherer Zustand“ bezeichnet wird. Wendet man sichere Antriebsfunktionen an, könnte eine Applikation folgendermaßen aussehen: Beim Öffnen einer Schutztür wird der Motor sicher über eine definierte Rampe gebremst und verharrt anschließend im Stillstand bei aktiver Regelung. Anschließend bewegt sich der Motor im Tippbetrieb mit sicher reduzierter Geschwindigkeit. Mit anderen Worten: Auf die Verletzung einer statischen Schutzraumüberwachung folgt die Fortführung der Produktion mit reduzierter Taktzahl und sicher überwachten Bewegungen.

Was hier an einem einfachen Beispiel dargestellt ist, entspricht dem Übergang von der statischen zur dynamischen Sicherheit. Dynamik hat in den verschiedenen Disziplinen unterschiedliche Bedeutungen. In der Sicherheitstechnik versteht man unter Dynamik die Anpassung der Sicherheitsfunktionen an sich verändernde Schutzräume. Die in der Norm EN/IEC 61800-5-2 spezifizierten Anforderungen an die funktionale Sicherheit drehzahlvariabler Antriebe eröffnen hierzu neue Perspektiven.

Die Hauptanforderungen an sichere Antriebssysteme bezüglich einer dynamischen Sicherheit sind:

- sichere Überwachung von kinematischen Größen wie z. B. Beschleunigung, Geschwindigkeit, Weg
- kurze Reaktionszeiten zur Reduzierung der Nachlaufwege
- variable Grenzwerte, die der Laufzeit angepasst werden können

Mit der antriebsintegrierten Sicherheitstechnik, schnellen sicheren Antriebsbussen, performanten Sicherheitssteuerungen und sicheren Kamerasystemen stehen Produkte für High-End-Sicherheitslösungen zur Verfügung. Der Begriff Safe Motion wird, je nach Sichtweise, unterschiedlich ausgelegt. Antriebshersteller verstehen in der Regel antriebsintegrierte Sicherheit als Safe Motion, während Steuerungshersteller damit externe Lösungen in Verbindung bringen. Bei einer unabhängigen Betrachtung des Themas ist festzustellen, dass der Begriff Safe Motion zunächst nur aussagt, dass es um die Realisierung einer sicheren Bewegung geht.

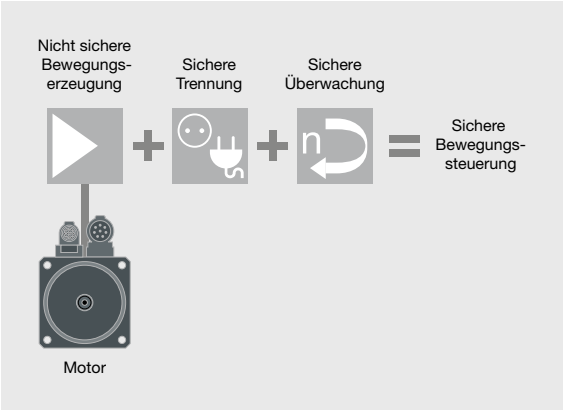


Vergleich von statischer und dynamischer Sicherheit

7.2 Grundprinzip

Ziel der Sicherheitstechnik war stets, Gefahr bringende Bewegungen zu verhindern. Nichts liegt daher näher, als die Sicherheitstechnik mit der Bewegungserzeugung eng zu verzahnen. Aus technischen wie wirtschaftlichen Gründen ist die Antriebselektronik – Servoverstärker und Frequenzumrichter – eine nicht sichere Komponente innerhalb der Automatisierung geblieben. Die Sicherheit wird daher durch zusätzliche sichere Komponenten gewährleistet, die den Motor im Fehlerfall in den kraftfreien sicheren Zustand überführen bzw. die Bewegung des angeschlossenen Motors sicher überwachen. Am Markt etabliert sich aktuell der Trend, diese zusätzlichen sicheren Komponenten in den Antrieb zu integrieren.

Nach dem heutigen Stand der Technik ergibt sich eine sichere Bewegungssteuerung aus der Kombination einer sicheren Bewegungsüberwachung, einer sicheren Trennung des Motors von der krafterzeugenden Energiezufuhr und einer nicht sicheren Bewegungserzeugung.

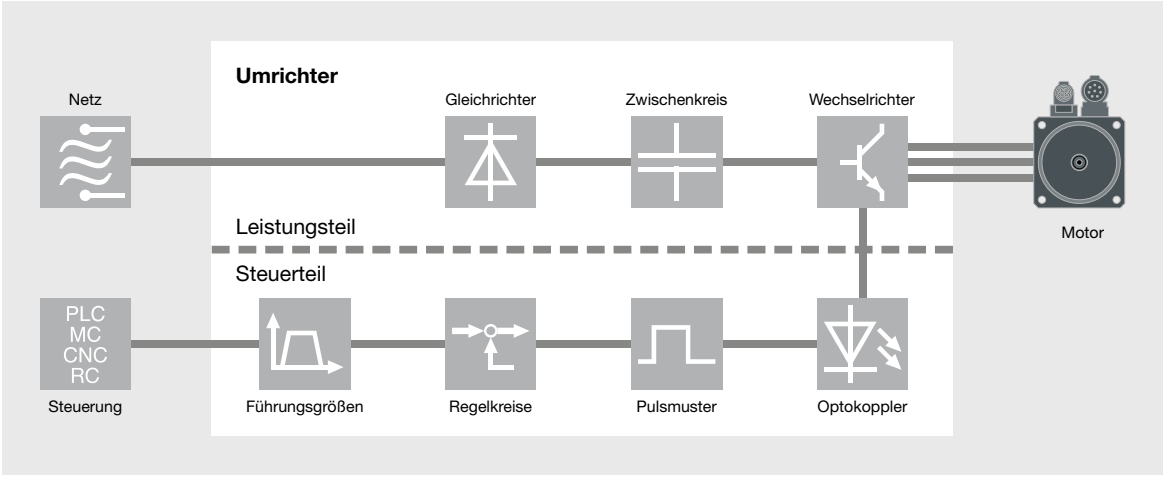


Komponenten einer sicheren Bewegungssteuerung

Die folgenden Ausführungen beziehen sich auf dreiphasige Antriebssysteme, wie sie heute im industriellen Umfeld eingesetzt werden. Eine Übertragung auf andere Aktorsysteme (wie z. B. DC-Antriebe, Servoventile …) ist nur bedingt möglich und bedarf einer gesonderten Betrachtung.

7.2.1 Sichere Trennung der krafterzeugenden Energiezufuhr

Bevor die unterschiedlichen Abschaltpfade eines Umrichters erläutert werden, ist ein Verständnis für die grundlegende Funktionsweise notwendig.

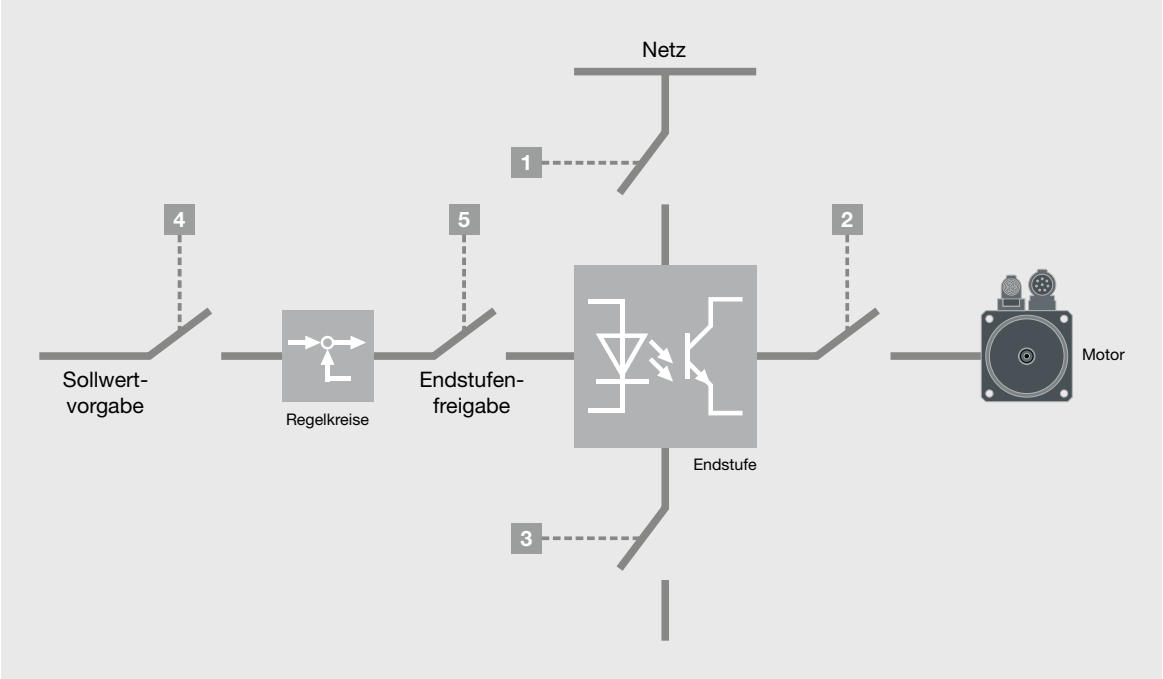


Grundlegende Funktionsweise eines Umrichters

7.2 Grundprinzip

Der interne Aufbau eines Umrichters gliedert sich in einen Steuer- und einen Leistungsteil. Mittels Optokoppler werden beide Teile galvanisch voneinander getrennt. Im Leistungsteil findet die Aufbereitung der vom Netz eingespeisten Leistung statt. Aus der Netzspannung mit konstanter Amplitude und Frequenz wird eine in Amplitude und Frequenz variable Klemmenspannung erzeugt. Dabei wird zunächst die sinusförmige Netzspannung im Gleichrichter zu einer pulsierenden Gleichspannung umgeformt. Diese wird durch einen nachgeschalteten Kondensator – auch Zwischenkreis genannt – geglättet. Der Zwischenkreis dient außerdem zur Aufnahme von Bremsenergie. Anschließend erzeugt der Wechselrichter durch zyklisches Schalten von positiven und negativen Zwischenkreisspannungen eine Ausgangsspannung mit sinusförmiger Grundwelle. Der Steuerteil des Umrichters generiert aus Führungsgrößen Pulsmuster, die zur Ansteuerung der Leistungshalbleiter des Wechselrichtermoduls dienen. Um den Motor von der krafterzeugenden Energiezufuhr zu trennen, gibt es mehrere Möglichkeiten:

Abschaltpfad	Prinzip oder Umsetzung	Technik
1 netzseitige Trennung	Netzschütz	Trennung der Versorgungsspannung des Umrichters
2 motorseitige Trennung	Motorschütz	Trennung der Klemmenspannung des Motors
3 antriebsintegrierte Trennung	sichere Pulssperre	Trennung der Ansteuersignale der Leistungshalbleiter
4 Trennung der Führungsgröße	Sollwertvorgabe zu Null setzen	Regler bzw. Steuerung erzeugen keine Stellgrößen (prozessorbasiert)
5 Trennung der Stellgröße	Reglerfreigabe	Es werden keine Ansteuersignale für die Leistungshalbleiter erzeugt.



Abschaltpfade eines Umrichters

7.2 Grundprinzip

Bei der netz- und motorseitigen Trennung der krafterzeugenden Energiezufuhr muss das Netz- oder Motorschütz über zwangsgeführte Kontakte verfügen. Wird der Öffnerkontakt mit dem Startsignal des Umrichters verknüpft, kann ein Fehler des Schützkontakts erkannt werden. Werden zwei Schütze in Reihe geschaltet und jeweils die Öffnerkontakte rückgeführt, kann die höchste Sicherheitskategorie erreicht werden. Die netzseitige Trennung hat den Nachteil, dass der Zwischenkreiskondensator des Leistungsteils bei jeder Trennung entladen wird und bei einem Wiederanlauf erst wieder neu aufgeladen werden muss. Dies wirkt sich negativ auf die Wiederanlaufzeit und Maschinenverfügbarkeit aus und hat eine geringere Lebensdauer der Zwischenkreiskondensatoren zur Folge, da durch die Auf- und Entladevorgänge die Alterung der Kondensatoren rasch voranschreitet.

Bei der motorseitigen Trennung würde zwar der Zwischenkreis geladen bleiben, da aber das Auftrennen der Motorleitung zur Verdrahtung des Schützes sehr aufwendig ist, wird dies nur selten praktiziert. Außerdem ist die Verwendung von Motorschützen nicht bei allen Umrichtern zugelassen. Eventuelle Überspannungen beim Trennen der Kontakte können den Wechselrichter schädigen. Wird die Trennung der krafterzeugenden Energiezufuhr als Sicherheitsfunktion häufig angefordert, führt dies auch zu einem starken Verschleiß der zwangsgeführten Kontakte von Netz- bzw. Motorschütz. Die Trennung der Führungsgröße (Sollwert-Vorgabe) bzw. der Stellgröße (Endstufen-Freigabe) kann mit den oben genannten Abschaltpfaden kombiniert werden. Da die Sollwert-Vorgabe und die Endstufen-Freigabe häufig prozessorbasierte Funktionen sind, dürfen sie nicht kombiniert benutzt werden, um Fehler gemeinsamer Ursache (Common-Cause-Fehler) auszuschließen.

Die antriebsintegrierte Lösung basiert auf dem Prinzip, dass die vom Prozessor erzeugten Pulsmuster sicher von den Leistungshalbleitern getrennt werden. Bei den hier betrachteten Antriebssystemen entsteht eine Bewegung des Motors aufgrund einer phasenrichtigen Bestromung der Wicklungsstränge. Diese muss so erfolgen, dass die Überlagerung der drei entstehenden Magnetfelder ein sogenanntes Drehfeld ergibt. Durch Wechselwirkung mit der beweglichen Komponente des Motors entsteht eine Kraftwirkung, die den Motor antreibt. Ohne Pulsmuster kann also kein Drehfeld entstehen und damit auch keine Bewegung des Motors stattfinden. Die Optokoppler, die für die galvanische Trennung zwischen Steuer- und Leistungsteil innerhalb eines Umrichters eingesetzt werden, sind als Abschaltpfad hervorragend geeignet. Wird z. B. die Anodenspannung des Optokopplers unterbrochen und mit der zuvor erwähnten Trennung der Stellgröße (Reglerfreigabe) kombiniert, wird eine Bewegung des Motors zweikanalig verhindert. Ein Testen der Abschaltpfade ist in der Praxis unerwünscht, da das Stoppen des Motors zu einer Unterbrechung der Produktion führt.

7.2.2 Sichere Überwachung der Bewegung

Eine Bewegung ist durch die kinematischen Größen Beschleunigung, Geschwindigkeit und Weg beschrieben. Aus der Sicht potenzieller Gefährdungen spielen auch Momente bzw. Kräfte eine wichtige Rolle. Durch die in der Norm EN/IEC 61800-5-2 aufgelisteten Sicherheitsfunktionen werden die oben genannten Größen abgedeckt. Die Umsetzung einer sicherheitsgerichteten Überwachung hängt sehr stark von der im System verwendeten Sensorik ab. Die in der Antriebstechnik verwendete Sensorik ist in der Regel nicht sicher und muss somit auf Fehler überwacht werden. Ein kritischer Zustand läge z. B. dann vor, wenn der Drehgeber aufgrund eines Defektes kein Signal liefern könnte, während der Motor bestromt wird und beschleunigt.

7.2 Grundprinzip

Bewegte Achsen in sicherheitsgerichteten Anwendungen benötigen redundante Positionsinformationen, um entsprechende Sicherheitsfunktionen erfüllen zu können. Unabhängige Positionswerte gewinnt man über unterschiedliche Wege: Eine Möglichkeit ist, durch einen zweiten Geber den Defekt zu erkennen. Eine sichere Komponente muss nun beide Geber überwachen und bei einem aufgetretenen Fehler gewährleisten, dass die Anlage in den sicheren Zustand überführt wird. Der Vorteil dieser Lösung liegt mitunter darin, dass die zwei Gebersysteme an verschiedenen Stellen der Maschine die Bewegung erfassen und somit defekte mechanische Übertragungselemente erkennen können.

In der Regel besitzen Drehgeber mehrere Signalspuren, um z. B. die Drehrichtung oder definierte Positionen innerhalb einer Umdrehung erkennen zu können. Diese Signale lassen sich ebenfalls für Plausibilitätstests heranziehen, ohne dass ein zweites Gebersystem benötigt wird. Allerdings ist hier keine durchgängige zweikanalige Struktur gegeben, da die Bewegung von einer Welle bzw. von einer Optik abgegriffen wird. Doppelt aufgebaute Gebersystem sind heute am Markt ebenfalls verfügbar. Solche Systeme bieten sich für Funktionen wie z. B. sichere Absolutlage an. Durch einen konsequent diversitären zweikanaligen Aufbau wird sogar SIL 3 nach EN/IEC 61508 erreicht. Hierbei kommt beispielsweise neben einem optischen auch ein magnetisches Abtastsystem zum Einsatz.

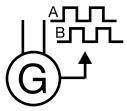
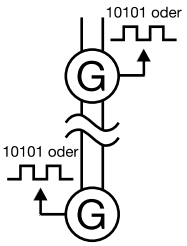
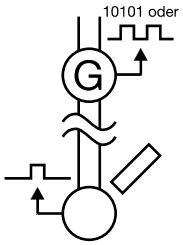
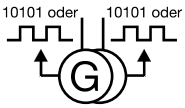
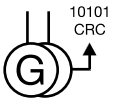
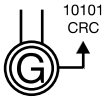
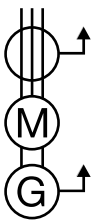
Eine kostengünstigere Möglichkeit bieten Multiturn-Geber, die ihre getrennten Multiturn- und Singleturn-Spuren ins Verhältnis setzen und somit Fehler aufdecken können. Hier findet eine sicherheitsbezogene Vorverarbeitung im Gebersystem selbst statt. Eine weitere Möglichkeit stellt die Verwendung von Motorsignalen dar: Durch die Erfassung von Spannungen und/oder Strömen kann mithilfe von Berechnungen auf die mechanische Bewegung des Motors geschlossen werden. Ein Vergleich mit den Gebersignalen deckt gefährliche Fehler auf. Die Produktnorm für elektrische Antriebssysteme mit integrierten Sicherheitsfunktionen EN 61800-5-2 enthält eine Liste mit Fehlerannahmen für verschiedene Bewegungs- und Lagesensoren (Anhang D, Tabelle D.16).

Die Kombination aus Gebersystem und sicherer Auswertung muss gewährleisten, dass durch Fehlerausschlüsse oder fehlererkennende Maßnahmen gefahrbringende Ausfälle verhindert werden.

Gebersignal	Beschreibung
	Initiatorsignal: entsteht durch Abtastung eines Nockens oder eines Zahnrads, Analogsignal mit 24-V-Pegel
	zwei um 90° phasenverschobene Analogsignale, entweder rechteck- oder sinusförmig (Pegel: TTL, 24 V, 1 Vss)
10101	digitale Schnittstelle, die Positionsinformationen kodiert überträgt (SSI, Feldbus)
10101 sin cos	digitale Motorfeedback-Schnittstelle mit zusätzlichen analogen Signalen (EnDat, Hiperface, BiSS)
10101 CRC	sichere digitale Schnittstelle, die Positionsinformationen kodiert überträgt (SafetyNET p, CANopen Safe, PROFIBUS und PROFINET mit PROFIsafe ...)

Marktübliche Geberschnittstellen

7.2 Grundprinzip

Gebersystem	Beschreibung	Sicherheitsintegrität
Standardgeber 	Auswertung von zwei Signalspuren einer gemeinsamen Optik	gering
zwei Geber 	zwei vollständig getrennte Kanäle, teuer	sehr hoch
ein Geber und Initiator 	zwei vollständig getrennte Kanäle, teuer, ungenau	mittel
sicherer Geber 	zwei unabhängige Gebersysteme in einem Gehäuse ohne sichere Vorverarbeitung	hoch
sicherer Geber 	zwei unabhängige Gebersysteme in einem Gehäuse mit sicherer Vorverarbeitung	hoch
sicherer Geber 	zweikanalig diversitäre Struktur in einem Gebergehäuse mit sicherer Vorverarbeitung	hoch
Standardgeber und Motorsignale 	zwei vollständig getrennte und diversitäre Kanäle	sehr hoch

Gebersysteme für sicherheitsbezogene Anwendungen

7.2 Grundprinzip

Ob ein Gebersystem in Kombination mit einer antriebsintegrierten Lösung oder einem externen Überwachungsgerät die von der Anwendung geforderte Sicherheitsintegrität erreicht, muss im Einzelfall geprüft werden. Sichere Gebersysteme stellen häufig Anforderungen an das Auswertegerät (z. B. Diagnosetests) oder geben die Fehler an, die vom Geber selbst nicht beherrscht werden. Diese müssen dann gegen die fehlererkennenden Maßnahmen des speziellen Auswertegerätes geprüft werden. Häufig werden hierbei auch Abstufungen in der maximal erreichbaren Sicherheitsintegrität gemacht.

7.2.3 Sichere Grenzwertvorgabe

Eine sichere Bewegungsüberwachung benötigt neben der sicheren Erfassung der Bewegung auch eine Möglichkeit, Grenzwerte sicher vorzugeben. Die Art und Weise hängt vom Maß der Dynamik und von der Flexibilität innerhalb der Maschine ab.

Grenzwerte	Beschreibung	Dynamik
konstant	Werden zur Inbetriebnahme fest eingestellt und können während des Betriebs nicht geändert werden.	-
auswählbar	Aus einem fest vorgegebenen Satz von Grenzwerten kann während des Betriebs der passende ausgewählt bzw. gewechselt werden.	o
dynamisch	Grenzwerte werden während des Betriebs berechnet und angepasst.	+

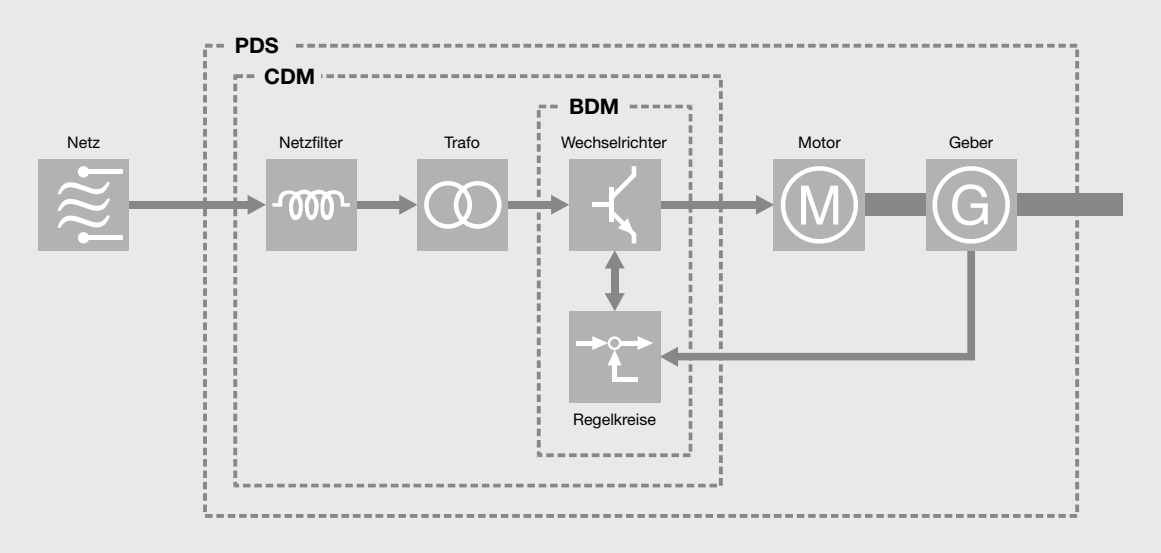
Dynamische und statische Grenzwerte

Schaltgeräteähnliche Systeme verwenden häufig konstante Grenzwerte. Dort kann beispielsweise durch Setzen von Drahtbrücken oder über Einstellmöglichkeiten am Gerät ein fester Grenzwert definiert werden. In sicheren Steuerungen können über Bedienoberflächen zur Konfiguration oder Programmierung mehrere Grenzwerte definiert werden. Die Auswahl während des Betriebs kann beispielsweise durch eine sichere E/A-Kopplung, durch eine Auswertung von Sensorsignalen oder durch Vorgabe über einen sicheren Feldbus erfolgen. Die Verwendung von dynamischen Grenzwerten setzt eine leistungsfähige sichere Steuerung bzw. ein sicheres, echtzeitfähiges Bussystem voraus. In Kombination mit einer optischen Schutzfeldüberwachung kann z. B. in Robotikanwendungen die sichere Geschwindigkeit in Abhängigkeit des Abstands der Person zur Gefahrenstelle reduziert werden: Je näher man der Gefahrenstelle kommt, desto langsamer bewegen sich die Motoren.

7.3 Norm EN 61800-5-2

Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit: Der Teil 5-2 der Normenreihe EN 61800 ist eine Produktnorm für elektrische Antriebssysteme mit integrierten Sicherheitsfunktionen. Er legt Anforderungen für die Entwicklung sicherer Antriebe hinsichtlich ihrer funktionalen Sicherheit gemäß der Norm EN 61508 fest. Er gilt für elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl; im Allgemeinen Servo- und Frequenzumrichter, die in den anderen Teilen der Normenreihe EN 61800 behandelt werden.

Der Teil EN 61800-2: Allgemeine Anforderungen, Festlegungen für die Bemessung von Niederspannungs-Wechselstrom-Antriebssystemen mit einstellbarer Frequenz, führt eine Reihe neuer Begriffe ein, die im Folgenden näher erklärt werden:



Definition Leistungsantriebssystem (PDS)

Leistungsantriebssystem/
Power Drive System (PDS)
System, das aus der Starkstrom-Ausrüstung (Stromrichterbaugruppe, Wechselstrommotor, Speisebaugruppe ...) und der Steuer- und Regeleinrichtung besteht. Die Hardware-Konfiguration setzt sich aus einem vollständigen Antriebsmodul (CDM) und einem Motor oder Motoren mit Messfühlern zusammen, die mit der Motorwelle mechanisch gekoppelt sind (die angetriebene Ausrüstung ist nicht eingeschlossen).

PDS/Safety-Related (SR)
Wechselstrom-Leistungsantriebssystem für sicherheitsbezogene Anwendungen

Vollständiges Antriebsmodul/
Complete Drive Module (CDM)
Antriebssystem ohne Motor und die mechanisch mit der Motorwelle verbundenen Messfühler, das aus dem BDM und aus Erweiterungen wie z. B. der Speisebaugruppe und Hilfsausrüstungen besteht, aber nicht darauf beschränkt ist.

Antriebsgrundmodul/Basic Drive Module (BDM)
Antriebsmodul, das aus einer Stromrichterbaugruppe, einer Steuer- und Regeleinrichtung für Drehzahl, Drehmoment, Strom, Frequenz oder Spannung und einem Steuersystem für die Leistungshalbleiterbauelemente usw. besteht.

7.3 Norm EN 61800-5-2

Hersteller und Lieferanten von sicheren Antrieben können durch die Umsetzung der normativen Festlegungen dieses Teils von EN 61800 die Sicherheitsintegrität ihrer Produkte nachweisen. Dies ermöglicht den Einbau eines sicheren Antriebs in ein sicherheitsbezogenes Steuerungssystem unter Anwendung der Grundsätze von EN/IEC 61508 bzw. ihrer Sektornormen (z. B. IEC 61511, IEC 61513, IEC 62061) oder von EN ISO 13849.

Dieser Teil von EN 61800 legt
KEINE Anforderungen fest für:

- *die Gefahren- und Risikoanalyse für eine bestimmte Anwendung*
- *die Angabe von Sicherheitsfunktionen für diese Anwendung*
- *die Zuordnung von SILs zu diesen Sicherheitsfunktionen*
- *das Antriebssystem mit Ausnahme der Schnittstellen*
- *Sekundärgefahren (z. B. durch Ausfälle in einem Produktionsprozess)*
- *elektrische, thermische und energetische Sicherheitsbetrachtungen, die in der EN 61800-5-1 behandelt werden*
- *das Herstellungsverfahren des PDS(SR)*
- *die Gültigkeit von Signalen und Befehlen für das PDS(SR)*

7.4 Sicherheitsfunktionen

7.4.1 Stopp-Funktionen und deren Normenbezug

Stopp-Funktionen sind nahezu an allen Maschinen anzutreffen. Für die verschiedenen funktionalen Anforderungen wurden drei Kategorien von Stopp-Funktionen in der EN 60204-1 definiert:

- Stopp-Kategorie 0
- Stopp-Kategorie 1
- Stopp-Kategorie 2

Die Stopp-Kategorie 0 führt zu einer sofortigen Unterbrechung der krafterzeugenden Energiezufuhr zu den Antriebselementen. Eine Aktivierung der Netz-Trenneinrichtung löst automatisch einen Stopp der Kategorie 0 aus, da keine Energie mehr für die Bewegungserzeugung zur Verfügung steht. Bei der Stopp-Kategorie 1 bleibt die krafterzeugende Energiezufuhr zu den Antriebselementen erhalten, um ein gesteuertes Stillsetzen zu ermöglichen. Wird auch noch im Stoppzustand Energie benötigt, kommt die Stopp-Kategorie 2 zum Einsatz, bei der nach dem gesteuerten Stillsetzen die Energiezufuhr erhalten bleibt. Die Stopp-Kategorien dürfen nicht mit Kategorien nach EN ISO 13849-1 verwechselt werden, die dort eine Kategorisierung von Strukturen mit einem spezifizierten Verhalten im Fehlerfall darstellen. Für den Bereich der drehzahlgeregelten Antriebssysteme wurden in der EN 61800-5-2 den Stopp-Kategorien nach EN 60204-1 Stopp-funktionen zugeordnet.

EN 60204-1	EN 61800-5-2
Stopp-Kategorie 0	Sicher abgeschaltetes Moment (STO)
Stopp-Kategorie 1	Sicherer Stopp 1 (SS1)
Stopp-Kategorie 2	Sicherer Stopp 2 (SS2)

7.4.2 Sicherheitsfunktionen nach EN 61800-5-2

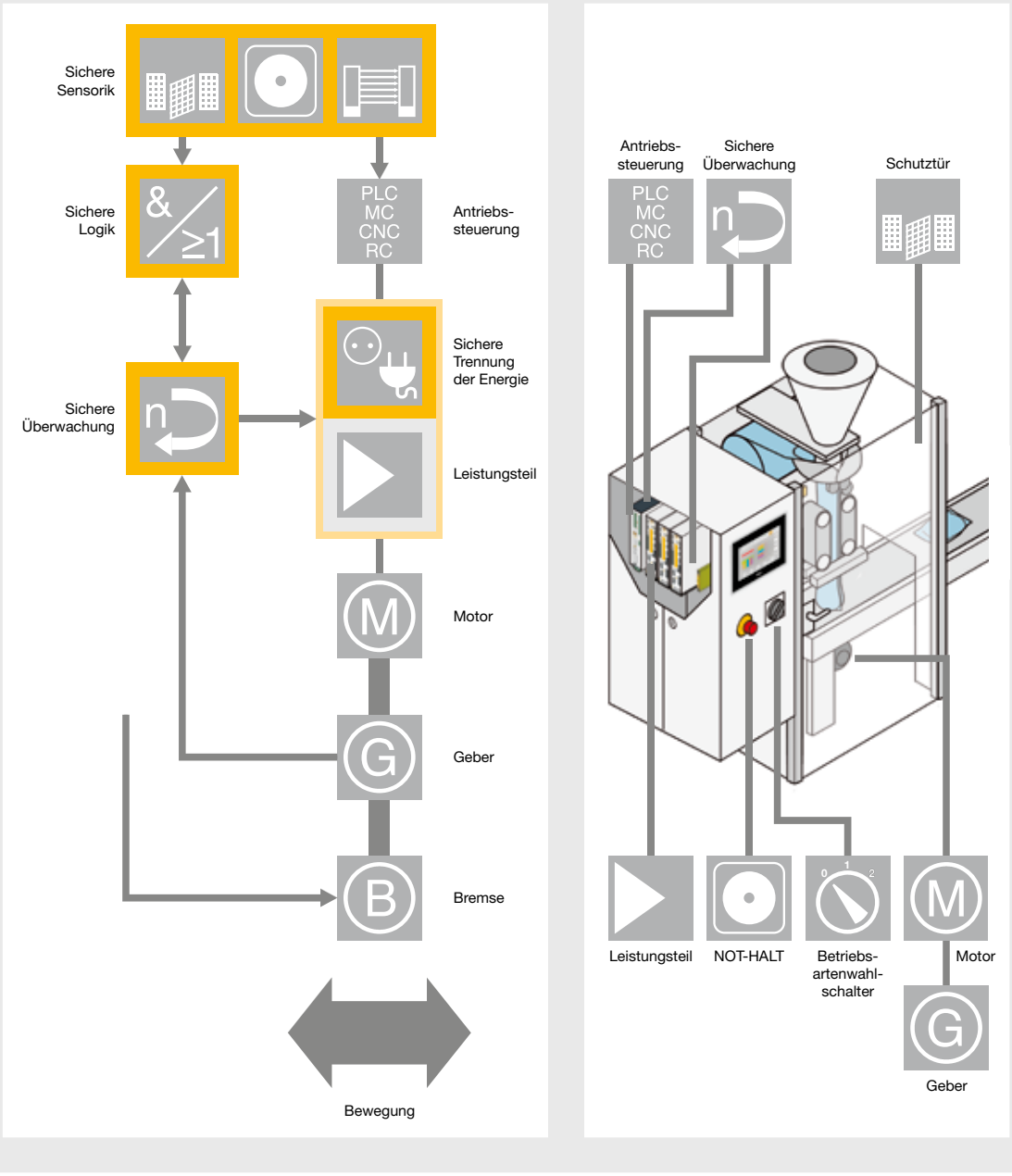
Der Stand der Technik ermöglicht heute eine antriebsintegrierte Lösung der Stopp-Funktionen. Bei dieser Lösung reduziert sich der Platzbedarf im Schaltschrank und auch der Verdrahtungsaufwand, da bisher notwendige externe Zusatzkomponenten wie z. B. Schütze jetzt entfallen können. Auch zusätzliche Komponenten zur Überwachung von Stillstand oder Drehzahl werden nun nicht mehr benötigt. Servoverstärker mit integrierten Sicherheitsfunktionen nach EN 61800-5-2 sind heute verfügbar und führen zu wesentlich einfacheren Lösungen selbst bei komplexen Sicherheitsanforderungen. Die Norm EN 61800-5-2 teilt die Sicherheitsfunktionen in Stoppfunktionen und sonstige Sicherheitsfunktionen ein. Die Beschreibung ist nur rudimentär und lässt sehr viel Freiheit bei der Umsetzung und Interpretation. Dies wird vor allem bei den Stoppfunktionen deutlich, die zu den komplexesten Sicherheitsfunktionen gehören. Nicht nur die Art und Weise der Umsetzung, sondern auch das Verhalten der Sicherheitsfunktionen nach außen kann dabei sehr unterschiedlich sein.

Im praktischen Betrieb der Sicherheitsfunktionen treten häufig Effekte auf, die auf eine schlechte Qualität der Sensorsignale oder allgemein auf das reale Verhalten eines elektrischen Antriebs zurückzuführen sind. Schlecht eingestellte Regelkreise und EMV sind häufige Ursachen für eine eingeschränkte Verfügbarkeit von sicheren Antriebsachsen. Ein Beispiel dafür ist die Definition des Stillstands: In einem geregelten System ist die Geschwindigkeit null mehr ein theoretischer Wert. Je nach Qualität der Regelkreise ist ein Zittern des Motors um die Null-Lage zu beobachten, was bei einem eingestellten Grenzwert von null sofort zu einer Reaktion aufgrund einer Grenzwertverletzung führen würde. Die Sicherheitsfunktion würde den Antrieb sicher abschalten – zu Lasten der Verfügbarkeit des Systems. In diesem Fall hilft die Definition einer Stillstandsschwelle > 0, deren zulässige Geschwindigkeit noch ungefährlich ist. Eine Alternative ist die Definition eines Positionsfensters, das der Motor nicht verlassen darf. Hiermit würden auch kleinste Bewegungen nicht zu einer Grenzwertverletzung führen.

7.4 Sicherheitsfunktionen

Um neben der Sicherheit von Personen auch die Sicherheit des Fertigungs- bzw. Produktionsprozesses zu gewährleisten, können die Sicherheitsfunktionen auch permanent aktiv sein, ohne dass sich die Anlage in einer Sonderbetriebsart befindet. Zur Umsetzung der Sicherheitsfunktionen müssen mehrere Komponenten und deren Schnittstellen sowie für die Berechnung der geforderten Sicherheitsintegrität die gesamte Sicherheitskette betrachtet werden.

Die in der EN 61800-5-2 aufgeführten Sicherheitsfunktionen müssen nicht zwingend mittels antriebsintegrierter Sicherheit umgesetzt werden. Eine externe Lösung ist hier ebenfalls möglich.



Sicherheitskette

7.4 Sicherheitsfunktionen

7.4.2.1 Reaktionsfunktionen

Werden von den Sicherheitsfunktionen Fehler oder Grenzwertverletzungen erkannt, müssen definierte Reaktionsfunktionen eingeleitet werden. In der EN 61800-5-2 wird häufig von der Begrenzung von Geschwindigkeiten oder Positionen gesprochen. Dies wird dadurch erreicht, dass bei einer Verletzung von Grenzwerten ein Stillsetzen des Motors als Reaktionsfunktion ausgelöst wird. Es gibt aber auch Anwendungen, in denen das direkte Abschalten bei einer Grenzwertverletzung nicht gewünscht ist. Bei Mehrachsanwendungen kann es z. B. sinnvoll sein, dass eine Grenzwertverletzung von der Einzelachse nur gemeldet wird und eine übergeordnete Sicherheitssteuerung für das koordinierte Abbremsen des gesamten Achsverbundes sorgt. Externe Überwachungsgeräte können ebenfalls die Grenzwertverletzung nur melden. In Kombination mit einem sicheren Abschaltpfad können dann die Anforderungen der normative Sicherheitsfunktionen erfüllt werden.

7.4.2.2 Sichere Stoppfunktionen

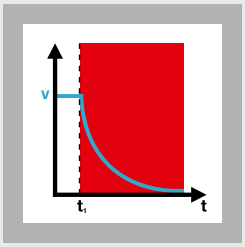
Wenn die Sicherheit an Achsen betrachtet wird, geht es einerseits darum, einen unerwarteten Anlauf von Achsen zu verhindern und andererseits in Bewegung befindliche Achsen im Gefahrenfall sicher abzuschalten. Die zugehörigen Funktionen sind hier unter der Überschrift „Sichere Stoppfunktionen“ zusammengefasst.

Sichere Stoppfunktionen

Sicher abgeschaltetes Moment (STO)

Die krafterzeugende Energiezufuhr zum Motor wird sicher unterbrochen, sodass keine Bewegung mehr entstehen kann. Eine Überwachung des Stillstands muss nicht erfolgen. Ist mit einer Krafteinwirkung von außen zu rechnen, sind zusätzliche Maßnahmen vorzusehen, die eine mögliche Bewegung sicher verhindern (z. B. mechanische Bremsen). Klassische Beispiele sind hierfür Vertikalachsen oder Anwendungen mit großen Massenträgheiten. Diese Sicherheitsfunktion entspricht einem Stopp der Kategorie 0 (ungesteuertes Stillsetzen) nach IEC 60204-1. Wird die Funktion im laufenden Betrieb ausgelöst, „trudelt“ der Motor unkontrolliert aus, was in der Praxis nicht gewünscht ist. Deshalb wird diese Funktion in der Regel als sichere Wiederanlaufsperre oder in Verbindung mit der Sicherheitsfunktion SS1 verwendet.

Mit modernen Servoverstärkern einschließlich integriertem sicherem Abschaltpfad stehen heute sichere Geräte zur Verfügung, die einen unerwarteten Anlauf verhindern und im Gefahrenfall sicher abschalten.



Sicher abgeschaltetes Moment

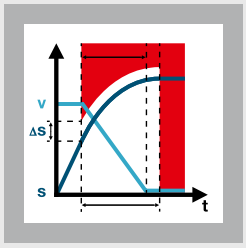
7.4 Sicherheitsfunktionen

Sicherer Stopp 1 (SS1)

Beim Sicheren Stopp 1 (SS1) ist das definierte Abbremsen des Motors Teil der Sicherheitsfunktion. Befindet sich der Motor im Stillstand, so wird die STO-Funktion ausgelöst. Bei der Umsetzung dieser Anforderungen gibt es nun mehrere Möglichkeiten, entscheidend ist hierbei die Verzahnung zwischen Sicherheits- und Antriebstechnik. Diese Sicherheitsfunktion entspricht einem Stopp der Kategorie 1 (gesteuertes Stillsetzen) nach IEC 60204-1.

Umsetzung	Beschreibung
überwachte Zeitverzögerung	Das Auslösen der Sicherheitsfunktion startet eine anwendungsspezifische sichere Zeitverzögerung, nach der der Motor sicher von der Energie getrennt wird. Das Abbremsen des Motors ist eine Funktion der nicht sicheren Antriebstechnik. Beschleunigt der Motor während dieser Zeitverzögerung, wird dies nicht erkannt.
automatische Stillstandserkennung mit überwachter Zeitverzögerung	Die überwachte Zeitverzögerung wird mit einer Stillstandserkennung kombiniert. Ist der Motor vor Ablauf der Zeitverzögerung im Stillstand, so wird dadurch die STO-Funktion ausgelöst. Auch hier wird ein Beschleunigen des Motors während der Zeitverzögerung nicht erkannt.
Überwachung der Bremsrampe	Eine überwachte Bremsrampe hat die höchste Qualität bezüglich der funktionalen Sicherheit. Während des Bremsvorgangs findet ein kontinuierlicher Vergleich mit einem Grenzwert oder einem zulässigen Schleppfehler statt. Wird der Grenzwert verletzt, wird die STO-Funktion ausgelöst.

In vielen Applikationen können Antriebe nicht einfach abgeschaltet werden, da diese dann austrudeln würden, was zu Gefährdungen führen kann. Oft dauert ein derartiger ungesteuerter Auslauf auch wesentlich länger als das geregelte Abbremsen einer Achse. Die Funktion Sicherer Stopp 1 (SS1) überwacht direkt im Servoverstärker das geregelte Abbremsen der Achse. Nach Ablauf der parametrierten Abbremsrampe wird der Antrieb sicher abgeschaltet. Im Vergleich zu externen Überwachungslösungen reduzieren sich die Reaktionszeiten, wodurch in vielen Fällen die Sicherheitsabstände zu den Gefahrenstellen reduziert werden können. Daraus ergeben sich Vorteile wie z. B. verbesserte Ergonomie für die Anlagenbediener, Platzersparnis durch geringere Abstände von Schutzgittern zu den Gefahrstellen und nicht zuletzt Kosteneinsparungen.



Sicherer Stopp 1

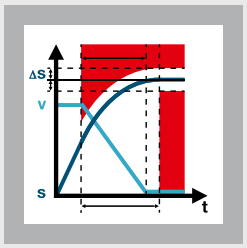
7.4 Sicherheitsfunktionen

Sicherer Stopp 2 (SS2)

Beim Sicheren Stopp 2 (SS2) ist das definierte Abbremsen des Motors ebenfalls Teil der Sicherheitsfunktion. Befindet sich der Motor im Stillstand, so wird der Sichere Betriebshalt (SOS) ausgelöst. Anders als beim Sicheren Stopp 1 (SS1) befindet sich der Motor im Stillstand im geregelten Betrieb. Das bedeutet, dass die Stillstandsposition durch den aktiven Regelkreis exakt gehalten wird. In der Umsetzung dieser Anforderungen gibt es wiederum mehrere Möglichkeiten. Diese Sicherheitsfunktion entspricht einem Stopp der Kategorie 2 (gesteuertes Stillsetzen) nach IEC 60204-1.

Umsetzung	Beschreibung
überwachte Zeitverzögerung	Das Auslösen der Sicherheitsfunktion startet eine anwendungsspezifische sichere Zeitverzögerung, nach der der sichere Betriebshalt ausgelöst wird. Das Abbremsen des Motors ist eine Funktion der nicht sicheren Antriebstechnik. Beschleunigt der Motor während dieser Zeitverzögerung, wird dies nicht erkannt.
automatische Stillstandserkennung mit überwachter Zeitverzögerung	Die überwachte Zeitverzögerung wird mit einer Stillstandserkennung kombiniert. Ist der Motor vor Ablauf der Zeitverzögerung im Stillstand, so wird dadurch der sichere Betriebshalt ausgelöst. Auch hier wird ein Beschleunigen des Motors während der Zeitverzögerung nicht erkannt.
Überwachung der Bremsrampe	Eine überwachte Bremsrampe hat die höchste Qualität bezüglich der funktionalen Sicherheit. Während des Bremsvorgangs findet ein kontinuierlicher Vergleich mit einem Grenzwert oder einem zulässigen Schleppfehler statt. Wird der Grenzwert verletzt, wird die STO-Funktion ausgelöst, andernfalls folgt der sichere Betriebshalt.

Welcher Nutzen ergibt sich nun aus der Funktion Sicherer Stopp 2 (SS2)? Wenn die Achsen im Stillstand nicht mehr abgeschaltet werden müssen, halten diese aktiv ihre aktuelle Position, wodurch die Synchronisation zwischen Achsen und Prozess nicht mehr verloren geht. Damit ist ein sofortiger Neustart der Achsen jederzeit möglich, wodurch die Anlagenverfügbarkeit spürbar steigt. Auch hier führt die antriebsintegrierte Funktion zu reduzierten Reaktionszeiten und damit zu einer Minimierung von Risiken. Die Ansprechzeiten von Überwachungsfunktionen gehen direkt in die im Fehlerfall möglichen Wege ein, bis eine Sicherheitsabschaltung erfolgt. Da die Reaktionszeiten in die Berechnung von Sicherheitsabständen Eingang finden, gelten auch hier die schon bei der Funktion Sicherer Stopp 1 genannten Vorteile.



Sicherer Stopp 2

7.4 Sicherheitsfunktionen

7.4.2.3 Sichere Bewegungsfunktionen

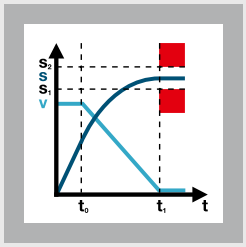
Moderne Antriebslösungen betrachten nicht nur das Ein- und Abschalten von Achsen, sondern auch die potenziellen Risiken, die beim Betrieb der Achsen auftreten können. Die Funktionen zur Vermeidung bzw. Reduzierung dieser Risiken werden hier unter der Überschrift „Sichere Bewegungsfunktionen“ zusammengefasst.

Sichere Bewegungsfunktionen

Sicherer Betriebshalt (SOS)

Der Sichere Betriebshalt (SOS) wurde schon mit der Sicherheitsfunktion Sicherer Stopp 2 (SS2) vorgestellt. Er überwacht die Stillstandsposition, während sich der Motor im geregelten Zustand befindet. Nach dem Aufheben der Sicherheitsfunktion kann der Fertigungs- oder Bearbeitungsprozess ohne Genauigkeitsverlust fortgesetzt werden. In aller Regel wird die Funktion in Kombination mit einem Stopp als Sicherer Stopp 2 (SS2) angewendet, da eine Stillstandsüberwachung meist mit einem Bremsvorgang einhergeht. Wie oben beschrieben, kann der Grenzwert sowohl als Geschwindigkeitsschwelle als auch als Positionsfenster vorgegeben werden.

Die Anwendung der Funktion Sicherer Betriebshalt (SOS) ist in der Regel für die Stillstandsphasen eines Prozesses vorgesehen. Eine typische Situation ist der Zugang zu einer Gefahrstelle bei einem Prozesseingriff. Ein Bediener stoppt die Produktion z. B. durch ein Kommando „Halt bei Takt Ende“. Wenn die Anlage steht, wird zuerst die Funktion Sicherer Betriebshalt (SOS) aktiviert und danach die Zuhalteeinrichtung an der Zugangstür entriegelt. Jetzt ist ein gefahrloser Zugang zur Anlage möglich.



Sicherer Betriebshalt

Sicher begrenzte Beschleunigung (SLA) und Sicherer Beschleunigungsbereich (SAR)

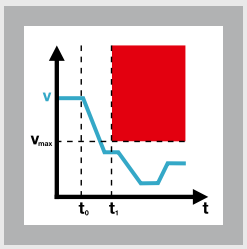
Sicherheitsfunktionen bezüglich der Überwachung von Beschleunigungen haben nach dem aktuellen Stand kaum Verbreitung. Die Erfassung von Beschleunigungen erfolgt in der Servoantriebstechnik mit Ferraris-Sensoren ausschließlich in speziellen Applikationen von Werkzeug- oder Druckmaschinen. Standardantriebe können diese Signale in ihren Regelkreisen nicht verarbeiten, eine Überwachung dieser Beschleunigungssignale ist in der Praxis sehr aufwendig. Eine andere Möglichkeit besteht darin, sichere Geschwindigkeits- bzw. Positionsänderungen nach der Zeit zu differenzieren und die daraus berechneten Augenblickbeschleunigungen mit Grenzwerten zu vergleichen. Bei stationären Brems- bzw. Beschleunigungsrampen werden solche Verfahren erfolgreich eingesetzt. Bei weniger stabilen Bewegungsverläufen führen bereits kleine Geschwindigkeitsschwankungen durch die zeitliche Ableitung zu hohen Beschleunigungswerten und damit zur Abschaltung des Antriebs.

7.4 Sicherheitsfunktionen

Sicher begrenzte Geschwindigkeit (SLS)

Die Sicher begrenzte Geschwindigkeit (SLS) ist wohl die bekannteste Sicherheitsfunktion. In der Praxis wird diese Sicherheitsfunktion häufig als sicher reduzierte Geschwindigkeit angewendet. Daher muss ein definierter Übergang von der Betriebsgeschwindigkeit im Automatikbetrieb auf die reduzierte Geschwindigkeit im Einrichtbetrieb gewährleistet sein. Erkennt die Überwachungsfunktion eine Verletzung des Grenzwerts, muss der Antrieb sicher abgeschaltet werden. Die Art und Weise des Abschaltens hängt von der Anwendung ab, es ist ein definiertes Abbremsen mittels der SS1-Funktion mit anschließender Trennung der krafterzeugenden Energie anzustreben.

Ohne antriebsintegrierte Sicherheitsfunktionen war die Realisierung dieser Funktion mit großem Materialaufwand bzw. Funktionseinschränkungen verbunden. Werden Achsen beim Einrichten im Tippbetrieb verfahren, ist die mögliche Geschwindigkeit der Achse im Fehlerfalle ein wesentlicher Aspekt jeder Risikoanalyse. Die Bediener müssen vor der Gefahr geschützt werden, die im Fehlerfall zu einem unkontrollierten Anlaufen einer Achse führt. Wenn die Funktion Sicher begrenzte Geschwindigkeit (SLS) für diese Tippfunktionen verwendet wird, kommt eine Lösung zum Einsatz, die im Fehlerfall die kürzestmögliche Reaktionszeit ergibt. Dies reduziert die Risiken für einen Bediener signifikant, da bereits im Ansatz ein unkontrolliertes Anlaufen einer Achse erkannt würde und ein sicheres Abschalten zur Folge hätte.

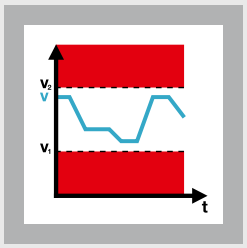


Sicher begrenzte Geschwindigkeit

Sicherer Geschwindigkeitsbereich (SSR)

Der Sichere Geschwindigkeitsbereich (SSR) kann beispielsweise dafür genutzt werden, eine sichere Minimalgeschwindigkeit zu überwachen. Die Reaktion bezüglich einer Unterschreitung des Grenzwertes hängt wiederum stark von der Applikation ab. Ein Abschalten des Antriebs muss bei eventuell gekoppelten Antriebsachsen zu geeigneten Reaktionen führen (z. B. Gruppenabschaltung).

Generell kann der Sichere Geschwindigkeitsbereich (SSR) zur permanenten Prozessüberwachung genutzt werden. Nicht in allen Fällen sind die Risiken allein durch eine Begrenzung von abrupt zunehmenden Geschwindigkeiten beseitigt. Auch aufgrund eines Fehlers sich plötzlich reduzierende Geschwindigkeiten können eine Gefahr bedeuten. Arbeiten Achsen in einem definierten Abstand zueinander, kann eine abrupt fallende Geschwindigkeit an lediglich einer der beiden Achsen zu einer Quetschgefahr führen. Für diese Fälle wurde die Funktion Sicherer Geschwindigkeitsbereich (SSR) definiert und entwickelt. Mittels dieser Funktion würden die beteiligten Achsen abgeschaltet, eine Gefährdung des Maschinenbedieners ist damit ausgeschlossen.



Sicherer Geschwindigkeitsbereich

7.4 Sicherheitsfunktionen

Sicher begrenztes Moment (SLT) und Sicherer Momentenbereich (STR)

Eine Momenten- oder Kraftüberwachung hat, ähnlich wie bei der Überwachung der Beschleunigung, das Problem einer geeigneten bzw. etablierten Sensorik. Drehmoment-Messsysteme sind bei Standardantrieben nicht verbreitet, allerdings bietet die Servoantriebstechnik die Möglichkeit der indirekten Messung über den Motorstrom. Der Motorstrom ist proportional zur Kraft oder zum Drehmoment des Motors, die Gefährdung durch eine Gefahr bringende Bewegung wird damit begrenzt. Ungefährliche Werte hinsichtlich der Einwirkung von Kräften sind in der Grenzwertliste 2015 im BIA-Report enthalten.

Sicher begrenzte Position (SLP)

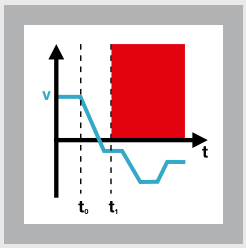
Durch eine sichere Positionsüberwachung wird erreicht, dass der Motor einen vorgegebenen Positionsgrenzwert nicht überschreitet. Bei einer Grenzwertverletzung wird der Motor mit einem sicheren Stopp heruntergebremst. Dabei muss der technisch mögliche Nachlaufweg berücksichtigt werden. Unterhalb des Grenzwerts gibt es keine Einschränkungen bezüglich der Beschleunigung oder Geschwindigkeit des Motors. Für diese Sicherheitsfunktion wird eine absolute Positionserfassung benötigt. Entweder kommen Absolutwertgeber zum Einsatz oder relative Messsysteme werden mit einer sicheren Referenzfahrt kombiniert.

Sicher begrenztes Schrittmaß (SLI)

Nach einem Startbefehl darf der Motor eine zulässige Weglänge abfahren. Nach Erreichen des Grenzwerts muss eine sichere Stoppfunktion ausgelöst werden. Ein Überschreiten der zulässigen Weglänge muss erkannt und der Antrieb sicher stillgesetzt werden. Für diese Sicherheitsfunktion sind relativ messende Gebersysteme ausreichend.

Sichere Bewegungsrichtung (SDI)

Es wird verhindert, dass sich der Motor in die unzulässige Richtung bewegt. Diese Sicherheitsfunktion tritt häufig in Kombination mit der Sicher begrenzten Geschwindigkeit (SLS) im Einrichtbetrieb auf. Durch die antriebsintegrierte Lösung wird auch hier die schnellstmögliche Abschaltung erreicht.



Sichere Bewegungsrichtung

Sicherer Nocken (SCA)

Ein sicheres Ausgangssignal zeigt an, ob sich die Position des Motors innerhalb eines festgelegten Bereichs befindet. Diese Bereiche sind absolute Positionsfenster innerhalb einer Motorumdrehung. Basisfunktion hierfür ist also eine sichere Überwachung von Absolutpositionen, weshalb passende Sensorsysteme eingesetzt werden müssen.

Sichere Geschwindigkeitsüberwachung (SSM)

Die Sicherheitsfunktion Sichere Geschwindigkeitsüberwachung (SSM) ist sehr eng mit der Sicher begrenzten Geschwindigkeit (SLS) verwandt. Allerdings erfolgt bei einer Grenzwertverletzung keine Reaktionsfunktion der überwachenden Komponente, sondern lediglich eine sichere Meldung, die von einer übergeordneten sicheren Steuerung ausgewertet und weiterverarbeitet werden kann. Zum einen kann die Steuerung komplexere Reaktionsfunktionen ausführen, zum anderen kann diese Sicherheitsfunktion zur Prozessüberwachung eingesetzt werden.

7.4 Sicherheitsfunktionen

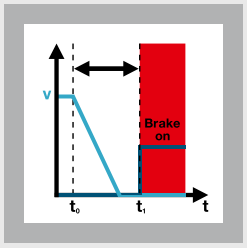
7.4.2.4 Sichere Bremsfunktionen

Funktionen im Zusammenhang mit Halte- und Betriebsbremsen wurden unter dem Begriff sichere Bremsfunktionen zusammengefasst.

Sichere Bremsfunktionen

Sichere Bremsenansteuerung (SBC)

Die Sichere Bremsenansteuerung (SBC) liefert ein sicheres Ausgangssignal zur Ansteuerung einer externen mechanischen Bremse. Bei den verwendeten Bremsen muss es sich um sogenannte Sicherheitsbremsen handeln, bei denen ein Ruhestrom gegen eine Federkraft arbeitet. Wird der Stromfluss unterbrochen, fällt die Bremse ein. Ansteuermodule enthalten häufig eine Leistungsabsenkung bei gelüfteter Bremse, um den Energieverbrauch bzw. die Erwärmung der Bremse zu reduzieren. Je nach Risikoanalyse wird ein sicherer Bremsentest benötigt, der Fehler während des Betriebs aufdeckt. An Achsen mit hängenden Lasten kommen oft Halte- oder Betriebsbremsen zum Einsatz. Neben der Bremse ist auch die Ansteuerung der Bremse ein wichtiger Bestandteil der Sicherheitsfunktion. Die Funktion Sichere Bremsenansteuerung (SBC) wird in der Regel zusammen mit der Sicherheitsfunktion STO ausgelöst. Die Sichere Bremsenansteuerung beeinflusst das gesamte Bremsenmanagement der Antriebsachse und sollte mit den rein funktionalen Anforderungen abgestimmt sein.

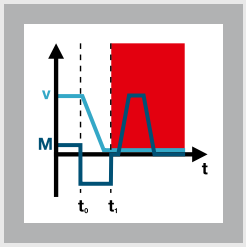


Sichere Bremsenansteuerung

Sicherer Bremsentest (SBT)

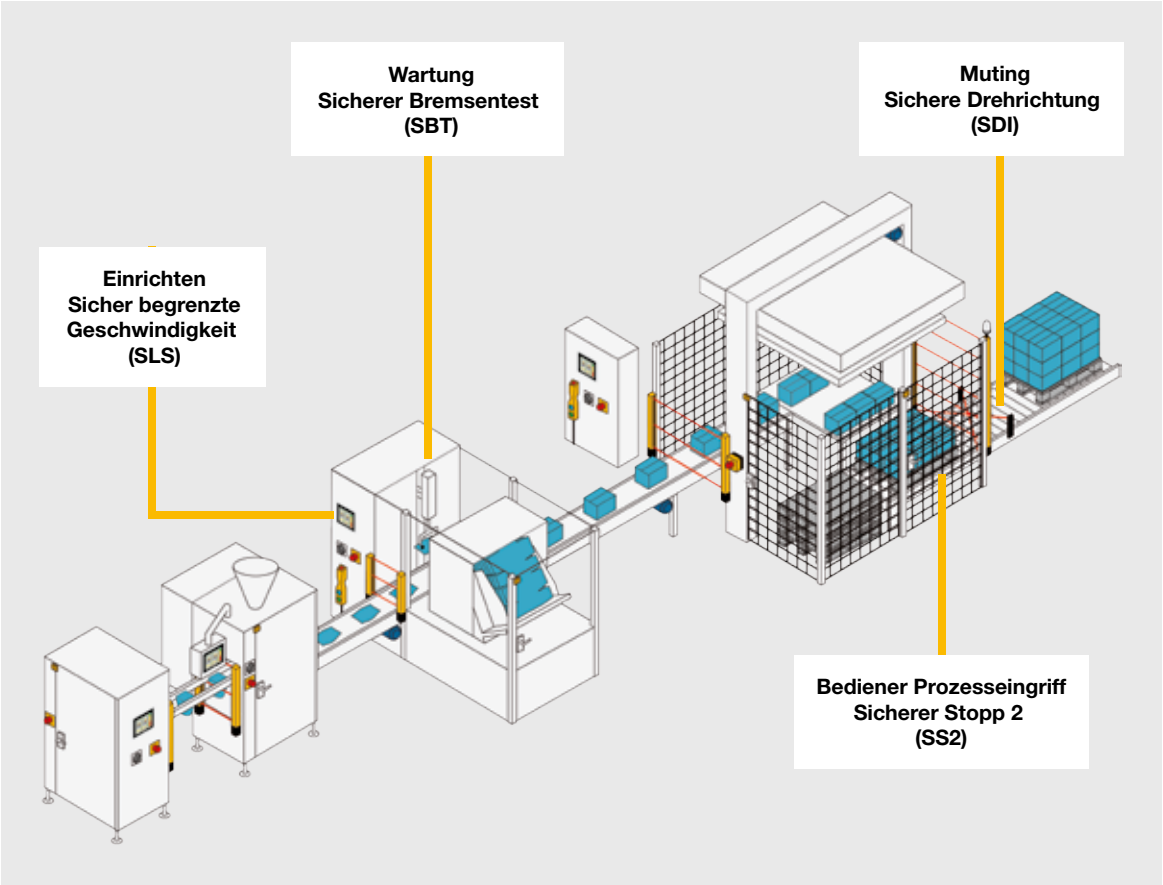
Häufig kommen mechanische Bremsen als Standardbauteile in Sicherheitsfunktionen zum Einsatz. In diesem Fall muss der Anwender eine sicherheitstechnische Betrachtung durchführen und den Nachweis erbringen, dass die Bremsen alle auf eine übergeordnete Sicherheitsfunktion bezogenen Anforderungen erfüllen.

Ein wesentlicher Zuwachs an Sicherheit entsteht durch Nutzung der Funktion Sicherer Bremsentest (SBT). Allein eine sichere Ansteuerung einer Haltebremse reicht oft nicht aus, um eine Vertikalachse sicher zu machen. Wird der verschleißbehaftete mechanische Anteil der Bremse nicht regelmäßig gewartet, kann im Gefahrenfall nicht garantiert werden, dass die Haltebremse die vorgesehene Bremswirkung entfaltet. Die Funktion Sicherer Bremsentest (SBT) ersetzt bisher allein durch organisatorische und manuelle Arbeiten durchzuführende Maßnahmen durch einen automatischen Test, der bei negativem Ergebnis ein Stillsetzen der Anlage und Signalisierung des Fehlers ermöglicht. Dies führt zu einer wesentlichen Reduzierung des Instandhaltungsaufwands.



Sicherer Bremsentest

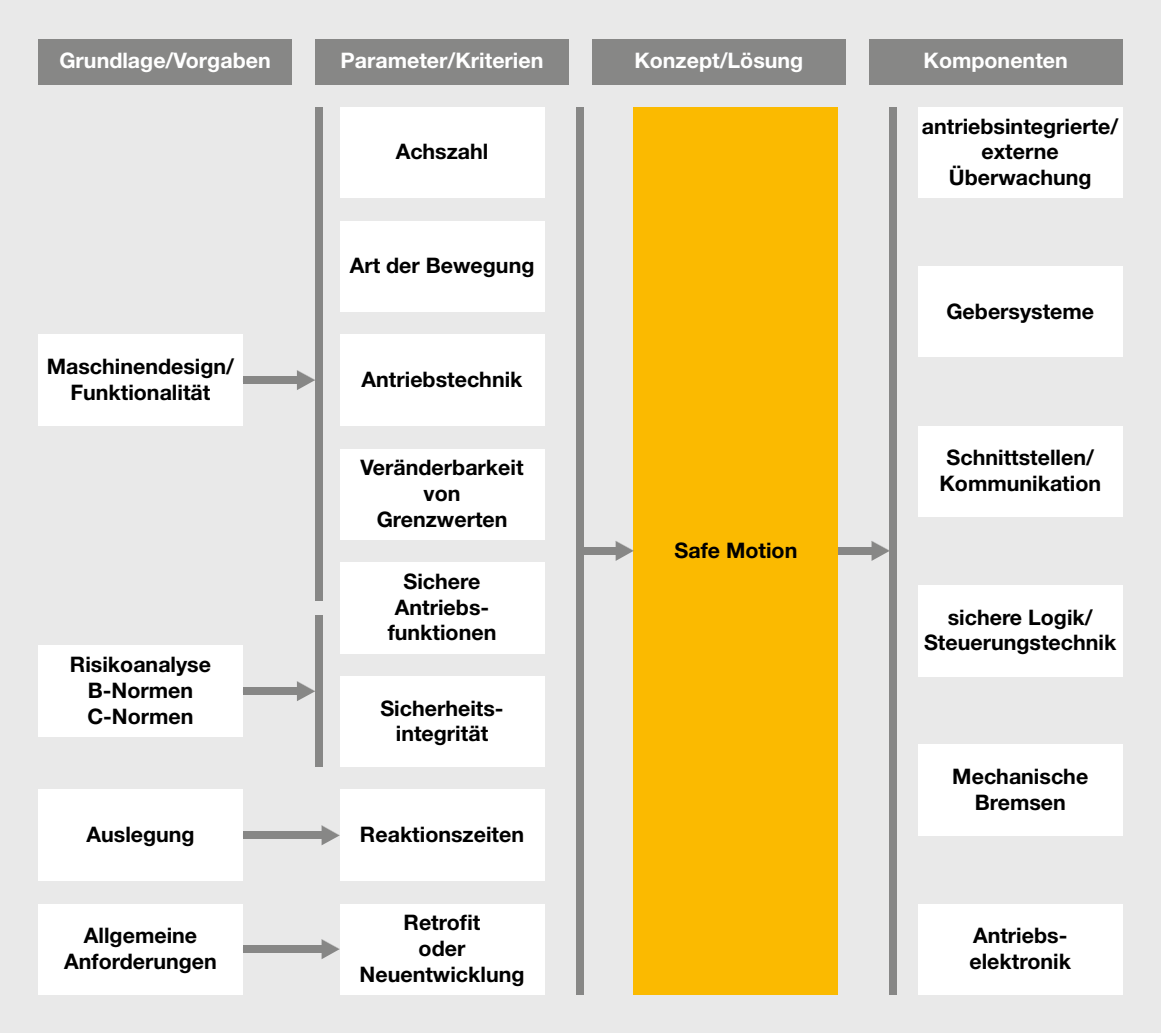
7.4 Sicherheitsfunktionen



Sicherheitsfunktionen am Beispiel einer Verpackungsmaschine

7.5 Systembetrachtung

Bei der sicheren Antriebstechnik verschmelzen zwei Themengebiete miteinander, die einzeln betrachtet schon einen hohen Komplexitätsgrad aufweisen. Die Herausforderung besteht darin, eine für den Anwender transparente und nachvollziehbare Logik im Lebenszyklus einer Safe Motion-Anwendung bereitzustellen. Die Schwierigkeit bei der Projektierung bzw. Auswahl von sicheren Antriebskomponenten ist, die unterschiedlichen Einflussfaktoren auf Anforderungen an die Produkte zu übertragen. Oder anders formuliert: Aus welchen Vorgaben lassen sich welche Parameter ableiten, um Produkte für eine optimale sichere Antriebslösung auszuwählen?



Vorgehensweise für die Auslegung und Auswahl einer sicheren Antriebslösung

7.5 Systembetrachtung

Das Maschinendesign bzw. die vom Endkunden geforderte Funktionalität bestimmt im Wesentlichen die verwendete Antriebstechnik sowie die Art und Weise, wie die Maschine steuerungstechnisch betrieben wird. Daraus abgeleitete Parameter sind:

- Wie viele Antriebsachsen?
- Werden Servoverstärker oder Frequenzumrichter eingesetzt?
- Sind die Antriebe dezentral – also außerhalb des Schaltschranks – platziert?
- Welche sicheren Antriebsfunktionen werden benötigt, wie sollen diese parametriert werden?
- Handelt es sich bei der zu überwachenden Bewegung um eine Bahnkurve, synchrone Antriebsachsen oder im einfachsten Fall um eine Einzelbewegung?

Die normativen Vorgaben aus B- und C-Normen bzw. die Risikoanalysen ergeben die Anforderung bezüglich der Sicherheitsintegrität (SIL und PL). Diese haben natürlich auch Einfluss auf die benötigten Sicherheitsfunktionen. Die Reaktionszeiten der sicheren Antriebskomponenten sind Teil der Gesamtauslegung der Maschine und müssen in einem iterativen Prozess abgestimmt werden. Hier spielen z. B. Nachlaufwege, Sicherheitsabstände, Trägheiten der bewegten Massen oder das Reaktionsvermögen der Maschinensteuerung eine entscheidende Rolle.

Allgemeine Anforderungen können z. B. sein, ob die Maschine mit sicheren Antriebsfunktionen nachgerüstet werden soll. Dann müssen unter Umständen bestehende Komponenten weiterhin Verwendung finden, was häufig für eine externe Sicherheitslösung spricht. Diese Kriterien und Parameter müssen zu einem Konzept verarbeitet werden. Das Ergebnis ist eine sichere Antriebslösung, die aus marktüblichen Komponenten besteht.

7.5.1 Antriebselektronik

Moderne Frequenzumrichter oder Servoverstärker verfügen heute über einen integrierten sicheren Abschaltpfad, über den die Sicherheitsfunktion STO ausgeführt werden kann. Dieser Abschaltpfad ist in der Regel über ein Klemmenpaar von außen zugänglich und muss an 24 V DC angeschlossen sein. Wird die Sicherheitsfunktion nicht verwendet, liegen an den Klemmen dauerhaft 24 V DC an. Wird der Abschaltpfad als STO oder als sichere Wiederanlaufsperre verwendet, müssen die Klemmen mit einem sicheren Ausgang einer Sicherheitssteuerung oder einem Sicherheitsschaltgerät verbunden werden. Hierbei ist darauf zu achten, dass der Testtakt des sicheren Ausgangs nicht zum Auslösen der Sicherheitsfunktion führt. Als Gegenmaßnahme verwendet man einen Eingangsfilter mit entsprechender Verzögerungszeit. Je nach Ausführung steht ein Rücklesepfad zur Fehlererkennung zur Verfügung, um eine höhere Sicherheitsintegrität zu erreichen.

Die Vorteile der antriebsintegrierten Abschaltung liegen hauptsächlich

- im geringeren Verdrahtungsaufwand,
- dem schnellen Wiederanlauf, da der Zwischenkreis geladen bleibt,
- der kurzen Reaktionszeit (gemessen von der fallenden Flanke am Eingang bis zur Abschaltung der Optokoppler liegt die Reaktionszeit im Bereich weniger Millisekunden).

7.5 Systembetrachtung

7.5.2 Motor

Die relevanten Eigenschaften von Motoren bezüglich ihrer Verwendung in sicherheitsbezogenen Systemen sind

- die Bewegungsart (rotierend, linear),
- Beschleunigungsvermögen (massenträger Asynchronmotor oder luftgelagerter Linearantrieb),
- integrierter Motorgeber,
- integrierte Haltebremse, die ins Sicherheitskonzept einbezogen ist.

Das Beschleunigungsvermögen des Motors hat Einfluss auf die maximal zulässige Gesamtreaktionszeit des Systems. Hochdynamische Linearmotoren verfügen über extrem kleine elektrische Zeitkonstanten der Wicklung und eine hohe Überlastfähigkeit, sodass in wenigen Millisekunden ein Vielfaches der Nennkraft anliegt. Resolver sind als Motorgeber in der Servoantriebstechnik weit verbreitet. Sie werden in rotierenden Motoren eingesetzt, sind robust und kostengünstig. Das Messsystem liefert eine absolute Position innerhalb einer Motorumdrehung, ist aber aufgrund des Funktionsprinzips in der Auflösung beschränkt. Resolversignale können von sicheren Überwachungskomponenten nur selten ausgewertet werden. Deshalb sind bei sicherheitsbezogenen Anwendungen mit Bewegungsüberwachung Motorgebersysteme mit Sinus/Cosinus-Analogspuren vorzuziehen. Motorgebersysteme mit volldigitaler Schnittstelle können nur mit speziellen, herstellerspezifischen Sicherheitskomponenten überwacht werden. Fremdprodukte können nicht angeschlossen werden.

7.5.3 Sichere Logik

Sicherheitsschaltgeräte oder Sicherheitssteuerungen können in Systemen mit sicheren Antriebsfunktionen je nach Anwendung folgende Aufgaben übernehmen:

- Auswertung von Sensoren von Schutzeinrichtungen
- Aktivieren von Sicherheitsfunktionen,
- Abschalten der Antriebe
- Auswerten der Zustände von sicher überwachten Antriebsachsen in einem Mehrachssystem
- Herstellen der Gesamtsicherheit der Anlage
- Vorgabe von neuen Grenzwerten während des Betriebs
- Schnittstelle zwischen der Antriebssteuerung und den Sicherheitsfunktionen

Die sichere Logik kann entweder als eigenständige externe oder als antriebsintegrierte Komponente realisiert sein. Sie ist die Schnittstelle zwischen Sensoren von Schutzeinrichtungen und der sicheren Überwachungseinheit. Mit antriebsintegrierten Lösungen sind einfache Funktionen in Einzelachsensystemen kostengünstig möglich. Sensoren werden direkt am Antrieb angeschlossen und ausgewertet. Durch die begrenzte Anzahl an sicheren Schnittstellen sind eine Querkommunikation zwischen den Antrieben sowie komplexe Verknüpfungen nicht möglich. Die Zykluszeit der Sicherheitssteuerung muss immer dann in die Betrachtung der Gesamtreaktionszeit einfließen, wenn zur Aktivierung einer Sicherheitsfunktion zuvor eine Vorverarbeitung in einer sicheren Logik erforderlich ist. Sie bewegt sich, je nach Größe des Anwenderprogramms, im Bereich 50 bis 200 ms und ist somit dominant gegenüber der Verzögerung im Abschaltpfad. Zusätzlich muss eine Verzögerungszeit bei sicheren digitalen Eingängen berücksichtigt werden, die aufgrund von Eingangsfiltern entsteht.

7.5 Systembetrachtung

7.5.4 Sichere Bremse

Greifen an den Abtriebswellen von Motoren oder Getrieben Kräfte an, die bei abgeschaltetem Motor eine Bewegung zur Folge hätten, müssen mechanische Bremsen eingesetzt werden. Beispielhafte Anwendungen sind Vertikalachsen oder Motoren mit großen Massenträgheiten. Der Betrieb von Vertikalachsen stellt im Sinne der Sicherheitstechnik eine besondere Situation dar. Das sonst in der Sicherheitstechnik angewendete Fail-safe-Prinzip – das Abschalten der Antriebsenergie im Fehlerfall – führt zu keinem sicheren Zustand, da herunterfallende Lasten eine Gefährdung zur Folge haben. Als Maßnahme werden mechanische Bremsen eingebaut, die ihre Funktionsfähigkeit in speziellen Wiederholungsprüfungen ständig nachweisen müssen. Ähnlich wie bei den Gebersystemen gibt es bezüglich der Sicherheitsanforderungen verschiedene Ausführungen. Die Zweikanaligkeit kann entweder durch zwei eigenständige Bremsen oder durch eine Bremse mit zwei getrennten Bremskreisen erfolgen. Zwei separate Bremsen haben den Vorteil, dass sie Fehler innerhalb von mechanischen Übertragungselementen zwischen Antrieb und Prozess abdecken können. Bei der Auslegung von Bremsen kommt es sehr auf das Design der Maschine und das gesamte Sicherheitskonzept an.

7.5.5 Bewegungsüberwachung

Die Bewegungsüberwachung hat zwei Hauptaufgaben: Zum einen muss sie eine Verletzung von Grenzwerten erkennen und daraufhin eine geeignete Reaktionsfunktion auslösen. Zum anderen muss sie mögliche Fehler des Gebersystems erkennen, um dann ebenfalls eine geeignete Fehlerreaktionsfunktion auszulösen. Beide Funktionen hängen sehr stark mit der Verfügbarkeit des Antriebssystems zusammen. Verrauschte Signale oder schlecht eingestellte Regelkreise können dazu führen, dass sensibel ausgelegte Überwachungsmechanismen Reaktionsfunktionen auslösen und damit die Verfügbarkeit der Anlage herabsetzen. Eine ordnungsgemäße Schirmung der Motor- und Geberleitungen ist dabei zwingend erforderlich. Über Hysterese- oder Filtereinstellungen können die Algorithmen der Überwachungsfunktionen appliziert werden. Die Reaktionszeiten dieser Komponente liegen im Bereich weniger Millisekunden. Die Bewegungsüberwachung ist sowohl als externe als auch als antriebsintegrierte Lösung verfügbar. Die integrierte Lösung hat bezüglich Verdrahtungsaufwand und Komfort deutliche Vorteile gegenüber einem externen Gerät. Nachteile sind die höheren Aufwendungen bei der Nachrüstung bei bestehenden Anlagen und die Abhängigkeit vom verwendeten Umrichter. Das bedeutet, dass sowohl die antriebstechnischen Eigenschaften als auch die Schnittstellen und die Leistungsfähigkeit der Sicherheitsfunktionen zur Applikation passen müssen. Mit einer externen Überwachungseinheit können Sicherheitsfunktionen bei Frequenz- wie auch bei Servoumrichtern verschiedener Leistungsklassen und Hersteller einheitlich umgesetzt werden.

7.5 Systembetrachtung

7.5.6 Bewegungssteuerung

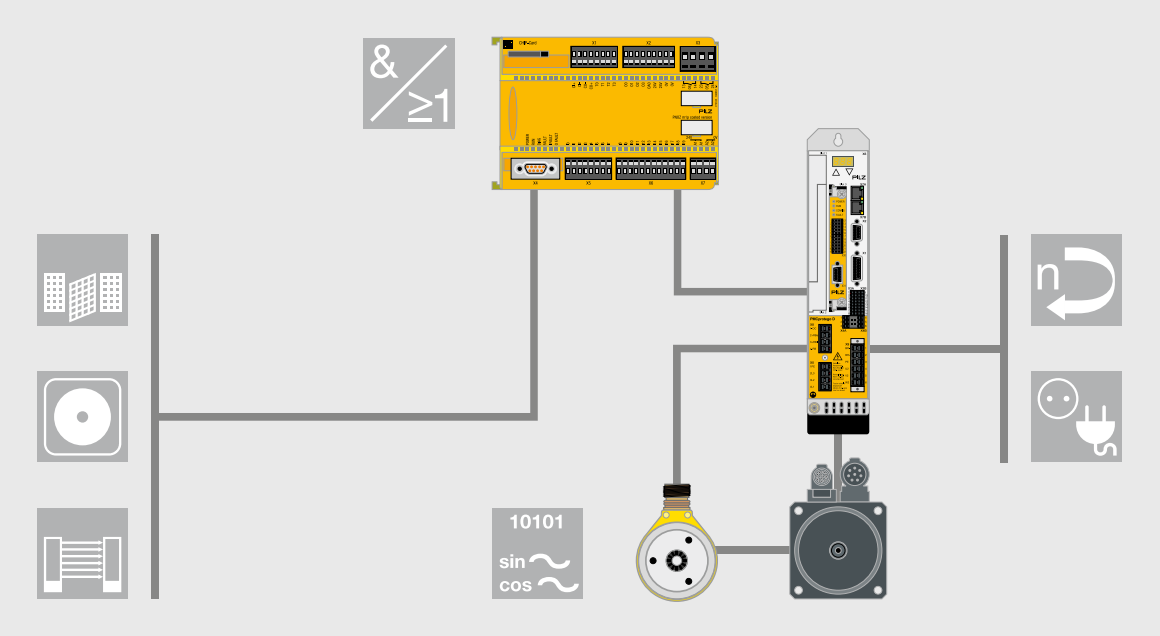
Die Bewegungssteuerung ist nach heutigem Stand eine nicht sichere Antriebskomponente. Je nach Aufgabenstellung sind die Funktionen antriebsintegriert oder werden von einer externen Steuerung mittels Feld- oder Antriebsbus ausgeführt. Die klassische Einteilung der Steuerungen erfolgt gemäß der geforderten Bewegung.

Bewegung	Steuerung	Sichere Bewegungsüberwachung
Positionierung einer Einzelachse	Positioniersteuerung	Überwachung der Einzelachse antriebsintegriert oder extern
elektronische Kurvenscheibe (synchrone Bewegungen)	Motion Control Steuerung	Grenzwert und Überwachung müssen je Antriebsachse betrachtet werden. Zustände der einzelnen Achsen werden in einer zentralen sicheren Logik ausgewertet.
Bahnkurve (resultierende Bewegung)	NC oder RC Steuerung	sichere zentrale Berechnung der aktuellen Position aus den Positionen der Einzelachsen

7.5.7 Realisierungsbeispiele

Servoumrichter mit antriebsintegrierter Bewegungsüberwachung und sicherer Pulssperre für die Abschaltung

Die Auswertung von Sensoren übernimmt beispielsweise eine sichere Kleinsteuerung, die über eine sichere E/A-Kopplung die Sicherheitsfunktionen im Antrieb aktiviert. Zur Motorführung und Positionierung hat der Servomotor einen Sinus-/Cosinus-Motorgeber integriert. Die Reaktionszeit bis zur Aktivierung der Sicherheitsfunktion liegt im Bereich von 60 ms, die Reaktionszeit bei einer Verletzung von Grenzwerten < 10 ms.

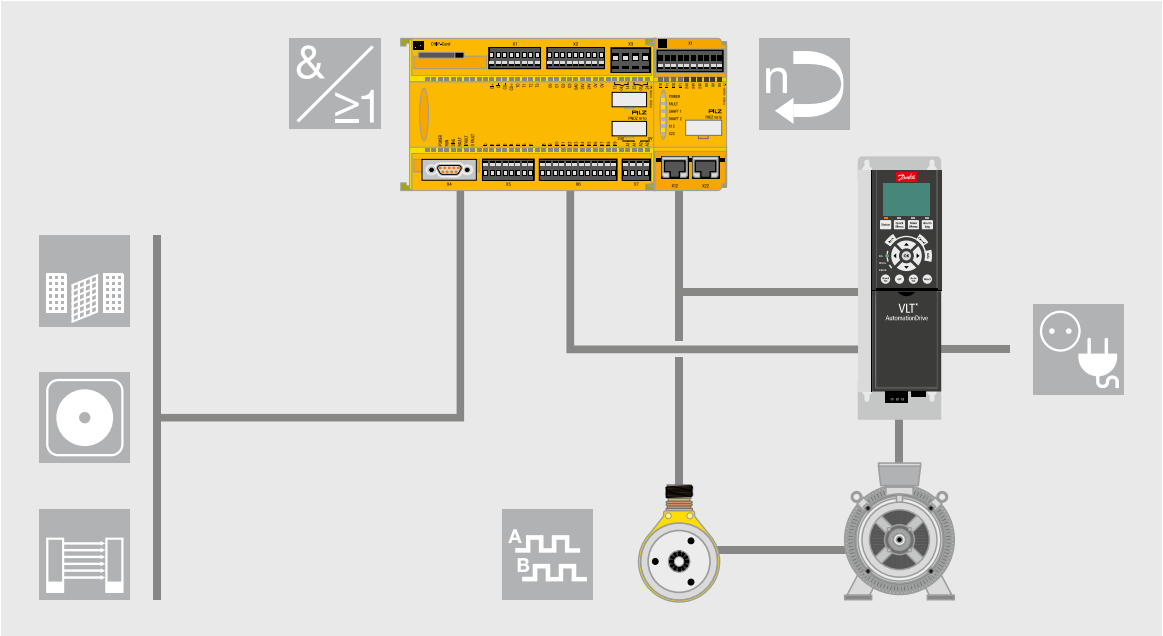


Realisierungsbeispiel mit Servoverstärker

7.5 Systembetrachtung

Sicher überwachter Antrieb mit Frequenzumrichter und Asynchronmotor

Ein Inkrementalgeber dient zur Erfassung der Bewegung. Ein Sicherheitsschaltgerät oder eine sichere Kleinsteuerung mit Bewegungsüberwachung werten die Sensorsignale aus und lösen im Fehlerfall die STO-Funktion aus.



Realisierungsbeispiel mit Frequenzumrichter

7.6 Beispiele für Safe Motion

7.6.1 Performance Level von Sicherheitsfunktionen

7.6.1.1 Normative Basis

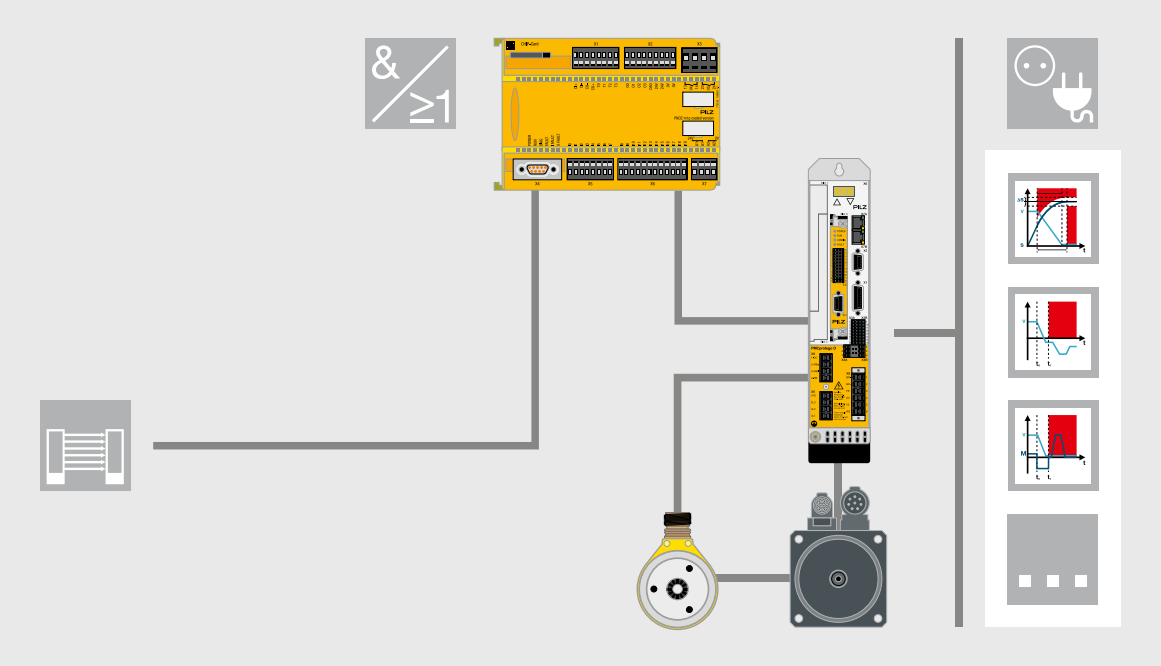
Für die Ermittlung des erreichten Sicherheitsniveaus des sicherheitsrelevanten Teils einer Steuerung stehen mehrere Normen (Sicherheitsgrund- und Sicherheitsfachgrundnormen; Typ A- und Typ B-Normen) zur Verfügung. Im Bereich des Maschinenbaus wird in der Regel die EN ISO 13849-1 angewendet. Das zu erreichende Sicherheitsniveau kann für viele Maschinen den jeweiligen Maschinensicherheitsnormen (Typ C-Normen) entnommen werden (Pressen ➔ EN 692, EN 693; Roboter ➔ EN ISO 10218-1, Verpackungsmaschinen ➔ EN 415). Stehen keine C-Normen für ein Produkt zur Verfügung, sind die Anforderungen aus den A- und B-Normen abzuleiten.

7.6.1.2 Sichere Stoppfunktion

Exemplarisch sei hier die Sicherheitsfunktion „Not-Halt bei Eingriff in Lichtvorhang“ betrachtet, die eine sichere Stoppfunktion für eine motorisch angetriebene Achse darstellt. Die nachfolgend beschriebene Methodik basiert auf der EN ISO 13849-1 und kann so nur dann angewendet werden, wenn alle Teilelemente der Sicherheitsfunktion über einen eigenen Performance Level verfügen. Es handelt sich dabei in der Terminologie der Norm um eine Reihenschaltung von sicherheitsrelevanten Teilen einer Steuerung (SRP/CS).

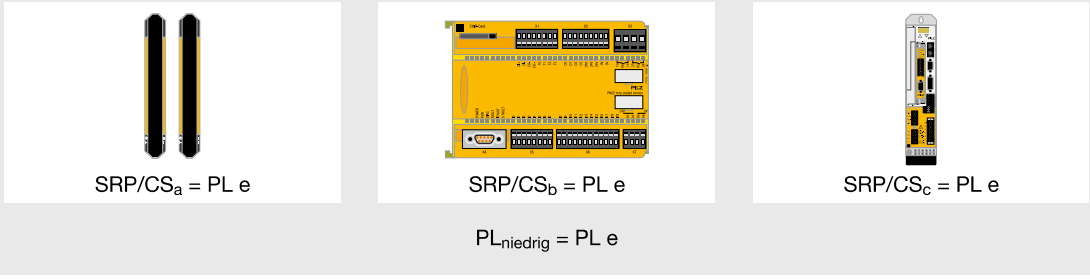
Verwendet werden in diesem Beispiel ein Lichtvorhang, eine konfigurierbare Sicherheitssteuerung sowie ein Servoverstärker mit integrierten Sicherheitsfunktionen. Am Servoverstärker ist ein Servomotor mit Feedbacksystem angeschlossen.

Die Risikoanalyse lässt eine Stoppkategorie 1 für die Achse zu.



Struktur der Sicherheitsfunktion

7.6 Beispiele für Safe Motion



Das Blockdiagramm zeigt die logische Struktur der Sicherheitsfunktion, die aus der Reihenschaltung der sicherheitsrelevanten Teilschaltungen besteht.

Ermittlung des Performance Levels der Gesamtschaltung

EN ISO 13849-1: Tabelle 11 – Berechnung des PL für die Reihenschaltung von SRP/CS

PL$_{niedrig}$	N$_{niedrig}$	→	PL
a	> 3	→	kein PL, nicht erlaubt
	≤ 3	→	a
b	> 2	→	a
	≤ 2	→	b
c	> 2	→	b
	≤ 2	→	c
d	> 3	→	c
	≤ 3	→	d
e	> 3	→	d
	≤ 3	→	e

Anmerkung: Die für das Nachschlagen berechneten Werte basieren auf Zuverlässigkeitswerten für die Mitte jedes PL.

Im Beispiel der sicheren Stoppfunktion verfügen alle drei beteiligten Komponenten über einen Performance Level e. Damit ist auch der niedrigste Performance Level einer sicherheitsrelevanten Teilschaltung (SRP/CS) ebenfalls PL e. In der Terminologie der Norm verfügt man damit über:

- 3 x SRP/CS mit jeweils PL e
- Der niedrigste Performance Level der 3 Teilschaltungen (SRP/CS) beträgt PL e und wird dem Parameter PL$_{niedrig}$ zugewiesen.
- Der niedrigste Performance Level tritt in 3 Teilschaltungen auf und deshalb ist der Parameter N$_{niedrig}$ = 3.

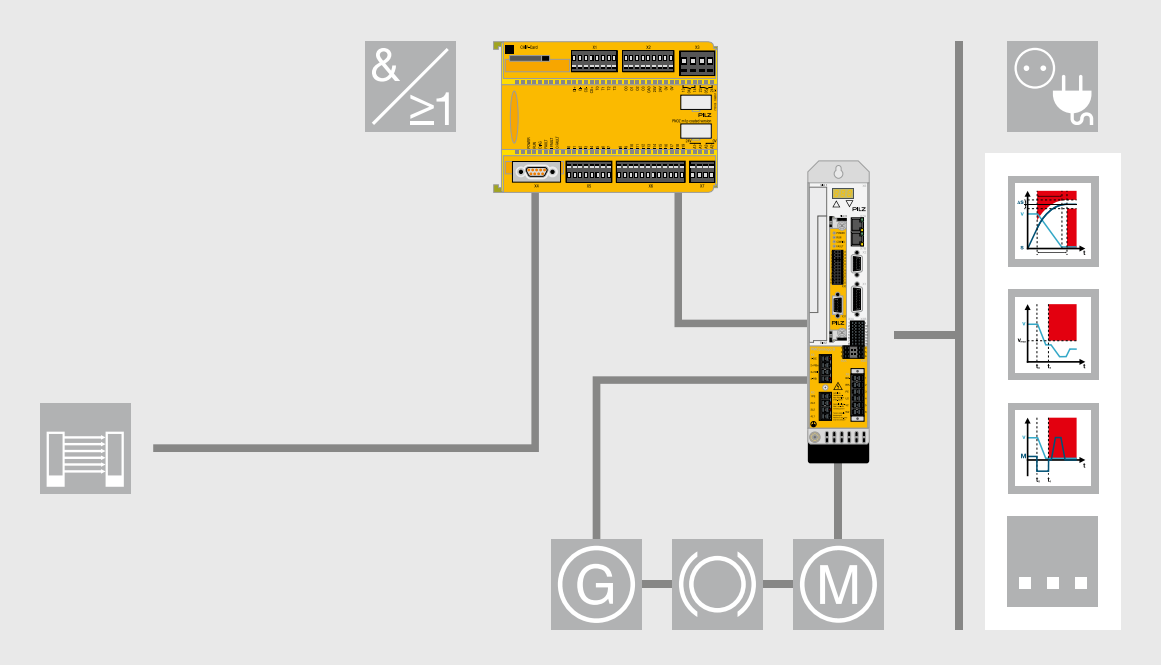
Geht man mit diesen Angaben in die Tabelle 11 der Norm, dann ergibt sich als Gesamteinstufung für das Beispiel ein PL e.

7.6 Beispiele für Safe Motion

7.6.1.3 Sichere Stoppfunktion an Vertikalachsen

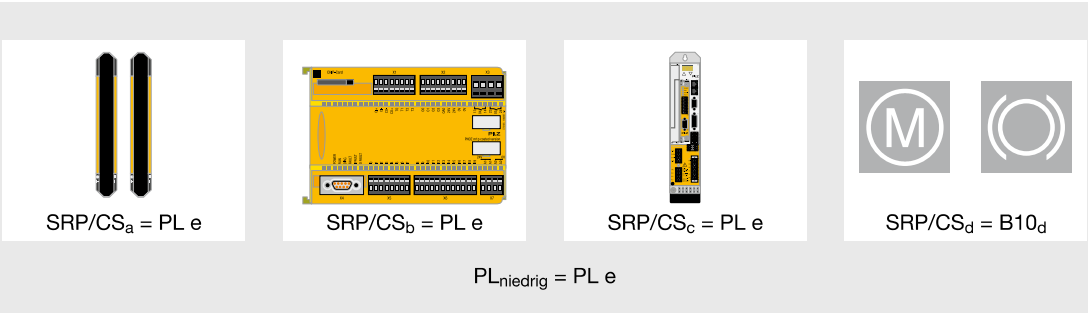
Betrachtet man die potenziellen Risiken an Servoachsen, dann eignet sich eine Vertikalachse gut als Beispiel, um auch den mechatronischen Blick zu schärfen. Die Abschaltung der Energieversorgung reicht nicht aus, um eine Achse in einen sicheren Zustand zu bringen. Das Eigengewicht der Last genügt in vielen Fällen, um diese absinken zu lassen. Masse und Reibung bestimmen die dabei auftretende Geschwindigkeit. Im Rahmen der Risikoanalyse werden die potenziellen Gefahren in den verschiedenen Betriebsarten der Maschine und bei den durch die Werker durchzuführenden Arbeiten analysiert. Daraus werden anschließend die notwendigen Maßnahmen abgeleitet. Bei Vertikalachsen hängen die zu treffenden Maßnahmen im Wesentlichen davon ab, ob ein Werker mit seinem kompletten Körper unter die Vertikalachse treten kann oder ob sich nur Arme und Hände unter der Vertikalachse befinden. Ein weiterer Aspekt ist die Häufigkeit, mit der man sich im Gefahrbereich aufhalten muss. Aus der Summe dieser Faktoren ergibt sich der für die Sicherheitsfunktionen zu erreichende „Performance Level“.

Aufbauend auf dem Beispiel „Sichere Stoppfunktion“ wird die Struktur noch um eine Bremse erweitert. Gängig sind sowohl Halte- als auch Betriebsbremsen.



Struktur der Sicherheitsfunktion

7.6 Beispiele für Safe Motion



Das Blockdiagramm zeigt die logische Struktur der Sicherheitsfunktion, die aus der Reihenschaltung der sicherheitsrelevanten Teilschaltungen besteht.

Ermittlung des Performance Levels der Haltebremse

Hier wird der Anwender der EN ISO 13849-1 mit einem der positiven Ansätze dieser Norm konfrontiert. Die Norm ermöglicht nicht nur die Betrachtung des elektrischen Teils der Sicherheitsfunktion, sondern auch des mechanischen, hydraulischen und pneumatischen Anteils.

Die in diesem Beispiel verwendete Haltebremse verfügt jedoch über keinen Performance Level, da dieser nur für intelligente Bauteile angegeben werden kann. Der Hersteller der Bremse kann nur einen $B10_d$-Wert zur Verfügung stellen, da er den genauen Einsatz seiner Komponenten in den Applikationen nicht kennt und deshalb nur eine Aussage bezüglich der Schaltzyklen bis zu einem Ausfall seiner Komponente machen kann. Der Konstrukteur, der den sicherheitsrelevanten Teil der Steuerung plant, muss jetzt die Zeit berechnen, die bis zu einem gefährlichen Ausfall des Bauteils verstreicht. Bei dieser Berechnung ist neben dem $B10_d$ die mittlere Zeit, die zwischen zwei aufeinander folgenden Zyklen vergeht, der wesentliche Faktor, der den Wert des $MTTF_d$ beeinflusst.

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

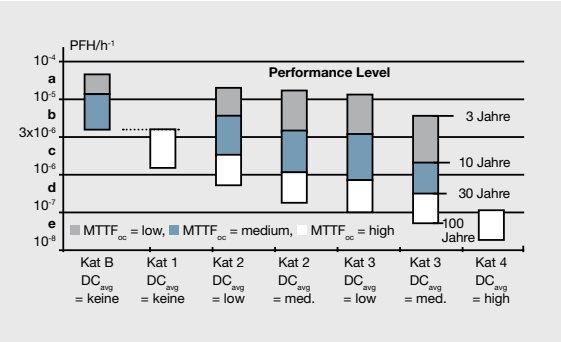
$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ s/h}{t_{Zyklus}}$$

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

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

In der Annahme, dass die Berechnung des $MTTF_d$ der Haltebremse einen Wert von > 100 Jahren ergibt, führt dies zu einer Einstufung des $MTTF_d$ von „HOCH“. Die EN ISO 13849-1 stellt für eine vereinfachte Ermittlung des Performance Levels eine Grafik zur Verfügung. Um aus dieser Grafik jetzt den Performance Level ablesen zu können, fehlt noch der Diagnosedeckungsgrad DC. Für die Ermittlung des Diagnosedeckungsgrads ist es wichtig, ob durch Tests alle denkbaren Fehler erkannt werden können. Auf Basis dieser Überlegung ist eine hohe Einstufung dann möglich, wenn ein sicherer Umrichter zur Ansteuerung des Motors verwendet wird und die Haltebremse vor jedem Zugang zur Gefahrstelle automatisch getestet wird. Hierzu wird ein Moment mit Faktor 1,3 zum Nennhaltemoment der Bremse aufgebaut und dann mindestens eine Sekunde gewartet. Hält die Achse während des gesamten Tests ihre Position, kann davon ausgegangen werden, dass die Haltebremse in Ordnung ist. Eine Festlegung des Diagnosedeckungsgrads auf 99 % ist auf dieser Basis möglich.

7.6 Beispiele für Safe Motion



Graph zur Bestimmung des PL nach EN ISO 13849-1

Damit liegen nun folgende Daten vor:

- Kategorie = 4
- MTTF$_d$ = hoch
- DC = hoch

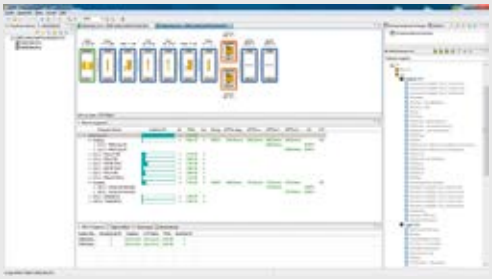
Geht man mit diesen Daten in die Grafik, dann kann ein PL e abgelesen werden.

Ermittlung des Performance Levels der Gesamtschaltung

Im dargestellten Beispiel der sicheren Stoppfunktion einer Servoachse mit Haltebremse verfügen alle vier beteiligten Komponenten über einen Performance Level e. Damit ist auch der niedrigste Performance Level einer Teilschaltung ebenfalls PL e. In der Terminologie der Norm verfügt man damit über:

- 4 x SRP/CS mit jeweils PL e
- Der niedrigste Performance Level der 4 Teilschaltungen (SRP/CS) beträgt PL e und wird dem Parameter PL$_{niedrig}$ zugewiesen.
- Der niedrigste Performance Level tritt in 4 Teilschaltungen auf und deshalb ist der Parameter N$_{niedrig}$ = 4.

Geht man mit diesen Angaben in die Tabelle 11 der EN ISO 13849-1 zur vereinfachten Berechnung, ergibt sich als Gesamteinstufung für das Beispiel ein PL d. Im Unterschied zum Beispiel sichere Stoppfunktion (ohne Bremse) greift jetzt ein Reduktionsfaktor: Gemäß der EN/ISO 13849-1 reduziert sich der erreichte Performance Level um eine Stufe, wenn mehr als drei Teilschaltungen mit PL$_{niedrig}$ an der Gesamtschaltung beteiligt sind. Eine ausführliche Berechnung mit den erreichten PFH$_D$-Werten kann in diesem Fall durchaus ein PL e zeigen. Hier bieten sich Software-Tools wie der Safety Calculator PAScal an.

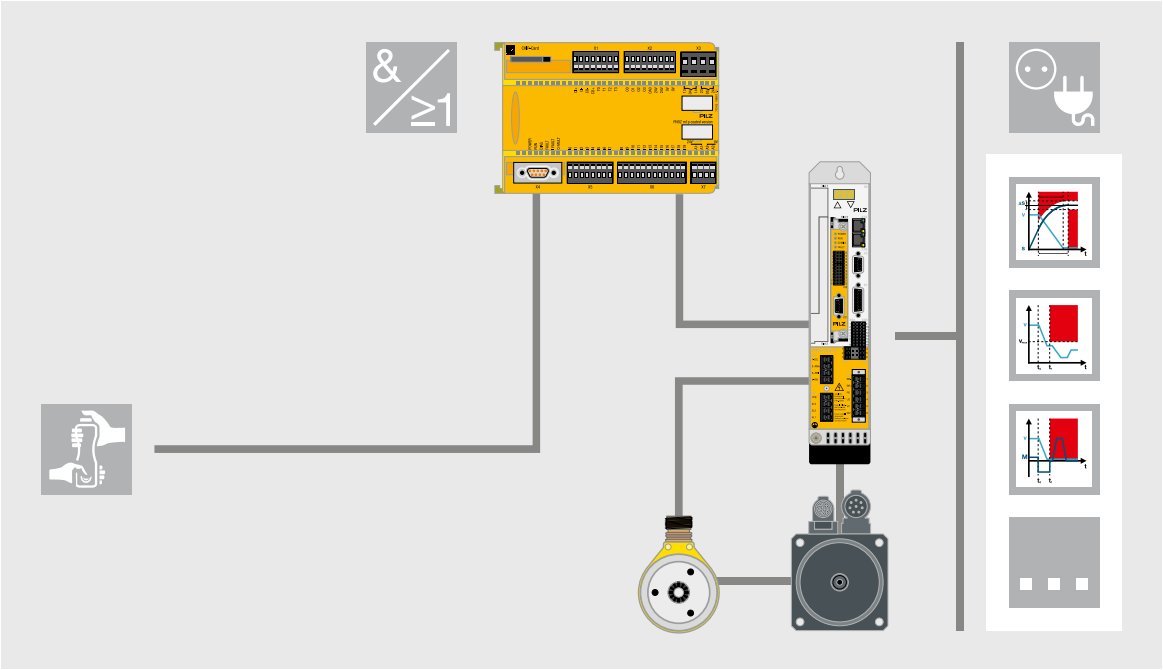


Safety Calculator PAScal

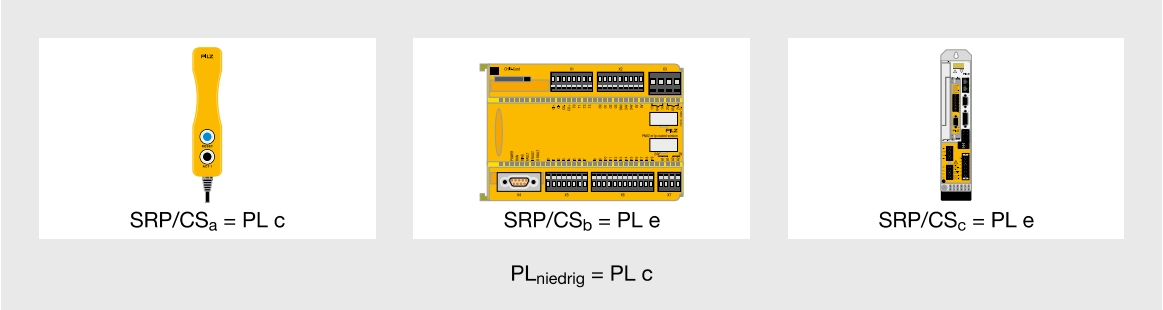
7.6 Beispiele für Safe Motion

7.6.1.4 Tippfunktion mit Sicher begrenzter Geschwindigkeit (SLS)

Durch die Funktion Sicher begrenzte Geschwindigkeit (SLS) können heute in der Regel Tippfunktionen bei offenen Schutzgittern realisiert werden. Das als ungefährlich einstufbare Schrittmaß ist hierbei von der jeweiligen Applikation abhängig. Hilfreich kann dabei die Betrachtung der EN 349 und der EN ISO 13855 sein.



Struktur der Sicherheitsfunktion



Das Blockdiagramm zeigt die logische Struktur der Sicherheitsfunktion, die aus der Reihenschaltung der sicherheitsrelevanten Teilschaltungen besteht.

7.6 Beispiele für Safe Motion

Ermittlung des Performance Levels der Gesamtschaltung

Die Tippfunktion mit Sicher begrenzter Geschwindigkeit (SLS) gleicht strukturell der in Kapitel 7.6.1.2 behandelten sicheren Stoppfunktion. Der wesentliche Unterschied sind die für die Tippfunktion verwendeten Taster und die Auswirkungen auf die Berechnung des Performance Levels. Drucktaster (Zustimmschalter) sind in der EN ISO 13849-1 mit einem $B10_d$ von 100 000 angegeben. Für die Berechnung des $MTTF_d$ ist die Zeit zwischen zwei Betätigungen (Zyklen) der wesentliche Faktor.

Berechnungsformel für $MTTF_d$

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

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

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

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

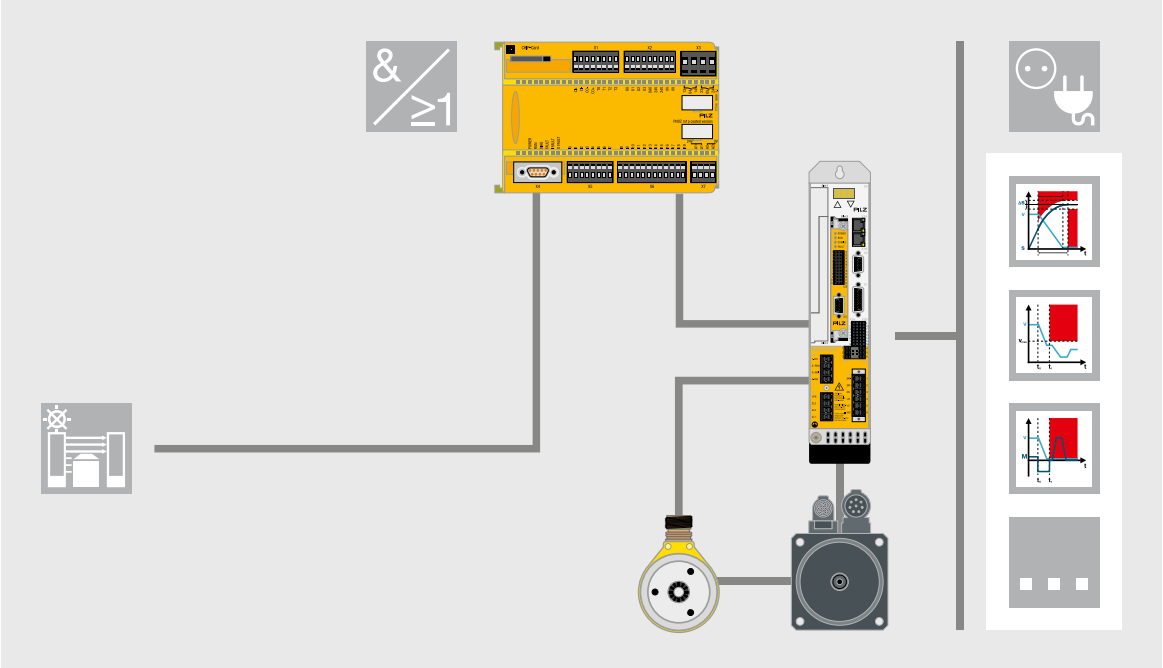
Annahmen:
- $B10_d$ = 100 000
- h_{op} = 16 h/Tag
- d_{op} = 220 T/Jahr

Berechnung $MTTF_d$:
- t_{Zyklus} = 5 s → $MTTF_d$ = 0,395 Jahre
- t_{Zyklus} = 3 600 s → $MTTF_d$ = 284,1 Jahre

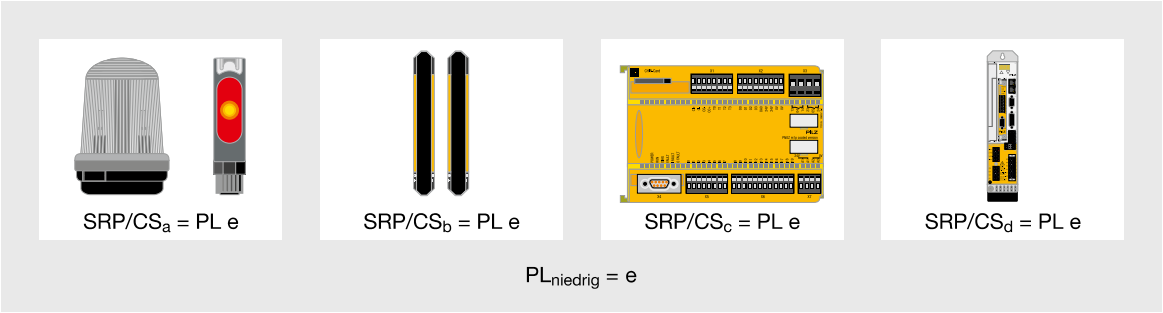
Wie das Beispiel mit einer zyklischen Betätigung im Abstand von 5 s zeigt, ist mit einem $B10_d$-Wert von 100 000 im besten Falle nur noch ein PL c erreichbar. Dabei zeigt sich sehr deutlich, dass der Einsatzbereich von verschleißbehafteten Komponenten direkt in die Berechnung des Performance Levels eingeht und somit Einfluss auf das erreichbare Sicherheitsniveau hat. Der Konstrukteur muss sich also den Einsatzbereich seiner Komponenten in der jeweiligen Applikation sehr genau anschauen. Auch wenn die EN ISO 13849-1 100 000 Zyklen als $B10_d$ angibt, kann es durchaus spezielle Komponenten geben, die mit einem größeren $B10_d$-Wert angeboten werden. Wird in einer Applikation ein Taster als Not-Halt-Befehlsgerät eingesetzt, wird dieser sicher nicht konstant im 5-Sekunden-Raster betätigt. Eine völlig andere Situation ergibt sich, wenn ein Taster als Befehlsgerät für die zyklische Auslösung eines Maschinenzyklus verwendet wird und beim Loslassen einen sicheren Stopp einleiten muss. Ist ein hoher Performance Level gefragt, werden die im Beispiel genannten Werte unter Umständen zum Problem.

7.6 Beispiele für Safe Motion

7.6.1.5 Muting mit Sicherer Drehrichtung (SDI)



Struktur der Sicherheitsfunktion



Das Blockdiagramm zeigt die logische Struktur der Sicherheitsfunktion, die aus der Reihenschaltung der sicherheitsrelevanten Teilschaltungen (SRP/CS) besteht.

Die Funktion Sichere Drehrichtung (SDI) wirkt sich in Verbindung mit Lichtvorhängen mit Mutingschaltung positiv auf die Sicherheit aus, weil während der Mutingphase auch die zugehörige Drehrichtung der Antriebsachse überwacht wird und im Fehlerfall eine sichere Abschaltung folgt.

Ermittlung des Performance Levels der Gesamtschaltung

Der Performance Level entspricht dem Ergebnis im Beispiel Sichere Stoppfunktion.

7.6 Beispiele für Safe Motion

7.6.1.6 Bewegungsüberwachung mit externen Geräten

Der antriebsintegrierten Bewegungsüberwachung steht die externe Überwachung gegenüber. Dabei besitzt der Antrieb im einfachsten Falle keinerlei Sicherheitsfunktion. Die Abschaltung eines Antriebs zur Realisierung einer Sicherheitsfunktion kann dann auf konventionelle Weise beispielsweise mit Schützen erfolgen. Heute haben Antriebe jedoch häufig bereits eine STO-Funktion und damit den „Sicheren Halt“ implementiert. Damit kann ein vorgelagertes Sicherheitsschaltgerät für eine einfache sichere Abschaltung der gefahrbringenden Bewegung sorgen. Die eigentliche sicherheitsgerichtete Bewegungsüberwachung findet aber in der externen Überwachungskomponente statt.

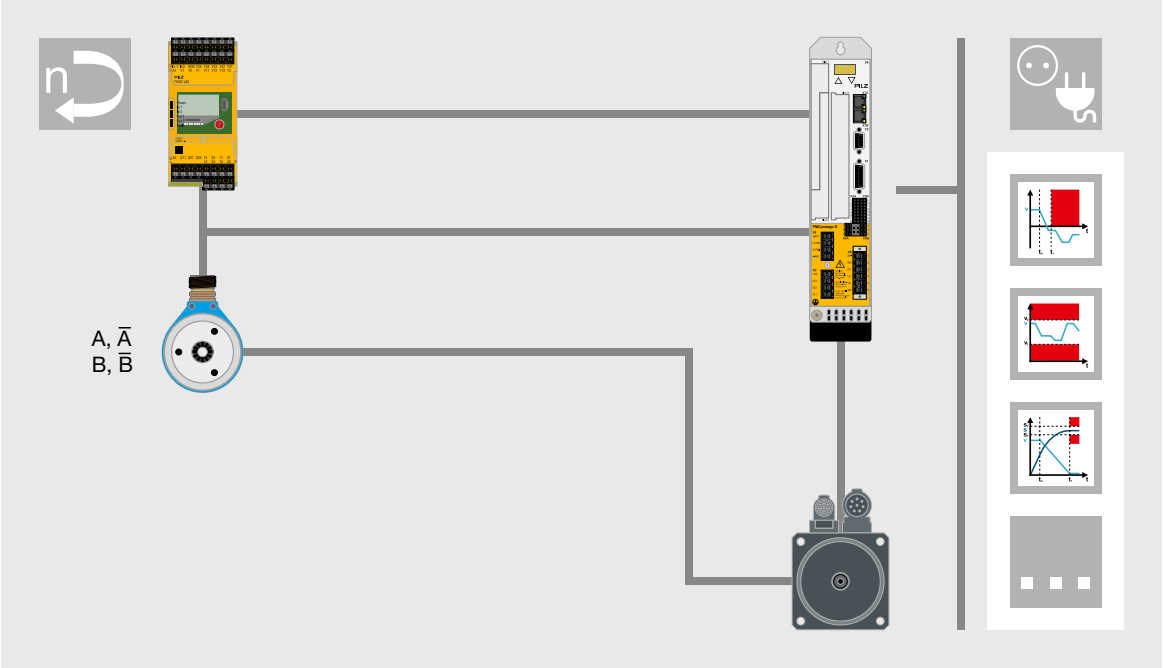
Aufgabe der externen Geräte ist die Erfassung der Bewegung. Die Sicherheitskennwerte der eingesetzten Sensoren, z. B. Drehgeber oder Initiatoren, bestimmen den erreichbaren Sicherheitslevel maßgeblich. Zur Überwachung von Bewegungen mit externen Überwachungsgeräten stehen verschiedene Lösungen für die unterschiedlichen Anforderungen zur Verfügung. Auf oberster Ebene ist dabei die Differenzierung in sogenannte Standardgeber und „sichere“ Geber zu finden. Beim Einsatz von Standardgebern ist entscheidend, ob ein oder zwei Geber erforderlich sind.

Abhängig von den jeweils implementierten Überwachungsfunktionen in den externen Überwachungsgeräten lassen sich z. B. folgende Sicherheitsfunktionen realisieren:

- Sicher begrenzte Geschwindigkeit (SLS)
- Sichere Bewegungsrichtung (SDI)
- Sicherer Betriebshalt (SOS)
- Sicherer Geschwindigkeitsbereich (SSR)
- Sicher begrenzte Beschleunigung (SLA)
- Sicherer Beschleunigungsbereich (SAR)

Die folgenden Beispiele illustrieren mögliche Varianten der Bewegungsüberwachung mit externen Geräten. Dargestellt sind der Übersichtlichkeit halber nur jene Teile der Bewegungsüberwachung, die die Überwachung von Bewegungssensoren wie Drehgeber oder Initiatoren zur Aufgabe haben. Der grundsätzliche Berechnungsweg entspricht der in den vorangegangenen Beispielen dargestellten Methode.

7.6 Beispiele für Safe Motion



Bewegungsüberwachung mit einem Standardgeber

7.6.1.7 Externe Bewegungsüberwachung mit einem Standardgeber

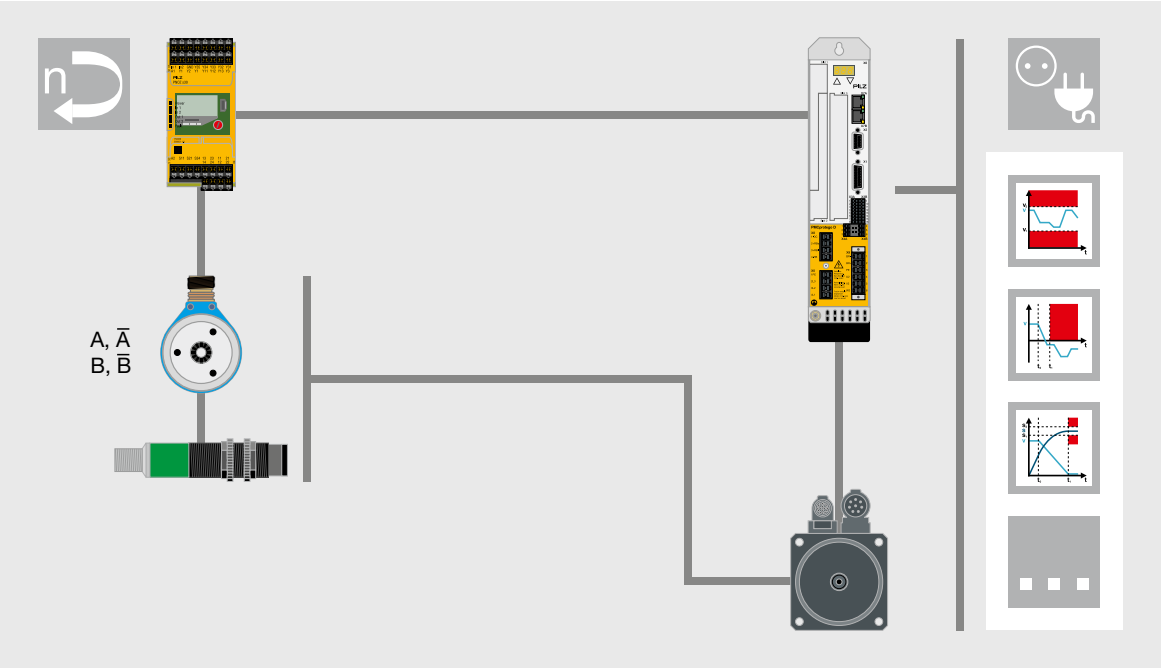
In diesem Beispiel ist ein Standard-Drehgeber als Sensor für die Bewegungserfassung verantwortlich. Verschiedene Kombinationen im Zusammenspiel mit der Antriebssteuerung sind möglich. Die Abschaltung der gefahrbringenden Bewegung erfolgt durch eine im Antrieb vorhandene STO-Funktion. Wertet nur das Überwachungsgerät die Gebersignale für die Sicherheitsfunktion aus, verwendet die Antriebssteuerung also keinen oder nur einen separaten Geber, ist maximal ein Performance Level PL c erreichbar. Dazu ist ein Geber mit $MTTF_d$ = hoch und der Einstufung als „Bewährtes Bauteil“ oder Kategorie 1 oder alternativ die Einstufung direkt in PL c notwendig.

Wenn das Überwachungsgerät die Gebersignale auswertet und die Antriebssteuerung zur Positionsregelung gleichzeitig dieselben Signale verwendet, ist ein Performance Level bis zu PL d erreichbar. Dazu ist ein Geber mit $MTTF_d$ = mittel/hoch notwendig. Die Antriebsregelung fungiert als zusätzliche Diagnoseinstanz für die Sicherheitsfunktion, indem die Schleppfehlererkennung (inkl. Abschaltung) entsprechend parametriert und aktiviert wird. Ein reiner Frequenzumrichter (FU) ohne Regelfunktion ist hier nicht einsetzbar.
Mit der dargestellten Konfiguration sind folgende Sicherheitsfunktionen möglich:

- Sicher begrenzte Geschwindigkeit (SLS)
- Sichere Bewegungsrichtung (SDI)
- Sicherer Betriebshalt (SOS)
- Sicherer Geschwindigkeitsbereich (SSR)
- Sicher begrenzte Beschleunigung (SLA)
- Sicherer Beschleunigungsbereich (SAR)

Anmerkung: Welche Sicherheitsfunktionen realisierbar sind, hängt von den implementierten Überwachungsfunktionen im externen Überwachungsgerät ab.

7.6 Beispiele für Safe Motion



Bewegungsüberwachung mit redundanten Standardsensoren

7.6.1.8 Externe Bewegungsüberwachung mit Standardgeber und -initiator

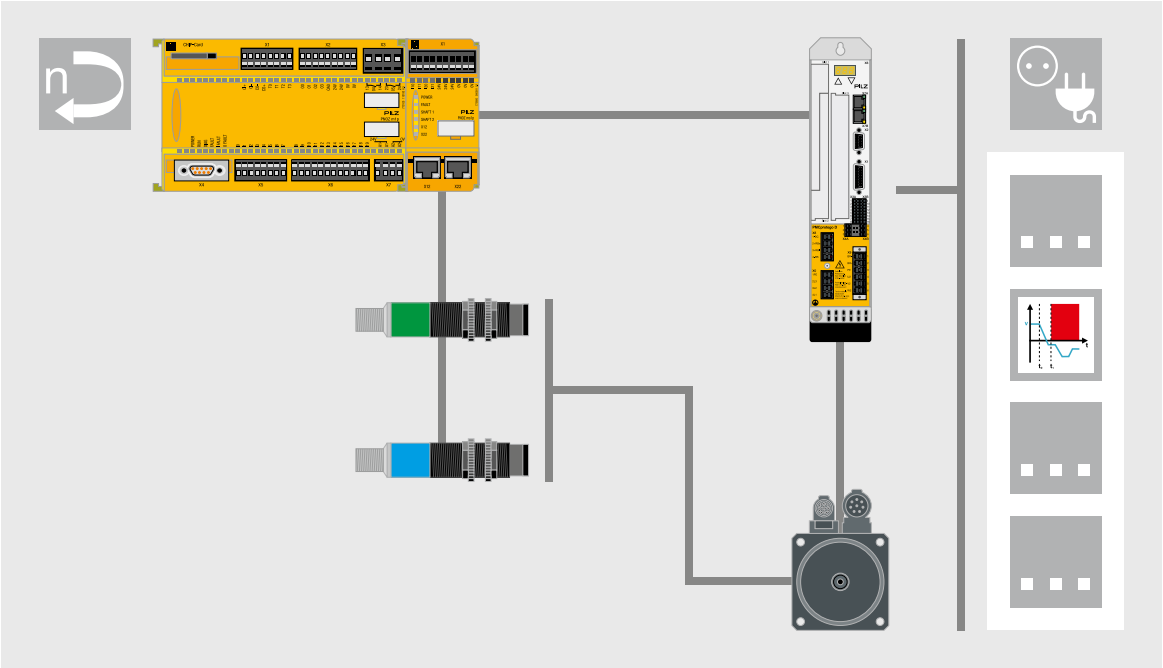
Um den höchsten Sicherheitslevel (PL e) mit Standardsensoren zu erreichen, sind in der Regel zwei separate Sensoren zur Bewegungserfassung erforderlich. Abhängig vom externen Überwachungsgerät können dies zwei Drehgeber oder, wie hier im Beispiel dargestellt, ein Drehgeber und ein zusätzlicher Initiator sein. Für die Sensoren sind die entsprechenden Werte für $MTTF_d$ notwendig. Damit lässt sich der Performance Level für das Sensor-Teilsystem, bestehend aus Geber und Initiator, und daraus schließlich der Performance Level der gesamten Sicherheitsfunktion berechnen. Die Abschaltung der gefahrbringenden Bewegung erfolgt hier durch eine im Antrieb vorhandene STO-Funktion.

Die vom Überwachungsgerät für die Sicherheitsfunktion ausgewerteten Gebersignale sind auch von der Antriebssteuerung zur Geschwindigkeits- bzw. Positionsregelung nutzbar. Dies ist jedoch für die Sicherheitsfunktion nicht zwingend notwendig. Mit der dargestellten Konfiguration sind folgende Sicherheitsfunktionen möglich:

- Sicher begrenzte Geschwindigkeit (SLS)
- Sichere Bewegungsrichtung (SDI)
- Sicherer Betriebshalt (SOS)
- Sicherer Geschwindigkeitsbereich (SSR)
- Sicher begrenzte Beschleunigung (SLA)
- Sicherer Beschleunigungsbereich (SAR)

Anmerkung: Welche Sicherheitsfunktionen realisierbar sind, hängt von den implementierten Überwachungsfunktionen im externen Überwachungsgerät ab.

7.6 Beispiele für Safe Motion



Bewegungsüberwachung mit Initiatoren

7.6.1.9 Externe Bewegungsüberwachung mit zwei Standard-Initiatoren

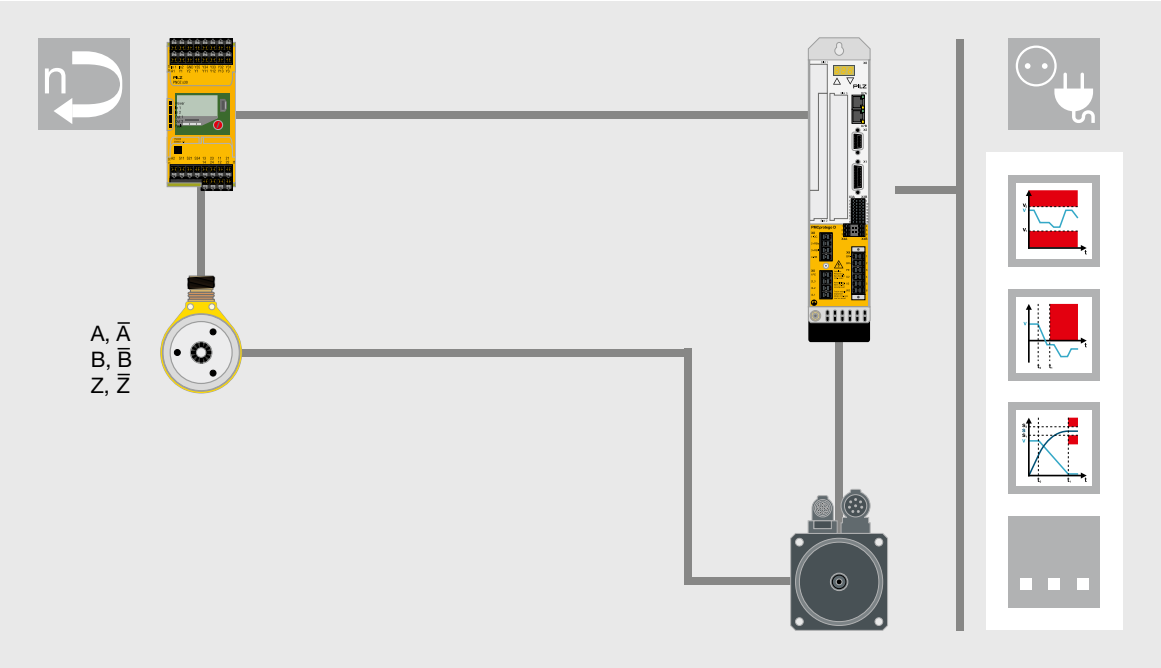
Auch ohne Drehgeber lässt sich eine sicherheitsgerichtete Bewegungsüberwachung beispielsweise mit Standardsensoren in Form von Initiatoren sogar bis zum höchsten Sicherheitslevel (PL e) realisieren. Analog zum vorigen Beispiel sind zwei separate Initiatoren zur Bewegungserfassung erforderlich. Wenn Fehler gemeinsamer Ursache (CCF, common cause failure), wie beispielsweise durch EMV, für die beiden Initiatoren nicht ausschließ- oder beherrschbar sind, empfiehlt sich der Einsatz diversitärer Komponenten unterschiedlicher Hersteller oder Typen. Für die Initiatoren sind die entsprechenden Werte für $MTTF_d$ erforderlich. Damit lässt sich der Performance Level für das Sensor-Teilsystem, bestehend aus den beiden Initiatoren, und daraus schließlich der Performance Level der gesamten Sicherheitsfunktion berechnen. Die Abschaltung der gefahrbringenden Bewegung erfolgt durch eine im Antrieb vorhandene STO-Funktion.

Mit der dargestellten Konfiguration ist die folgende Sicherheitsfunktion möglich:

- Sicher begrenzte Geschwindigkeit (SLS)
- Sicherer Geschwindigkeitsbereich (SSR)

Anmerkung: Welche Sicherheitsfunktionen realisierbar sind, hängt von den implementierten Überwachungsfunktionen im externen Überwachungsgerät ab.

7.6 Beispiele für Safe Motion



Bewegungsüberwachung mit sicherem Drehgeber

7.6.1.10 Externe Bewegungsüberwachung mit sicherem Geber

Verstärkt bieten Hersteller sogenannte „sichere“ Geber für Aufgaben der Bewegungsüberwachung an. Diese Geräte sind speziell für den Einsatz in Sicherheitsfunktionen ausgelegt und entsprechend zertifiziert. Abhängig von der Bauart ist damit ein Performance Level von PL d oder PL e erreichbar. Üblicherweise ist dies mit nur einem Geber möglich, es bedarf also nicht zweier Geräte, wie dies bei Verwendung von Standardbauteilen notwendig ist. Aber erst die Kombination mit einem sicheren Überwachungsgerät macht sichere Geber tatsächlich „sicher“, da Diagnose- und Plausibilitätsprüfungen nicht im Geber implementiert sind. Der Einsatz sicherer Geber erfordert daher eine detaillierte Kenntnis der Anforderungen für den Einsatz in sicherheitsgerichteten Applikationen, die der Geberhersteller in seiner Bedienungsanleitung beschreibt. Das Überwachungsgerät muss diese Anforderungen genau erfüllen können, indem es die vom Geberhersteller geforderten Überwachungsfunktionen ausführt.

Eine häufig geforderte Prüfung ist z. B. die Betragsprüfung für Sin/Cos-Geber: $\sin^2 + \cos^2 = 1$. Ist diese Prüfung in einem Überwachungsgerät nicht implementiert, kann dieses nicht in Kombination mit einem sicheren Geber eingesetzt werden, der genau diese Prüfung fordert. Da bislang noch keine einheitliche oder gar genormte Schnittstelle für sichere Geber existiert, sind die Anforderungen der Geberhersteller für ihre Produkte sehr unterschiedlich. Eine genaue Abstimmung zwischen sicherem Geber und sicherem Überwachungsgerät ist deshalb unbedingt erforderlich. Die Abschaltung der gefahrbringenden Bewegung erfolgt in diesem Beispiel durch eine im Antrieb vorhandene STO-Funktion. Mit der dargestellten Konfiguration sind die folgenden Sicherheitsfunktionen realisierbar:

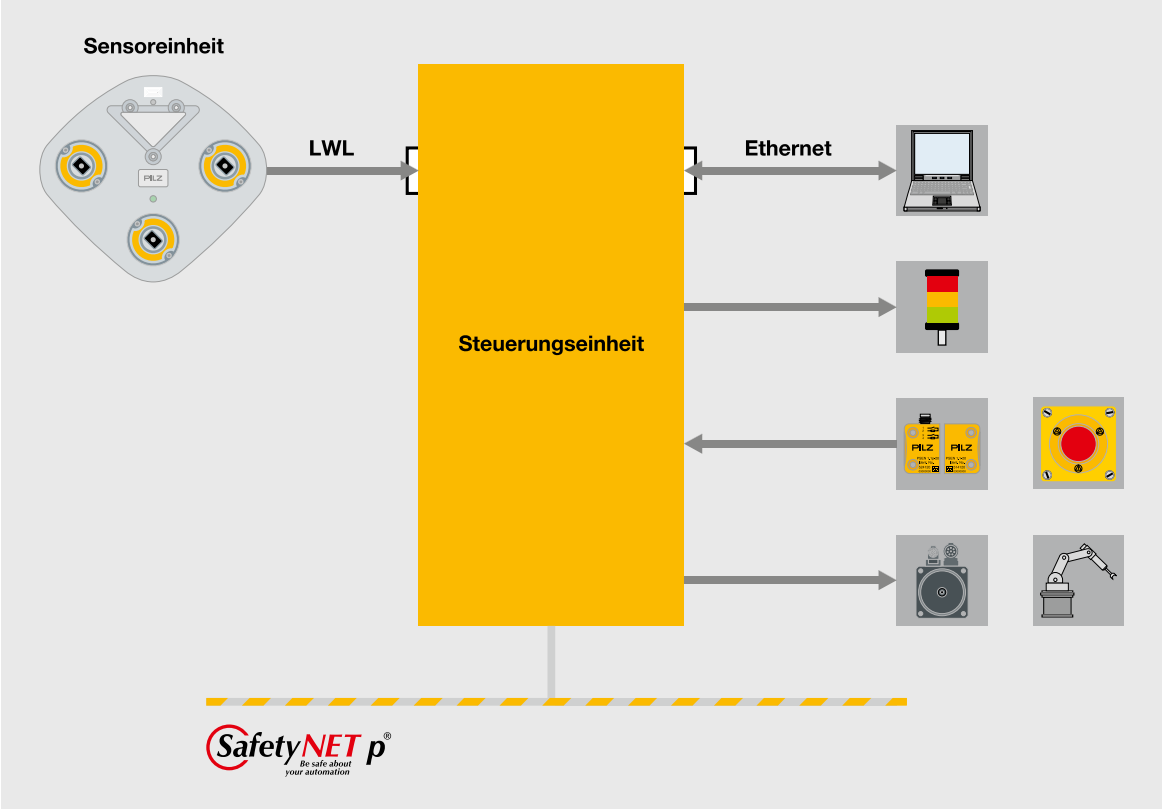
- Sicher begrenzte Geschwindigkeit (SLS)
- Sichere Bewegungsrichtung (SDI)
- Sicherer Betriebshalt (SOS)
- Sicherer Geschwindigkeitsbereich (SSR)
- Sicher begrenzte Beschleunigung (SLA)
- Sicherer Beschleunigungsbereich (SAR)

Anmerkung: Welche Sicherheitsfunktionen im Detail möglich sind, hängt von den implementierten Überwachungsfunktionen im externen Überwachungsgerät ab.

7.6 Beispiele für Safe Motion

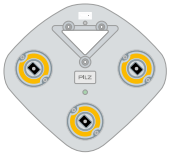
7.6.1.11 Schutzraumabsicherung mit sicherer kamerabasierter Lösung

Bisher war das Zusammenwirken von Mensch und Roboter stark von fest montierten Schutzeinrichtungen geprägt. Eine moderne kamerabasierte Lösung bietet hier ganz neue Möglichkeiten. Der Schutzraum umfasst alle drei Dimensionen, ein einziges Gerät leistet sämtliche Anforderungen beim Zugang zu einer Gefahrstelle sowie darüber hinaus noch einen Schutz gegen ein Übersteigen und Unterkriechen der Schutzzone. Die einzeln projektierbaren Schutzräume ermöglichen auch die Reduktion von Geschwindigkeiten der im überwachten Bereich aktiven Achsen bei einer Annäherung.

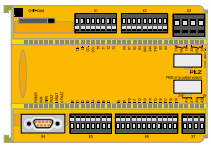


Struktur der Sicherheitsfunktion

7.6 Beispiele für Safe Motion



SRP/CS_a = PL d



SRP/CS_b = PL e

SRP/CS_c = PL e

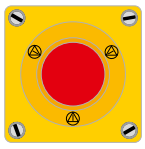
$PL_{niedrig}$ = d

Blockdiagramm der Sicherheitsfunktionen

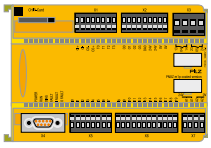
Ermittlung des Performance Levels der Gesamtschaltung

Es ergibt sich ein Performance Level d.

7.6.2 Reaktionszeiten von Sicherheitsfunktionen



SRP/CS_a = PL e



SRP/CS_b = PL e

SRP/CS_c = PL e

$PL_{niedrig}$ = e

Blockdiagramm der Sicherheitsfunktionen

Bei der Berechnung eines Sicherheitsabstands fließen mehrere Randbedingungen ein.

Ermittlung der Reaktionszeit bei externen Befehlen

Wirkt ein Not-Halt-Taster auf ein Auswertegerät, so addiert sich dessen Reaktionszeit zu der Reaktionszeit der antriebsintegrierten Sicherheitsfunktion. Dazu ist zusätzlich jene Zeit zu addieren, die eine beschleunigte Achse bis zum Stillstand benötigt:

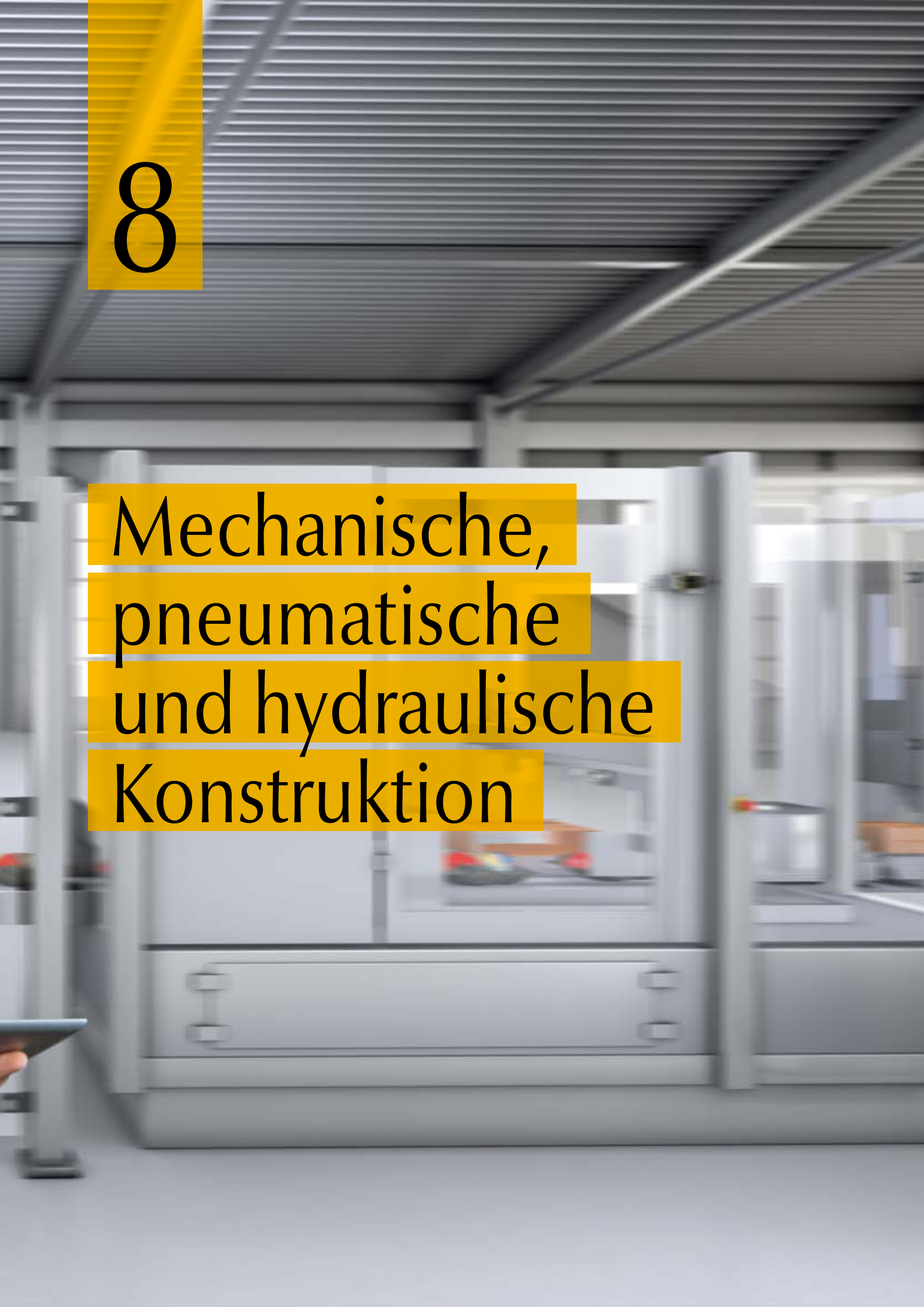
- $t_{reak} = t_{multi} + t_{PMC} + t_{rampe}$
- t_{multi} = Reaktionszeit des Auswertegeräts liegt bei ca. 20 ms
- t_{PMC} = Reaktionszeit der antriebsintegrierten Sicherheitsfunktionen auf externe Signale beträgt 6 ms
- t_{rampe} = Rampenzeit bis zum Stillstand hängt von der bewegten Masse, Geschwindigkeit und weiteren applikationsabhängigen Daten ab

Ermittlung der Reaktionszeit bei Grenzwertverletzungen

Spricht eine Überwachungsschaltung einer antriebsintegrierten Sicherheitsfunktion an, ist zusätzlich die Zeit zu addieren, die die beschleunigte Achse bis zum Stillstand benötigt.

- $t_{reak} = t_{PMC} + t_{rampe}$


Cylinder 1
Cylinder 2
2
Sequence valve
1
Directional valve
M
Pressure limiting valve



8

Mechanische, pneumatische und hydraulische Konstruktion

8 Mechanische, pneumatische und hydraulische Konstruktion

8 Mechanische, pneumatische und hydraulische Konstruktion
8.1 Einleitung in die mechanische, pneumatische und hydraulische Konstruktion 8-3
8.2 Mechanische Konstruktion 8-4
8.2.1 Einleitung 8-4
8.2.2 Gefahr, Gefährdung, Risiko 8-5
8.2.3 Festlegen und Umsetzen von Sicherheitsmaßnahmen 8-9
8.3 Pneumatische Konstruktion 8-21
8.3.1 Verwendete Einheiten 8-21
8.3.2 Einleitung 8-23
8.3.3 Bewährte Prinzipien und Schutzmaßnahmen 8-23
8.3.4 Schaltungstechnische Lösungen 8-27
8.3.5 Halten und Abbremsen 8-33
8.3.6 Schaltplan und Betriebsanleitung 8-35
8.4 Hydraulische Konstruktion 8-37
8.4.1 Physikalisches Basiswissen 8-37
8.4.2 Vorteile der hydrostatischen Energieübertragung 8-37
8.4.3 Nachteile der hydrostatischen Energieübertragung 8-37
8.4.4 Definitionen 8-37
8.4.5 Allgemeine hydraulische Beziehungen 8-38
8.4.6 Aufbau eines Hydrauliksystems 8-44
8.4.7 Einfacher Hydraulikkreislauf, Auffahrt 8-44
8.4.8 Einfacher Hydraulikkreislauf, Abwärtsfahrt 8-45
8.4.9 Einfacher Hydraulikkreislauf, Geschwindigkeit 8-45
8.4.10 Einfacher Hydraulikkreislauf-Schaltplan 8-46
8.4.11 Zweizylindersteuerungen mit elektrischen Ventilen 8-47
8.4.12 Zweizylindersteuerungen mit Folgeventilen 8-48
8.4.13 Serienschaltung 8-49
8.4.14 Parallelschaltung 8-49
8.4.15 Differenzialschaltung 8-50
8.4.16 Geschwindigkeitssteuerungen 8-51
8.4.17 Antriebspumpen, Konstantpumpen 8-52
8.4.18 Antriebspumpen, Schraubenpumpen 8-53
8.4.19 Antriebspumpen, Flügelzellenpumpen 8-54
8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik 8-55
8.5.1 Sicherheitsanforderungen im Allgemeinen 8-55
8.5.2 Entwurf und Auslegung 8-55
8.5.3 Weitere Sicherheitsanforderungen 8-55
8.5.4 Feststellung der Übereinstimmung mit den Sicherheitsanforderungen 8-56
8.5.5 Sicherheitsbezogene Teile von hydraulischen Steuerungen 8-57
8.5.6 Steuerungen nach Kategorie B, Performance Level a gemäß EN/ISO 13849-1 8-58
8.5.7 Steuerungen nach Kategorie 1, Performance Level b 8-59
8.5.8 Steuerungen nach Kategorie 2, Performance Level b 8-60
8.5.9 Steuerungen nach Kategorie 3, Performance Level d 8-61
8.5.10 Steuerungen nach Kategorie 4, Performance Level e 8-62
8.5.11 Weiteres Beispiel für Steuerungen nach Kategorie 4 8-63

8.1 Einleitung in die mechanische, pneumatische und hydraulische Konstruktion

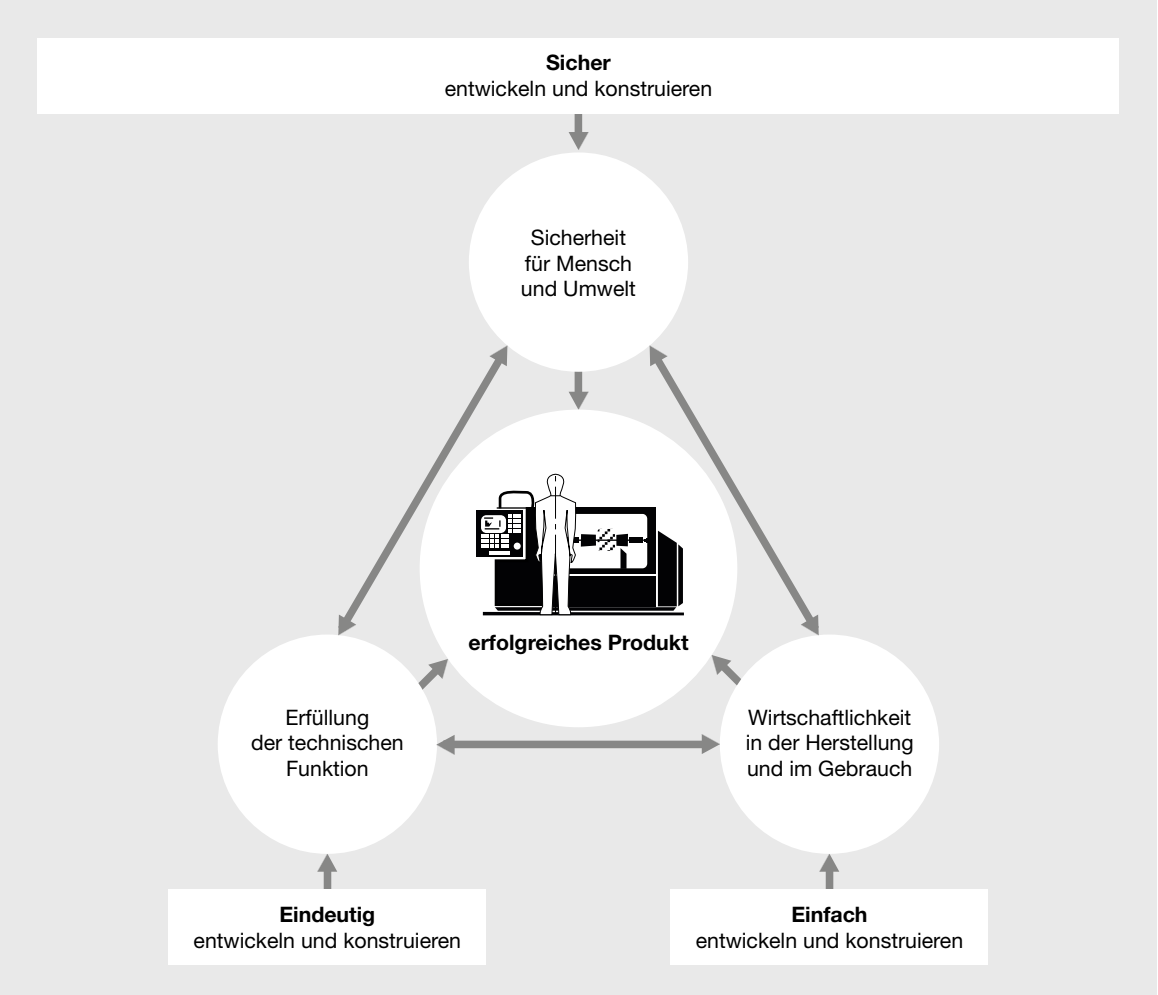
Die Sicherheitstechnik nimmt in der Konstruktion von Maschinen und Anlagen eine immer bedeutendere Rolle ein. Obwohl Maschinen bereits in der Vergangenheit über ein hohes Maß an Sicherheit verfügten, entwickelt sich die Sicherheitstechnik mit den steigenden Anforderungen an Effizienz und Produktivität ständig weiter. Die Maschinenrichtlinie leistet dazu einen großen Beitrag. In den folgenden drei Kapiteln wird auf die Mechanik, Pneumatik und Hydraulik eingegangen. Alle drei Antriebstechniken sind allerdings immer auch in ihrer Verknüpfung zur elektrischen Konstruktion zu betrachten.

8.2 Mechanische Konstruktion

8.2.1 Einleitung

Ingenieure und Konstrukteure haben schon immer gute Arbeit geleistet. Wie sonst wäre das heute beachtliche sicherheitstechnische Niveau von Maschinen und Anlagen erklärbar? Der erhebliche Wirbel um die EG-Maschinenrichtlinie (MRL) hat eigentlich keine (sicherheits-)technische Grundlage. Er beruht vielmehr auf der Tatsache, dass jemand aus der Firmenleitung mit seinem guten Namen dafür bürgen muss, dass die ausgelieferte Maschine tatsächlich über die notwendige und geforderte Sicherheit verfügt und dies darüber hinaus im Fall eines Rechtsstreits auch nachweisbar sein muss (Stichworte Dokumentation und Betriebsanleitung). Dennoch muss man sich über eines stets im Klaren sein: Perfekt sind unsere Maschinen noch immer nicht, wenn sie auch ständig besser werden. Denn Evolution in der Sicherheitstechnik bedeutet nicht die Realisierung völlig neuer Lösungen, ganz im Gegenteil: Unzulänglichkeiten sind der Antrieb zur Verbesserung und Irrtümer die Voraussetzung für ihre Korrektur!

Zur Begriffsbestimmung: Zuverlässigkeit und Sicherheit werden im allgemeinen Sprachgebrauch oft nicht scharf getrennt. Das rührt daher, dass beide Begriffe einige Gemeinsamkeiten haben: Sie beziehen sich auf zukünftige Ereignisse und haben Wahrscheinlichkeitscharakter. Aus Sicht der Arbeitssicherheit und des damit verknüpften sicherheitsgerechten Konstruierens sind beide Begriffe mit Ausschluss-Definitionen gegeneinander abzugrenzen:



Grundregeln zum Konstruieren erfolgreicher Produkte

8.2 Mechanische Konstruktion

Wenn ein Bauteil (aber auch eine Baugruppe, Maschine oder Anlage) die zugedachte Funktion unter Einhaltung vorher definierter Randbedingungen nicht erfüllt, gilt es als unzuverlässig. Verursacht ein Bauteil (aber auch eine Baugruppe, Maschine oder Anlage) einen Unfall mit Körperschaden, ist bzw. war es nicht sicher. Was unter „zuverlässig“ und „sicher“ zu verstehen ist, kann man aus dem Umkehrschluss herleiten. Es ist die logische Konsequenz aus dem Unfallgeschehen, dass man nur dann sinnvoll von Sicherheit (Unsicherheit) sprechen kann, wenn bei sämtlichen diesbezüglichen Betrachtungen technischer Systeme und deren Konstruktion auch der Mensch lebensnah mit all seinen Unzulänglichkeiten als untrennbare Komponente eines Arbeitssystems betrachtet wird.

8.2.2 Gefahr, Gefährdung, Risiko

Die EG-Maschinenrichtlinie legt in ihrem Anhang I als Basis für das Konstruieren sicherheitsgerechter Maschinen verbindlich fünf Schritte fest:

1. Festlegung der Grenzen der Maschine einschließlich der bestimmungsgemäßen Verwendung und in vernünftiger Weise voraussehbarer Fehlanwendungen
2. Systematisches Ermitteln potenzieller Gefahren in der Konstruktion und sich daraus ergebender Gefährdungssituationen
3. Abschätzen der gefährlichen Situationen beim Arbeiten mit oder an der Maschine (Risikoanalyse)
4. Beurteilung der mit den Gefährdungen verbundenen Risiken und ob eine Risikominderung erforderlich ist
5. Realisierung und Dokumentation aller Sicherheitsmaßnahmen zur Risikobeherrschung

Zur Begriffsbestimmung: Gefahren sind, objektiv betrachtet, ein vorhandenes energetisches oder stoffliches Potenzial, das relevante Grenzwerte des Menschen überschreitet und von sich aus zu unterschiedlich schweren gesundheitlichen Beeinträchtigungen oder Schäden führen kann.

Gefährdungen treten auf, sobald die Möglichkeit besteht, dass Menschen mit den Gefahren räumlich und zeitlich zusammentreffen und daraus eine unerwünschte Situation eintreten kann. Die während der Gefährdung ablaufenden Effekte unterliegen unerbittlichen Naturgesetzen.

Der Begriff Risiko erfordert eine neue Denkweise. Er steht für die mit unterschiedlicher Häufigkeit auftretenden Auswirkungen von Gefährdungen auf Menschen oder Umwelt. Die Auswirkungen können unterschiedlich gravierend sein. Die Höhe des Risikos wird noch von der Möglichkeit oder Unmöglichkeit technischer oder organisatorischer Gegenmaßnahmen bestimmt. Aussagen zu Risiken sind kalkulierte Prognosen möglicher zukünftiger Ereignisse, also Ergebnisse menschlicher Überlegungen und folglich keine umgesetzten Naturgesetze.

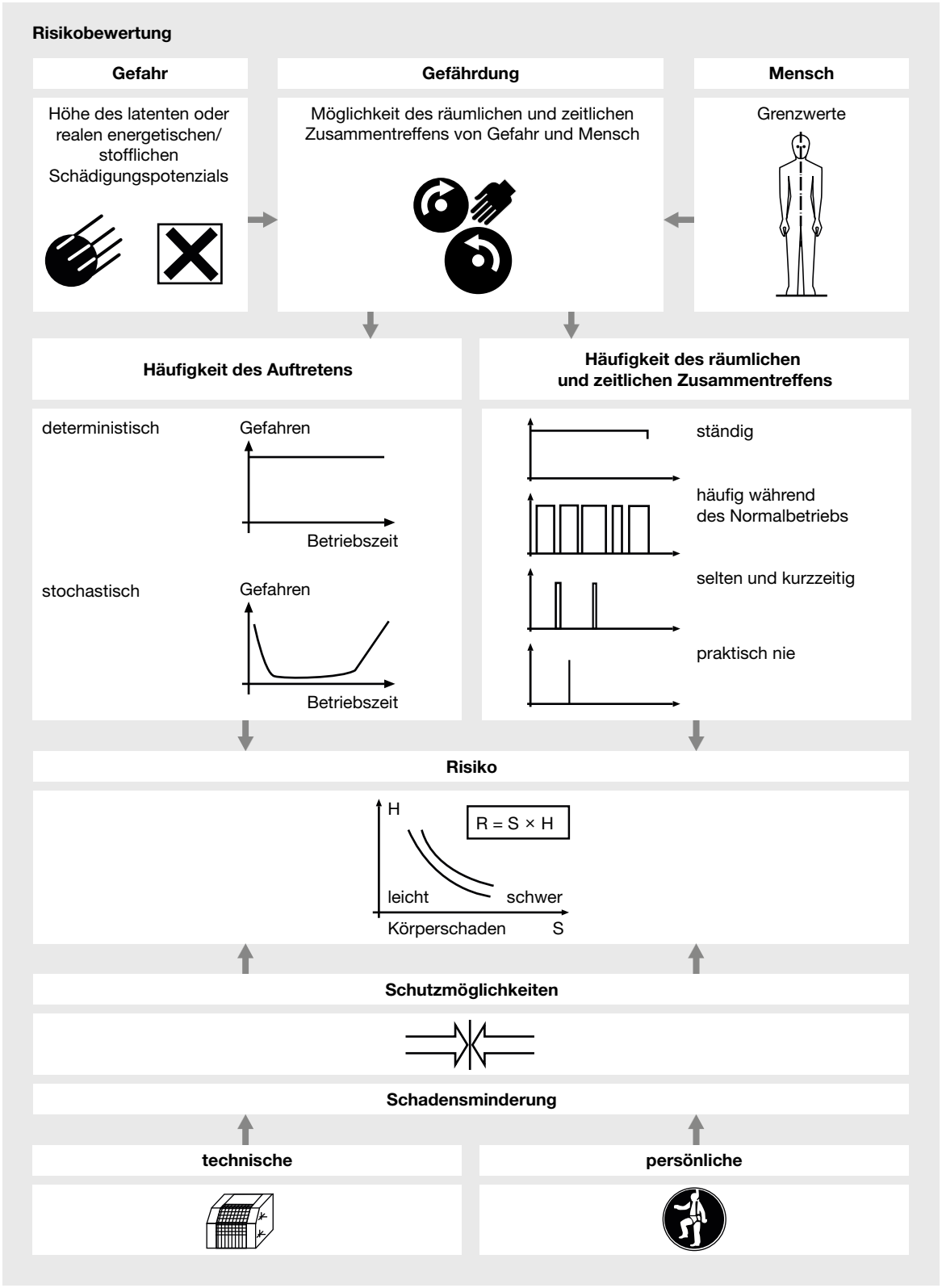
Für Konstrukteure ist wichtig zu wissen, dass Ursachen von Gefahren in den Wirkgrößen Stoff, Energie und Information liegen. Größen also, mit denen sie im Konstruktionsprozess operieren und daher sichere Zustände mit den gleichen Methoden erreichen können, mit denen sie funktionstüchtige technische Systeme gestalten.

Stoffe können nicht nur wegen ihrer chemischen oder biologischen Eigenschaften gefährlich werden. Auch aufgrund ihrer Eigenschaft als raumfüllende Materie (Geometrie) im Schwerefeld der Erde können sie Menschen beeinträchtigen: immer dann, wenn das geometrische Layout der Maschine zu erzwungenen Körperhaltungen führt oder wenn schwere Lasten von Hand getragen bzw. transportiert werden müssen (Beanspruchung der Wirbelsäule).

Energie: Jede Maschine braucht für ihre technologische Funktion Energie. Alle Energien, die zur Erfüllung der Arbeitsaufgabe benutzt werden, können Menschen gefährden, sobald sie unkontrolliert auf den Mensch wirken und dabei bestimmte Energiedichten überschreiten.

Informationen: Ungünstig gestalteter Informationsfluss zwischen Mensch und Maschine sowie der Randbedingungen können Verhalten hervorrufen, mit dem sich Maschinennutzer selbst oder andere gefährden. Die Grundgröße Information impliziert in diesem Zusammenhang, dass die Sicherheit der Menschen in Arbeitssystemen von den naturgegebenen Gesetzmäßigkeiten der Informationsverarbeitung und vom Verhalten der Menschen abhängen wird. Da in den Maschinen die Grundgrößen Stoff, Energie und Informationen genutzt werden, können auch nur von diesen Größen Gefahren ausgehen.

8.2 Mechanische Konstruktion



Zusammenhang der Risikobewertung

8.2 Mechanische Konstruktion

Wirkgröße	Wirkung	Beispiele		
1	2	Nr.	3	4
Stoff	räumliche Disposition	1		erzwungene Körperhaltungen, unerreichbare Funktionselemente
	physische Belastungen	2		Handhabung von Lasten, hohe Betätigungskräfte, hohe Taktzahl
	physikalische Einwirkungen	3		Lufttemperatur, Luftzug, Luftfeuchtigkeit, Über- oder Unterdruck
	biologische Einwirkungen	4		Pilzkulturen, Bakterien in der Atemluft, verunreinigte oder verkeimte Luftfilter
	chemische Einwirkungen	5		ätzende, giftige, gesundheitsschädigende, reizende Stoffe
	thermische Einwirkungen	6		hohe und tiefe Umgebungs- und Berührungstemperaturen, Feuer
Energie	Explosionen	7		chemische Explosionen (feste Stoffe, Dämpfe, Gase), physikalische Explosionen
	mechanische Einwirkungen	8		Absturzstellen, Gefahrquellen, Gefahrstellen, Kollisionen, Stoßstellen
	Lärm, Vibrationen	9		Schallemissionen, Handschwingungen, Ganzkörperschwingungen
	elektrische Einwirkungen	10		elektrostatische Aufladungen, Körperdurchströmungen, Lichtbogen
	elektromagnetische Felder	11		elektromagnetische Felder, magnetische Felder
	Strahlung	12		elektromagnetische Wellen, IR-, UV-Strahlung, Laser, ionisierende Strahlung
Information	Informations-darbietung	13		mangelhafte Gestaltung der Anzeigen, der Bedienteile oder deren Kompatibilität
	Licht-verhältnisse	14		Beleuchtungsstärke, Blendung, Lichtfarbe, Leuchtdichteverteilung
	psychomentale Belastung	15		missverständliche Betriebs- und Arbeitsanweisungen, Softwareergonomie
	Mängel in der Organisation	16		nicht durchdachte, falsch abgestimmte Betätigungsfolgen
	Hektik, Stress, Schock	17		Fehlbetätigungen, Kurzschlussreaktionen, Verwechslungen

Gefahren beim Umgang mit Maschinen

8.2 Mechanische Konstruktion

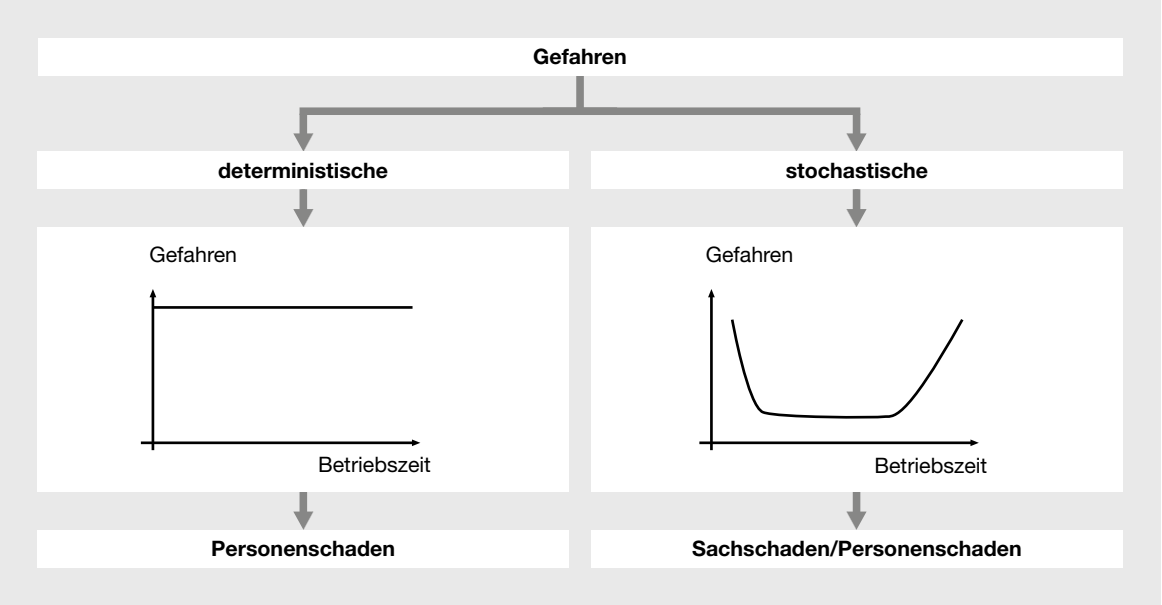
8.2.2.1 Mechanische Gefahren

Das grundlegende Unterscheidungsmerkmal bezieht sich auf die Art der mechanischen Energie (kinetische, potenzielle) sowie weiterhin auf die Frage, woran die Energie gebunden ist (Gegenstände oder Menschen) und welche Bewegungen einem möglichen Unfall vorangehen werden (kinematisch gebundene oder freie Bewegungen).

Gefährdungen: Zu Gefährdungen kommt es dann, wenn potenzielle Gefahren und Menschen räumlich und zeitlich zusammentreffen. Hier gibt es zwei Arten: stochastische (zufallsbedingte) und deterministische (vorbestimmte) Gefährdungen.

Deterministische Gefährdungen: Diese sind im funktionellen Aufbau der Maschine begründet, z. B. durch technologisch notwendige Gefahrenstellen an Werkzeugen mit ihren Sollbewegungen. Solche Gefährdungen sind latent während der ganzen Lebensdauer der Maschine mit einer gleichbleibend hohen Wahrscheinlichkeit vorhanden. Ein Unfall an virulenten Gefahrstellen ist deshalb nur eine Frage der Zeit, sofern ihnen nicht konstruktiv entgegengewirkt wird. Deterministische mechanische Gefahrstellen bilden immer noch den Schwerpunkt aller Maschinenunfälle, weil ihre zerstörerische Wirkung sowohl von den Konstrukteuren als auch von den Betroffenen unterschätzt wird. Im Unterschied zu stochastischen Gefahren sind Gefahrstellen nach einiger Übung von jedem technisch interessierten Menschen mit bloßem Auge erkennbar, sowohl in Zeichnungen und CAD-Darstellungen als auch an fertigen Maschinen. Es ist ein besonderer Vorteil, dass Konstrukteure ihnen heute mit relativ einfachen Mitteln entgegenwirken können.

Stochastische Gefährdungen treten während der Lebensdauer einer Maschine mit einer zeitabhängigen Wahrscheinlichkeit auf. Am häufigsten visualisiert mit der Badewannenkurve, obwohl diese genau genommen nur für wenige Baugruppen oder Bauteile gilt. Diese Gefährdungen bzw. deren Ursachen lassen sich nur selten unmittelbar erkennen und, wie spektakuläre Unfälle leider immer wieder belegen, praktisch nicht zuverlässig voraussagen.



Deterministische und stochastische Gefahren

8.2 Mechanische Konstruktion

8.2.2.2 Risikobeurteilung

Auf dem Markt und im Schrifttum gibt es heute mehr als 80 Verfahren zur Risikobeurteilung, Tendenz steigend. Keines davon ist aber (rechts-) verbindlich. Die Maschinenrichtlinie verweist zwar auf einige harmonisierte Normen zur Maschinensicherheit (EN ISO 13849, EN ISO 12100, IEC 61508 bzw. EN 62061), deren Umsetzung bereitet aber in der Praxis immer noch erhebliche Schwierigkeiten. Und daran sind nicht allein die Konstrukteure schuld: Ohne entsprechende Ausbildung sollen sie aus mehreren Wahrscheinlichkeitsaussagen verbindliche Maßnahmen für mehr Ereignisse herleiten, als eintreten werden. Zurzeit wird folgende Definition technischer Risiken allgemein akzeptiert:

Risiko ist keine Naturgesetzmäßigkeit, sondern eine Wahrscheinlichkeitsaussage (Prognose) über Auswirkungen von Gefährdungen auf Mensch bzw. Umwelt in einer fest umrissenen Sachlage. Risiken werden ermittelt aus der Kombination der Häufigkeit und des Schweregrades möglicher Verletzungen, Gesundheits- oder Sachschädigungen sowie der Möglichkeit oder Unmöglichkeit technischer, organisatorischer oder personenbezogener Schutz- oder Abwehrmaßnahmen. Das Ergebnis der Risikobeurteilung bestimmt letztlich Anforderungen an die Zuverlässigkeit der durch die sicherheitsrelevanten Teile der Steuerung zu erfüllenden Sicherheitsfunktionen. Das bezieht sich auch auf die zuverlässige Funktionserfüllung trennender Schutzeinrichtungen.

8.2.3 Festlegen und Umsetzen von Sicherheitsmaßnahmen

Maschinenhersteller sind verpflichtet, ihren Kunden nur sichere Produkte auf dem europäischen Binnenmarkt anzubieten. Sie müssen deshalb vorab alle mit der Maschine verbundenen Gefährdungen ermitteln und die von ihnen ausgehenden Risiken bewerten. Mit den Erkenntnissen aus der Risikoanalyse und der Risikobewertung müssen Hersteller ihre Maschinen so konstruieren, dass sie weder ihre Benutzer, andere Menschen noch die Umwelt schädigen können. Mit anderen Worten: Die Maschinen müssen sicher sein.

Der Begriff „sicher“ wird von vielen gerne benutzt, gehört doch das Gefühl der Sicherheit zu den wichtigsten menschlichen Grundbedürfnissen. Die Werbe- und Versicherungswirtschaft, aber auch die Politik verstehen es vorzüglich, dieses Grundbedürfnis anzusprechen und für ihre Belange auszunutzen. In der Technik wird unter „sicher“ oft das Erfüllen maschineller Funktionen über einen festgelegten Zeitraum verstanden. Damit wird aber Zuverlässigkeit angesprochen, hier müssen wir präzisieren: Unter Sicherheit im eigentlichen Sinne verstehen wir das Freisein von potenziellen und realen Gefahren für Mensch und Umwelt. Sicherheit und Zuverlässigkeit haben viele Gemeinsamkeiten: Beide beschreiben ein zukünftiges Verhalten der Maschine und sind daher Wahrscheinlichkeitsaussagen.

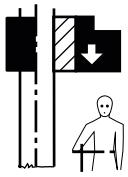
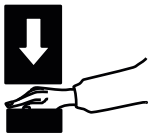
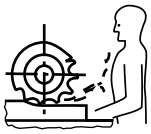
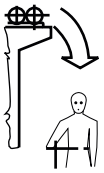
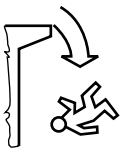
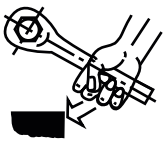
Das oberste Gebot beim sicherheitsgerechten Konstruieren: Alle Gefährdungsarten müssen konstruktiv angegangen werden! Die dazu notwendigen Konstruktionsmaßnahmen müssen sowohl den unvorhersehbaren stochastischen als auch deterministischen Gefährdungen entgegenwirken. Die unterschiedlichen Wirkungsweisen beider Gefährdungsarten bedingen auch unterschiedliche Konstruktionsmethoden.

Bei der Wahl der Konstruktionsmethoden muss Folgendes beachtet werden:

1. Grundsätzlich müssen vorhandene Risiken mit konstruktiven Maßnahmen so weit herabgesetzt werden, dass ein individuell und gesellschaftlich tolerierbares Restrisiko erreicht wird (das aber eintreten kann und dann auch akzeptiert werden muss).
2. Da sich stochastische und deterministische Gefährdungen wesentlich voneinander unterscheiden, ist es nur logisch, dass sich auch die gegen sie gerichteten Maßnahmen voneinander unterscheiden müssen.

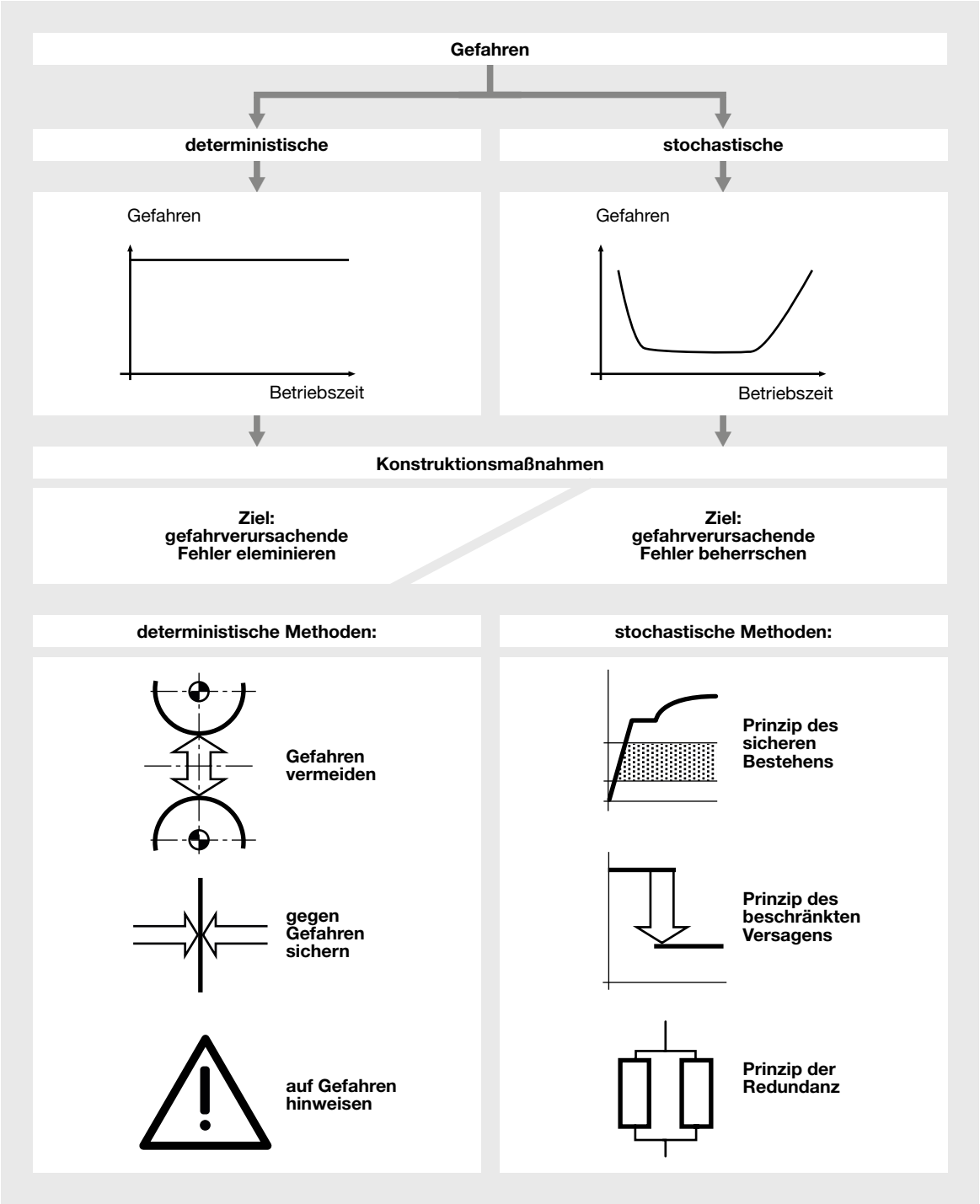
Erklärung:
- stochastisch: von Zufällen beeinflusste Gefährdungen, deren Gefahrenpotenzial nicht exakt vorhergesagt werden kann, d. h. einer Wahrscheinlichkeit unterliegt
- deterministisch: Gefährdungen mit einem konstanten Gefahrenpotenzial, das zu jeder Zeit in gleicher Höhe existiert

8.2 Mechanische Konstruktion

Art der Energie	Träger der Energie	Bewegung	Abbildung		Gefährdung durch
1	2	3	Nr.	4	5
potenzielle Energie	Gegenstände	Bewegung in festgelegten Bahnen	1		Gefahrstellen an kontrolliert bewegten Teilen: Gefahr ist an einen bestimmten Ort gebunden.
kinetische Energie			2		
		freie Bewegung	3		Gefahrquellen durch unkontrolliert bewegte Teile: Gefahr geht von einem bestimmten Ort aus.
potenzielle Energie			4		
	Personen, Körperteile		5		Absturzstellen
kinetische Energie			6		Anstoßstellen
		Bewegung in festgelegten Bahnen	7		
			8		Trägheitskräfte

Grundlegende mechanische Gefahren

8.2 Mechanische Konstruktion



Wichtige Konstruktionsmaßnahmen zur Gefahrenabwendung

8.2 Mechanische Konstruktion

8.2.3.1 Konstruktionsmaßnahmen gegen stochastische Gefährdungen

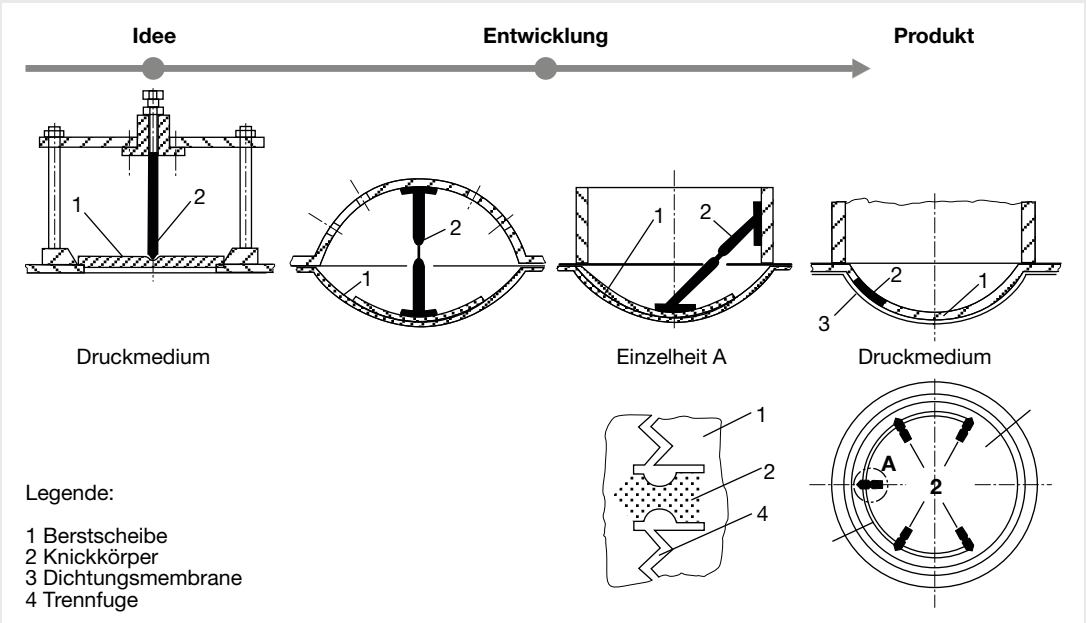
Stochastische Gefährdungen lassen sich vor allem auf Bauteilausfälle oder Softwarefehler zurückführen. Sie berühren zwar die Zuverlässigkeit von Maschinen, können bzw. müssen aber nicht die Sicherheit von Menschen beeinträchtigen. Die gegen sie gerichteten Konstruktionsmaßnahmen verfolgen das Ziel, die zeitabhängige Wahrscheinlichkeit zu erhöhen, dass Maschinen innerhalb einer vereinbarten Betriebsdauer die ihnen zugedachte Funktion erfüllen und störfest gegenüber zufälligen Bauteilausfällen bleiben. Somit können sie weder Menschen noch Umwelt schädigen. Die bekanntesten Konstruktionsmaßnahmen sind:

- Prinzip des sicheren Bestehens (Safe life)
- Prinzip des beschränkten Versagens (Fail safe)
- Prinzip der Redundanz

Maßnahmen des **Safe-life-Prinzips** gehen davon aus, dass die Maschine während der zugesicherten Lebensdauer durch ausreichende Dimensionierung und funktionsgerechte Gestaltung so funktioniert, wie es vorgesehen ist: ohne Störungen, Ausfälle und Gefahren. Von besonderer Bedeutung ist dieses Konstruktionsprinzip bei Sicherheitseinrichtungen wie z. B. bei Berstscheiben. Bei der dargestellten Ausführung wurde das äußerst zuverlässige Prinzip des Knickstabs umgesetzt.

Die Anwendung dieses Prinzip setzt voraus, dass

1. alle Beanspruchungen, die auf die Maschine zukommen werden, bekannt sind,
2. die angewendeten Berechnungsmethoden und das angenommene Werkstoffverhalten der Realität entsprechen,
3. während der Lebensdauer der Maschine keine anderen Einflüsse als die in der Berechnung berücksichtigten auftreten werden.

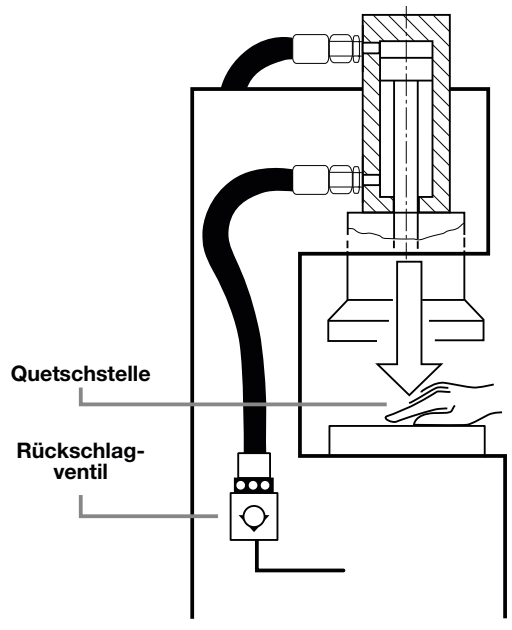
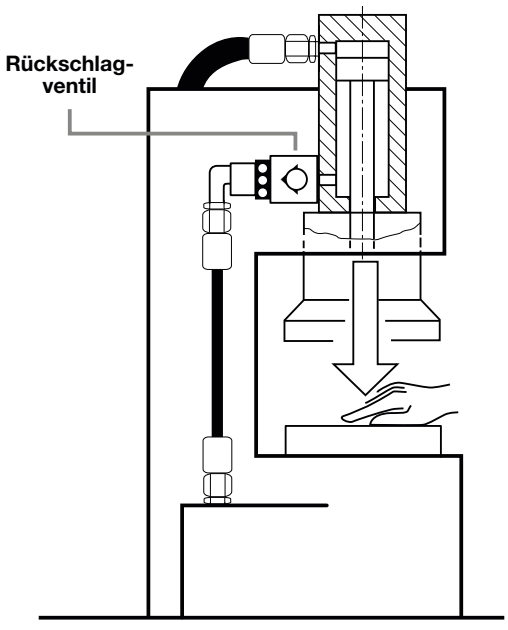


Berstscheibe mit stabilem Vorhalten (Knickstabumkehr-Berstscheibe)

8.2 Mechanische Konstruktion

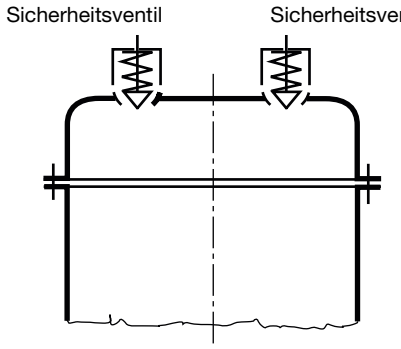
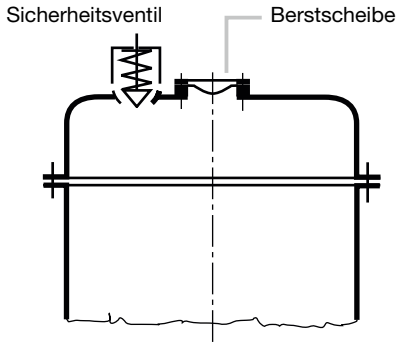
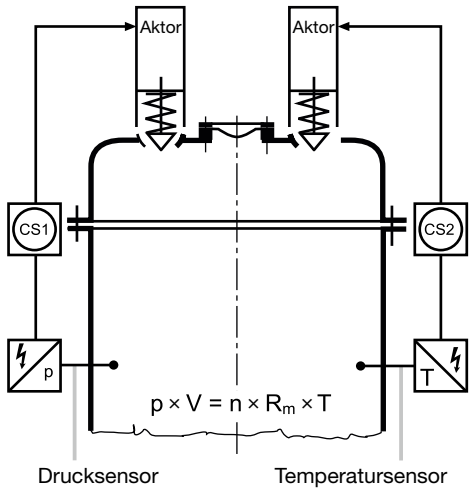
Lebensnah betrachtet lässt sich keine dieser Voraussetzungen garantieren. Deshalb ist es ratsam, einen anderen Weg einzuschlagen. Das **Fail-safe-Prinzip** lässt bewusst Fehler zu. Die Systeme sind aber so konzipiert und gestaltet, dass ein sicherheitstechnischer Absturz nicht ins Bodenlose führt, sondern auf einem vereinbarten Niveau stehen bleibt. Auf Fehler – und das gilt nur für bekannte bzw. erkennbare und vorhersehbare Fehler – reagieren die Systeme so, dass sie zur sicheren Seite „fallen“. Das setzt voraus, dass in diesem System für diese Funktion nicht erst im Falle des Falles Energie zugeführt werden darf, sondern dass schon vorab immer genügend Energie gespeichert sein muss. Diese wird im Gefahrenfall abgebaut und das System in einen energiearmen und somit stabilen Zustand überführt. Zur Verwirklichung dieses Prinzips lassen sich oft Effekte ausnutzen, die immer vorhanden sind, wie beispielsweise die Gravitations- oder Reibungskräfte und die mit ihnen erreichbare Selbsthemmung.

In **redundanten Systemen** sind zur Erfüllung der Funktion mehr Baugruppen vorgesehen, als eigentlich notwendig wären. Man geht davon aus, dass im Falle des Versagens oder Ausfalls einer dieser Baugruppen die andere deren Funktion vollständig übernimmt. Hier gilt der Grundsatz, mit einem Minimum an Redundanz möglichst viel Zuverlässigkeit zu erreichen. So einsichtig das Prinzip auch ist, es hat jedoch einen entscheidenden Schwachpunkt: Die Erfahrung zeigt, dass es immer wieder Situationen gibt und auch künftig geben wird, in denen alle redundanten Komponenten gleichzeitig aufgrund eines Fehlers gleicher Ursache versagen. Diese Situationen lassen sich nur sehr schwer voraussagen und konstruktiv beherrschen. Die besten Ergebnisse zeigt eine konsequente, aber teure Diversität, insbesondere bei der physikalischen Diversität.

ungünstig	günstig
	
Nach Versagen der Schlauchleitung entweicht das Medium vor dem Rückschlagventil. Werkzeug senkt sich unkontrolliert ab.	Nach Versagen der Schlauchleitung verhindert das gesteuerte Rückschlagventil das Zusammenbrechen der Flüssigkeitssäule. Werkzeug bleibt oben.

Schlauchleitung mit Rückschlagventilen

8.2 Mechanische Konstruktion

Redundanz		Beispiel	Erläuterungen
1	Nr.	2	3
homogene	1		Verdoppelung erhöht die Sicherheit nur dann, wenn keine systematischen Fehler auftreten können, z. B. Korrosion, Materialverwechslung, die beide Sicherheitseinrichtungen gleichzeitig unwirksam machen können.
diversitäre (Bauteile)	2		Diversität im Wirkprinzip der Sicherheitsrichtung: Wechsel des Wirkprinzips macht ein gleichzeitiges Versagen der prinzipverschiedenen, gegenseitig unabhängigen Sicherheitseinrichtungen unterschiedlicher Hersteller unwahrscheinlich.
diversitäre (Prozessgrößen)	3		Diversität im physikalischen Prinzip: Jedes der zwei diversitär konstruierten gesteuerten Ventile wird von den Steuerungen CS1 bzw. CS2 aktiviert, die bei Grenzwertüberschreitung zweier über ein physikalisches Gesetz (z. B. allg. Zustandsgleichung) gekoppelter Prozessgrößen reagieren.

Homogene und diversitäre Redundanz

8.2 Mechanische Konstruktion

8.2.3.2 Konstruktionsmaßnahmen gegen deterministische Gefährdungen

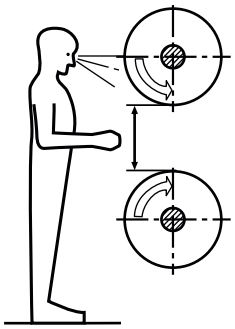
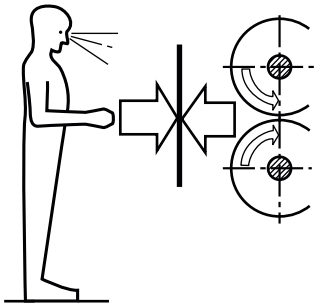
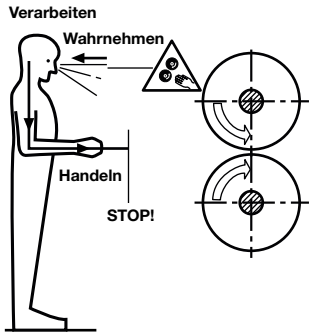
Deterministische Gefährdungen lassen sich auf den technologisch notwendigen funktionellen Aufbau der Maschinen und die eingesetzten Verfahren zurückführen. Die gegen sie gerichteten Konstruktionsmaßnahmen wollen verhindern, dass sich latente Gefahren auf Menschen auswirken können. Im Laufe des technischen Fortschritts hat man dazu drei Methoden entwickelt

1. unmittelbare Sicherheitstechnik
2. mittelbare Sicherheitstechnik
3. hinweisende Sicherheitstechnik

Im Unterschied zu den Maßnahmen gegen stochastische Gefährdungen, die grundsätzlich als gleichwertig angesehen werden, ist in der EG-Maschinenrichtlinie für die Anwendung der jeweiligen Maßnahmen gegen deterministische Gefährdungen die Reihenfolge und Priorität

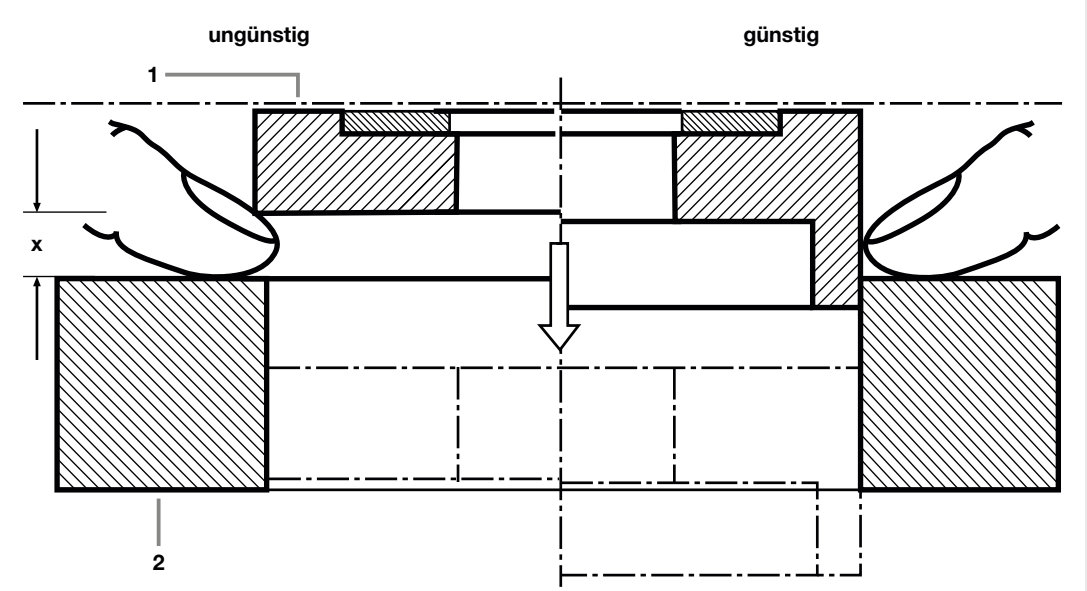
1. unmittelbar
2. mittelbar
3. hinweisend

verbindlich vorgeschrieben.

Methoden der Sicherheitstechnik			
Sicherheitstechnik	unmittelbare	mittelbare	hinweisende
Wirkprinzip	Gefahren vermeiden	gegen Gefahren sichern	vor Gefahren warnen
Schema			
Maßnahmen (EG-Maschinenrichtlinie, EN ISO 12 100)	Beseitigung oder Minimierung von Gefahren	Ergreifen von notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Gefahren	Unterrichten der Benutzer über Restgefahren

Methoden der Sicherheitstechnik

8.2 Mechanische Konstruktion



Konstruktiv vermiedene Scherstelle

8.2.3.2.1 Unmittelbare Sicherheitstechnik

Methoden der unmittelbaren Sicherheitstechnik versuchen, Baugruppen, Maschinen und Prozesse so zu gestalten, dass von ihnen keine oder nur geringe, akzeptierte Risiken für Menschen ausgehen. Dazu stehen geometrische und energetische Maßnahmen zur Verfügung.

Geometrische Maßnahmen versuchen, die gefährliche Wirkung von Gefahrstellen an bewegten Maschinenteilen zu vermeiden, indem man gefährliche Engstellen durch Einhalten genormter Mindestabstände gar nicht erst aufkommen lässt oder sie durch Einhalten von Sicherheitsabständen unerreichbar macht.

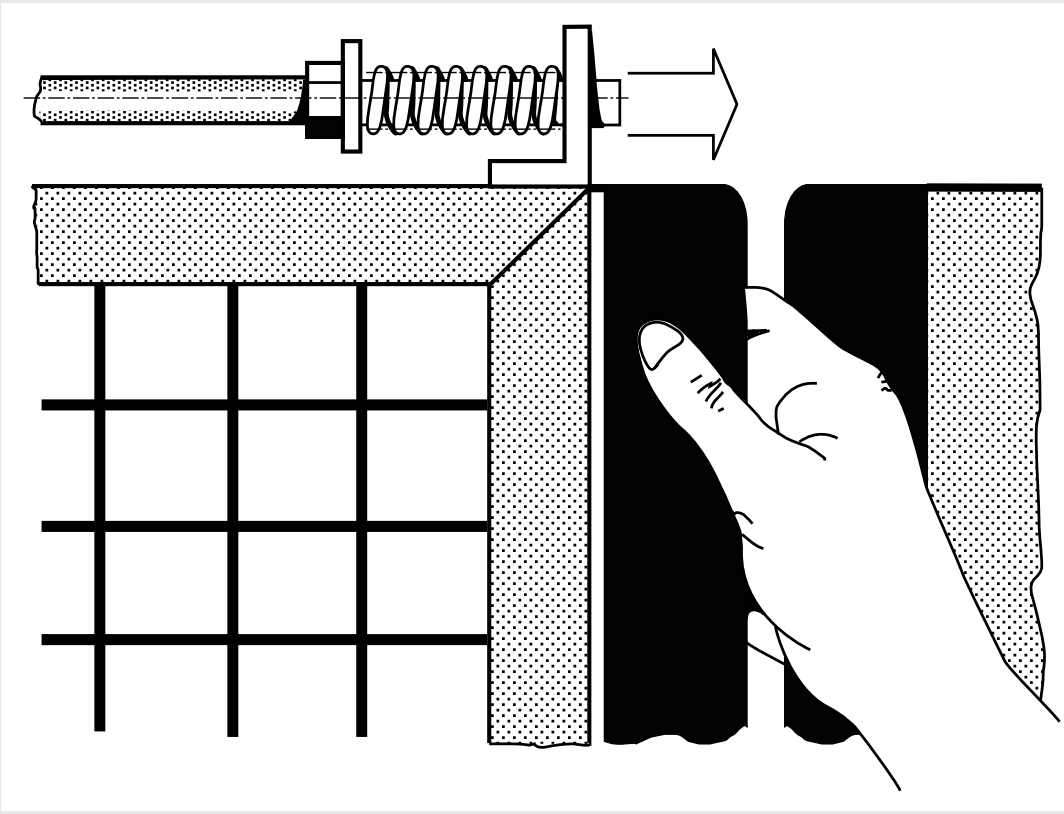
Energetische Maßnahmen versuchen, die den Gefährdungen zugrunde liegenden Energien sich nicht schädigend auf Menschen auswirken zu lassen, und zwar durch:

- Begrenzen der wirksamen Energien
- Unterbrechung des Energieflusses zum Menschen hin
- zielgerichtete Verformung der Maschinenteile statt des menschlichen Körpers

Die erste Maßnahme versucht, die in einer Gefahrstelle aufkommenden Energien und Kräfte so zu begrenzen, dass ihre Auswirkung unterhalb verträglicher physiologischer Werte bleibt. Ein solches Energieniveau ist aber technologisch in der Regel nur beschränkt nutzbar. Die zweite Maßnahme verhindert die schädigende Wirkung auf Menschen, indem sie den Energie- oder Kraftfluss in Richtung des menschlichen Körpers noch vor dem Erreichen der Schmerzgrenze unterbricht. Die dritte Maßnahme setzt die Steifigkeit der Maschinenteile so weit herab, dass beim Eingriff in eine Gefahrstelle sich Maschinen-, nicht aber Körperteile verformen.

Vorsicht ist jedoch geboten: Die unmittelbare Sicherheitstechnik, oft als Königsweg propagiert, lässt sich nicht auf Gefahrstellen mit technologischen Funktionen anwenden. Deren Gefahren sind mit besonderen Maßnahmen wie beispielsweise Schutzeinrichtungen zu sichern.

8.2 Mechanische Konstruktion



Elastische Schließkanten an Schutzeinrichtungen

8.2.3.2.2 Mittelbare Sicherheitstechnik

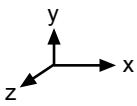
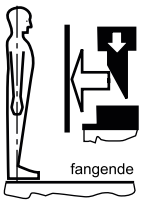
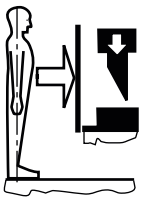
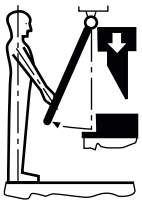
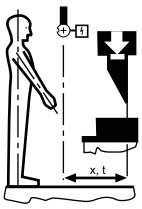
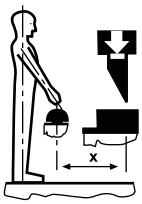
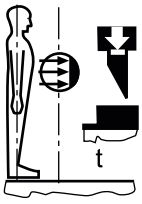
Baugruppen der mittelbaren Sicherheitstechnik sichern Gefahren, die zur Funktion der Maschinen notwendig sind und sich daher nicht vermeiden lassen. Schutzeinrichtungen sind zwischen Mensch und Gefahr angeordnet. Sie unterbrechen die Möglichkeit des räumlichen und zeitlichen Zusammentreffens. Dazu werden trennende oder nicht trennende Schutzeinrichtungen verwendet.

Trennende Schutzeinrichtungen, z. B. Schutzgitter oder Hauben, bilden materielle Barrieren, die den Zutritt bzw. Zugriff zu gefährlichen Situationen mit ihrer Undurchdringlichkeit vermeiden. Zusätzlich können sie verhindern, dass Menschen von Gegenständen getroffen werden, die aus den geschützten Bereichen herausgeschleudert werden.

Nicht trennende Schutzeinrichtungen, z. B. Zweihandschaltungen oder Lichtschranken, verhindern zwar nicht den Zugriff und Zutritt zu gefährlichen Situationen, machen diese aber sicher, indem sie über die Steuerung der Maschine auf den Bearbeitungsprozess einwirken, sobald sie aktiviert werden.

Ergonomische Gesichtspunkte entscheiden über die Handhabbarkeit und damit über die Akzeptanz von Schutzeinrichtungen. Die wichtigste ergonomische Anforderung besteht darin, dass die Beschäftigten beim täglichen Hantieren mit der Schutzeinrichtung nicht mehr als notwendig behindert werden dürfen.

8.2 Mechanische Konstruktion

Schutz gegen	Unterbrechung des Wirk-zusammenhangs	Wirkung durch	Schema		Benennung	Beispiele	Erläuterungen
1	2	3	Nr.	4	5	6	7
Gefahrquellen 	räumlich 	ruhende materielle Sperren 	1		feststehende trennende Schutz-einrichtung	Fanghauben, Schutzauf-bauten an Erdbau-Maschinen (ROPS, FOPS)	Schutzeinrichtungen halten die sich unkon-trolliert bewegenden Teile zurück, absorbieren deren kinetische Energie und verhindern, dass sie Personen erreichen.
			2			Verkleidungen, Verdeckungen, Umzäunungen	Schutzeinrichtungen trennen in der Schutz-stellung materiell Gefahr-stellen vom Arbeits- und Verkehrsbereich. Personen können Gefahrstellen nicht erreichen.
Gefahrstellen 	räumlich und zeitlich 	bewegte materielle Sperren 	3		abweisende Schutz-einrichtung	Finger-abweiser, Hand-abweiser	Schutzeinrichtungen sind kinematisch mit gefahrbringenden Bewegungen gekoppelt. Sie entfernen form-schlüssig Personen aus Gefahrenbereichen.
		bewegte materielle Sperren 	4		verriegelte bzw. zugehaltene bewegliche trennende Schutz-einrichtung	mit Positions-schaltern überwachte Verkleidungen, Umzäunungen	Öffnen der Schutzein-richtung unterbricht die gefahrbringende Bewegung und hebt die materielle Trennung der Gefahrstelle von Menschen auf. Seine Sicherheit hängt jetzt von der zuverlässigen Funktion sicherheitsrelevanter Teile der Steuerung ab.
	zeitlich 	zuverlässige steuerungs-technische Maßnahmen 	5		ortsbindende Schutz-einrichtung	Zustimm-schalter, Tippschalter, Zweihand-schaltungen	Schutzeinrichtungen binden während der gefahrbringende Bewegung Personen an einen sicheren Ort, von dem aus sie Gefahrstellen nicht erreichen können. Beim Verlassen des sicheren Ortes stoppt die gefahr-bringende Bewegung.
			6		Schutz-einrichtung mit Annähe-rungsreaktion	optoelek-tronische kapazitive Sensoren, Schaltleisten Trittschalt-matten, Lichtgitter, Scanner	Schutzeinrichtungen verhindern Gefährdungen durch Unterbrechen gefahrbringender Bewegungen, sobald Personen sichere Grenzen überschreiten und sie sich der Gefahrstelle nähern.

Grundtypen von Schutzeinrichtungen

8.2 Mechanische Konstruktion

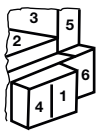
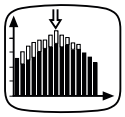
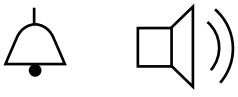
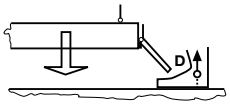
8.2.3.2.3 Hinweisende Sicherheitstechnik

Die hinweisende Sicherheitstechnik, als letzte Möglichkeit zur Bekämpfung deterministischer Gefährdungen, versucht mit ihren Methoden wie z. B. mit Sicherheitsschildern, Sicherheitshinweisen in Betriebsanleitungen, betriebsinternen Unterweisungen beim Maschinenbenutzer usw. bei gefährdeten Personen durch gezielte Botschaften und Informationen ein sicherheitsgerechtes Verhalten zu bewirken. Die Effektivität der Methode ist in den einzelnen Ländern sehr unterschiedlich. Kann man mit ihr in anderen Kulturkreisen durchaus beachtliche Erfolge erzielen, sollte man sich in europäischen Ländern aber nicht unbedingt auf sie verlassen. Aufgrund unterschiedlicher Mentalitäten in der Bevölkerung müssen zwangsläufig wirkende technische Sicherheitsmaßnahmen, die Gefahren verhindern oder sichern, Vorrang haben.

Es wird so gut wie unmöglich sein, eine Maschine mit akzeptiertem Risiko mit nur einer einzigen der hier aufgezählten Konstruktionsmaßnahmen zu bauen. Maßnahmen mit ihren unterschiedlichen Methoden müssen vielmehr aufeinander abgestimmt sein, um sich zu ergänzen und funktionell und in ihrer Summe zu wirken.[1)]

[1)] *Quelle: Neudörfer A.: Konstruieren sicherheitsgerichteter Produkte, 5. Auflage, Heidelberg, Berlin, New York u. a., Springer, 2013*

8.2 Mechanische Konstruktion

Informationsparameter			Beispiel	
Kanal	**Verlauf**	**Träger**		
1	2	3	Nr.	4
visuell	statisch	Text	1	Betriebsanleitung 
			2	**Schweißarbeiten Augen gefährdet**
		Bildzeichen	3	 Stopp, Anhalten einer Bewegung Schnellstopp **ISO 7000**
		Sicherheits-zeichen	4	
		Markierung	5	 Farbkombination: gelb-schwarz (permanente Gefahr) rot-weiß (temporäre Gefahr)
	dynamisch	Lichtsignale	6	
		aktive Schemata	7	 **1** • Hauptmotor **2** • Einführtisch offen **3** • Haube offen **4** • keine Druckluft **5** • Folie gebrochen **6** • Magazin leer
		Prozess-visualisierung, Simulation	8	
auditiv		akustische Signale	9	
taktil		bewegte Gegenstände	10	ausweichende Schutzeinrichtung 

Mittel der hinweisenden Sicherheitstechnik

8.3 Pneumatische Konstruktion

8.3.1 Verwendete Einheiten

Größe	Einheit	Symbol	Beziehung
Längen	Mikrometer	µm	1 µm = 0,001 mm
	Millimeter	mm	1 mm = 0,1 cm = 0,01 dm = 0,001 m
	Zentimeter	cm	1 cm = 10 mm = 10 000 µm
	Dezimeter	dm	1 dm = 10 cm = 10 mm = 100 000 µm
	Meter	m	1 m = 10 dm = 100 cm = 1 000 mm = 1 000 000 µm
	Kilometer	km	1 km = 1 000 m = 100 000 cm = 1 000 000 mm
Flächen	Quadratzentimeter	cm^2	1 cm^2 = 100 mm^2
	Quadratdezimeter	dm^2	1 dm^2 = 100 mm^2 = 10 000 mm^2
	Quadratmeter	m^2	1 mm^2 = 100 dm^2 = 10 000 cm^2 = 1 000 000 mm^2
	Ar	a	1 a = 100 m^2
	Hektar	ha	1 ha = 100 a = 10 000 m^2
	Quadratkilometer	km^2	1 km^2 = 100 ha = 10 000 a = 1 000 000 m^2
Volumen	Kubikzentimeter	cm^3	1 cm^3 = 1 000 mm^3 = 1 ml = 0,001 l
	Kubikdezimeter	dm^3	1 dm^3 = 1 000 cm^3 = 1 000 000 mm^3
	Kubikmeter	m^3	1 m^3 = 1 000 dm^3 = 1 000 000 cm^3
	Milliliter	ml	1 ml = 0,001 l = 1 cm^3
	Liter	l	1 l = 1 000 ml = 1 dm^3
	Hektoliter	hl	1 hl = 100 l = 100 dm^3
Dichte	Gramm/ Kubikzentimeter	$\frac{g}{cm^3}$	$1\frac{g}{cm^3} = 1\frac{kg}{dm^3} = 1\frac{t}{m^3} = 1\frac{g}{m1}$
Kraft/ Gewichtskraft	Newton	N	$1\ N = 1\frac{kg \times m}{s^2} = 1\frac{J}{m}$ 1 daN = 10 N
Drehmoment	Newtonmeter	Nm	1 Nm = 1 J
Druck	Pascal	Pa	$1\ Pa = 1\ N/m^2 = 0{,}01\ mbar = \frac{1\ kg}{m \times s^2}$
	Bar	bar	$1\ bar = 10\frac{N}{cm^2} = 100\,000\frac{N}{m^2} = 10^5\ Pa$
	$psi = \frac{pound}{inch^2}$	Psi	1 psi = 0,06895 bar
	$\frac{kp}{cm^2}$		$1\frac{kp}{cm^2} = 0{,}981\ bar$
Masse	Milligramm	mg	1 mg = 0,001 g
	Gramm	g	1 g = 1 000 mg
	Kilogramm	kg	1 kg = 1 000 g = 1 000 000 mg
	Tonne	t	1 t = 1 000 kg = 1 000 000 g
	Megagramm	Mg	1 Mg = 1 t

8.3 Pneumatische Konstruktion

Größe	Einheit	Symbol	Beziehung
Beschleunigung	Meter/ Sekundenquadrat	$\frac{m}{s^2}$	$1\frac{m}{s^2} = 1\frac{N}{kg}$ 1 G = 9,81 m/s²
Winkel-geschwindigkeit	Eins/Sekunde	$\frac{1}{s}$	$\omega = 2 \times \pi \times n$ n in 1/s
	Radiant/Sekunde	$\frac{rad}{s}$	
Leistung	Watt	W	$1\,W = 1\frac{Nm}{s} = 1\frac{J}{s} = 1\frac{kg \times m}{s^2} \times \frac{m}{s}$
	Newtonmeter/ Sekunde	Nm/s	
	Joule/Sekunde	J/s	
Arbeit/Energie, Wärmemenge	Wattsekunde	Ws	$1\,Ws = 1\,Nm = 1\frac{kg \times m}{s^2} \times m = 1\,J$
	Newtonmeter	Nm	
	Joule	J	
	Kilowattstunde	kWh	1 kWh = 1 000 Wh = 1 000 × 3 600 Ws = 3,6 × 10^6 Ws = 3,6 × 10^3 kJ = 3 600 kJ = 3,6 MJ
	Kilojoule	kJ	
	Megajoule	MJ	
Mechanische Spannung	Newton/ Millimeterquadrat	$\frac{N}{mm^2}$	$1\frac{N}{mm^2}$ = 10 bar = 1 MPa
Ebener Winkel	Sekunde	"	1" = 1'/60
	Minute	'	1' = 60"
	Grad	°	$1° = 60' = 3\,600'' = \frac{\pi}{180°}$ rad
	Radiant	rad	1 rad = 1m/m = 57,2957° 1 rad = 180°/π
Drehzahl	Eins/Sekunde	1/s	$\frac{1}{s} = s^{-1} = 60\ min^{-1}$
	Eins/Minute	1/min	$\frac{1}{min} = min^{-1} = \frac{1}{60\ s}$

Größe	Einheit	Symbol	Beziehung
Dichte	$\frac{kg}{m^3}$	ρ, roh	$\rho = \frac{m}{V}$
Druckverlust-beiwert	l	ζ, Zeta δ, Delta	$\zeta = \frac{2\,D \times p}{\rho \times v2}$
Reibungs-schubspannung	$\frac{N}{m^2}$	τ, Tau	$\tau = \frac{F}{A}$
Statische Viskosität	$Pa \times s = \frac{kg}{m \times s} = \frac{N \times s}{m}$	η, Eta	$\eta = v \times \rho$
Dynamische Viskosität	$\frac{m^2}{s}$	v, Ny	$v = \frac{\eta}{\rho}$
Durchfluss	l/min	Q	$Q = k_v \sqrt{\frac{\Delta p}{\rho}}$
Normal-nenndurchfluss	l/min	q_{nN}	bei T = 293,15 K (20 °C), p_1= 6 bar, p_2 = 5 bar, ρ_{Luft} = 1,292 kg/m³

8.3 Pneumatische Konstruktion

8.3.2 Einleitung

Die Pneumatik ist neben der Elektrik und Hydraulik eine der Antriebstechnologien im Maschinen- und Anlagenbau. Damit eine Maschine sicher betrieben werden kann, reicht es jedoch nicht aus, Gefahren zu erkennen und einer Steuerung oder Sicherheitsbauteilen diese Informationen mitzuteilen. Die Antriebe müssen in einen sichereren Zustand gebracht werden, erst dann ist die Maschine sicher.

8.3.3 Bewährte Prinzipien und Schutzmaßnahmen

Sichere Pneumatik kann in zwei grundsätzliche Felder unterteilt werden: Dies sind einerseits die grundlegenden und bewährten Prinzipien, wie sie in der DIN EN ISO 13 849-2 im Anhang B beschrieben sind, andererseits einschlägige Schutzmaßnahmen für pneumatische Antriebe. Darunter versteht man hier steuerungstechnische Lösungen, die einen Zylinder zu einem gewünschten Verhalten bewegen.

8.3.3.1 Grundlegende und bewährte Prinzipien

Hier zunächst einige grundlegende und bewährte Prinzipien der Pneumatik. Dazu gehört eine gute Druckluftaufbereitung: Druckluft muss gefiltert, frei von Wasser und von Kompressoröl sein. Schlecht aufbereitete Druckluft führt zu Funktionsausfällen der Elemente. Ventile schalten nicht mehr und bleiben hängen, Zylinder können sich aufgrund von Leckagen ungewollt bewegen. Immer wieder wird die Frage gestellt, ob Druckluft zu ölen sei oder nicht. Hier gilt: Wer einmal ölt, ölt immer. Heute haben Pneumatikkomponenten jedoch eine Lebensdauerschmierung und müssen nicht mehr geölt werden. Werden neue Komponenten in alte Maschinen eingebaut, bei denen die Druckluft geölt wird, werden auch die neuen Teile geölt. In diesen Fällen ist ein ventilverträgliches Öl zu wählen. Die Ölmenge sollte gering sein, denn ein „Überölen“ führt ebenfalls zu Funktionsausfällen.

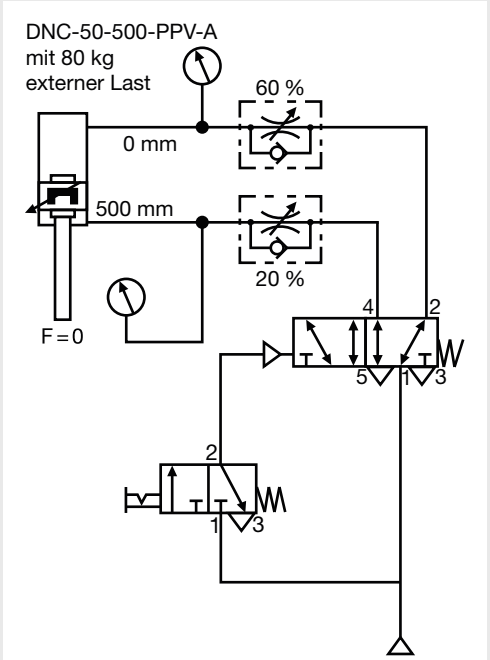
8.3.3.2 Auswahl und Dimension

Die pneumatischen Komponenten sind so zu dimensionieren und auszuwählen, dass sie den zu erwartenden Anforderungen standhalten. Hier sind einerseits Umgebungsbedingungen wie Temperatur, Öle, Säuren, Laugen und Reinigungsmittel zu beachten. Eine gute sicherheitsgerichtete Schaltung nützt nichts, wenn aggressive Reinigungsmittel den Pneumatikschlauch weich machen. Pneumatikzylinder werden üblicherweise so berechnet, dass sie die in der Maschine benötigte Kraft aufbringen. Bei der Bemessung ist jedoch auch die kinetische Energie zu beachten. Bewegt sich ein Zylinder zu schnell – häufig sind ja in den Anwendungen hohe Taktzahlen gefordert –, ist auch die Energie, mit der ein Pneumatikzylinder in die Endlage fährt, entsprechend hoch. Langfristig führt dies zur Zerstörung des Zylinders.

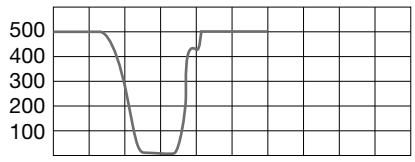
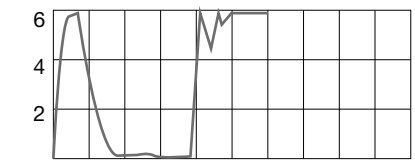
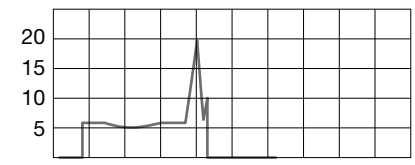
8.3 Pneumatische Konstruktion

8.3.3.3 Druckbegrenzung

Ein weiteres Grundprinzip ist die Druckbegrenzung. Am Windkessel hinter dem Kompressor sitzt ein Überdruckventil, das den Windkessel vor dem Bersten schützt. An der Maschine wird eine Wartungseinheit eingebaut, die den Betriebsdruck regelt. Stellt man den Betriebsdruck höher ein, steigen die Kräfte in der Anlage, was zu einer Überlastung führen kann. Der Maschinenbediener sollte daher den Betriebsdruck nicht eigenmächtig verändern können. Ein Überdruckventil in der Wartungseinheit ist somit sinnvoll und schützt die Maschine vor einem gefährlichen Ausfall des Druckreglers. Bei einem Defekt sähe sich die Maschine mit dem vollen Netzdruck konfrontiert. Für die Druckbegrenzung sind daher weitere Maßnahmen notwendig, die wiederum die Dimensionierung des Zylinders betreffen. Bei vertikal eingebauten Pneumatikzylindern kommt es durch die zu bewegende Masse, den Betriebsdruck und die Flächendifferenz am Zylinder zu einer Drucküberhöhung. Soll dieser Zylinder dann noch, z. B. durch Einsperren der Druckluft, pneumatisch gestoppt werden, sind Druckspitzen weit über 30 bar möglich. Dieser Druck überlastet wiederum alle in diesem Schaltungsbereich eingesetzten Pneumatikkomponenten.



Schaltplan Druckwerte (Quelle: Festo)

Komponentenbezeichnung	Kennung	Zustandsgröße	0 1 2 3 4 5 6 7 8 9 10
Zylinder, doppeltwirkend	DNC-50-500-PPV-A	Weg mm	
Druckmessgerät	Druck oben	Druck bar	
Druckmessgerät	Druck unten	Druck bar	

Druckwerte (Quelle: Festo)

8.3 Pneumatische Konstruktion

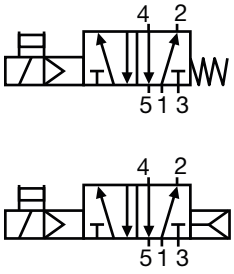
Diese Druckspitzen können reduziert werden, indem zwischen dem Arbeitsventil und dem oberen Anschluss des Zylinders ein Druckregler eingebaut wird. Die Abwärtsbewegung des Zylinders wird dann nicht mit dem normalen Betriebsdruck, sondern mit beispielsweise einem auf 2 bar reduzierten Druck unterstützt. Bei sehr großer Zylinderbelastung wird für die Abwärtsbewegung kein Druck benötigt. In diesen Fällen wird in den oberen Zylinderanschluss ein Schalldämpfer eingeschraubt. Der Zylinder kann dann mit einem 3/2-Wegeventil gesteuert werden, denn der Druck wird nur für die Aufwärtsbewegung benötigt.

8.3.3.4 Anordnungen von Schutzeinrichtungen

Einen weiteren Grund für die richtige und vollständige Auslegung einer pneumatischen Schaltung liefert die Anwendung in Verbindung mit einer Lichtschranke oder Zweihandschaltung. Nach DIN EN ISO 13855 „Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Köperteilen“ ist der Nachlaufweg eines gefahrbringenden Antriebs zu messen und daraus der Abstand der Lichtschranke oder Zweihandschaltung zu bestimmen. Für die Geschwindigkeit eines Pneumatikzylinders sind neben dem Betriebsdruck, der Masse und der Einbaulage vor allem die verwendeten Verschraubungen, Schläuche und Ventile sowie deren Durchflussmengen verantwortlich. Berechnet man Letztere nicht, bestimmt der auswählende Monteur, mehr oder minder bewusst, die Taktzahl der Maschine und damit auch den Nachlaufweg bei einer Lichtschranke. Tauscht ein Betreiber anschließend Schläuche und Verschraubungen und ermöglicht so eine höhere Durchflussmenge, verändert er damit gleichzeitig den Nachlaufweg. Der Abstand der Lichtschranke wäre für diesen Antrieb nicht mehr ausreichend, das Risiko für einen gefährlichen Zwischenfall nähme deutlich zu. Es empfiehlt sich also, den Antrieb komplett zu berechnen und die Werte für Schläuche und Verschraubungen auch im Schaltplan anzugeben. Zudem ist der Hinweis „sicherheitsrelevant“ sinnvoll. Ein Foto bei der Abnahme mit exakt diesem Aufbau ist als Hilfsmittel auch bei etwaigen Rechtsstreitigkeiten sehr hilfreich.

8.3.3.5 Grundprinzip mechanische Feder bzw. Luftfeder

Die mechanisch bewährte Feder ist ein weiteres Grundprinzip der Sicherheitstechnik, sowohl in der Mechanik als auch in der Pneumatik und Hydraulik. Bei Ventilen mit mechanischer Feder ist die Schaltstellung des Ventils eindeutig definiert, wenn das Steuersignal oder auch die Druckluftversorgung abgeschaltet wird. Bei Impulsventilen (bistabile Ventile mit zwei Spulen) ist dies nicht der Fall. Bei der Auswahl von monostabilen Ventilen ist ein besonderes Augenmerk auf diese Rückstellung zu richten, denn neben Ventilen mit mechanischer Feder gibt es auch Ventile mit Luftfeder zur Rückstellung. Das folgende Bild zeigt zwei monostabile Ventile. Das obere Ventil ist mit mechanischer Feder, das untere mit einer Luftfeder ausgestattet. Die Rückstellung ist auf der rechten Ventilseite dargestellt. Es handelt sich hier um 5/2-Wegeventile mit Vorsteuerung, Handhilfsbetätigung und elektrischer Ansteuerung.

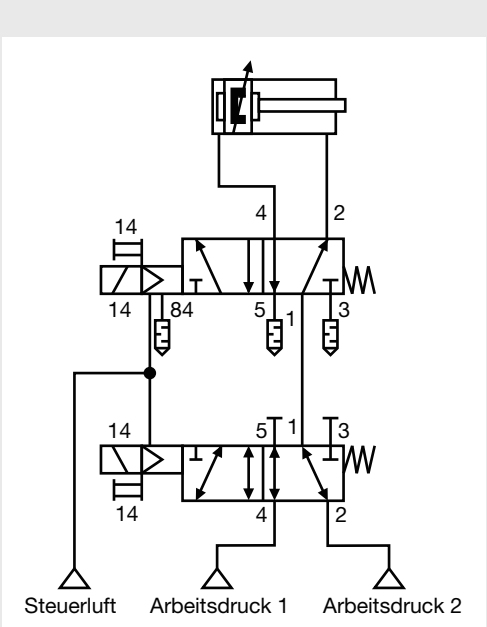


Monostabile Ventile mit mechanischer Feder bzw. Luftfeder (Quelle: Festo)

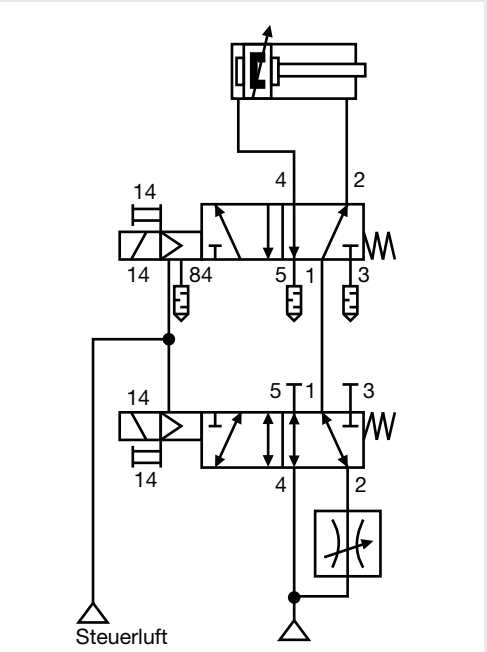
8.3 Pneumatische Konstruktion

Ventile mit Luftfeder lassen sich jedoch nur dann zurückstellen, wenn ausreichend Druck für die Luftfeder zur Verfügung steht. Die Druckluftversorgung der Luftfeder kann vom Druckanschluss 1 oder von einem separaten Steuerluftanschluss kommen. Dies ist letztlich von der Ventilbaureihe abhängig. Ob und unter welchen Bedingungen Ventile mit Luftfeder in sicherheitsgerichteten Schaltungen einsetzbar sind, müssen Fachleuten klären. In pneumatischen Schaltplänen ist daher sehr genau auf die Ventildarstellung zu achten.

Das Verringern der Kraft bzw. der Geschwindigkeit sind weitere Sicherheitsprinzipien in der Pneumatik. Sie kommen hauptsächlich beim Einrichtbetrieb zum Einsatz. Die Kraft wird reduziert, indem man den Betriebsdruck für den Zylinder verringert. Geschwindigkeit erzeugt man in der Pneumatik über die Intensität des Volumenstromes. In beiden Fällen schaltet man dabei die Druckversorgung zum Arbeitsventil einfach um. Ob die Umschaltung ein- oder zweikanalig auszuführen ist, hängt von der Risikobeurteilung ab.



Reduzierte Kraft (Quelle: Festo)



Reduzierte Geschwindigkeit (Quelle: Festo)

Der Schaltplan für reduzierte Geschwindigkeit, stellt lediglich das Prinzip dar. Da die Schläuche und Verschraubungen zwischen dem Arbeitsventil und dem Zylinder ebenfalls einen Einfluss auf die Geschwindigkeit haben, wird die reduzierte Geschwindigkeit meist durch Ventile erreicht, die direkt am Zylinder sitzen.

8.3 Pneumatische Konstruktion

8.3.4 Schaltungstechnische Lösungen

Nach den Beispielen für grundlegende und bewährte Prinzipien in der Pneumatik nun zu den eigentlichen Schutzmaßnahmen. Schutzmaßnahmen sicherheitsgerichteter Pneumatik beschreiben schaltungstechnische Lösungen. Diese sind u. a.:

- Schutz gegen unerwartetes Anlaufen
- Be- und Entlüften
- Abbremsen der Bewegung
- Blockieren der Bewegung
- Umkehren der Bewegung = Reversieren
- freie Bewegungsmöglichkeit
- Kräftegleichgewicht am Antrieb

Schutz gegen unerwarteten Anlauf

Zunächst bietet ein Handeinschaltventil an der Wartungseinheit einen wirkungsvollen Schutz gegen unerwartetes Anlaufen. Mit diesem Handventil kann der Instandhalter die Maschine entlüften und mit einem Vorhängeschloss gegen Wiedereinschalten sichern. Die nächste sinnvolle Maßnahme ist ein elektrisches Einschaltventil, das durch eine übergeordnete Steuerung aktivierbar ist. Zu dieser Maßnahme zählt auch ein Drucksensor, der den Betriebsdruck überwacht. Die Steuerung erkennt den Druckausfall, reagiert und schaltet konsequent alle Ausgänge und das Druckeinschaltventil ab. Sobald der entsprechende Betriebsdruck wieder anliegt, schaltet die Steuerung die Druckluft wieder ein und belüftet die Maschine mit ihren Antrieben.

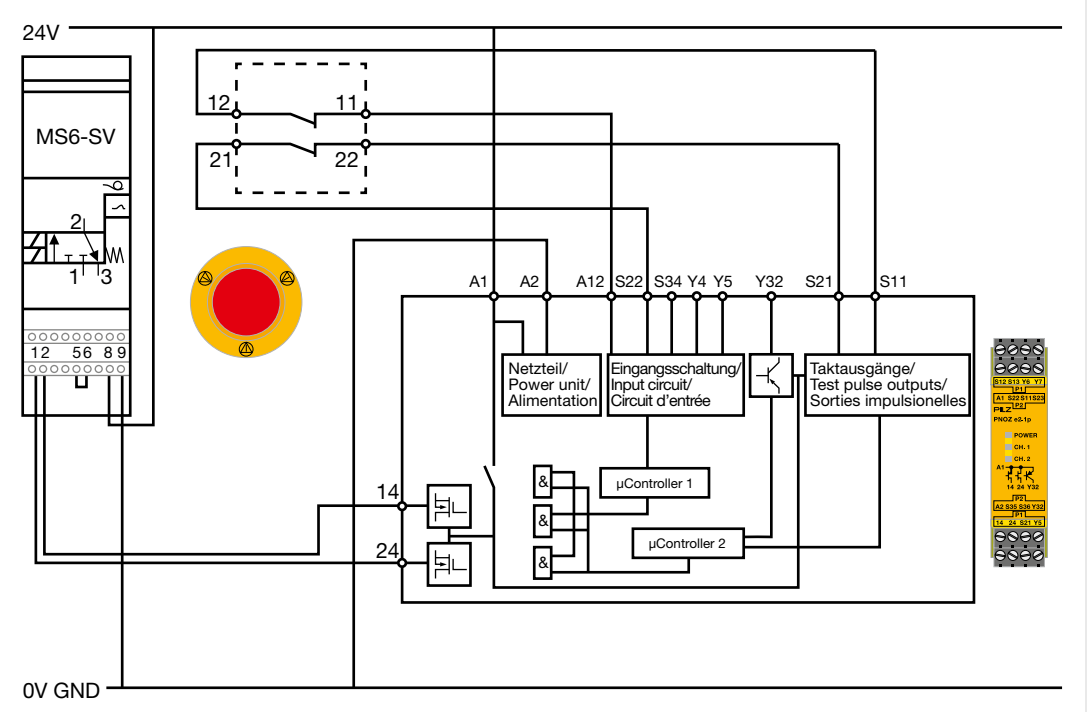
Die richtige Auswahl der Arbeitsventile ist eine weitere wirksame Schutzmaßnahme. Sind Ventile mit separater Steuerluftversorgung im Einsatz, lassen sich diese ohne Steuerluft nicht schalten. Damit wäre auch das Schalten von Ventilen bei elektrischen Fehlern unterbunden. Sind darüber hinaus Arbeitsventile installiert, die in Ruhestellung gesperrt sind, findet beim Belüften der Maschine noch keine Zylinderbewegung statt, da ja noch keine Druckluft zum Zylinder strömen kann. Falls Arbeitsventile im Einsatz sind, die beim Einschalten der Druckluft bereits einen Luftstrom zum Zylinder zulassen, ist in der Regel ein langsamer Druckaufbau gewünscht. Dazu setzt man ein Sanftanlauf- oder Softstart-Ventil ein. Dieses Ventil belüftet die Maschine zunächst nur langsam über eine Drosselstelle. Wenn sich ein Betriebsdruck von z. B. 3 bar eingestellt hat, schaltet das Ventil vollständig durch. Erst dann steht der komplette Betriebsdruck mit dem vollen Volumenstrom zur Verfügung. In der ersten Belüftungsphase lassen sich mit diesem Ventil somit langsame und kontrollierte Zylinderbewegungen realisieren. Sollte eventuell ein Schlauch nicht korrekt montiert sein, wäre dies durch Abblasen sofort hörbar, ohne dass der Schlauch, wie unter vollem Druck, mit großer Wucht um sich schlagen würde.

8.3 Pneumatische Konstruktion

8.3.4.1 Entlüften

Eine häufig praktizierte Schutzmaßnahme ist das Entlüften. Sie kommt zum Zuge, wenn die Zylinder im drucklosen Zustand keine Gefahr darstellen. Hierbei sind jedoch die jeweilige Einbaulage und die Masse an den Zylindern zu berücksichtigen. Gedanklich kommt diese Maßnahme von der Energietrennung in der Elektrik: Damit Gefahren durch Berühren der elektrischen Leitungen verhindert werden, schaltet man die elektrische Spannung einfach ab. Genauso handhabt man das in der Pneumatik, denn ohne Energie/Druckluft besteht keine Gefahr. Stets ist bei der Sicherheitstechnik jedoch die Mechanik zu betrachten, die ja letztlich die Bewegungen ausführen muss. Wird ein vertikal eingebauter Zylinder entlüftet, bewegt sich der Zylinderkolben, der Trägheit gehorchend, nach unten. Gerade hier muss man zusätzliche Schutzmaßnahmen in Betracht ziehen. Aus anderen Gründen jedoch hinterfragt man in der Industrie die Praxis des Ent- und Belüftens immer kritischer: Das Prozedere kostet sehr viel Zeit und damit Geld, die Produktivität sinkt.

Ohne Frage steht die Sicherheit an erster Stelle. Das Be- und Entlüften einer Maschine kann durchaus im Performance Level PL = „e“ erfolgen. Das Druckaufbau- und Entlüftungsventil MS6-SV ist ein Sicherheitsbauteil nach MRL 2006/42 EG und erfüllt den Performance Level „e“. Es ist ein eigensicheres, redundantes mechatronisches System nach den Forderungen der DIN EN ISO 13849-1, bei dem das sicherheitsgerichtete pneumatische Schutzziel, sicheres Entlüften, auch bei einem Fehler im Ventil (z. B. durch Verschleiß, Verschmutzung) gewährleistet ist.



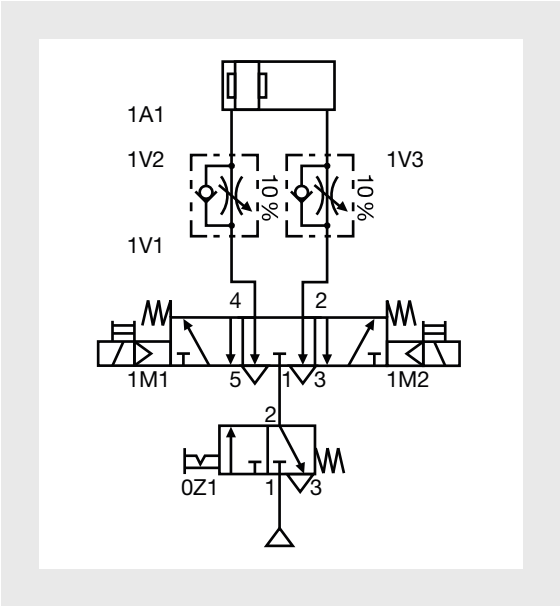
Schaltschema sicheres Be- und Entlüften (Quelle: Festo)

8.3 Pneumatische Konstruktion

Das Schaltschema auf Seite 8-26 zeigt eine Schaltung mit einem zweikanaligen Aufbau zum sicheren Be- und Entlüften. Vom elektronischen Sicherheitsschaltgerät gehen zwei Freigabesignale auf das MS6-SV an die Pins 1 und 2. Ein zusätzlich installiertes elektronisches Sicherheitsschaltgerät würde auf den Fehler „Querschluss“ zwischen diesen beiden Geräten aufmerksam machen. Der Performance Level „e“ ist damit erreichbar. Im Schaltplan nicht dargestellt ist eine mögliche Rückmeldung vom MS6-SV zum PNOZ. Dafür steht ein potenzialfreier Kontakt zur Verfügung, der in den Rückführkreis eingebunden wird. Damit erkennt das PNOZ, ob das MS6-SV betriebsbereit ist.

Festo MS6-SV (Quelle: Festo)

Natürlich ist auch ein einkanaliges Be- und Entlüften möglich. Diesen Zweck erfüllen elektropneumatische Ventile in der Wartungseinheit, die ihre Befehle von der übergeordneten Steuerung oder von einem einkanaligen Sicherheitskreis erhalten. Ein Entlüften ist auch über das Arbeitsventil 1V1 realisierbar.



Entlüften mit 5/3-Wegeventil (Quelle: Festo)

8.3.4.2 Normalbetrieb

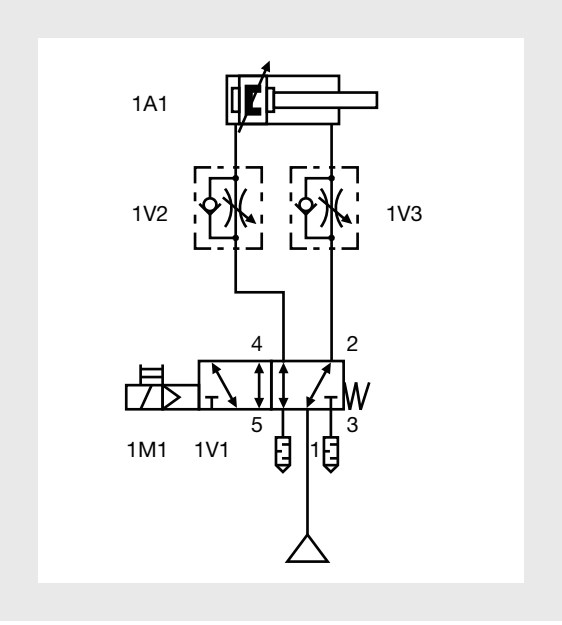
Im Normalbetrieb steht immer eine der beiden Ventilspulen 1M1 oder 1M2 unter Spannung. Damit ist das Ventil geschaltet. Der Zylinderkolben steht somit entweder in einer Endlage oder er bewegt sich von der einen in die andere Endlage. Die Entlüftung des Zylinders erfolgt dann, wenn das Arbeitsventil in der Mittelstellung steht. Dies ist der Fall, wenn beide Spulen spannungslos sind. Der Entlüftungsvorgang am Arbeitsventil ist schneller als das Entlüften über die Wartungseinheit, weil der Weg der Druckluft kürzer und das zu entlüftende Druckvolumen kleiner ist. Wird über die Wartungseinheit entlüftet, so lassen sich mehrere Zylinder entlüften, gleichzeitig ist das Druckvolumen größer. Über das Arbeitsventil zu entlüften, hat noch einen anderen Vorteil: Parallel lassen sich bei anderen Zylindern problemlos zusätzliche Schutzmaßnahmen realisieren, wie beispielsweise „Reversieren“.

8.3 Pneumatische Konstruktion

8.3.4.3 Reversieren

Die Schutzmaßnahme „Reversieren“ ist dann die richtige Wahl, wenn nur eine Bewegungsrichtung des Zylinderkolbens gefährlich ist.

Das monostabile 5/2-Wegeventil, wie im Bild mit 1V1 dargestellt, benötigt ein elektrisches Steuersignal an der Spule 1M1, um das Ventil umzuschalten. Die Kolbenstange des Zylinders fährt folgerichtig aus. Schaltet man die Spule ab, fehlt die Steuerkraft auf der linken Seite des Ventils. Nun kann die mechanische Feder auf der rechten Seite das Ventil wieder zurückschalten, die Kolbenstange fährt wieder ein. Im normalen Maschinenablauf schaltet die Steuerung die Ventilspule ein und aus. Ebenso kann ein Sicherheitsschaltgerät, das zwischen Steuerung und Ventilspule geschaltet ist, die Spule abschalten. In diesem Falle wäre es unerheblich, ob der Ausgang der Steuerung (beispielsweise eine nicht sicherheitsgerichtete SPS) noch eingeschaltet ist.



Reversieren einkanalig (Quelle: Festo)

Selbst bei Ausfall der elektrischen Versorgungsspannung würde das Ventil wieder in seine Grundstellung zurückgeschaltet. Die Kolbenstange kann erst dann wieder zurückfahren, wenn wieder Druckluft anliegt. Die Not-Halt-Funktion erfordert daher für das Reversieren eine Stopp-Kategorie 1. Erst wenn der Zylinder seine sichere Endlage erreicht hat, wird die Druckluft abgeschaltet. Die Stopp-Kategorie 0 schaltet die Druckluftversorgung sofort ab, ist hier aber nicht einsetzbar, weil ein Reversieren dann nicht mehr möglich wäre.

Sämtliche pneumatischen Schaltpläne müssen einen Totalausfall der Druckluftversorgung berücksichtigen. Die elektronische Steuerung erkennt den Druckluftausfall: Damit die Kolbenstange noch ausreichend Luft zur Verfügung hat, um das Zurückfahren der Kolbenstange sicherzustellen, ist dem Arbeitsventil ein Speichervolumen vorgeschaltet. Damit sich der Speicher nicht in Richtung der Druckluftversorgung entleeren kann, schaltet man vor das Speichervolumen noch ein Rückschlagventil. Die Druckluft strömt somit immer in Richtung Zylinder.

8.3.4.4 Ausfallverhalten

Betrachtet man das Ausfallverhalten des Arbeitsventils, sind folgende Möglichkeiten denkbar:

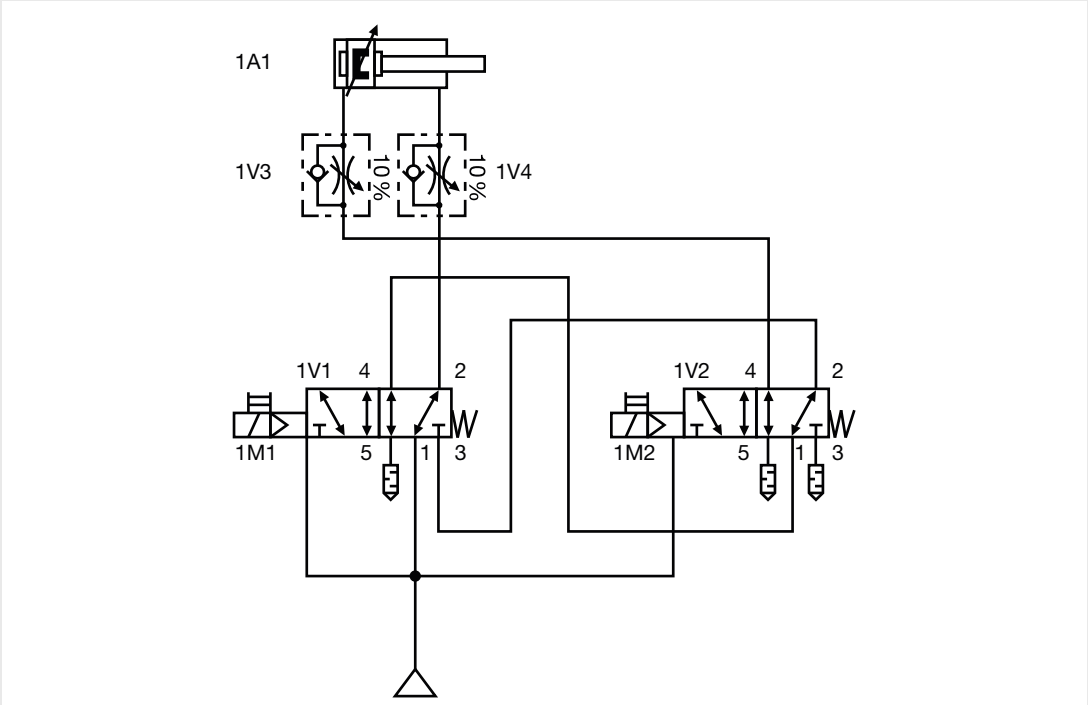
- Das Ventil schaltet nicht, somit bewegt sich auch die Kolbenstange nicht. Es besteht keine Gefahr. Die Ursachen können vielseitig sein: Möglicherweise kommt keine Spannung an der Ventilspule an, ggf. ist das Ventil defekt. Mitunter klemmt der Anker in der Spule oder der Kolben im Ventil sitzt fest.
- Ein Fehler anderer Art liegt vor, wenn das Ventil nicht zurückschaltet. Dann fährt die Kolbenstange weiter aus oder bleibt ausgefahren. Auf der elektrischen Seite kann ein Querschluss die Ursache sein, möglicherweise hängt der Ventilkolben. Dieser Fehler ist in jedem Fall ein gefährlicher Ausfall.

8.3 Pneumatische Konstruktion

- Eine weitere Fehlerquelle liegt ausschließlich im Ventil: Der Ventilkolben bleibt in einer Zwischenposition hängen. Um diesen Fehler konkreter beschreiben zu können, muss der innere Aufbau des Ventils bekannt sein. Hier stellt sich die Frage, ob in der Zwischenposition des Ventilkolbens alle Anschlüsse des Ventils abgesperrt oder miteinander verbunden sind. Sind alle Anschlüsse abgesperrt, kann keine Druckluft mehr durch das Ventil strömen. Ist der Zylinderkolben ausgefahren, würde zwar keine Druckluft mehr in, aber auch keine Luft mehr aus dem Zylinder strömen. Damit läge ein gefährlicher Ausfall des Ventils vor. Stehen alle Anschlüsse des Ventils miteinander in Verbindung, würde der Zylinder zwar möglicherweise nicht komplett drucklos, seine Kraft jedoch wesentlich geringer werden. Schlussendlich wären noch die Einbaulage des Zylinders und die zu bewegende Masse zu berücksichtigen, um die Gefahr abschätzen zu können.

Deutlich wird, dass einkanalige Systeme bei einem gefährlichen Ausfall einer Komponente in der Sicherheitskette ausfallen. Sie sind daher nur bei geringem Risiko einsetzbar. Für höhere Risiken sind somit immer zweikanalige Systeme zu wählen.

Bei einem zweikanaligen System sind beide Arbeitsventile 1V1 und 1V2 zu schalten, damit die Kolbenstange ausfährt. Schaltet ein Ventil nicht, fährt die Kolbenstange nicht aus. Sind beide Ventile geschaltet und ein Ventil schaltet aus, weil beispielsweise das Kabel zur Spule gebrochen ist, fährt die Kolbenstange ein, selbst wenn das andere Ventil noch geschaltet ist. Bleibt eines der beiden Ventile geschaltet hängen und das andere Ventil lässt sich noch schalten, fährt die Kolbenstange ein oder aus, je nachdem, wie das noch funktionierende Ventil geschaltet ist. Man spricht hier von einer Einfehlersicherheit, denn ein gefährlicher Ausfall führt noch nicht zum Verlust der Sicherheitsfunktion.



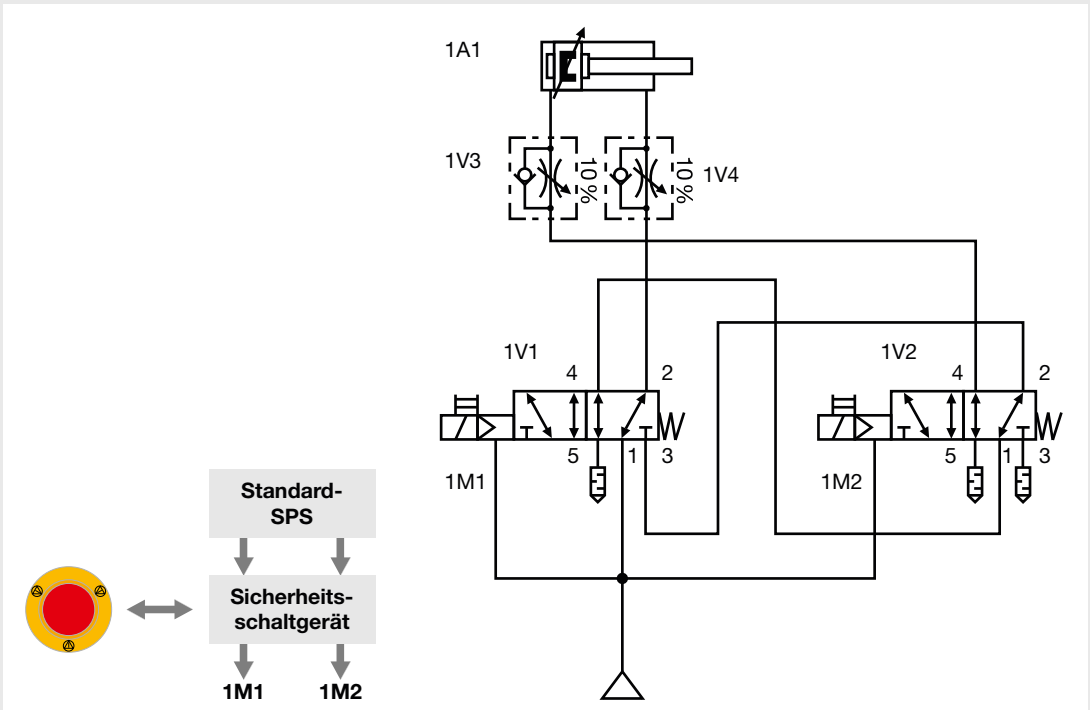
Reversieren zweikanalig (Quelle: Festo)

8.3 Pneumatische Konstruktion

Wie erkennt man einen gefährlichen Ausfall eines Ventils? Eine Möglichkeit bieten Ventile mit integrierter Schaltstellungsabfrage. Bei diesen Ventilen ist ein Sensor im Ventilkörper integriert, der die Schaltstellung des Ventilkolbens abfragt. Bei der Berechnung des Performance Levels kann für dieses Ventil ein Diagnosedeckungsgrad von 99 % angesetzt werden. Eine weitere Möglichkeit bieten Drucksensoren an einem der beiden Ausgänge des Ventils. Bei einem Signalwechsel an der Ventilspule muss innerhalb kurzer Zeit ein Signalwechsel am Sensor erfolgen, dann sind sowohl das Ventil als auch der Sensor und seine Verkabelung in Ordnung. Dies gilt sowohl für den Drucksensor als auch für den in das Ventil integrierten Sensor.

Eine dritte Möglichkeit bietet die Diagnose der Ventile mithilfe der üblicherweise am Zylinder angebauten Sensoren zur Schaltstellungsabfrage des Zylinders. Hier ist jedoch das Geschick des Programmierers gefordert. Die Kolbenstange des Zylinders steht in der hinteren Endlage, der Sensor meldet diese Position. Zunächst schaltet man nur ein Arbeitsventil, die Kolbenstange darf die Endlage noch nicht verlassen. Erst wenn das zweite Ventil schaltet, darf die Kolbenstange die Endlage verlassen. Würde die Kolbenstange bereits beim Schalten des ersten Ventils ausfahren, wäre dies der Hinweis, dass das zweite Ventil bereits geschaltet ist. Folglich läge ein Fehler vor. Im nächsten Zyklus muss das andere Arbeitsventil zuerst geschaltet werden, nur so lässt sich auch ein gefährlicher Ausfall des zweiten Ventils erkennen. Wichtig ist dabei, sämtliche Sensoren auf einen Signalwechsel hin zu überprüfen, denn nur der Signalwechsel bestätigt die ordnungsgemäße Funktion des Sensors und seiner Verkabelung. Nachfolgend ein Beispiel für das Zusammenwirken zwischen Pneumatik und Elektrotechnik:

Eine Standard-SPS steuert den normalen Maschinenablauf. Da der Zylinder als gefährlicher Antrieb eingestuft ist, führte eine Risikoanalyse zu einem zweikanaligen Aufbau zum Ansteuern des Zylinders. Wirkt ein zweikanaliger Sicherheitsschalter auf ein zweikanaliges Sicherheitsschaltgerät, so schaltet



Zusammenwirken der Elektrotechnik mit der Pneumatik (Quelle: Festo)

8.3 Pneumatische Konstruktion

das Sicherheitsschaltgerät die Spulen der beiden Ventile 1V1 und 1V2 ab, wenn der Sicherheitsschalter betätigt wird. Die SPS benötigt ein Signal, um auch die Ausgänge zu den Spulen abzuschalten. Die Sicherheitsfunktion wirkt jedoch an der SPS vorbei. Je nach Diagnose kann ein Performance Level „d“ bis „e“ erreicht werden. Für PL = „e“ wird bei den Ventilen ein Diagnosedeckungsgrad von 99 % benötigt.

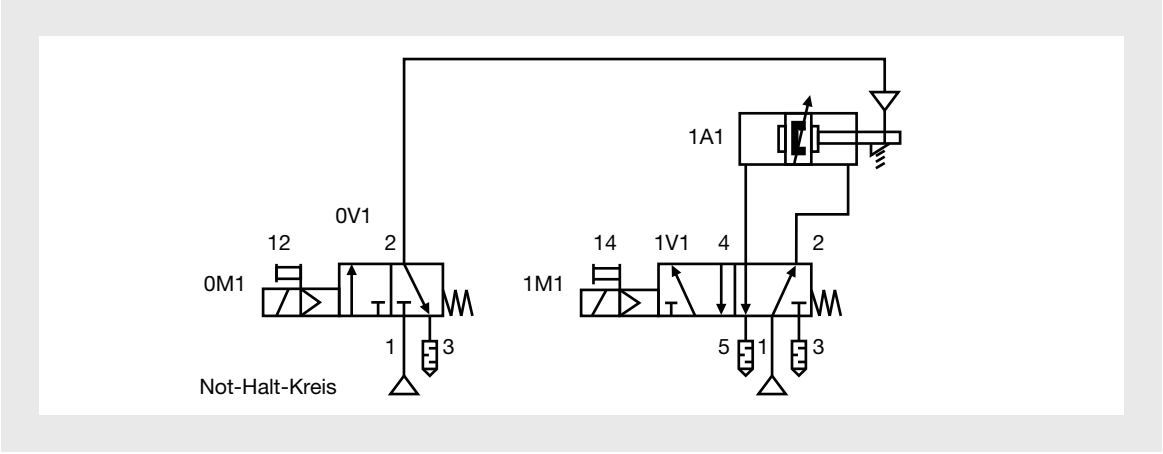
8.3.5 Halten und Abbremsen

Eine weitere Schutzmaßnahme ist das Halten bzw. Abbremsen einer Bewegung. Hier muss vorab ganz klar die bestimmungsgemäße Verwendung bzw. der Einsatz geklärt sein. Die Klemmpatrone ist eine Haltebremse, diese dient allein dazu, die Kolbenstange zu halten, nachdem sie bereits steht. Eine Betriebsbremse kann kinetische Energie aufnehmen, eine Kolbenstange, die in Bewegung ist, kann folglich durch eine Betriebsbremse abgebremst werden.

Zylinder mit Klemmpatrone (Quelle: Festo)

Klemmpatrone

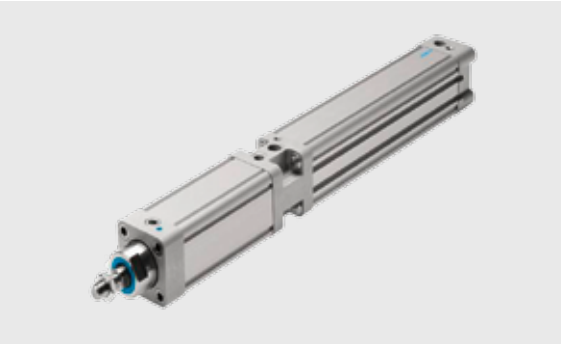
Eine Klemmpatrone kommt zum Einsatz, wenn ein vertikal eingebauter Zylinder in einer Endlage gehalten werden soll, um bei Druckluftausfall jede weitere Bewegung der Kolbenstange nach unten zu stoppen. Wichtig ist dabei, dass die Klemmpatrone erst dann schließt, wenn sich die Kolbenstange in der Endlage befindet und steht. Setzt man anstatt einer Klemmpatrone einen Zylinder mit Betriebsbremse ein, lässt sich die Bewegung jederzeit stoppen. Was aber geschieht, wenn die Kolbenstange bei Öffnen der Bremse gerade in einer Zwischenposition zwischen den beiden Endlagen steht? Ist der Zylinder vertikal eingebaut und drucklos, wird sich die Kolbenstange mit ihrer Masse nach unten bewegen. Dies bedeutet in aller Regel Gefahr. Bei einem horizontalen Einbau bestünde diese Gefahr freilich nicht. Wäre noch Druckluft im Zylinder und die Kolbenstange befände sich in einer Zwischenposition, so entstünde ebenfalls eine gefährliche Bewegung beim Öffnen der Bremse. Eine Seite des Zylinder ist be-, die andere Seite ist entlüftet. Sogenannte „vorentlüftete“ Systeme erzeugen sehr hohe Beschleunigungswerte und Geschwindigkeiten. Eine elegante Lösung bieten hier die 3/2-Wegeventile.



Zylinder mit Klemmpatrone und monostabilem 5/2-Wegeventil (Quelle: Festo)

8.3 Pneumatische Konstruktion

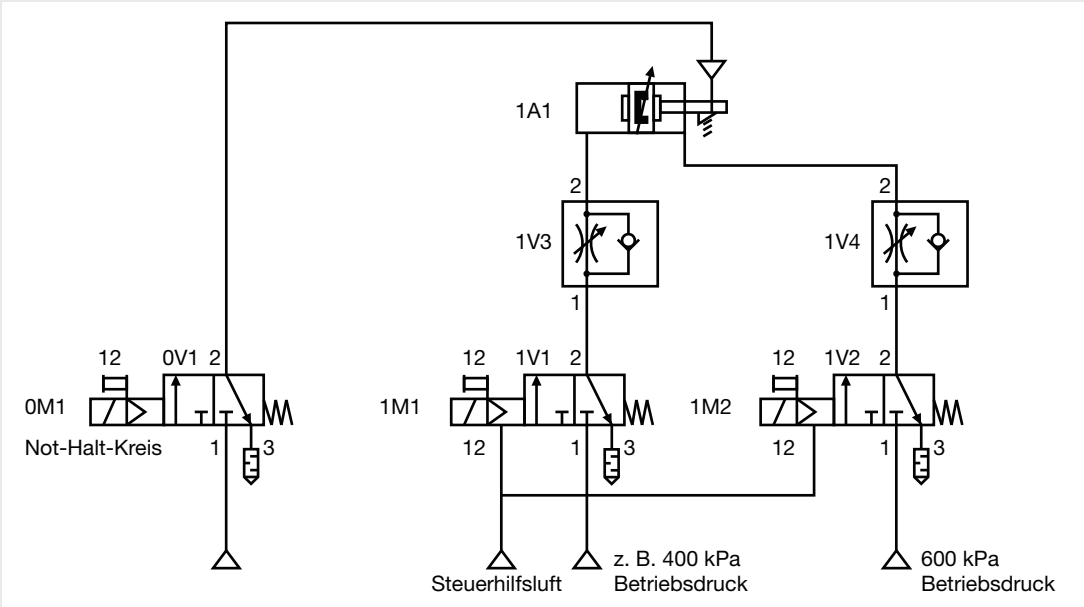
Mit zwei 3/2-Wegeventilen sind vier Schaltvarianten möglich: Der Zylinder ist auf beiden Seiten drucklos, wenn beide Ventile ausgeschaltet sind (wie im Schaltplan dargestellt). Sind beide Ventile geschaltet, wird der Zylinder auf beiden Seiten belüftet. Es bedarf eines Kräftegleichgewichts am Ventilkolben, damit beim Öffnen der Bremse die Kolbenstange bewegungslos bleibt. Dies erfordert an den beiden 3/2-Wegeventilen unterschiedliche Betriebsdrücke. Welche Werte hier notwendig sind, hängt von der Einbaulage und der Masse an der Kolbenstange ab.



Zylinder mit Bremse (Quelle: Festo)

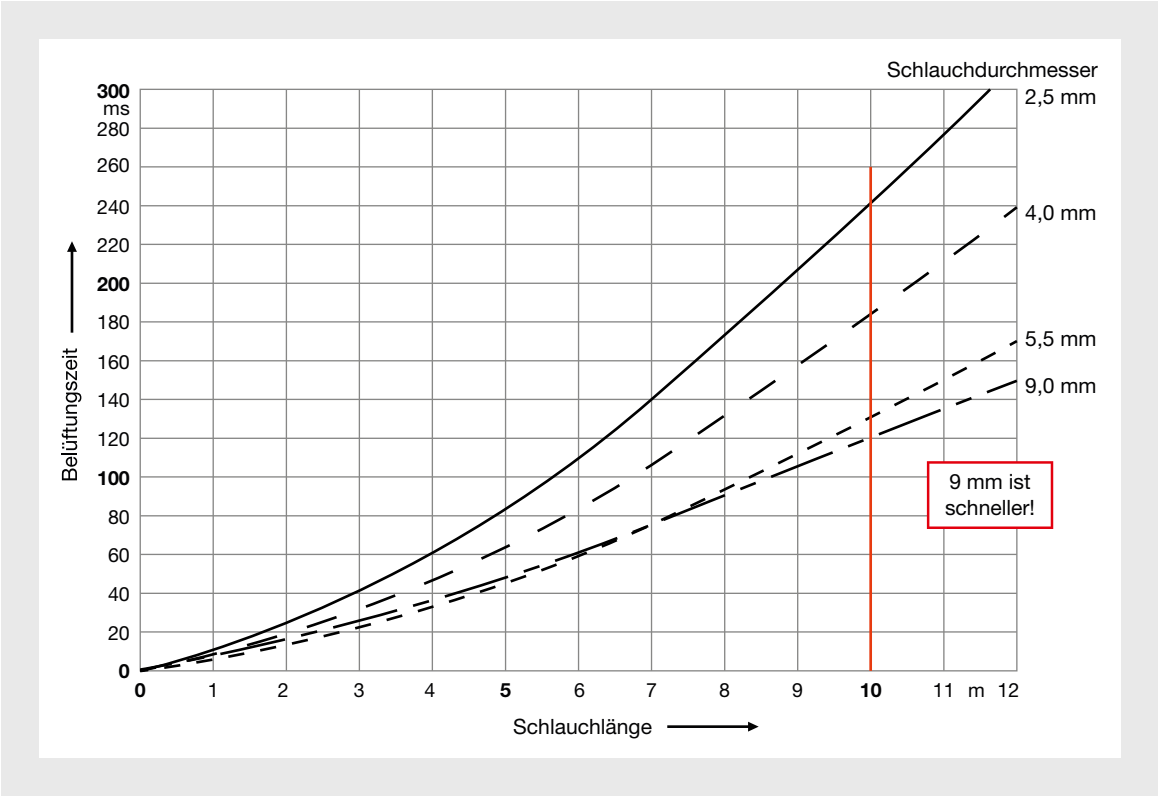
Nachdem die Bremse offen ist, schaltet eines der beiden Ventile 1V1 oder 1V2 ab, die Kolbenstange bewegt sich langsam in die gewünschte Richtung. Zwei Drossel-Rückschlagventile 1V3 und 1V4 sind für die langsame Bewegung verantwortlich. Diese Ventile sind als Abluftdrosseln eingebaut, um die aus dem Zylinder ausströmende Druckluft zu drosseln. Abluftdrosseln wirken nur, wenn sich Luft im Zylinder befindet, auch deshalb ist er vor dem Öffnen der Bremse zu belüften.

In diesem Zusammenhang sei nochmals an die richtige Auslegung der pneumatischen Antriebe erinnert, wie zuvor bei den grundlegenden und bewährten Prinzipien beschrieben. Denn die Auslegung erhält bei der Bremse eine besondere Bedeutung. Es ist eine häufig verbreitete Meinung, dass ein Druckluftsignal in einem dünnen Schlauch eine höhere Geschwindigkeit erreicht als in einem dicken Schlauch. Als Grund wird meist das geringere Volumen genannt. Das Strömungsverhalten im Schlauch hat jedoch eine weitaus höhere Bedeutung, wie die nachfolgende Grafik zeigt.



Zylinder mit Bremse (Quelle: Festo)

8.3 Pneumatische Konstruktion



Belüftungszeit in Abhängigkeit von Schlauchlänge und Durchmesser bei 6 bar (600 kPa) (Quelle: Festo)

Die Belüftungszeit nimmt mit steigender Schlauchlänge zu, bei dünnen jedoch stärker als bei dicken Schläuchen. Das Verhalten beim Entlüften ist gleich, die Reaktionszeit der Bremse hängt also vom Schlauch ab. Bei einem langen und dünnen Schlauch spricht die Bremse später an als bei einem kurzen und dicken Schlauch. Von Vorteil ist es deshalb immer, das Schaltventil direkt an die Bremse zu bauen. Die Bremse schließt, wenn der Druck unter ca. 3,5 bar fällt. Bei Druckluftabfall unter den eingestellten Betriebsdruck reagiert die Bremse folglich schneller. Vorsicht ist jedoch geboten, wenn der Maschinenbediener den Betriebsdruck an der Maschine selbst verstellen kann. Wird der Betriebsdruck höher, verlängert sich auch die Entlüftungszeit. Die Bremse reagiert später, der Nachlaufweg wird länger. Bremsen und Klemmpatronen sind 0-fehlersicher, d. h. sie können ausfallen. Eine Bremse ist, wie die Bremsen beim Auto, ständigem Verschleiß unterworfen. Sie muss daher in geeigneten Zeitabständen geprüft werden.

Nähere Angaben zur Auslegung und zum Test der Bremse sind dem Handbuch zu entnehmen bzw. beim Hersteller zu erfragen. Der Einfluss von Schlauchlänge und Durchmesser ist auch für die Geschwindigkeit von Zylindern wichtig. Je kürzer und dicker der Schlauch, desto schneller wird der Zylinder, desto höher ist die kinetische Energie und umso größer wird der Anhalteweg. Dies ist im Zusammenhang mit Lichtschranken etc. und dem erforderlichen Abstand zur Gefahrenstelle wichtig.

8.3.6 Schaltplan und Betriebsanleitung

Zum Abschluss einige Gedanken zu pneumatischen Schaltplänen: Die Maschinenrichtlinie fordert in Anhang 7 eine Betriebsanleitung. Diese Betriebsanleitung soll allen Personen, die an der Maschine arbeiten, sämtliche Informationen liefern, damit sie alle erforderlichen Arbeiten an der Maschine sicher durchführen können. Für den Instandhalter bedeutet dies, Schaltpläne zur Verfügung zu haben,

8.3 Pneumatische Konstruktion

die vollständig und richtig sind und mit der Maschine übereinstimmen. Er muss die Bauteile, die er auf dem Schaltplan sieht, an der Maschine wiederfinden können, sonst ist sicheres Arbeiten unmöglich. Anschlussbezeichnungen der Elemente sind im Schaltplan anzubringen, danach ist zu verschlauchen. Die Bauteilekennzeichnung der Komponenten und die Anschlussbezeichnung ist vorzunehmen. Diese muss über die gesamte Lebensdauer der Maschine erkennbar sein. Auf den Schaltplänen sind Hinweise auf sicherheitsrelevante Bauteile sinnvoll. Der Instandhalter erkennt damit die besondere Bedeutung der Bauteile. Neben den Bauteilbezeichnungen sind auch die richtigen Anschlussbezeichnungen anzugeben. Werden Schläuche wegen nicht korrekten Anschlussbezeichnungen falsch angeschlossen, so fährt die Kolbenstange plötzlich aus anstatt ein, wenn das Ventil elektrisch angesteuert wird.

Unter welchen Bedingungen wird nun ein Schaltplan gezeichnet und betrachtet? Alle Antriebe und Ventile befinden sich in der Ausgangsstellung, Druckluft ist vorhanden, selbst wenn das Einschaltventil an der Wartungseinheit ausgeschaltet dargestellt wird. Die Ausgangsstellung ist die Stellung der Antriebe, bevor man den Automatikbetrieb startet, und unterscheidet sich von der Stellung der Maschine in drucklosem Zustand. Bei vertikal eingebautem Zylinder ist die Kolbenstange ausgefahren, während bei diesem Zylinder die Kolbenstange in der Grundstellung eingefahren ist. Vor dem Start des Automatikbetriebes muss der Steuerungstechniker die Antriebe zunächst in die Ausgangsstellung bringen. Mit Ausnahme mechanisch direkt betätigter Endschalter sind alle Ventile im unbetätigten Zustand dargestellt. Bei monostabilen Ventilen und bei Mittelstellungsventilen ist diese Schaltstellung durch die mechanische Feder definiert.

Die Schaltplandarstellung beginnt links unten mit der Wartungseinheit oder Druckquelle und wird nach oben rechts weitergeführt. Beim Entwurf, also im Zuge der Planung des Schaltplans, sollte bei den Antrieben jedoch oben begonnen und erst am Ende die Wartungseinheit gezeichnet werden. Bevor der Konstrukteur sich über die Steuerventile für die Zylinder Gedanken macht, sollte er sich über die Einbaulage, das Verhalten bei Energieausfall und Wiederkehr (Pneumatik und Elektrik), die erforderliche Schutzmaßnahme, die Steuerungs- und Stoppkategorie im Klaren sein. Die häufige gedanklich fixe Zuordnung von 5/2-Wegeventilen zu doppelt wirkenden Zylindern führt meist zu dem vergeblichen Versuch, einzelne Zylinder mit sinnvollen, wirkungsvollen und vor allem preisgünstigen Sicherheitsschaltungen zu versehen.

Erst dann, wenn alle Anforderungen an die Zylinder definiert sind, kann über die Wartungseinheit nachgedacht werden. Möglicherweise verlangen die Zylinder unterschiedliche Betriebsdrücke, folglich sind mehrere Druckregler einzusetzen. Bei einem Not-Halt soll nur ein Teil der Druckluft abschalten, in einem anderen Teil der Maschine der volle Druck weiterhin verfügbar sein. Ventilinseln benötigen eine separate Steuerluftversorgung, dafür muss die Wartungseinheit eine passende Lösung anbieten. Bei Beachtung dieser Aspekte sieht eine Wartungseinheit oft ganz anders aus, als sie ursprünglich geplant war. Von Nachteil ist, wenn die Wartungseinheit bereits frühzeitig bestellt wurde: Zusätzlich erforderliche Teile müssen ausgesucht, bestellt und montiert werden, der dadurch notwendige Umbau ist aufwendig und kostet dementsprechend mehr Zeit und Geld. Die Angaben von Schlauchfarben und Schlauchquerschnitten, Verschraubungen und Schlauchnummern tragen zur Klarheit beim Aufbau und bei der Fehlerbehebung bei. Klarheit bedeutet immer ein Plus an Sicherheit und Geschwindigkeit, DIN ISO 1219, DIN ISO 5599 und DIN EN 81346-1 sind Normen zur Schaltplanerstellung und Kennzeichnung.

Ist die Sicherheitstechnik in der Pneumatik schwieriger als die Elektrotechnik? Im Grunde genommen: nein. Grundprinzipien und Grundgedanken sind gleich oder ähnlich. Das Medium Druckluft ist anders, für viele neu und ungewohnt. Wie bei elektrischen Antrieben ist in der Pneumatik auch die Mechanik zu betrachten: Ein Elektromotor wirkt nicht allein durch seine Welle, in der Regel folgt hier wie auch in der Pneumatik eine mehr oder minder umfangreiche Mechanik. Die Ausführungen dieses Kapitels mit seinen Beispielen, Gedanken und Anregungen sind lediglich eine erste Einführung in das Thema „Sicherheit und pneumatische Konstruktionen“ und reichen freilich nicht aus, um den sicheren Betrieb einer Maschine oder Anlage zu gewährleisten.

8.4 Hydraulische Konstruktion

8.4.1 Physikalisches Basiswissen

In der Hydraulik spricht man von hydrodynamischer Energieübertragung, d. h. es wird z. B. von einer Pumpe mechanische Energie auf das Öl übertragen und Strömungsenergie zum Antrieb z. B. eines Turbinenrades verwendet.

8.4.2 Vorteile der hydrostatischen Energieübertragung

Bei der hydrostatischen Energieübertragung spielen folgende Vorteile eine Rolle:

- Übertragung großer Kräfte und Leistungen auf kleinstem Raum
- feinfühlige stufenlose Regelbarkeit von Geschwindigkeiten
- problemlose Geschwindigkeitsregelungen unter Last innerhalb eines großen Verstellbereichs
- große Übersetzungsspanne bei Antrieben
- ruhiger Lauf, rasche und weiche Bewegungsumkehr
- einfacher und sicherer Überlastungsschutz
- hohe Abschaltgenauigkeit beim Stoppen des Arbeitsglieds
- hohe Lebensdauer und geringe Wartung der Anlagen dank Selbstschmierung der gleitenden Komponenten durch die Hydraulikflüssigkeit

8.4.3 Nachteile der hydrostatischen Energieübertragung

Folgende Nachteile sind zu erwähnen:

- Änderung der Arbeitsgenauigkeit bei Öl-Viskositätsschwankungen infolge Temperaturwechsels
- Dichtungsprobleme, vor allem bei hohen Systemdrücken und -temperaturen
- Löslichkeit von Luft in Hydraulikflüssigkeit. Entstehung von Luftblasen bei Druckabfall, dadurch Beeinträchtigung der Steuerungsgenauigkeit
- Führung der Hydraulikflüssigkeiten in einem Kreislauf mit Kühler und Filter

8.4.4 Definitionen

- Fluidtechnik: Übertragung, Steuerung und Verteilung von Energie und Signalen unter Verwendung eines unter Druck stehenden flüssigen oder gasförmigen Mediums
- Anlage: Anordnung miteinander verbundener Bauteile zur Übertragung und Steuerung fluidtechnischer Energie
- Bauteil: eine einzelne Einheit (z. B. Zylinder), bestehend aus einem oder mehreren Teilen, als funktionaler Bestandteil fluidtechnischer Anlagen
- Hydraulik: Wissenschaft und Technik, die sich mit der Nutzung einer Flüssigkeit als Druckmedium befassen
- Maximaler Betriebsdruck: der höchste Druck, mit dem eine Anlage unter gleichförmigen Bedingungen betrieben werden soll
- Bemessungsdruck: der höchste Druck, bei dem das Bauteil mit einer ausreichenden Anzahl von Lastwechseln betrieben werden kann
- Steuereinrichtung: eine Einrichtung, die eine Bestätigungseinrichtung mit einem Eingangssignal versorgt (Schalter)
- Bestätigungseinrichtung: eine Einrichtung, die ein Bauteil mit einem Ausgangssignal versorgt (Magnetspule)
- Leitungssystem: jede Kombination von Anschlussstücken, Kupplungen oder Verbindungsteilen mit Leitungen, Schläuchen oder Rohren, die das Strömen von Druckmedien zwischen den Bauteilen erlaubt

8.4 Hydraulische Konstruktion

8.4.5 Allgemeine hydraulische Beziehungen

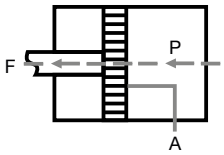
8.4.5.1 Druck, Absolutdruck und Überdruck

Druck p ist die auf die Fläche A entfallende Druckspannung, die auch kurz Druck genannt wird. Die Größe des Drucks an einem beliebigen Punkt ist unabhängig von der Lage. Die Maßeinheit des Drucks wird unter Verwendung der Basiseinheiten des internationalen Einheitensystems Kilogramm, Meter und Sekunde mit Pascal festgelegt.

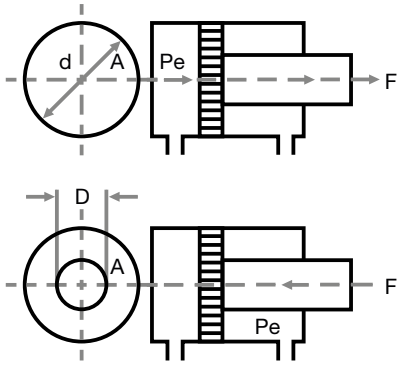
Absolutdruck: Die Absolutdruckskala beginnt mit $p_{abs} = 0$, da der Absolutdruck der Druck Null des leeren Raumes ist.

Überdruck: Die Differenz zwischen einem Absolutdruck und dem vorliegendem Atmosphärendruck p_{amb} wird als Überdruck bezeichnet.

Kolbendruckkraft

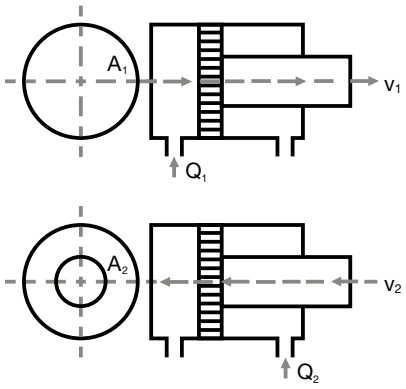
Abbildung	Gleichung/Gleichungsumstellung	Formelzeichen/Einheiten
	$F = 10 \times p \times A$ $F = p \times A \times \eta \times 10$ $A = \frac{d^2 \times \pi}{4}$ $A = \sqrt{\frac{4 \times F \times 0{,}1}{\pi \times p}}$ $p = 0{,}1 \times \frac{4 \times F}{\pi \times d^2}$	F = Kolbendruckkraft [N] p = Flüssigkeitsdruck [bar] A = Kolbenfläche [cm²] d = Kolbendurchmesser [cm] η = Wirkungsgrad Zylinder

Kolbenkräfte

Abbildung	Gleichung/Gleichungsumstellung	Formelzeichen/Einheiten
	$F = Pe \times A \times 10$ $F = Pe \times A \times \eta \times 10$ $A = \frac{d^2 \times \pi}{4}$ A für Kreisringfläche: $A = \frac{(D^2 - d^2) \times \pi}{4}$	F = Kolbendruckkraft [N] Pe = Überdruck auf den Kolben [bar] A = wirksame Kolbenfläche [cm²] d = Kolbendurchmesser [cm] η = Wirkungsgrad Zylinder d = Stangendurchmesser [cm]

8.4 Hydraulische Konstruktion

Kolbengeschwindigkeit

Abbildung	Gleichung/Gleichungsumstellung	Formelzeichen/Einheiten
	$v_1 = \frac{Q_1}{A_1}$ $v_2 = \frac{Q_2}{A_2}$ $A_1 = \frac{d^2 \times \pi}{4}$ $A_2 = \frac{(D^2 - d^2) \times \pi}{4}$	$v_{1,2}$ = Kolbengeschwindigkeit [cm/s] $Q_{1,2}$ = Volumenstrom [cm³/s] A_1 = wirksame Kolbenfläche (Kreis) [cm²] A_2 = wirksame Kolbenfläche (Ring) [cm²]

8.4.5.2 Gesetz von Pascal

Das Gesetz von Pascal bildet das Grundgesetz der Hydrostatik und gilt für inkompressible und nicht der Schwerkraft unterworfene Flüssigkeiten:

Wird auf eine in einem Behälter befindliche Flüssigkeit an irgendeiner Stelle ein Druck ausgeübt, so herrscht überall an der Innenwand des Behälters und dem Inneren der Flüssigkeit der gleiche Druck.

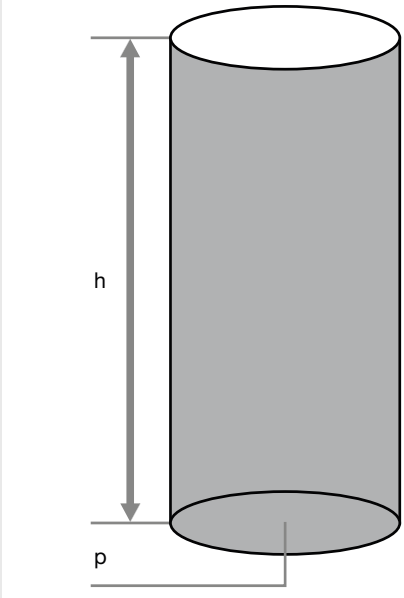
8.4.5.3 Schweredruck

Der allein von der Schwerkraft in der Flüssigkeit erzeugte Druck p_h ist gegeben durch

$$p_h = \rho \times g \times h$$

- ρ: Dichte der Flüssigkeit
- g: Gravitationskonstante (= 9,81 m/s²)
- h: Höhe der Flüssigkeitssäule

Bei der Auslegung von hydraulischen Systemen ist zu prüfen, ob der Schweredruck gegenüber den im System auftretenden Drücken eine beachtenswerte Größe annimmt. Meist findet der Schweredruck keine Beachtung, weil er oft kleiner ist als der benötigte Systemdruck.



Schweredruck

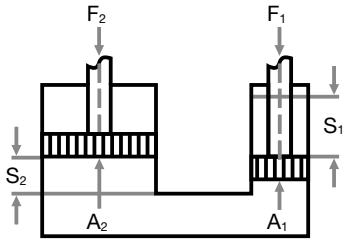
8.4 Hydraulische Konstruktion

8.4.5.4 Kraft- und Wegübersetzung

Das Prinzip der Kraft- und Wegübersetzung lässt sich am besten am Beispiel der hydraulischen Presse erläutern: Der von der Kraft F_1 erzeugte Druck p herrscht nach dem Gesetz von Pascal an allen Stellen der Flüssigkeit, somit auch an der Fläche A_1. Dies ergibt:

Somit lässt sich das Prinzip der Kraftübersetzung verdeutlichen: Ist beispielsweise die Fläche A_2 um das Zehnfache größer als die Fläche A_1 (A_2=10*A_1), so wird auch die Kraft F_1 um das Zehnfache ihres Wertes auf die Kraft F_2 übersetzt, gleichzeitig wird der zurückgelegte Weg S_1 auf den 10. Teil S_2 übersetzt.

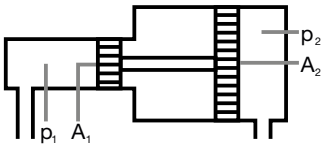
Kraft- und Wegübersetzung

Abbildung	Gleichung/Gleichungsumstellung	Formelzeichen/Einheiten
	$\frac{F_1}{A_1} = \frac{F_2}{A_2}$ $F_1 \times s_1 = F_2 \times s_2$ $\varphi = \frac{F_1}{F_2} = \frac{A_1}{A_2} = \frac{s_2}{s_2}$	F_1 = Kraft am Pumpenkolben [N] F_2 = Kraft am Arbeitskolben [N] A_1 = Fläche des Pumpenkolbens [cm²] A_2 = Fläche des Arbeitskolbens [cm²] s_1 = Weg des Pumpenkolbens [cm] s_2 = Weg des Arbeitskolbens [cm] φ = Übersetzungsverhältnis

8.4.5.5 Druckübersetzung

Das Prinzip der Druckübersetzung:

Druckübersetzer

Abbildung	Gleichung/Gleichungsumstellung	Formelzeichen/Einheiten
	$p_1 \times A_1 = p_2 \times A_2$	p_1 = Druck im kleinen Zylinder [bar] A_1 = Kolbenfläche [cm²] p_2 = Druck am großen Zylinder [bar] A_2 = Kolbenfläche [cm²]

Ist beispielsweise die Fläche A_1 doppelt so groß wie die Fläche A_2 (A_1=2*A_2), so wird der Druck p_1 auf das Doppelte seines Wertes zu p_2 übersetzt.

8.4.5.6 Hydraulische Arbeit

Wird bei der hydraulischen Presse der Kolben 1 mit der Fläche A_1 und Kraft F_1 um den Weg S_1 nach unten bewegt, so ist die dabei verrichtete hydraulische Arbeit W_1. Die bei diesem Vorgang am Kolben 2 mit der Fläche A_2 verrichtete hydraulische Arbeit ist W_2.

8.4.5.7 Volumetrischer Wirkungsgrad

Er berücksichtigt die sogenannten volumetrischen Verluste, die sich aufgrund von Leckströmen ergeben. Der hydraulisch-mechanische Wirkungsgrad ist ein Maß für Verluste, die sich durch Strömungsverluste und aufeinandergleitende Maschinenteile ergeben.

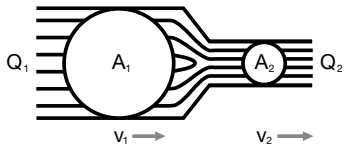
8.4 Hydraulische Konstruktion

8.4.5.8 Kontinuitätsgleichung

Voraussetzung: Durch ein Rohr mit unterschiedlich großen Querschnittsflächen strömt eine Flüssigkeit. Da zwischen den unterschiedlichen Querschnittsflächen kein Verlust an Flüssigkeit auftritt, gilt für die durch diese Flächen hindurchströmenden Massenströme:

$$A_1 \times V_1 = A_2 \times V_2 = A_3 \times V_3 = \text{konst.}$$

Kontinuitätsgleichung

Abbildung	Gleichung/Gleichungsumstellung	Formelzeichen/Einheiten
	$Q_1 = Q_2$ $Q_1 = A_1 \times v_1$ $Q_2 = A_2 \times v_2$ $A_1 \times v_1 = A_2 \times v_2$	$Q_{1,2}$ = Volumenströme [cm³/s, dm³/s, m³/s] $A_{1,2}$ = Querschnittsflächen [cm², dm², m²] $v_{1,2}$ = Strömungsgeschwindigkeiten [cm/s, dm/s, m/s]

8.4.5.9 Bernoulli-Gleichung

Die Bernoulli-Gleichung stellt einen Sonderfall der aus der Strömungsmechanik bekannten Navier-Stokes-Gleichung dar, die für dreidimensionale zähigkeitsbehaftete Strömungen gültig sind.
Die Gleichung für die Energieform ist:

$$\frac{V^2}{2} + g \times z + \frac{p}{\rho} = \text{konst.}$$

8.4.5.10 Strömungsformen

In den Rohrleitungen hydraulischer Anlagen treten laminare oder turbulente Strömungsformen auf. Bei der laminaren Strömung bewegen sich die Flüssigkeitsteilchen in geordneten voneinander getrennten Schichten. Man spricht deshalb von einer Strömungsrichtung. Die Strömungslinien verlaufen parallel zur Rohrachse. Bei der turbulenten Strömung bewegt sich die strömende Flüssigkeit nicht mehr in geordneten Schichten.

Die axial verlaufende Hauptströmung ist jetzt an allen Stellen überlagert durch regellos auftretende Längs- und Querbewegungen, die zu einer verwirbelten Strömung führen. Die Strömung wird dabei durchmischt. Der Umschlag von der laminaren in die turbulente Strömung erfolgt bei der Strömungsgeschwindigkeit v_{krit} in geraden Rohren mit Kreisquerschnitt d und Viskosität des Fluids v bei der kritischen Reynoldszahl Re_{krit} = 2 300.

$$\mathbf{v}_{krit} = \frac{\mathbf{Re}_{krit} \times \mathbf{v}}{d}$$

8.4 Hydraulische Konstruktion

8.4.5.11 Viskosität

Auf einer Flüssigkeitsschicht mit einer definierten Höhe h wird eine aufliegende Platte mit einer Fläche A mit konstanter Geschwindigkeit v bewegt. Zum Aufrechterhalten der Bewegung ist die Kraft F erforderlich. Zwischen Platte und Flüssigkeitsgrund bildet sich bei nicht zu großer Schichtdicke h ein lineares Geschwindigkeitsgefälle dv/dz aus.

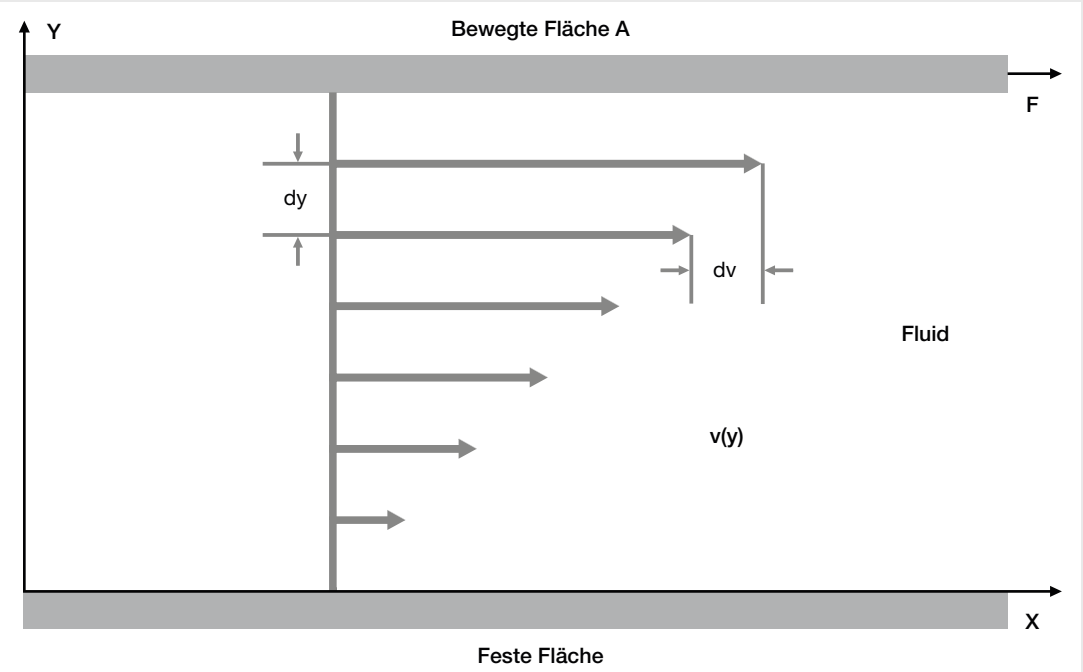
Die von Newton gefundene Gesetzmäßigkeit

$$\frac{F}{A} = \tau = \eta \times \frac{dv}{dz}$$

ist als newtonsches Reibungsgesetz bekannt.

Hierbei bedeuten τ die Reibungsschubspannung und η die dynamische Viskosität der Flüssigkeit, die als Stoffgröße ein Maß für die innere Reibung die erschwerte Verschiebbarkeit der Flüssigkeitsteilchen gegeneinander darstellt. Die für die Verschiebung aufgewendete Arbeit wird in Wärme umgewandelt. Die Definition der in der Hydraulik verwendeten Viskosität:

$$[\eta] = N \times \frac{s}{m^2} \qquad v = \frac{\eta}{\rho}$$



Newtonsches Reibungsgesetz

8.4 Hydraulische Konstruktion

8.4.5.12 Druckverluste in Rohren, Formstücken und Ventilen

Bei der reibungsfreien Strömung einer Flüssigkeit ist die aus Druckenergie, kinetischer und potenzieller Energie zusammengesetzte Gesamtenergie konstant. Bei der Strömung realer (reibungsbehafteter) Flüssigkeiten wird aufgrund des Einflusses der Viskosität ein Teil der Strömungsenergie in Wärmeenergie umgewandelt, die technisch nicht genutzt werden kann und deshalb auch als Strömungsverlust bezeichnet wird. Von Verlusten durch Reibungseinflüsse kann nur die Druckenergie betroffen werden. In Formstücken (Rohrbögen, Rohrabzweigungen, Erweiterungen, Verengungen) treten durch Reibungseinflüsse u. U. erhebliche Druckverluste auf. Die rechnerische Erfassung erfolgt unter Verwendung der ermittelten Größe des Widerstandbeiwerts.

8.4.5.13 Kavitation

Kavitation bezeichnet die Entstehung von Blasen (Luft- und Dampfblasen) an Engstellen von Hydraulik-Bauteilen als Folge von Druckabsenkungen und des schlagartigen Zusammenfallens der Blasen nach Verlassen der Engstelle. Zwei Kavitationsarten sind zu unterscheiden: die Luftblasen- und die Dampfblasenkavitation. Beide Kavitationsarten haben ähnlich negative Auswirkungen auf die Bauteile von Hydraulikanlagen.

8.4.5.14 Luftblasenkavitation

Flüssigkeiten besitzen die Eigenschaft, Gase in sich aufzulösen. Man spricht in diesem Zusammenhang vom Gaslösevermögen der Flüssigkeiten. In Hydrauliköl befindet sich insbesondere Luft in gelöstem Zustand. Neben der gelösten Form kann die Luft auch als Luftblasen im Öl auftreten. Das geschieht dann, wenn der statische Druck des Öls örtlich bis auf den Gaslösedruck absinkt und damit die Aufnahmefähigkeit des Öls für Luft erschöpft ist.

8.4.5.15 Dampfblasenkavitation

Diese tritt ein, wenn sich Dampfblasen im Öl durch Absinken des statischen Drucks bis auf oder unter den Dampfdruck des Öls bilden. Auch hier geschieht das Absinken des Drucks durch die an Engstellen in Hydraulik-Bauteilen vorliegenden erhöhten Strömungsgeschwindigkeiten.

8.4.5.16 Hydropumpen

Das Herzstück eines hydraulischen Systems ist die Hydropumpe. Die über ihre Antriebswelle in der Regel durch einen Elektromotor zugeführte mechanische Energie wird dazu benötigt, die Energie bzw. den Druck des durch die Pumpe strömenden Öls zu erhöhen und alle in der Pumpe auftretenden Verluste zu decken. Die Energie des am Druckanschluss der Pumpe austretenden Volumenstroms, auch hydrostatische Energie genannt, steht dann für den Betrieb von hydraulischen Anwendungen zur Verfügung. Hydrosysteme erfordern in der Regel hohe Drücke bei kleinen Förderströmen, die nur in seltenen Fällen größer als 300 l/min sind. Deshalb sind Kreißelpumpen für diesen Einsatz nicht geeignet. Hydropumpen arbeiten nach dem Verdrängerprinzip wie z. B. Radialkolbenpumpen. Dieses System basiert auf dem sich verkleinernden und vergrößernden Raum. Unter dem Verdrängervolumen, auch Hubvolumen genannt, versteht man das bei einer Umdrehung der Pumpe geförderte Ölvolumen.

Bei den Hydropumpen ist zu unterscheiden zwischen Konstant- und Verstellpumpen: Bei Konstantpumpen kann das Verdrängungsvolumen Vi nicht verändert werden. Bei Verstellpumpen ist das Verdrängungsvolumen Vi eine veränderbare Größe und von der Volumeneinstellung abhängig. Der theoretische Förderstrom der Pumpe ergibt sich aus der Multiplikation des Verdrängervolumens mit der Drehzahl der Pumpe.

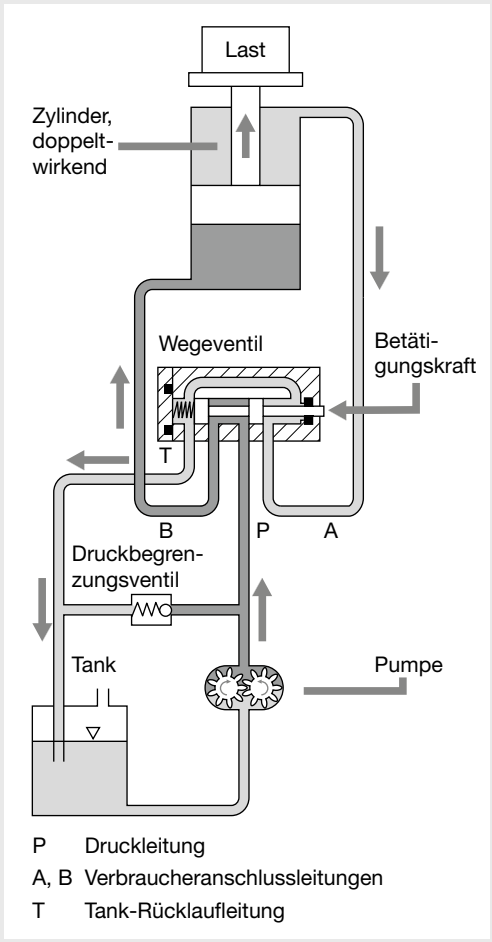
8.4 Hydraulische Konstruktion

8.4.6 Aufbau eines Hydrauliksystems

Der hydraulische Schaltplan zeigt den Aufbau eines Hydraulikkreislaufes. Die einzelnen Hydraulikgeräte sind durch genormte Bildzeichen (Symbole) dargestellt und durch Leitungslinien miteinander verbunden. Die nächsten Bilder zeigen einfache Hydraulikkreisläufe. Die Geräte sind hier nicht durch genormte Symbole, sondern schematisch so dargestellt, dass ihre Wirkungsweise zu erkennen ist. Die Pumpe saugt das Hydrauliköl aus dem Behälter und drückt es in das Leitungssystem mit den eingebauten Geräten. Das Öl strömt von P nach B durch ein Wegeventil in den Hydrozylinder. Der Kolben (mit Werkzeug) stellt für das Öl einen Widerstand dar. Der Druck steigt im Leistungsteil zwischen Pumpe und Kolben so lange an, bis die Kolbenkraft zum Überwinden der Belastung ausreicht und der Kolben sich bewegt.

8.4.7 Einfacher Hydraulikkreislauf, Auffahrt

Das Wegeventil wird durch eine beliebige Betätigungskraft in Stellung gehalten. Der Kolben fährt in die obere Endlage. Das verdrängte Öl fließt über das Wegeventil von A nach T in den Tankbehälter zurück. Das Wegeventil steuert also die Richtung des Ölstroms. Damit das System vor zu hohen Belastungen (Drücken) geschützt wird, ist in der Druckleitung hinter der Pumpe ein Druckbegrenzungsventil eingebaut. Wird der eingestellte Druck überschritten, öffnet sich das Ventil und das restliche Öl fließt in den Tank. Der Druck steigt nicht weiter an.



Aufbau eines Hydrauliksystems

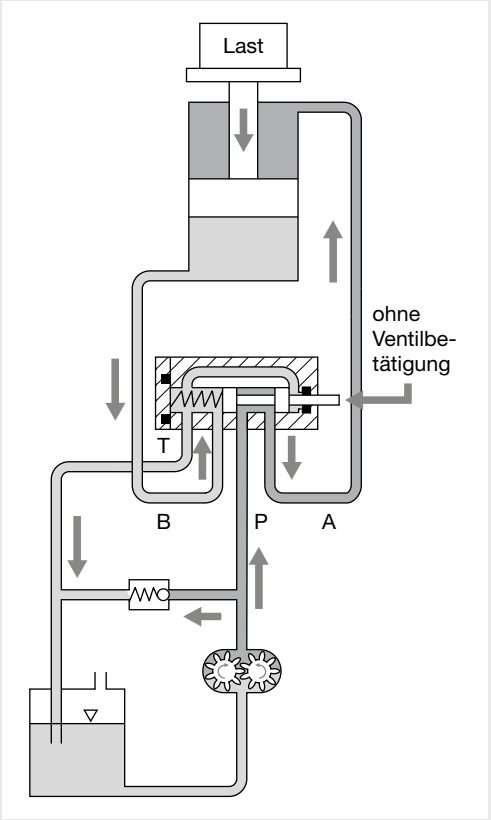
8.4 Hydraulische Konstruktion

8.4.8 Einfacher Hydraulikkreislauf, Abwärtsfahrt

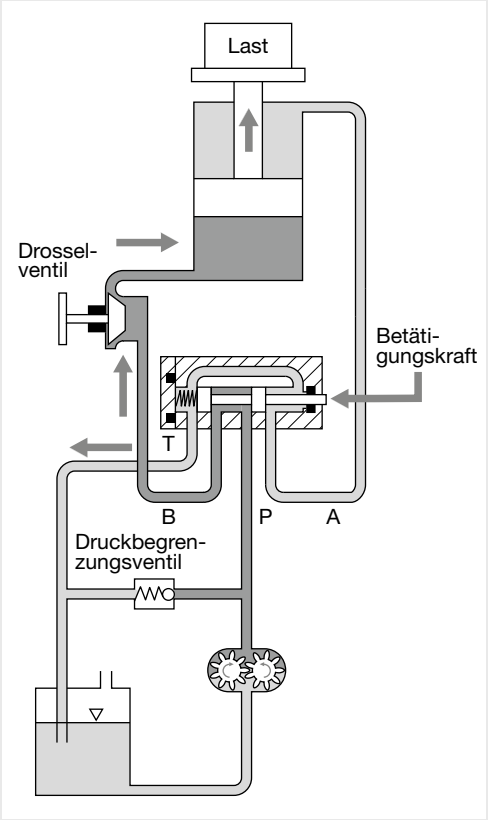
Wird die Betätigungskraft zurückgenommen, so wird das Wegeventil über die Federkraft zurückgestellt. Der Ölstrom fließt jetzt von P nach A zur Stangenseite des Kolbens. Der Kolben bewegt sich nun auf die untere Endlage zu, das verdrängte Öl fließt über das Wegeventil von B nach T in den Tankbehälter zurück. Das Umschalten des Wegeventils ermöglicht so eine ständige Hin- und Herfahrt des Kolbens.

8.4.9 Einfacher Hydraulikkreislauf, Geschwindigkeit

Soll nicht nur die Bewegungsrichtung des Kolbens, sondern auch noch die Geschwindigkeit gesteuert werden, so ist die in den Zylinder einfließende und abfließende Ölmenge zu verändern. Das lässt sich mit einem Drosselventil erreichen: Verringert man den Ventilquerschnitt, strömt in einer definierten Zeiteinheit weniger Öl in den Zylinder. Der Ölstrom ist kleiner als vor der Drosselung, die Kolbengeschwindigkeit wird gemäß Kontinuitätsgleichung ebenfalls kleiner, d. h. die Kolbengeschwindigkeit ist proportional zum Ölstrom. Die Geschwindigkeitssteuerung erfolgt also durch eine Ölstromsteuerung.



Abwärtslauf beim einfachen Hydraulikkreislauf

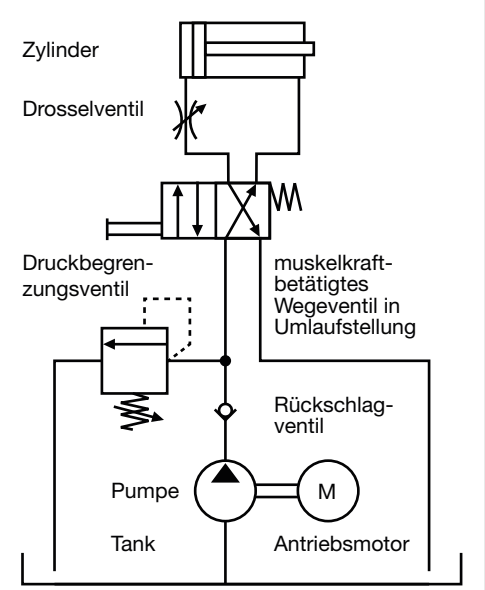


Steuerung der Geschwindigkeit beim einzelnen Hydraulikkreislauf

8.4 Hydraulische Konstruktion

8.4.10 Einfacher Hydraulikkreislauf-Schaltplan

Nachfolgend ist der eben erklärte Hydraulikablauf als hydraulischer Schaltplan dargestellt. Das Wegeventil ist handbetätigt. Es wird federzentriert durch Federkraft unbetätigt in der Abwärtsstellung gehalten.



Schaltplan eines einfachen Hydraulikkreislaufs

8.4 Hydraulische Konstruktion

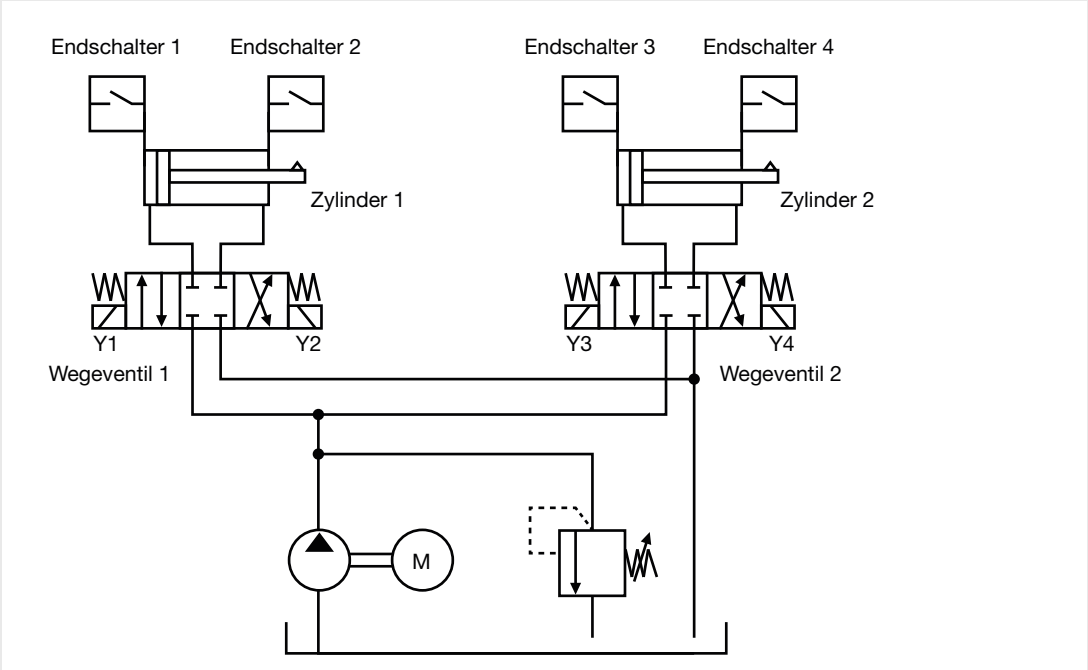
8.4.11 Zweizylindersteuerungen mit elektrischen Ventilen

Sollen in einer Hydraulikanlage zwei oder mehr Zylinder zum Einsatz kommen, können damit verschiedene Forderungen verbunden sein, die sich mit unterschiedlichen Schaltungen realisieren lassen:

- Folgeschaltungen
- Gleichlaufschaltungen
- Serienschaltungen
- Parallelschaltungen

Nachstehend ist eine Folgeschaltung zu sehen (Folgeschaltung mit Endschaltern und Magnetventilen): Bei der Version mit Endschaltern betätigen die Kolbenstangen wegabhängig Endschalter (die Elektrik ist nicht dargestellt):

1. Start: Spule Y1 bestromt, Wegeventil 1 nach links, Kolben von Zylinder 1 nach rechts
2. Endschalter 2 betätigt: Spule Y1 stromlos, Spule Y3 bestromt, Wegeventil 2 nach links, Kolben von Zylinder 2 nach rechts
3. Endschalter 4 betätigt: Spule Y3 stromlos, Spule Y2 bestromt, Wegeventil 1 nach rechts, Kolben von Zylinder 1 nach links
4. Endschalter 1 betätigt: Spule Y2 stromlos, Spule Y4 bestromt, Wegeventil 2 nach rechts, Kolben von Zylinder 2 nach links
5. Endschalter 3 betätigt: Spule Y4 stromlos, Spule Y1 bestromt, Wegeventil 1 nach links, Kolben von Zylinder 1 nach rechts (weiter mit Schritt 2)



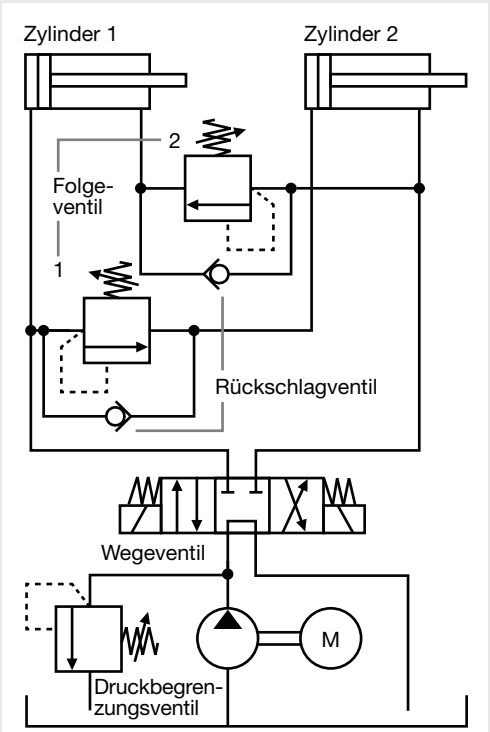
Schaltplan Zweizylindersteuerungen mit elektrischen Ventilen

8.4 Hydraulische Konstruktion

8.4.12 Zweizylindersteuerungen mit Folgeventilen

Die Folgeventile 1 und 2 sind Druckventile, die sich bei einem bestimmten einstellbaren Druck öffnen. Sie schließen sich wieder, wenn der anliegende Druck abfällt. Daraus ergibt sich folgender Bewegungsablauf:

1. Wegeventil links angesteuert: Die Kolbenseite des Zylinders 1 wird beaufschlagt, der Zylinder fährt aus. Beim Anschlag des Kolbens steigt der Druck über den am Druckbegrenzungsventil eingestellten Druck.
2. Folgeventil 1 öffnet: Das Fluid strömt zur Kolbenseite des Zylinders 2, der Zylinder fährt ebenfalls aus.
3. Wegeventil rechts angesteuert, die Stangenseite des Zylinders 2 wird beaufschlagt, der Zylinder fährt ein. Beim Anschlag des Kolbens steigt der Druck über den am Druckbegrenzungsventil eingestellten Druck.
4. Folgeventil 2 öffnet: Das Fluid strömt zur Stangenseite des Zylinder 1. Der Kolben fährt ebenfalls ein.



Schaltplan Zweizylindersteuerungen mit Folgeventilen

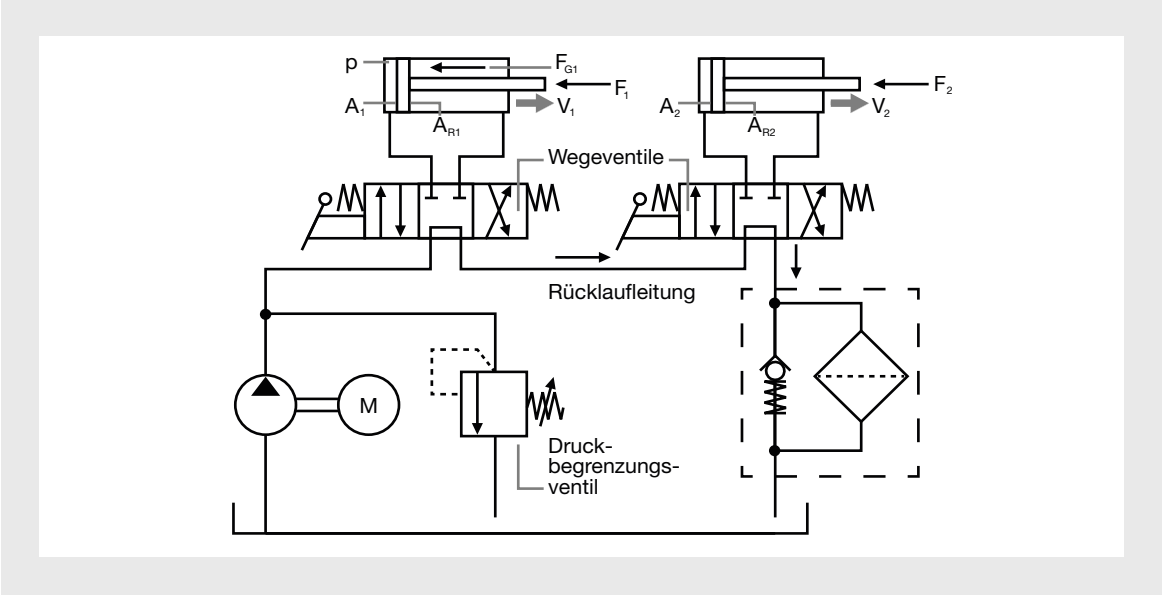
8.4 Hydraulische Konstruktion

8.4.13 Serienschaltung

Die Serienschaltung wird wie bei hintereinander geschalteten Ventilen realisiert. Dabei führt man die Rücklaufleitung nicht wie bei der Einzelschaltung in den Tank zurück, sondern zum Wegeventil des zweiten Zylinders. Betreibt man bei dieser Schaltung beide Zylinder gleichzeitig, so tritt eine gegenseitige Beeinflussung von Kolbenkraft und Kolbengeschwindigkeit ein. Damit ergeben sich folgende Verhältnisse: Der Systemdruck p, der auf die Kolbenfläche des Zylinders 1 wirkt, muss so groß sein, dass nicht nur die eigene Hubkraft F_1 erzeugt, sondern auch die vom Zylinder 2 erzeugte Gegenkraft F_{G1} überwunden wird. Diese Gegenkraft entsteht dadurch, dass der zum Arbeiten von Zylinder 2 erforderliche Öldruck auf die Kolbenringfläche von Zylinder 1 zurückwirkt. Die Ringfläche von Zylinder 1 verdrängt das Öl und fördert es zum Zylinder 2. Dessen Geschwindigkeit hängt also vom Rücklaufstrom des Zylinders 1 ab. Die Ausfahrgeschwindigkeit des Zylinders 1 verhält sich zur Ausfahrgeschwindigkeit von Zylinder 2 wie die Kolbenfläche des Zylinders 2 zur Ringfläche des Zylinders 1.

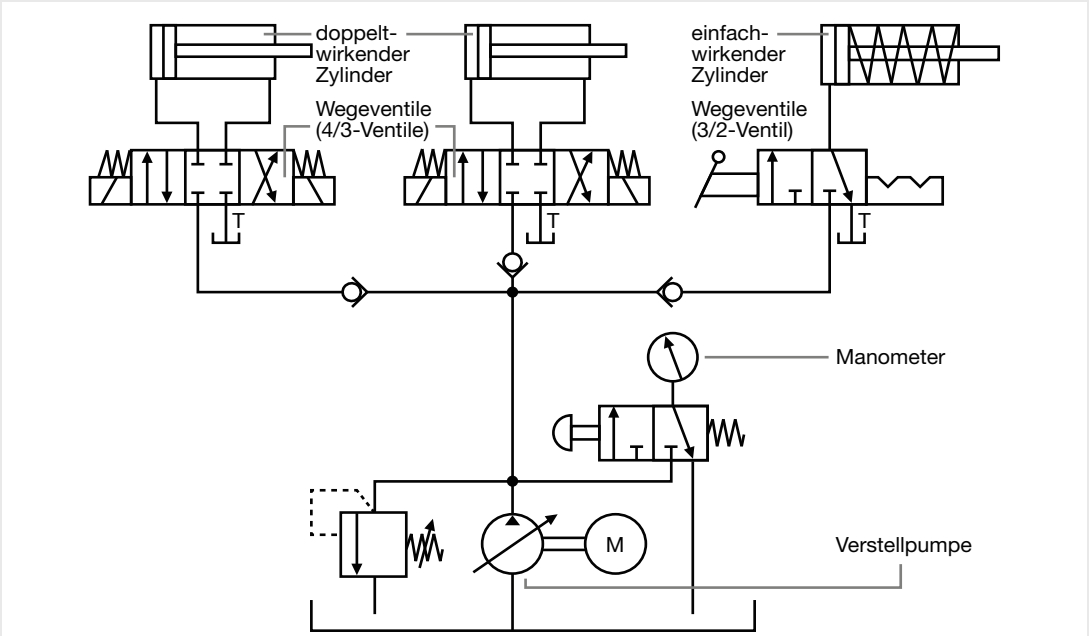
8.4.14 Parallelschaltung

Im Gegensatz zur Serienschaltung tritt bei der Parallelschaltung keine gegenseitige Beeinflussung auf, wenn alle Zylinder gleichzeitig arbeiten. Die Ölversorgung erfolgt über eine Leitungsverzweigung. Bis zu den Wegeventilen herrscht der am Druckbegrenzungsventil eingestellte Systemdruck. Bei der Parallelschaltung muss genügend Flüssigkeit zur Verfügung stehen, um den erforderlichen Systemdruck aufrechtzuerhalten, wenn die Zylinder gleichzeitig ausfahren sollen. Fördert die Pumpe zu wenig, fährt der Zylinder mit dem geringsten Arbeitswiderstand zuerst aus. Ist er in der Endlage, steigt der Druck weiter, bis er für den nächsten Zylinder ausreicht. Die Zylinder fahren also in Abhängigkeit vom erforderlichen Arbeitsdruck aus.



Schaltplan Serienschaltung

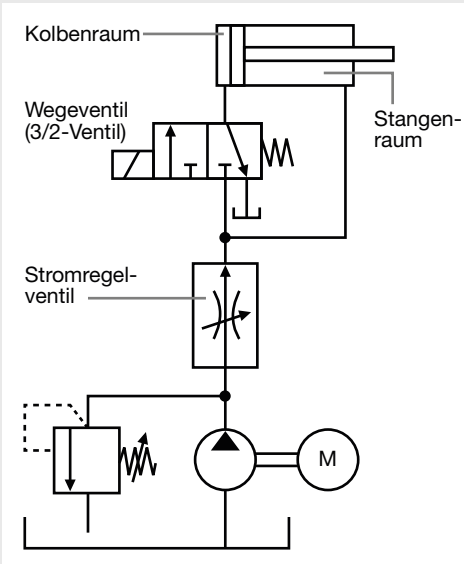
8.4 Hydraulische Konstruktion



Schaltplan Parallelschaltung

8.4.15 Differenzialschaltung

Der Stangenraum steht ständig unter Druck, der Kolbenraum ist mit einem Wegeventil verbunden. Man nennt diese Schaltung Differenzialschaltung, weil die an der Kolbenstange wirkende Kraft sich im Verhältnis Kolbenfläche zu Stangenfläche ausdrückt. Die Differenzialschaltung wird eingesetzt, wenn der Kolben hydraulisch eingespannt und die Pumpe möglichst klein sein soll oder eine schnelle Bewegung des Kolbens gefordert ist. Fährt der Kolben über das Wegeventil aus, wird die von der Ringfläche verdrängte Flüssigkeit vor dem Wegeventil mit dem Pumpenförderstrom vereinigt und der Kolbenseite des Zylinders wieder zugeführt. Bei dieser Schaltung ergibt sich die von der Kolbenstange ausgeübte Kraft aus dem Produkt Druck mal Stangenfläche.



Schaltplan Differenzialschaltung

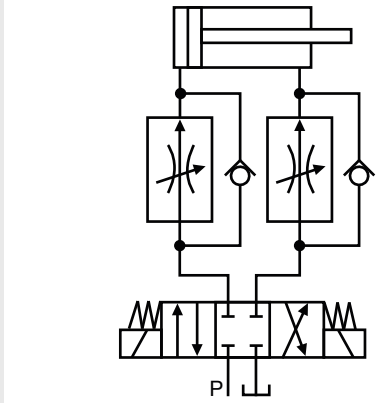
8.4 Hydraulische Konstruktion

8.4.16 Geschwindigkeitssteuerungen

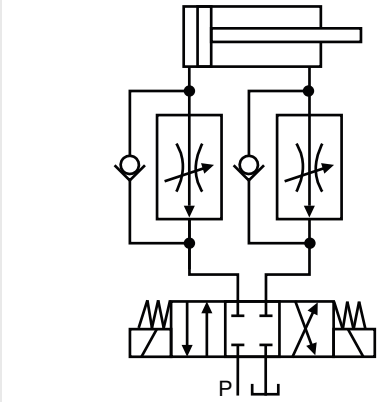
Zur Geschwindigkeitssteuerung setzt man Stromventile ein. Stromventile sind z. B. Drossel- oder Stromregelventile. Hier gibt es zwei Möglichkeiten: Primärsteuerung oder Sekundärsteuerung.

Primärsteuerung: Bei der Primärsteuerung sitzt das Stromventil im Zulauf zwischen Wegeventil und Zylinder. Es steuert die zuströmende Druckflüssigkeit. Das Schaltzeichen zeigt ein Zweiwege-Stromregelventil. Parallel dazu ist ein Rückschlagventil geschaltet, das den Zulaufstrom sperrt und den Rücklaufstrom durchlässt. Es bewirkt also, dass der Flüssigkeitsstrom nur im Vorlauf, nicht aber im Rücklauf durch das Stromventil fließt. Gesteuert wird also nur eine Richtung des Kolbens. Ist auch die Steuerung der anderen Richtung erforderlich, sind zwei Stromregelventile zu installieren. Die Primärsteuerung hat den Nachteil, dass bei einem plötzlich abfallenden Arbeitswiderstand der Kolben springt. Ein Gegenhalteventil kann das verhindern.

Sekundärsteuerung: Bei der sekundären Steuerung sitzt das Stromventil im Ablauf zwischen Wegeventil und Zylinder. Es steuert somit den Rücklaufstrom. Das Schaltzeichen zeigt ein Zweiwege-Stromregelventil. Parallel dazu ist ein Rückschlagventil geschaltet, das den Rücklaufstrom sperrt, den Vorlaufstrom jedoch durchlässt. Es bewirkt also, dass der Flüssigkeitsstrom nur im Rücklauf, nicht aber im Vorlauf durch das Stromventil fließt. Gesteuert wird also nur eine Richtung des Kolbens. Wenn auch die andere Richtung zu steuern ist, sind zwei Stromregelventile einzubauen. Die Sekundärsteuerung hat nicht den Nachteil, dass der Kolben springen kann.

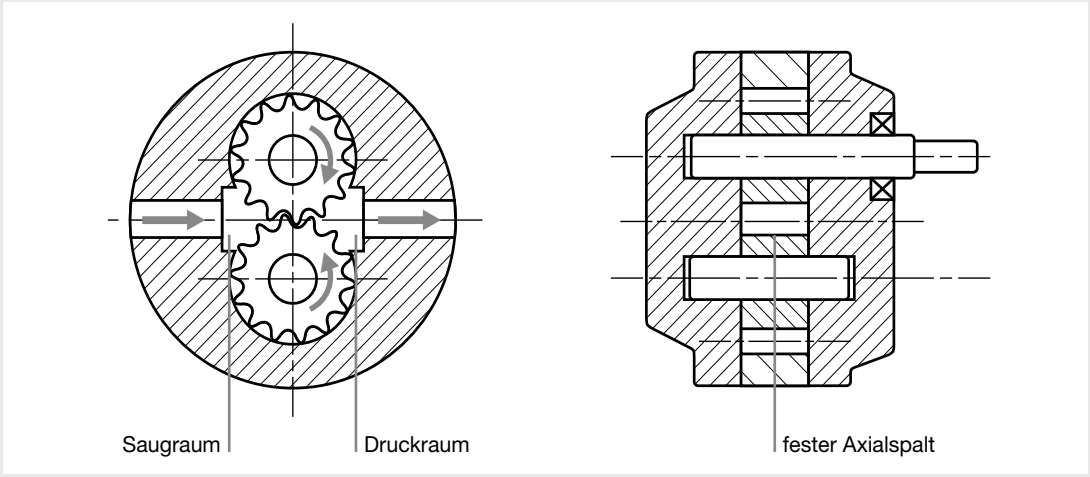


Schaltplan Primärsteuerung



Schaltplan Sekundärsteuerung

8.4 Hydraulische Konstruktion

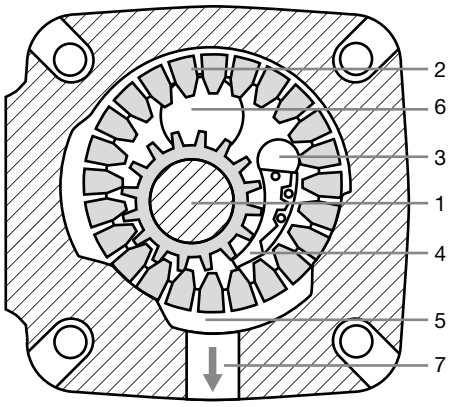


Außenverzahnte Zahnradpumpen

8.4.17 Antriebspumpen, Konstantpumpen

Außenverzahnte Zahnradpumpe: Die von der Saug- zur Druckseite geförderte Flüssigkeit wird durch das Ineinandergreifen der Zähne wechselseitig aus den Lücken verdrängt. Vorteile: preiswerte Standardpumpe mit hohem Wirkungsgrad, die mit anderen Pumpen gleichen Prinzips zusammenschaltbar ist. Nachteile: sehr hoher Geräuschpegel. Einsatz: in offenen Kreisläufen industrieller Nutzungen.

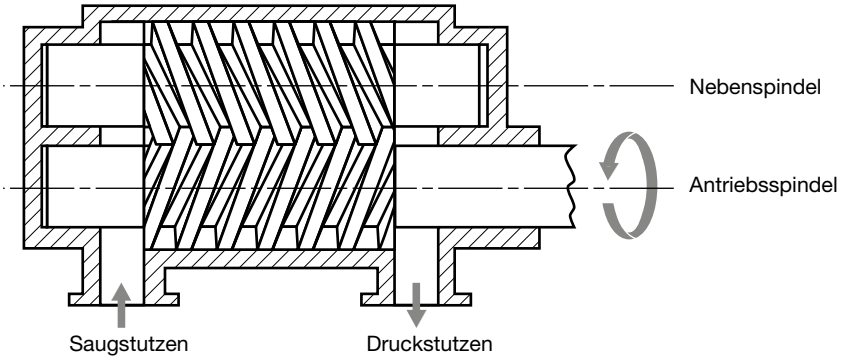
Innenverzahnte Zahnradpumpen: Eine angetriebene Ritzelwelle (1) nimmt ein Hohlrad (2) mit. Die Zahnkammern füllen sich saugseitig, das Füllstück trennt druckseitig Saug- und Druckzone. Druckseitig wird das Öl so durch das Hohlrad hindurch verdrängt. Vorteile: geräuscharme Standardpumpe mit hohem Wirkungsgrad, die mit anderen Pumpen gleichen Prinzips zusammenschaltbar ist, niedrigerer Geräuschpegel. Nachteile: teurer als die übliche Zahnradpumpe. Einsatz: in offenen Kreisläufen industrieller Anwendungen mit hohen Anforderungen an die Laufruhe.



1 Ritzelwelle
2 Hohlrad
3 Füllstückstift
4 Füllstück
5 hydrostatisches Lager
6 Sauganschluss
7 Druckanschluss

Innenverzahnte Zahnradpumpen

8.4 Hydraulische Konstruktion

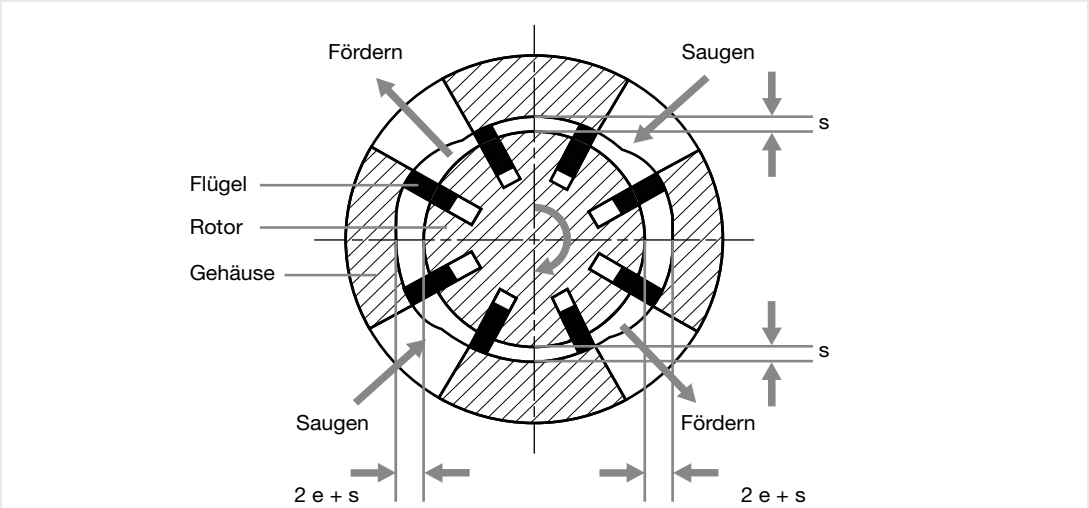


Schraubenpumpe

8.4.18 Antriebspumpen, Schraubenpumpen

Zwei miteinander angetriebene sich kämmende Spindeln bilden im Gehäuse Ölkammern, die bei Rotation vom Saug- zum Druckstutzen bewegt werden. Vorteile: pulsfreier Förderstrom, geringer Geräuschpegel. Nachteile: relativ niedriger Wirkungsgrad durch hohe volumetrische Verluste, dadurch hohe Ölviskosität erforderlich. Einsatz: in offenen Kreisläufen der Industrie, z. B. bei Präzisionsmaschinen und in der Aufzugsindustrie. Hohe Volumenströme.

8.4 Hydraulische Konstruktion



Antriebspumpe mit Flügelzellen

8.4.19 Antriebspumpen, Flügelzellenpumpen

Bewegliche Flügel in Schlitzen des Rotors, die durch Fliehkraft und Druck an die Gehäusewand gepresst werden. Die Zellen vergrößern sich bei ihrer Verbindung mit dem Sauganschluss, sie verkleinern sich bei ihrer Verbindung mit dem Druckanschluss. Vorteile: pulsfreier Förderstrom, geringer Geräuschpegel, zu Mehrstrompumpen zusammenflanschbar. Nachteile: niedrigerer Wirkungsgrad als Zahnradpumpen, schmutzempfindlicher. Einsatz: in offenen Kreisläufen der Industrie, z. B. bei Präzisionsmaschinen mit niedrigerem Druck.

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik

8.5.1 Sicherheitsanforderungen im Allgemeinen

Beim Entwurf hydraulischer Anlagen für Maschinen sind alle beabsichtigten Betriebszustände und Anwendungen zu berücksichtigen. Zur Ermittlung der Gefahren ist nach EN ISO 12100 eine Risikobewertung durchzuführen. Soweit realisierbar, sind möglichst alle identifizierten Risiken beim Entwurf der Anlage auszuschalten. Wo dies nicht möglich ist, sind geeignete Schutzmaßnahmen vorzusehen.

8.5.2 Entwurf und Auslegung

Alle sicherheitsrelevanten Bauteile einer Anlage sind so auszuwählen, dass sie die Sicherheit während des Betriebes gewährleisten und innerhalb der festgelegten Grenzen zuverlässig arbeiten.

- Alle Teile der Anlage müssen für den maximalen Betriebsdruck der Anlage ausgelegt sein oder durch anderweitige Schutzmaßnahmen gegen Drücke oberhalb der zulässigen Grenzwerte gesichert werden.
- Bevorzugte Schutzeinrichtungen gegen unzulässig hohen Druck sind ein oder mehrere Druckbegrenzungsventile, die den Druck in allen Teilen der Anlage begrenzen.
- Anlagen sind so zu entwerfen, zu bauen und einzustellen, dass sie Druckstöße und Druckverstärkungen minimieren können. Druckstoß und verstärkter Druck dürfen keine Gefährdungen verursachen.

8.5.3 Weitere Sicherheitsanforderungen

Leckagen:

- Im System auftretende Leckagen dürfen keine Gefährdungen verursachen.

Energieversorgung:

- Die elektrische oder hydraulische Energieversorgung darf keine Gefährdung hervorrufen. Dies gilt im besonderen für
- Ein- oder Ausschalten der Energieversorgung,
- Energiereduzierung,
- Ausfall und/oder Wiederkehr der Energie.

Unerwarteter Anlauf:

- Die Anlage ist so zu konzipieren, dass bei vollkommener Trennung im druckbeaufschlagten Medium in der Anlage ein unerwarteter Wiederanlauf verhindert wird.
- Möglichkeit der mechanischen Verriegelung von Sperrventilen in der Absperrposition und Abbau des Drucks im Steuersystem
- Trennung von der elektrischen Energieversorgung (EN 60204-1)

Mechanische Bewegungen:

- Diese dürfen weder beabsichtigt noch unbeabsichtigt zu einer Personen gefährdenden Situation führen.

Geräuscharme Konstruktion:

- Die Anforderungen der EN ISO 11688-1 sind unbedingt zu beachten.

Betriebstemperaturen:

- Die Temperatur des Druckmediums darf die für alle Bauteile der Anlage als Grenzwert festgelegte maximale Arbeitstemperatur nicht überschreiten.

Betriebsdruckbereich:

- Der für die jeweiligen Anlageteile zulässige Betriebsdruck muss eingehalten werden.

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik

Kupplungen oder Befestigungsteile:

- Antriebskupplungen und Befestigungsteile müssen unter sämtlichen Betriebsbedingungen das maximale Drehmoment dauerhaft übertragen können.

Drehzahl:

- Die Drehzahl darf das in der Herstellerdokumentation angegebene Maximum nicht überschreiten.

Hubanschläge:

- Einstellbare Hubanschläge sind durch geeignete Mittel sicherzustellen.

Ventile mit definierter Schaltstellung:

- Jeder Antrieb, der bei einem Versagen der Steuerung seine Stellung beibehalten oder eine bestimmte Sicherheitsstellung einnehmen muss, ist durch ein Ventil zu steuern, das eine definierte Schaltstellung entweder durch Federvorspannung oder per Einrastvorrichtung gewährleistet.

Hydraulische Anlagen mit Hydrospeicher:

- Hydraulische Anlagen mit Hydrospeichern dienen dazu, den Speicherflüssigkeitsdruck automatisch zu regulieren. Bei Wartungsarbeiten an der Anlage ist es notwendig, den Druck im System zu entlasten oder den Hydrospeicher sicher abzusperren. Hydrospeicher und die damit verbundenen druckbeaufschlagten Bauteile müssen innerhalb der vorgegebenen Grenzen, Temperaturen und Umgebungsbedingungen betrieben werden.

8.5.4 Feststellung der Übereinstimmung mit den Sicherheitsanforderungen

Da eine hydraulische Anlage in der Regel keine verwendungsfertige Maschine ist, lassen sich viele Prüfabläufe so lange nicht durchführen, bis die hydraulische Anlage in eine Maschine eingebaut ist. Vgl. nachfolgend EN ISO 4413 Kap. 6:

Kap. 6: Feststellung der Übereinstimmung der Sicherheitsanforderungen und Abnahmeprüfung

Die Hydraulikanlage muss einer Kombination aus Inspektion und Prüfung unterzogen werden, um zu bestätigen, dass:

- *a) die Anlage und deren Bauteile mit der Anlagenbeschreibung übereinstimmen;*
- *b) die Verbindungen der Bauteile in der Anlage mit dem Schaltplan übereinstimmen;*
- *c) die Anlage einschließlich aller Sicherheitsbauteile ordnungsgemäß funktioniert; und*
- *d) bei allen Bauteilen keine messbare unbeabsichtigte Leckage auftritt, außer einer Flüssigkeitsmenge, die nicht ausreicht, um einen Tropfen auf einer Zylinderstange nach mehreren Zyklen zu bilden.*

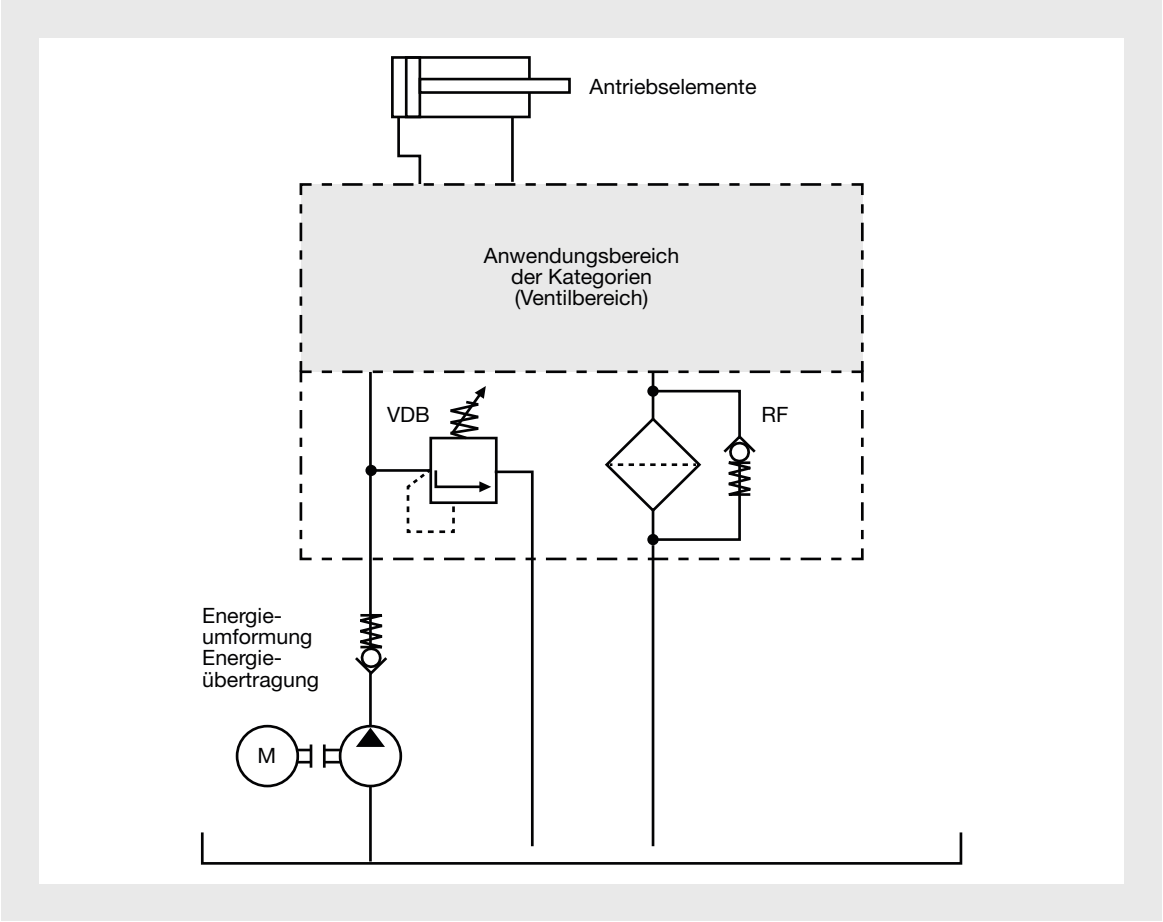
ANMERKUNG: Da eine Hydraulikanlage in der Regel keine verwendungsfertige Maschine ist, können viele Prüfabläufe so lange nicht durchgeführt werden, bis die Hydraulikanlage in eine Maschine eingebaut ist. Eine Funktionsprüfung muss dann nach dem Einbau entsprechend der Absprache zwischen Auftraggeber und Auftragnehmer durchgeführt werden.

Die Ergebnisse der Bestätigung durch Inspektion und Prüfung müssen dokumentiert sein und die folgenden Informationen müssen in dem Bericht enthalten sein:

- *Typ und Viskosität der verwendeten Hydraulikflüssigkeit;*
- *Temperatur der Hydraulikflüssigkeit im Behälter, nachdem sich die Temperatur stabilisiert hat.*

Wichtig: Zulässige Leckage wird definiert als Feuchtigkeit, die nicht ausreicht, einen Tropfen zu bilden.

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik



Fluidtechnische Anlage

8.5.5 Sicherheitsbezogene Teile von hydraulischen Steuerungen

Bei fluidtechnischen Anlagen sind als sicherheitsrelevante Teile der Steuerung jene Ventile zu betrachten, die gefahrbringende Bewegungen oder Zustände steuern. Bei hydraulischen Anlagen sind außerdem die Maßnahmen zur Druckbegrenzung im System (VDB), zur Filtration der Druckflüssigkeit (RF), zur Temperaturbereichsüberwachung (T) und zur Füllstandskontrolle des Tanks (N) zu berücksichtigen, obwohl diese Bauteile keine direkten Steuerungsteile sind.

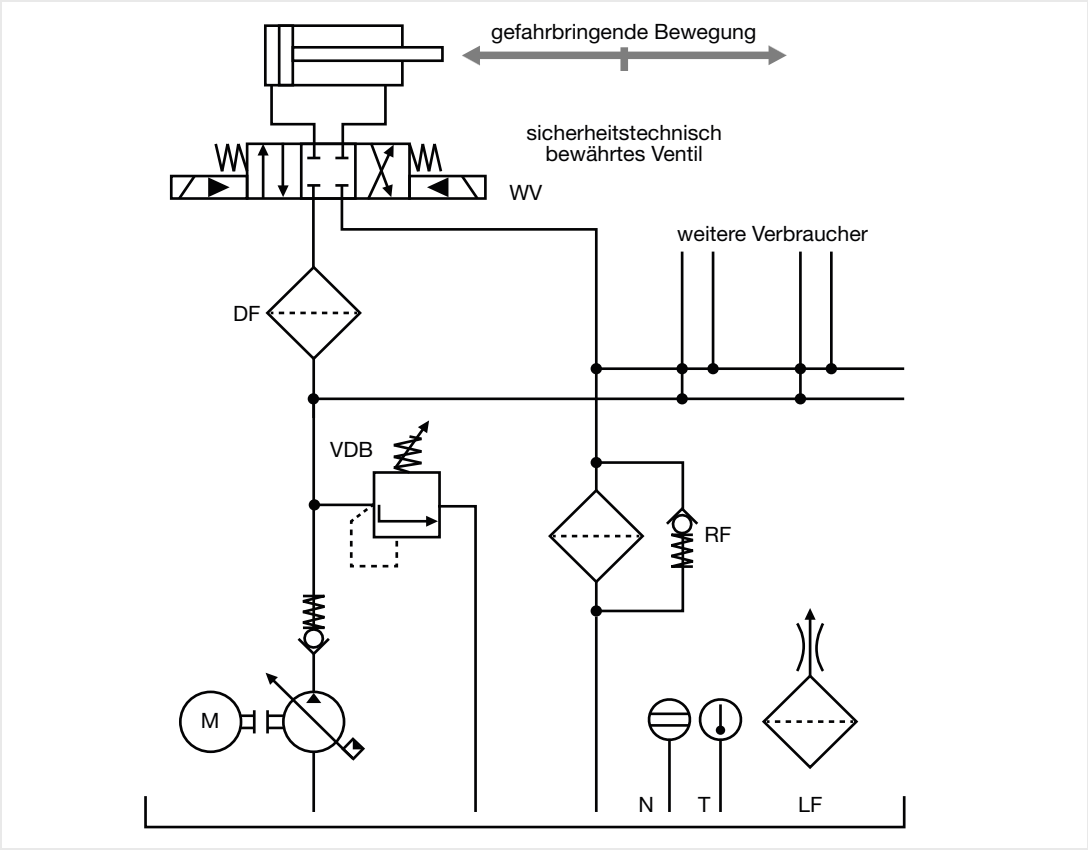
8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik

8.5.6 Steuerungen nach Kategorie B, Performance Level a gemäß EN/ISO 13849-1

Kategorie B ist die Basiskategorie, deren Anforderungen bei allen Kategorien einzuhalten sind. Diese Anforderungen umfassen auch die grundlegenden Sicherheitsprinzipien. Für die Fluidtechnik besonders relevante, spezifische und grundlegende Sicherheitsprinzipien sind:

- Ausfall eines Bauteils kann zum Verlust der Sicherheitsfunktion führen.
- Ruhestromprinzip (positive Signalgabe zum Starten)
- Beherrschung von Energieänderungen, Energieausfall und Energiewiederkehr
- Druckbegrenzung im System
- Auswahl einer geeigneten Druckflüssigkeit
- ausreichende Filtration des Druckmediums
- Verhinderung von Schmutzeinzug
- Trennung von der Energiezufuhr
- Einhalten der Grundanforderungen an Bauteile (Schock, Temperatur, Druck, Viskosität usw.)
- sicherheitsrelevante Schaltstellung der Ventile durch die Wegnahme des Steuersignals (wirksame Federn)
- Art und Zustand des Druckmediums

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik



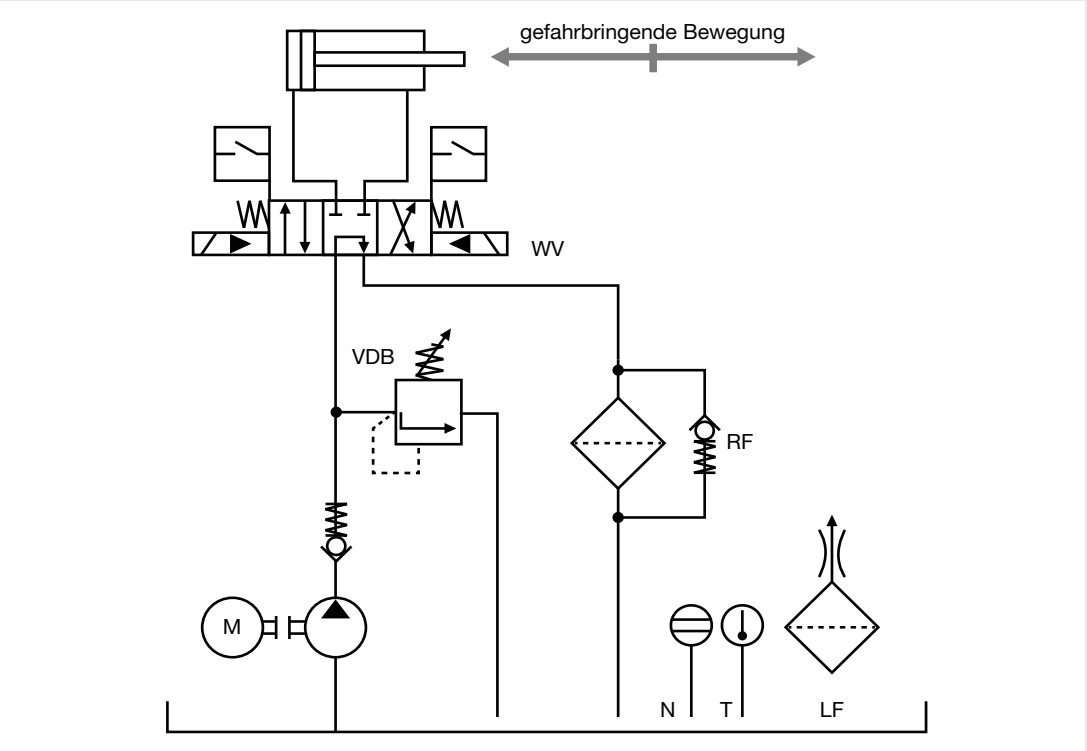
Hydraulisches Schaltungsbeispiel (Kat 1, PL b)

8.5.7 Steuerungen nach Kategorie 1, Performance Level b

Zusätzlich zu den Anforderungen aus Kategorie B sind Steuerungen der Kategorie 1 unter Verwendung bewährter Sicherheitsprinzipien und bewährter Bauteile zu gestalten und herzustellen. Allgemein bewährte Prinzipien der Hydraulik sind:

- Drehmoment-/Kraftbegrenzung (reduzierter Druck)
- reduzierte Drehzahl/Geschwindigkeit (reduzierter Volumenstrom)
- Überdimensionieren
- wegbegrenzender Tippbetrieb
- ausreichende positive Überdeckung bei Schieberventilen
- formschlüssige Krafteinwirkung (zwangsläufige Betätigung)
- gezielte Auswahl von Werkstoffen und Werkstoffpaarungen
- Beanspruchung von sicherheitsrelevanten Federn mindestens 10 % unterhalb der Dauerfestigkeitsgrenze, bezogen auf 10^7 Lastwechsel (siehe EN 13906-1)

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik



Hydraulisches Schaltungsbeispiel (Kat 2, PL b)

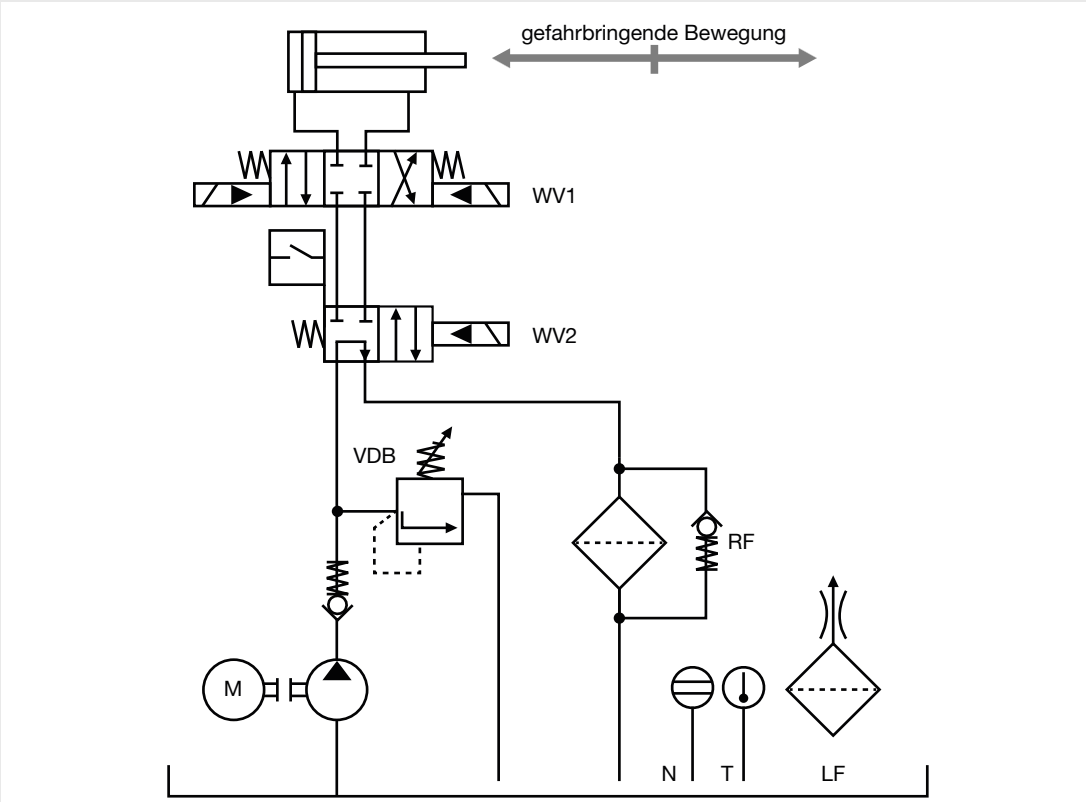
8.5.8 Steuerungen nach Kategorie 2, Performance Level b

Zusätzlich zu den Anforderungen von Kategorie B und der Verwendung bewährter Sicherheitsprinzipien müssen Steuerungen der Kategorie 2 so aufgebaut sein, dass die Testeinrichtung (TE) in der Lage ist, die Sicherheitsfunktionen in geeigneten Zeitabständen zwangsweise zu prüfen und darauf zu reagieren.

In dem oben dargestellten Beispiel steuert lediglich ein Wegeventil die gefahrbringende Bewegung. Die elektrische Maschinensteuerung testet die Sicherheitsfunktion des Ventils zyklisch sowie grundsätzlich bei jedem Anlaufen der Maschine. Der Ausfall des Wegeventils darf nicht die Testfunktion beeinflussen. Fällt die Testfunktion aus, darf dies umgekehrt nicht die Zuverlässigkeit des Wegeventils in Mitleidenschaft ziehen. Positionsschalter erfassen bei der Testung die Rückkehr des Ventil-Schiebekolbens in seine sicherheitsrelevante Mittelstellung. Erkennt die Maschinensteuerung den Ausfall eines Wegeventils, leitet sie unverzüglich die Abschaltung der Hydraulikpumpe ein.

Hierbei muss die Gesamtzeit zum Erkennen des Ausfalls und zur Überführung in einen nicht gefahrbringenden Zustand (in der Regel der Stillstand) kürzer sein als die Zeit bis zum Erreichen der Gefahrenstelle (siehe auch EN ISO 13849-1 und EN ISO 13855).

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik



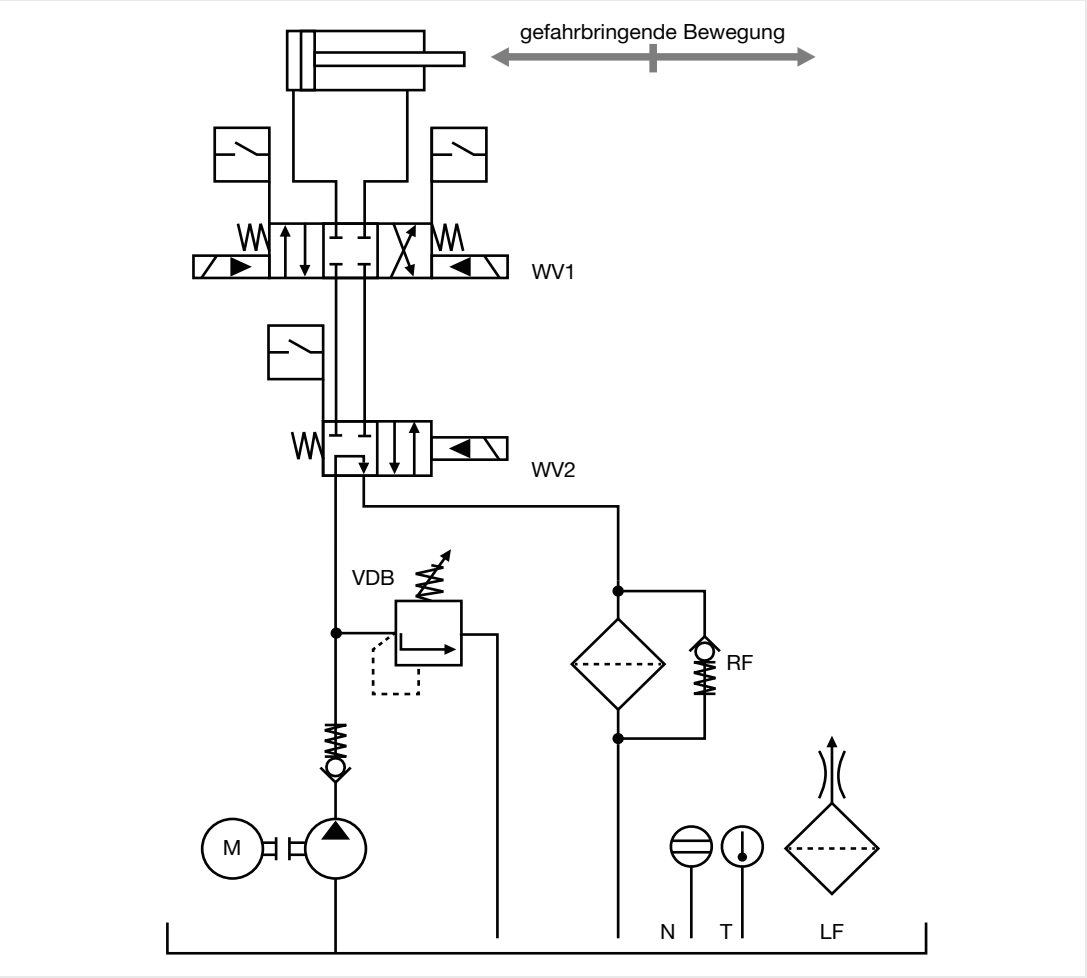
Hydraulisches Schaltungsbeispiel (Kat 3, PL d)

8.5.9 Steuerungen nach Kategorie 3, Performance Level d

Zusätzlich zu den Anforderungen aus Kategorie B und der Verwendung bewährter Sicherheitsprinzipien müssen Steuerungen der Kategorie 3 so gestaltet sein, dass ein einzelner Fehler nicht zum Verlust der Sicherheit führt. Wann immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

Die gefahrbringende Bewegung wird durch das zyklisch schaltende Wegeventil WV1 sowie durch das Druckventil WV2 sicherheitstechnisch gesteuert. Das zusätzliche Abschalten des Pumpen-Antriebsmotors ist nicht zwingend erforderlich. Die Bewegung des Ventil-Schiebkolbens WV1 aus der sicherheitsrelevanten Mittelstellung wird in diesem Falle nicht abgefragt, redundant wird das Druckventil WV2 mit eingeschaltet. Die Einkanalfehlersicherheit ist hiermit gegeben. Ein Hängenbleiben des Druckventils WV2 wird durch die elektrische Stellungsüberwachung im Steuersystem erkannt. Ein Versagen des Wegeventils WV1 kann während des Betriebs erkannt werden, wenn in regelmäßigen Intervallen der Zylinder außerhalb der Endlagen angehalten wird.

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik



Hydraulisches Schaltungsbeispiel (Kat 4, PL e)

8.5.10 Steuerungen nach Kategorie 4, Performance Level e

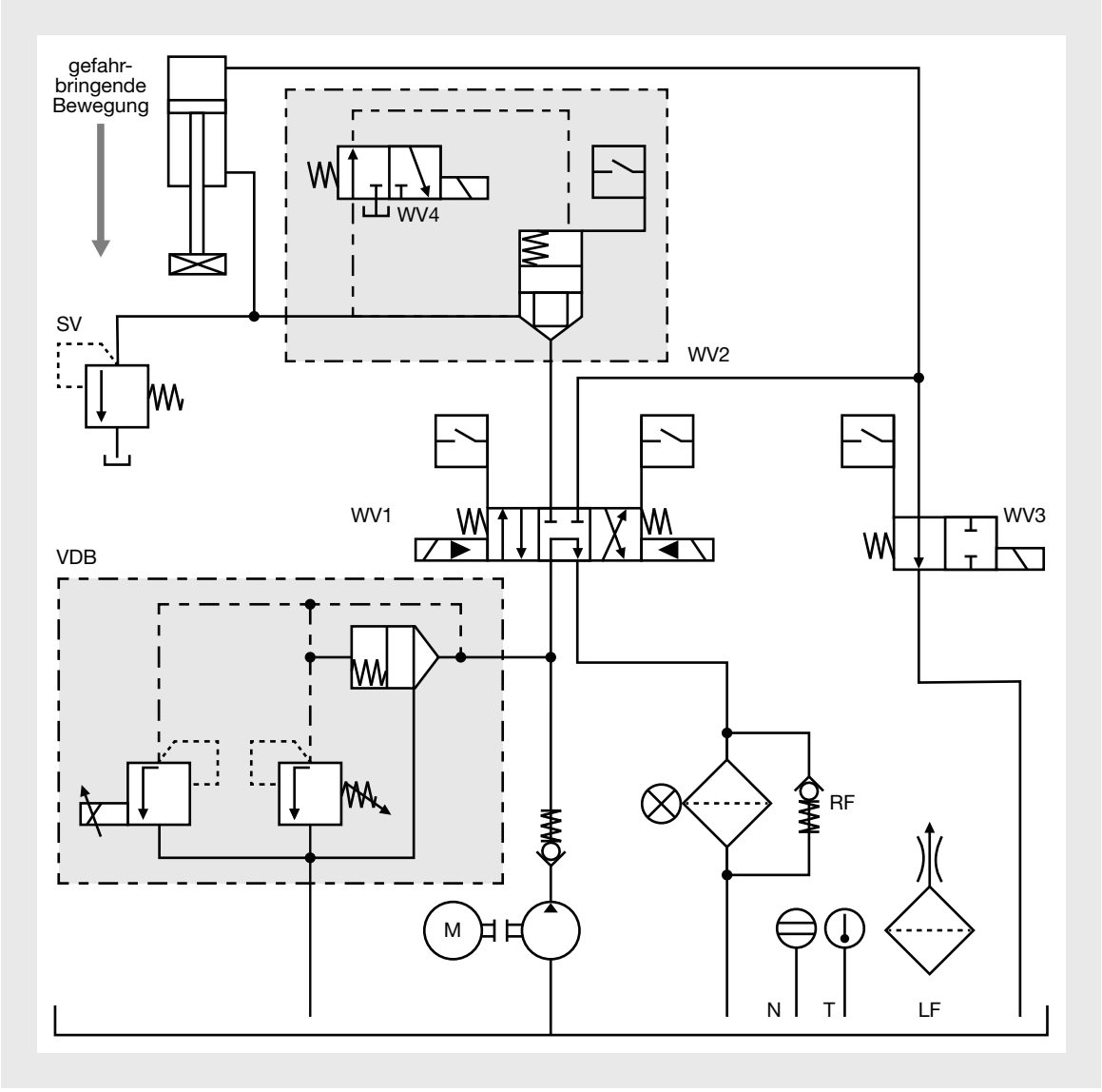
Zusätzlich zu den Anforderungen von Kategorie B und der Verwendung bewährter Sicherheitsprinzipien müssen Steuerungen der Kategorie 4 so ausgelegt sein, dass ein einzelner Fehler nicht zum Verlust der Sicherheit führt. Ziel von Sicherheitskonzepten ist, dass ein einzelner Fehler sofort oder spätestens vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird.

Zwei Ventile steuern die gefahrbringende Bewegung. Dabei ist jedes Ventil in der Lage, die gefahrbringende Bewegung alleine abzuschalten, die Einfehlersicherheit ist damit gegeben. Beide Ventile sind darüber hinaus mit einer elektrischen Stellungsüberwachung ausgerüstet. Diese stellt sicher, dass die Steuerung alle möglichen Einzelfehler frühzeitig erkennt.

8.5 Sicherheitsanforderungen an hydraulische Schaltungstechnik

8.5.11 Weiteres Beispiel für Steuerungen nach Kategorie 4, Performance Level e

In dieser hydraulischen Steuerung wird nur die Abwärtsbewegung sicherheitstechnisch überwacht (vgl. hydraulische Presse). Zwei elektrisch überwachte Ventile WV1 und WV3 steuern den Druckaufbau auf die Kolbenoberseite, für den Druckabbau sind die Ventile WV2 und WV1 zuständig. Die Ventile WV1, WV2, WV3 sind mit einer elektrischen Stellungsüberwachung ausgerüstet. Im Zusammenwirken mit der Steuerung gewährleistet dies die Erkennung aller Fehler. Die Überwachung der Hauptstufe des Ventils WV2 erfasst gleichzeitig einen etwaigen Ausfall des Vorsteuerventils WV4. Das Druckbegrenzungsventil VDB ist als elektrisch einstellbares Druckventil mit Druckbegrenzungsfunktion ausgeführt.



Hydraulisches Schaltungsbeispiel (Kat 4, PL e)

9

Anhang

9 Anhang

9 Anhang
9.1 Stichwortverzeichnis 9-3
9.2 Haftungsausschluss 9-15

9.1 Stichwortverzeichnis

Symbole, 0–9

1999/5/EG 3-16
2001/95/EG 3-16
2003/10/EG 3-16
2006/42/EG 3-5, 3-10, 3,11, 3-16, 3-17, 3-44, 3-53, 4-4, 4-6
2009/104/EG 3-80
2014/30/EU 3-16
2014/35/EU 3-16
2014/53/EU 3-16
3-Schütz-Kombination 5-3, 5-6
89/686/EWG 3-16
β-Faktor 3-31
λ_D 3-32
λ_{DD} 3-26
λ_{Dtotal} 3-26

A

A-, B- und C-Normen 3-41, 3-43
Abbremsen 7-15, 7-16, 7-18, 8-27, 8-33
Abluftdrosseln 8-34
Abschalten 4-18, 4-21, 5-3, 5-30, 5-35, 7-3, 7-14, 7-17, 7-18, 7-24, 7-25, 8-61
Abschaltpfad 7-4, 7-5, 7-6, 7-14, 7-23, 7-24
Absolutdruck 8-38
Abstandsüberwachung 3-55, 5-31
Abwärtsfahrt 8-45
Achsen 5-19, 5-36, 7-7, 7-14, 7-16, 7-17, 7-18, 7-20, 7-26, 7-41
Akkreditierungsrichtlinie 765/2008/EG 3-75
aktive optoelektronische Schutzeinrichtungen 4-16
Aktor 5-3, 5-4, 5-6, 5-31, 5-41, 6-6
Alleinhersteller 2-17
Altmaschine 3-7
Amtsblatt der EU 3-3, 3-4
Analogverarbeitung 5-12, 5-20
Anforderungen an Schutzeinrichtungen 4-4
Annäherungsgeschwindigkeit 3-19, 3-28, 4-7, 4-16, 8-25
Annäherungsrichtung 3-28
Anschlussbezeichnung 8-36
ANSI (American National Standards Institute) 3-18, 3-41
anthropometrische Daten 3-28
Antrieb 4-11, 4-21, 7-4, 7-12, 7-15, 7-18, 7-19, 7-24, 7-25, 7-26, 7-27, 7-36, 7-37, 7-38, 7-39, 7-40, 8-4, 8-25, 8-32, 8-37
Antriebsbus 7-3, 7-26
Antriebselektronik 7-4, 7-23
Antriebsgrundmodul/Basic Drive Module (BDM) 7-10
antriebsintegrierte Bewegungsüberwachung 7-26, 7-36
antriebsintegrierte Sicherheit 4-21, 5-35, 7-3, 7-13, 7-18
antriebsintegrierte Sicherheitstechnik 7-3
antriebsintegrierte Trennung 7-6, 7-9, 7-12, 7-19, 7-24, 7-25
Antriebskomponenten 7-22, 7-23
Antriebspumpe 8-52, 8-53, 8-54
Antriebssystem 3-38, 5-19, 7-3, 7-4, 7-6, 7-7, 7-10, 7-11, 7-12, 7-25
Antriebstechnik 3-54, 4-21, 5-36, 5-37, 7-6, 7-15, 7-16, 7-22, 7-23, 8-3
Antriebsumfeld 5-19
Anwendungsbereich 2-22, 3-17, 3-24, 3-29, 3-33
Applikationsschicht 6-8, 6-11
arbeitsteilige Produktion 2-17
Assembler 2-9, 2-18
Assemblertätigkeit 2-9
Assembling 2-9
Associação Brasileira de Normas Técnicas (ABNT) 3-44
Asynchronmotor 7-24, 7-27
ATEX 2-22
Auffahrt 8-44
Ausfallverhalten 8-30
Auslegung 3-28, 3-57, 4-17, 5-26, 7-22, 7-25, 8-25, 8-34, 8-35, 8-39, 8-55
Ausreißer 2-15, 2-19
Ausschluss der Haftung 2-10
Auswertelogik 5-4
Automatik 5-18
Automatisierungstechnik 5-11, 5-22, 5-28, 5-30, 5-36, 6-6

B

$B10_d$ 3-26, 3-31, 3-60, 3-68, 5-26, 7-31, 7-34
Bahnkurve (resultierende Bewegung) 7-26
Baumusterprüfung 3-17, 3-45, 3-48
Bauteilekennzeichnung 8-36
befähigte Personen 3-80
Befestigungs- und Überwachungsmodalitäten 4-28
Belüftungszeit 8-35
Beobachtungspflicht 4-27
Berechnungstool 3-24, 3-75
Bereichsüberwachung 5-20
Bernoulli-Gleichung 8-41
berührungslos wirkende Schutzeinrichtungen 3-37, 3-75, 3-80, 4-7, 4-8, 4-16, 4-18, 5-18
Bescheinigungsverfahren 3-17
beschränktes Versagen 8-12
Betreiber 2-17, 3-6, 3-39, 3-43, 3-44, 3-46, 3-49, 3-50, 3-73, 3-75, 4-26, 4-27, 5-7, 5-26, 8-25

9.1 Stichwortverzeichnis

Betrieb 3-39, 3-40, 4-3, 4-21, 6-11, 7-12 7-14, 7-17, 7-25, 8-36, 8-43
Betriebsanleitung 3-6, 3-14, 3-75, 4-3, 4-22, 4-25, 8-4, 8-19, 8-35
Betriebsartenwahl 5-32
Betriebsdruck 8-24, 8-26, 8-27, 8-35, 8-55
Betriebsdruckbereich 8-55
Betriebstemperaturen 8-55
Beurteilung ...2-10, 3-14, 3-26, 3-31, 3-67, 4-23, 8-5
Bevollmächtigter 3-6, 3-9, 3-75
bewegliche Schutzeinrichtungen 5-4
bewegliche trennende Schutzeinrichtungen 3-19, 4-5, 4-7, 4-9, 4-11, 4-12, 4-14, 4-15
Bewegungserzeugung 7-4, 7-12
Bewegungssteuerung 4-21, 7-4, 7-26
Bewegungsüberwachung 7-4, 7-9, 7-24, 7-25, 7-26, 7-27, 7-36, 7-37, 7-38, 7-39, 7-40
Bewegungsüberwachung mit externen Geräten 7-36
Beweislastverteilung 2-12
Bewertungsverfahren 3-11
BG 5-11, 5-30
BGB
- § 823 Abs. 1 BGB 2-14, 2-22
- § 823 BGB 2-4, 2-14, 2-15, 2-19
BGIA 3-23
Blockdiagramm 7-29, 7-31, 7-33, 7-35, 7-42
bmwfi 3-78
Bottom-up 3-70
Bremse 7-20, 7-25, 7-30, 7-31, 7-32, 8-33, 8-34, 8-35
Bremsentest 7-20
Bremsrampe 7-15, 7-16
British Standard (BS) 3-18
Bussysteme 5-4, 5-21, 5-22,
Buszykluszeit 6-7, 6-8
BWS 4-16, 4-17, 4-19

C

CAN 6-11
CANopen 6-8, 6-11
CANopen-Standard 6-11
CCC 3-47
CCF-Faktor 3-26, 3-31
CE-Kennzeichnung 2-22, 3-5, 3-6, 3-7, 3-10, 3-12, 3-15, 3-17, 3-53, 3-75
CEN 3-18, 3-41, 3-42
CENELEC 3-18, 3-41, 3-42
CE-Zeichen 3-5, 3-10, 3-11, 3-15, 3-40, 3-42, 3-51
CLC/TS 61496-2:2006 3-20
CLC/TS 61496-3:2008 ..... 3-20, 3-37, 4-7
CNC 5-27
Common-Cause-Faktor 3-31
Communauté Européenne 3-5
Counter No. 6-12
CRC 6-12
CSA (Canadian Standards Association) 3-42

D

DACH 3-78
Daisy Chain-Verkabelung 6-10
DAkkS (Deutsche Akkreditierungsstelle) 3-75, 3-78, 3-79, 3-80, 3-81
Dampfblasenkavitation 8-43
DAP 3-78
Datensicherungsmechanismus 6-4
Dauer der Gefährdungsexposition 3-25
DC-Wert 3-26, 3-70
DC_{avg} 3-26
deliktische Haftung 2-4, 2-17
Designgrundsätze 3-21
deterministische Gefährdungen 8-9, 8-15
Deutsches Institut für Normung (DIN) 3-18
dezentrale Sicherheitstechnik 6-3
Diagnose Testintervall (T_2) 3-34
Diagnosedaten 5-13
Diagnosedeckungsgrad (DC) 3-26, 3-27, 3-60, 4-14, 7-31, 8-32, 8-33
Diagnosefähigkeit 5-6
Diagnosezwecke 5-4
Differenzialschaltung 8-50
DIN 3-18, 3-34
DIN EN ISO 14118 4-21
DIN EN ISO 17020 3-75
DIN-Vorschriften 2-7
DKD 3-78
Dokumentation 3-7, 3-14, 3-48, 3-62, 3-66, 3-67, 3-72, 4-13, 5-26, 8-4, 8-5
d_{op} 7-31, 7-34
Drehgeber 6-8, 7-6, 7-7, 7-36, 7-38, 7-39, 7-40
Drehmoment-Messsystem 7-19
Drehmomentüberwachung 5-36
Drehrichtung 7-7, 7-35
Drehrichtungsüberwachung 5-32
Drehzahl 3-20, 3-38, 5-4, 5-10, 5-12, 7-10, 7-12, 8-22, 8-43, 8-56, 8-59
Drehzahlüberwachung 4-21
Drossel-Rückschlagventile 8-34
Druck 3-56, 4-23, 4-27, 5-20, 8-24, 8-25, 8-26, 8-35, 8-36, 8-37, 8-38, 8-39, 8-40, 8-43, 8-44, 8-48, 8-49, 8-50, 8-54, 8-55, 8-56
Druckabsenkungen 8-43
Druckbegrenzung 8-24, 8-57, 8-58

9.1 Stichwortverzeichnis

Druckbegrenzung im System (VDB) 8-57
Druckquelle 8-36
Druckübersetzer 8-40
Druckübersetzung 8-40
Druckverluste 8-43
Druckwerte 8-24

E

E/A-Kopplung 7-9, 7-26
Echtzeit-Kommunikation 6-10
EG-Konformitätserklärung 3-5, 3-6, 3-9, 3-10, 3-15, 3-17, 3-53, 3-75
EG-Richtlinien 2-22
Eigenverwendung 3-7
Ein-/Ausgänge 5-11, 5-21
Einbauerklärung 3-10, 3-14
Einfügung von Nachrichten 6-4
Einrichtbetrieb 5-18, 7-18, 7-19, 8-26
Einzelachse 7-26
Einzelhub 5-18
elektrische Codes (NEC) 3-41
elektrische Sicherheit 3-33
Elektronik 3-18, 5-6, 5-37
elektronische Kurvenscheibe (synchrone Bewegungen) 7-26
elektronische Sicherheitsschaltgeräte ... 5-4, 5-6, 5-9
EMV-Anforderungen 3-20, 3-36
EMV-Belastung 6-7
EMV-Gesetz/EMVG 2-22
EMV-Richtlinie 3-12, 3-16
EMV-verursachte Störungen 6-4
EN 1005-1 bis -4:2008 3-19
EN 1005-5:2007 3-19
EN 1010 4-24
EN 1037 4-21
EN 1037:2008 3-19
EN 1088 3-36
EN 1088:2008 3-19
EN 12453:2000 3-19
EN 292 3-19
EN 349:1993+A1:2008 4-7
EN 349:2008 3-19
EN 415 7-28
EN 547-1 bis -3:2008 3-19
EN 574:2008 3-19
EN 60204-1 ..... 3-33, 7-12, 8-55
EN 60204-1:2010 ..... 3-20, 3-33
EN 60947-5-1:2009 3-20
EN 60947-5-2:2012 3-20
EN 60947-5-3:2005 3-20
EN 60947-5-4:2003 3-20
EN 60947-5-5:2013 3-20
EN 60947-5-6:2001 3-20
EN 60947-5-7:2003 3-20
EN 60947-5-8:2006 3-20
EN 60947-5-9:2007 3-20
EN 61326-3 Teile 1+2:2008 ..... 3-20, 3-36
EN 61496-1:2010 3-20
EN 61496-3:2003 3-20
EN 61508 ... 3-23, 3-29, 3-33, 3-34, 3-35, 3-38, 3-67
EN 61508 Teile 1-7:2010 ..... 3-20, 3-33
EN 61511 Teile 1-3:2004 ..... 3-20, 3-29
EN 61784-3:2010 ..... 3-20, 3-23
EN 61800 ..... 7-10, 7-11, 7-12, 7-13
EN 61800-5-2:2007 ..... 3-20, 3-38
EN 62061 3-24, 3-29, 3-32, 3-33, 3-67, 3-68, 3-72, 4-11
EN 62061:2016 ..... 3-20, 3-29
EN 692 7-28
EN 693 7-28
EN 953:2009 3-19
EN 954-1 ..... 3-9, 3-67, 4-20
EN 999 3-28
EN ISO 10218-1 ..... 3-52, 3-53, 7-28
EN ISO 11161:2010 ..... 3-19, 3-39
EN ISO 12100-1 und 2 ..... 3-19, 3-21
EN ISO 12100:2010 ..... 3-19, 3-21
EN ISO 13849-1 ..... 3-9, 3-21, 3-23, 3-24, 3-25, 3-26, 3-27, 3-29, 3-33, 3-38, 3-54, 3-60, 3-61, 3-62, 3-63, 3-64, 3-66, 3-67, 3-68, 3-74, 3-75, 4-11, 5-14, 5-19, 5-26, 7-12, 7-28, 7-29, 7-31, 7-32, 7-34, 8-28
EN ISO 13849-1:2009 3-19
EN ISO 13849-2 ..... 3-24, 3-66, 3-67, 3-73,
EN ISO 13849-2:2012 ..... 3-19, 3-24
EN ISO 13855 3-28, 3-57, 4-15, 4-16, 4-17, 7-33, 8-60
EN ISO 13855:2010 ..... 3-19, 3-28, 4-7
EN ISO 13857:2008 ..... 3-19, 3-28, 4-7
EN ISO 14119:2013 ..... 3-36, 4-7
EN ISO 14120:2015 4-7
EN/IEC 61508 ..... 7-7, 7-11
EN/IEC 61800-5-2 ..... 7-3, 7-6
Endeinrichtungs-Gesetz/FTEG 2-22
Endprodukthersteller 2-18
Energieversorgung 4-21, 5-3, 7-30, 8-55
Entlüften 8-27, 8-28, 8-29, 8-35
Entstörungsprozedur 4-25
Entstörverfahren 4-25
Entwicklungsfehler 2-11
Ersatzpflicht 2-11
Ethernet 5-15, 5-22, 6-4, 6-6, 6-7, 6-8, 6-9, 6-10, 6-11, 6-12, 6-13, 6-14
ethernetbasiertes Feldbussystem 6-6

9.1 Stichwortverzeichnis

Ethernetbasis 5-15
Ethernet-Technologie 6-8, 6-13
EU-Importeur 2-10
Europäische Normen 2-7
Europäische Richtlinie 85/374/EWG 2-5
Europäische Union 3-3, 3-4
European co-operation for Accreditation (EA) 3-78
Ex-Bereich 5-10
Exposition 3-24
externe Befehle 7-42
externe Bewegungsüberwachung mit einem Standardgeber 7-37
externe Bewegungsüberwachung mit sicherem Geber 7-40
externe Bewegungsüberwachung mit Standardgeber und -Initiator 7-38
externe Bewegungsüberwachung mit zwei Standard-Initiatoren 7-39

F

Fabrikationsfehler 2-14
Fail-safe-Prinzip 7-3, 7-25
falsche Abfolge von Nachrichten 6-4
Fehlerfreiheit 2-7, 2-18
Fehlerhaftigkeit 2-7, 2-9, 2-10, 2-11
Fehlerreaktionsfunktion 7-25
Fehlersimulation (Safety Check) 3-75
Fehlertoleranz 3-32
Fehlerzustände 5-13
Feldbus 3-20, 3-23, 5-13, 5-24, 6-10, 7-7, 7-9
Feldbusmodule 5-13
Feldbusstandard 6-11
Feldbussystem 5-13, 6-6, 6-14
feststehende trennende Schutzeinrichtungen 3-19, 4-6, 4-7, 4-8, 4-9, 4-11
Filtration der Druckflüssigkeit (RF) 8-57
Flügelzellenpumpen 8-54
fluidtechnische Anlage 8-37, 8-57
Flüssigkeitsstrom 8-51
Folgeventil 8-48
Formstücke 8-43
freier Warenverkehr 3-17
Frequenzumrichter 7-4, 7-10, 7-23, 7-27
Führungsgröße 7-5, 7-6
Funk- und Antennentechnologie 6-7
Funkanlagenrichtlinie 3-16
Funkkommunikation 6-7
funktionale Schutzeinrichtung 4-21
funktionale Sicherheit .. 3-17, 3-20, 3-24, 3-29, 3-33, 3-38, 3-73, 4-21, 5-40, 7-3, 7-10, 7-15, 7-16
Funktionsbausteine 3-61, 3-63, 3-66, 5-25, 5-33
Funktionselemente 5-25
Funktionsprüfung 3-73, 3-75, 8-56

G

Geber 5-19, 7-7, 7-8, 7-9, 7-36, 7-37, 7-38, 7-40
Geberleitung 5-19, 7-25
Gebersignal 5-19, 7-7, 7-37, 7-38
Gebersysteme 7-7, 7-8, 7-9, 7-19, 7-22, 7-25
Gebrauchsanleitung 2-16
Gebrauchsdauer (T_1) 3-34
Gefahrabwendung 8-11
Gefahrabwendungsmaßnahme 2-17, 2-20
Gefährdung 2-15, 3-8, 3-14, 3-16, 3-21, 3-25, 3-70, 4-4, 4-6, 4-8, 4-15, 4-16, 4-17, 4-21, 4-26, 4-28, 5-3, 5-40, 7-6, 7-15, 7-18, 7-19, 7-25, 8-5, 8-8, 8-9, 8-15, 8-16, 8-19
Gefährdungsbeurteilung 3-73
Gefährdungsexposition (Häufigkeit) 3-25, 3-30
Gefährdungshaftung 2-4, 2-5
Gefahren 2-14, 2-15, 2-16, 2-19, 2-20, 3-14, 4-3, 4-8, 4-22, 4-26, 4-28, 5-7, 5-30, 7-30, 8-5, 8-7, 8-8, 8-9, 8-10, 8-12, 8-15, 8-16, 8-17, 8-19, 8-23, 8-28, 8-55
Gefahrenhinweise 2-17
geräuscharme Konstruktion 8-55
geregelter Zustand 7-17
geregeltes Abbremsen 7-15
Gesamtheiten von Maschinen 3-6
Gesamtschaltung 7-29, 7-32, 7-34, 7-35, 7-42
Geschwindigkeitsschwelle 7-17
Geschwindigkeitssteuerung 8-45, 8-51
Gesetz über Arbeits- und Gesundheitsschutz (Industrial Safety and Health Law (Japan) 3-46
Gestaltung von Schutzeinrichtungen 4-11
gesteuertes Stillsetzen 7-12, 7-15, 7-16
Gesundheitsanforderungen 3-12, 3-14, 3-17
Gesundheitsgefahren 2-15
Gleichlaufschaltung 8-47
Gliedmaßen 3-19, 3-28, 4-7
GOST-R-Zertifizierung 3-45
Graph des PL 3-25, 3-27, 7-32
Grenzwert 2-7, 3-53, 3-56, 3-57, 3-58, 3-59, 3-65, 5-19, 7-3, 7-9, 7-12, 7-14, 7-15, 7-16, 7-17, 7-18, 7-19, 7-24, 7-25, 7-26, 8-5, 8-55
Grenzwertverletzung 7-12, 7-14, 7-19, 7-42

H

Haftung des Endproduktherstellers 2-18
Haftung des Lieferanten 2-10
Haftung des Quasi-Herstellers 2-9
Haftung des Zulieferers 2-19
Haftungsbefreiung 2-11
Haftungshöchstbetrag 2-12
Halbleiterausgänge 5-4, 5-6
Halte- und Betriebsbremsen 7-20, 7-30

9.1 Stichwortverzeichnis

Haltebremse 7-20, 7-24, 7-31, 7-32, 8-33
Halten 8-31
Handeinschaltventil 8-27
Handventil 8-27
hängende Lasten 7-20
harmonisierte Norm 3-3, 3-4, 3-12, 3-40, 3-41, 3-42, 3-43, 3-44, 3-45, 3-49, 3-50, 3-51, 3-67, 8-9
Harmonisierung 3-3, 3-4, 3-16, 3-18
Herstellbarkeitsanalyse (Feasibility Study) 2-19
Hersteller 2-3, 2-4, 2-5, 2-6, 2-7, 2-8, 2-9, 2-10, 2-11, 2-12, 2-13, 2-14, 2-15, 2-16, 2-17, 2-19, 2-20, 2-21, 3-3, 3-4, 3-5, 3-6, 3-7, 3-10, 3-12, 3-14, 3-15, 3-23, 3-33, 3-38, 3-40, 3-41, 3-42, 3-44, 3-49, 3-50, 3-51, 3-54, 3-56, 3-60, 3-62, 3-63, 4-22, 4-24, 4-26, 4-27, 5-11, 5-26, 5-31, 7-11, 7-25, 7-31, 7-39, 7-40, 8-9, 8-35
Herstellerhaftung 2-4
Herstellertätigkeit 2-9
Herstellungsverfahren 3-74, 5-30, 7-11
High Demand Mode 3-29
High-End-Sicherheitslösungen 7-3
Hintertretschutz 4-18, 4-19
hinweisende Sicherheitstechnik 8-15, 8-19
Hinweispflicht 2-15
h_{op} 7-31, 7-34
Hubanschläge 8-56
Hubauslösung 5-18
Hydraulik 3-33, 5-28, 8-3, 8-23, 8-25, 8-37, 8-42, 8-59
Hydraulikkreislauf 8-44, 8-45, 8-46
Hydrauliksystem 8-44
hydraulische Anlagen mit Hydrospeicher 8-56
hydraulische Arbeit 8-40
hydraulische Steuerung 8-57, 8-63
Hydropumpe 8-43
Hydrospeicher 8-56
hydrostatische Energieübertragung 8-37

I

IEC 60204-1 ..... 7-14, 7-15, 7-16
IEC 61131 5-25
IEC 61496-2:2013 ..... 3-20, 3-37
IEC 61508 ..... 3-18, 3-34, 3-36, 6-7, 6-11, 8-9
IEC/TR 62061-1:2009 3-20
IEC/TR 62685:2010 ..... 3-20, 3-23
IEC/TS 62046:2008 ..... 3-20, 3-37
IL (Instruction List) 5-21
Import 2-10, 3-7
Importeur 2-8, 3-48
Inbetriebnahme 3-10, 3-40, 3-42, 3-44, 3-49, 3-50, 3-57, 5-6, 5-39, 7-9
Industrial Safety and Health Law (Japan) 3-46
Industrie 4.0 ..... 5-38, 5-40, 5-41
industrielle Kommunikationsnetze 3-20, 3-23
inhärent gefährliche Produkte 2-8
Inkrementalgeber 7-27
Installation 3-56, 5-7
Installationsprozess 5-7
Instruktionsfehler 2-14
Instruktionspflicht 2-15
integrierte Fehlererkennung 4-13
integrierter sicherer Abschaltpfad 7-14, 7-23
International Accreditation Forum (IAF) 3-78
International Electrotechnical Commission (IEC) 3-18
International Laboratory Accreditation Coorporation (ILAC) 3-78
International Organization for Standardization (ISO) 3-18
Inverkehrbringen 2-11, 2-12, 2-13, 3-17
I_S 4-15
I_{Smax} 4-15
$I_{Smax}(i)$ 4-15
ISO 14118:2000 3-19
ISO 14119 ..... 3-19, 3-36, 4-9
ISO 15189 3-79
ISO 9001-Standard 3-79
ISO/TR 23849:2010 3-20
ISO/IEC 17020 3-79
ISO/IEC 17025 3-79
ISO/OSI-Referenzmodell 6-9

J

JIS-Normen (Japan Industrial Standards) 3-46

K

Kalibrierberichte 3-79
Kategorie 3-27, 3-32, 3-65, 3-68, 3-69, 7-12, 7-15, 7-16, 7-32, 7-37, 8-58, 8-59, 8-60, 8-61, 8-62, 8-63
Kategorien, Einstufung
- Performance Level b 8-59
- Performance Level b 8-60
- Performance Level d 8-61
- Performance Level e 8-62, 8-63
Kavitation 8-43
Kavitationsarten 8-43
Kleinsteuerungen 5-4, 5-6, 5-11, 5-12, 5-13, 5-14, 5-15, 5-16, 5-17, 5-18, 5-19, 5-20, 5-25, 5-32, 5-33, 536
Klemmenspannung 7-5
Klemmpatrone 8-33, 8-35
Kolbendruckkraft 8-38
Kolbengeschwindigkeit 8-39, 8-45, 8-49
Kolbenkräfte 8-38, 8-44, 8-49

9.1 Stichwortverzeichnis

Kommunikationsfehler 6-3
Kommunikationshierarchie 6-8
Kommunikationsmedien 6-7
Konfigurationstools 5-11
konfigurierbare Sicherheitsschaltgeräte 5-4, 5-11, 5-12, 5-13, 5-14, 5-15, 5-16, 5-17, 5-18, 5-19, 5-20
Konformität 3-5, 3-7, 3-12, 3-14, 3-76
Konformitätsbewertung 3-5, 3-9, 3-14, 3-76
Konformitätserklärung 3-10, 3-14, 3-17, 3-44, 3-45, 3-55, 3-59
Konstantpumpe 8-43, 8-52
Konstruktionsfehler 2-6, 2-7, 2-11, 2-14, 2-15, 4-27
Konstruktionspflichten 2-19
kontaktbehaftete Technologie 5-9, 5-13
Kontinuitätsgleichung 8-41, 8-45
körperliche Leistung 3-19
Körpermaße 3-19
Körperteile 3-19, 3-28, 4-7, 4-16, 8-16
Kraft- und Wegübersetzung 8-40
Kreuz-Muting 5-16
Kupplungen oder Befestigungsteile 8-56

L

Lärmrichtlinie 3-16
Laserscanner 3-37, 4-19, 5-10, 5-16
Lastenheft 3-7
Laufruhe 8-52
Laufwächterkontrolle 5-18
LD (Ladder Logic/Kontaktplan) 5-21
Lebensphasen 3-14
Lebenszyklus 3-33, 3-38, 3-63, 7-22
Leckagen 8-23, 8-55
Leistungsantriebssystem/ Power Drive System (PDS) 7-10
Leistungsschütz 5-4
Lichtgitter 2-15, 3-37, 3-59, 3-75, 4-17, 5-6
Lichtschranken 3-37, 3-75, 4-6, 4-8, 8-17, 8-25, 8-35
Lichtwellenleiter 6-7, 6-13
Lichtwellenleiter-Kommunikation (LWL) 6-7
Low Demand Mode 3-29
Luftblasenkavitation 8-43
Luftfeder 8-25, 8-26

M

Manipulation von Schutzeinrichtungen 4-22
Maschine 2-7, 2-12, 2-14, 2-15, 2-17, 3-5, 3-6, 3-7, 3-8, 3-9, 3-10, 3-11, 3-12, 3-14, 3-15, 3-16, 3-17, 3-19, 3-20, 3-21, 3-23, 3-24, 3-25, 3-28, 3-29, 3-33, 3-36, 3-37, 3-39, 3-40, 3-41, 3-42, 3-43, 3-44, 3-45, 3-46, 3-47, 3-48, 3-49, 3-50, 3-51, 3-53, 3-55, 3-56, 3-57, 3-58, 3-64, 3-67, 3-68, 3-69, 3-70, 3-72, 3-73, 3-75, 3-80, 4-3, 4-4, 4-5, 4-7, 4-8, 4-11, 4-12, 4-15, 4-16, 4-18, 4-19, 4-21, 4-22, 4-24, 4-25, 4-27, 4-29, 5-3, 5-4, 5-6, 5-7, 5-10, 5-14, 5-16, 5-22, 5-26, 5-27, 5-28, 5-31, 5-32, 5-35, 5-37, 5-38, 5-40, 5-41, 6-8, 6-14, 7-3, 7-7, 7-9, 7-12, 7-23, 7-25, 7-28, 7-30, 8-3, 8-4, 8-5, 8-7, 8-8, 8-9, 8-12, 8-15, 8-16, 8-17, 8-19, 8-23, 8-24, 8-25, 8-27, 8-28, 8-35, 8-36, 8-55, 8-56, 8-60
Maschinenrichtlinie 3-5, 3-6, 3-7, 3-8, 3-9, 3-10, 3-11, 3-12, 3-14, 3-15, 3-16, 3-17, 3-19, 3-24, 3-29, 3-41, 3-43, 3-44, 3-45, 3-47, 3-49, 3-50, 3-53, 3-81, 4-4, 4-7, 8-3, 8-9, 8-35
- Anhang I 3-10, 3-12, 3-44
- Anhang II B 3-10
- Anhang IV 3-10
- Anhang VI 3-10
Maschinenverfügbarkeit 7-6
Maschinenzyklus 7-34
Master-Slave-System 6-6
Materialfehler 2-7, 2-15
Mechanik 3-18, 3-33, 5-37, 5-38, 8-3, 8-25, 8-28, 8-36
mechanische Bewegung 7-7, 8-55
mechanische Feder 8-25, 8-30, 8-36
mechanische Gefahren 8-8, 8-10
mechatronische Einheiten 5-29, 6-14
Medizinproduktegesetz/MPG 2-22
Messungen 3-58, 3-74, 3-78, 6-6
Mikroprozessortechnologie 5-6, 5-9
Mindestabstände 3-19, 4-7, 4-17, 8-16
Minimalgeschwindigkeit 7-18
Minimum-Testintervall (T_1) 3-34
mittelbare Sicherheitstechnik 8-17
modularer Maschinenbau 6-14
MLA = Multilateral Recognition Arrangement 3-78
Modularisierung 5-27, 5-29, 5-38
Montageanleitung 3-10, 3-14
Motion 5-27, 5-28, 5-29
Motion Control Steuerung 7-26

9.1 Stichwortverzeichnis

Motor 2-14, 2-15, 7-3, 7-4, 7-5, 7-6, 7-7, 7-9, 7-10, 7-12, 7-14, 7-15, 7-16, 7-17, 7-19, 7-24, 7-25, 7-31
Motorfeedback 7-7
Motorschütz 7-5, 7-6
Motorstrom 7-19
MRA = Mutual Recognition Agreement 3-78
MS6-SV 8-28, 8-29
$MTTF_d$ – Mean time to dangerous failure 3-26, 3-27, 3-31, 3-60, 3-68, 5-26, 7-31, 7-32, 7-34, 7-37, 7-38, 7-39
Multiturn-Geber 7-7
Muting 4-18, 7-35
Muting-Funktion 4-18, 5-10, 5-16
Muting-Lampe 5-16, 5-17

N

Nachlaufweg 5-59, 7-3, 7-19, 7-23, 8-25, 8-35
Nachrüstung 2-20, 7-25
Näherungsschalter 4-13
nationales Recht 3-3
Navier-Stokes-Gleichung 8-41
NC Steuerung 7-26
Nennhaltemoment 7-31
Netzschütz 7-5
NFPA (National Fire Protection Association) 3-41
NFPA 79 ..... 3-39, 3-41
NFPA 79:2008 3-39
NFPA 79:2013 3-20
nicht sicherheitsrelevante Übertragungsfunktion 6-4
nicht trennende Schutzeinrichtungen 4-5, 4-7, 4-8, 4-16, 8-17
Niederspannungsrichtlinie 3-12, 3-16
Nockenschaltwerk 5-18, 5-31, 5-32
Normalbetrieb 4-27, 8-29
Normen 2-7, 2-11, 3-3, 3-4, 3-12, 3-14, 3-16, 3-17, 3-18, 3-19, 3-21, 3-24, 3-36, 3-37, 3-41, 3-42, 3-43, 3-44, 3-45, 3-46, 3-47, 3-49, 3-50, 3-51, 3-53, 3-67, 3-72, 3-75, 3-76, 3-79, 3-81, 4-7, 4-9, 5-4, 5-18, 5-30, 5-36, 7-3, 7-28, 8-9, 8-36
Normen für die Dimensionierung trennender Schutzeinrichtungen 4-7
Normen für trennende Schutzeinrichtungen 4-7
Normen zur Gestaltung nicht trennender oder berührungslos wirkender Schutzeinrichtungen 4-7
Normungsinstitut 3-18
Not-Halt 3-81, 5-3, 5-6, 5-28, 5-32, 5-37, 7-28, 8-36
Not-Halt-Befehlsgeräte 7-34

O

OD – Ordinary Device 6-10
Öffnerkontakte 4-12, 7-6
Öffnungshäufigkeit 4-28
Ölstromsteuerung 8-45
Optokoppler 7-5, 7-6, 7-23
OSHA (Occupational Safety and Health Organisation) 3-18, 3-40, 3-42
OSHA-Standards 3-40
OSI-Referenzmodell 6-9
OSSD 4-13, 4-15
Österreichisches Normungsinstitut (ÖNorm) 3-18

P

Packet Identifier 6-12
Parallelschaltung 8-47, 8-49, 8-50
Parametriertool 5-12
PDS/Safety-Related (SR) 7-10
Pendelbewegung 5-32
Performance Level 3-24, 3-25, 3-26, 3-57, 3-60, 3-61, 3-62, 3-63, 3-68, 3-72, 3-75, 5-14, 7-28, 7-29, 7-30, 7-31, 7-32, 7-34, 7-35, 7-37, 7-38, 7-39, 7-40, 7-42, 8-28, 8-29, 8-32, 8-33, 8-58, 8-59, 8-60, 8-61, 8-62, 8-63
Performance Level PL_r 3-24, 3-25, 3-27, 3-65, 3-68, 3-71
Personen- oder Sachschaden 2-4
PFD (Probability of failure on low demand) 3-31
PFH_D 3-27, 3-32, 3-60, 7-32
Pflichtenprogramm 2-19
physikalisches Basiswissen 8-37
PID (Packet Identifier) 6-12
PL 3-25, 3-26, 3-27, 3-57, 3-68, 3-70, 4-11, 4-13, 4-14, 7-23, 7-29, 7-32, 7-34, 8-28
PL e 3-61, 3-65, 4-13, 7-38, 7-39, 7-40, 8-62, 8-62
Plausibilitätstests 7-7
PMCprotego DS 5-35
Pneumatik 3-33, 5-28, 8-3, 8-23, 8-25, 8-26, 8-27, 8-28, 8-32, 8-36
Pneumatikkomponenten 8-23, 8-24
PNOZ 5-3, 8-29
PNOZelog 5-9
PNOZmulti 3-62, 4-21, 5-4, 5-32, 5-33
PNOZsigma 5-6
Positioniersteuerung 7-26
Positionierung 7-26
Positionsfenster 7-12, 7-17, 7-19
Positionsüberwachung 5-4, 5-20, 7-19
Pressenanwendungen 5-18
Pressenhub 5-31
Pressensicherheitsventil 5-18
Produkt- oder Produzentenhaftung 2-4

9.1 Stichwortverzeichnis

Primärsteuerung 8-51
Produktbeobachtung 2-3, 2-17, 2-20, 2-21
Produktbeobachtungsfehler 2-14
Produktbeobachtungspflicht 2-17
Produktfehler 2-5, 2-7, 2-8, 2-12, 2-20, 2-21
Produkthaftung 2-3
Produkthaftungsgesetz 2-4, 2-5, 2-6, 2-7, 2-8, 2-9, 2-10, 2-11, 2-12, 2-13, 2-15, 2-22
- § 1 ProdHaftG 2-5
- § 3 ProdHaftG 2-5
- § 4 Abs. 1 Satz 2 ProdHaftG 2-9
- § 4 ProdHaftG 2-10
Produktivitätssteigerung 5-22
Produktkomplettierung 2-9
Produktmigration 2-8
Produktnormen 3-36
Produktsicherheitsgesetz 2-22, 4-22, 4-27
Produktsicherheitsrichtlinie 3-16
Produktverbesserung 2-10
Produzentenhaftung 2-4, 2-13
Produzentenhaftungsrecht 2-3
Prozessdatenobjekt (PDOs) 6-11
Prüfstelle 3-17
Prüfungsergebnisse 3-14, 3-70
PSSu multi 5-33
Publisher/Subscriber-Prinzip 6-10

Q

Qualitätssicherung 2-18, 2-19, 3-79
Qualitätssicherungsmaßnahmen 2-19
Qualitätssicherungsvereinbarungen 2-18, 2-19
Quasi-Hersteller 2-9
Querschlusserkennung 5-21
Quetschen 3-19, 4-7

R

RC Steuerung 7-26
Reaktionsfunktion 7-14, 7-19, 7-25
Reaktionszeiten 3-59, 4-16, 4-17, 5-22, 5-24, 7-3, 7-15, 7-16, 7-18, 7-23, 7-25, 7-42, 8-35
Realisierungsgefahr 2-20
Rechtsgutsverletzung 2-14
Reduktionsfaktor 7-32
redundanter Aufbau 5-6
Redundanz 4-13, 6-3, 6-5, 8-12, 8-13, 8-14
Reed-Kontakte 4-15
Regelverstoß 4-26
Reglerfreigabe 7-5, 7-6
Reglersperre 4-21
Reibungsgesetz 8-42
Reibungsschubspannung 8-42
Reihenschaltung ... 4-12, 7-28, 7-29, 7-31, 7-33, 7-35
Reisepass für Europa 3-5
Relais 2-8, 3-74, 4-15, 5-3, 5-6
Relaistechnik 5-4, 5-6
Relaisverschaltungen 5-3
Restrisiko 2-15, 3-14, 4-26, 4-27, 8-9
Reynoldszahl 8-41
RFID 4-13
Richtlinien 2-5, 3-3, 3-4, 3-5, 3-12, 3-15, 3-16, 3-40, 3-42, 3-43, 3-44, 3-45, 3-51, 3-54, 3-64, 3-75
Richtlinien und Gesetze in Amerika 3-40
Richtlinien und Gesetze in Asien 3-45
Richtlinien und Gesetze in Australien 3-49
Richtlinien und Gesetze in Neuseeland 3-50
Richtlinie Persönliche Schutzausrüstungen 3-16
Ringfläche 8-49, 8-50
Risiko 2-4, 2-17, 3-14, 3-24, 3-25, 3-30, 4-5, 4-26, 4-28, 4-29, 5-3, 8-5, 8-9, 8-19, 8-25, 8-31
Risikoanalyse 3-24, 3-30, 3-46, 4-22, 7-11, 7-18, 7-20, 7-23, 7-28, 7-30, 8-5, 8-9, 8-32
Risikobeurteilung 3-9, 3-10, 3-12, 3-13, 3-14, 3-57, 3-59, 3-61, 3-67, 3-68, 3-75, 8-9, 8-26
Risikobewertung 3-19, 3-21, 3-22, 3-24, 3-27, 3-30, 3-32, 3-38, 4-17, 4-22, 8-9, 8-55
Risikofaktoren 3-21
Risikograph 3-24, 3-25, 3-29, 3-30
Risikominderung 3-19, 3-21, 3-22, 3-55, 5-4, 8-5
Risikominimierung 3-67
Risiko-Prävention 2-21
Root Device 6-10
R_{Pmin} 4-15
RSA 3-18
$R_{Smin}(i)$ 4-15
RTFL (Real Time Frame Line) 6-8, 6-9, 6-10
RTFN (Real Time Frame Network) 6-8, 6-9
Rückruf 2-17, 2-20
Rückschlagventil 8-13, 8-30, 8-51
Rückwirkungsfreiheit 5-22
Ruhestromprinzip 8-58

S

S = (K x T) 4-15
S = (K x T) + C 4-17
S = K* (t1 + t2) + C 4-16
Sabotage 4-24
Safe Motion 7-3, 7-28
Safe Motion Beispiele 7-28
Safety Calculator PAScal 3-24, 3-29, 3-57, 7-32
Safety Integrity Level (SIL) 3-30, 3-68, 3-72, 4-11
SafetyNET p 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9, 6-10, 6-11, 6-12, 6-13, 6-14, 7-7

9.1 Stichwortverzeichnis

Schadensursachenverlauf 2-21
Schaltmatten 4-17, 4-19
Schaltplan 5-11, 8-25, 8-26, 8-29, 8-34, 8-35, 8-36, 8-44, 8-46, 8-47, 8-48, 8-49, 8-50, 8-51, 8-56
Schaltschema 8-28, 8-29
Schaltstellungsabfrage 8-32
schaltungstechnische Lösungen 8-27
Schaltzyklen 7-31
Schlauchfarben 8-36
Schlauchnummern 8-36
Schlauchquerschnitte 8-36
Schleppfehlererkennung 7-37
Schließerprinzip 4-19
Schnittstellen/Kommunikation 7-22
Schraubenpumpe 8-53
Schreit- und Greifgeschwindigkeit 4-16, 4-17
Schutzeinrichtung 3-19, 3-20, 3-28, 3-36, 3-37, 3-43, 3-57, 3-59, 3-67, 3-75, 3-80, 3-81, 4-3, 4-4, 4-5, 4-7, 4-8, 4-9, 4-11, 4-12, 4-14, 4-15, 4-16, 4-17, 4-18, 4-19, 4-21, 4-22, 4-24, 4-26, 4-27, 4-28, 4-29, 5-4, 5-18, 7-24, 7-41, 8-9, 8-16, 8-17, 8-18, 8-25, 8-55
Schutzgesetze 2-22
Schutzraumabsicherung mit sicherer kamerabasierter Lösung 7-41
Schutztür 3-81, 4-9, 4-11, 4-12, 4-13, 4-15, 5-7, 5-9, 5-12, 5-19, 5-28, 5-32, 5-37, 7-3
Schutzzaun 3-58, 4-6, 4-15, 4-17
Schutzziele 3-3, 3-4, 3-70, 8-28
Schweredruck 8-39
Segmentabschaltungen 4-24
Sektornorm 3-29, 3-33, 3-36, 3-67, 7-11
Sekundärsteuerung 8-51
Sensor-Teilsystem 7-38, 7-39
Sensoren 3-37, 3-59, 4-11, 4-12, 4-14, 4-18, 4-19, 5-4, 5-6, 5-16, 5-17, 5-31, 5-41, 6-6, 7-17, 7-24, 7-26, 7-36, 7-38, 8-32
sequenzielles Muting 5-16
Serienschaltung 4-14, 4-15, 8-47, 8-49
Service-Daten-Objekte 6-11
Servo- und Frequenzumrichter 7-10
Servopressen 5-31
Servoumrichter 7-25, 7-26
Servoverstärker 2-9, 7-4, 7-12, 7-14, 7-15, 7-23, 7-26, 7-28
SFF 3-32
sicher abgeschaltetes Moment (STO) 7-12, 7-14, 7-15, 7-16, 7-20, 7-23, 7-27, 7-36, 7-37, 7-38, 7-39, 7-40
sicher begrenzte Beschleunigung (SLA) 7-17, 7-36, 7-37, 7-38, 7-40
sicher begrenzte Geschwindigkeit (SLS) 7-18, 7-19, 7-33, 7-34, 7-36, 7-37, 7-38, 7-39, 7-40
sicher begrenzte Position (SLP) 7-19
sicher begrenztes Moment (SLT) 7-19
sicher begrenztes Schrittmaß (SLI) 7-19
sicher reduzierte Geschwindigkeit 3-54, 3-55, 7-3, 7-18
sichere Absolutlage 7-7
sichere Analogverarbeitung 5-20
sichere Antriebsfunktion 7-3
sichere Bewegung 7-3
sichere Bewegungsfunktion 7-17
sichere Bewegungsrichtung (SDI) 7-19, 7-36, 7-37, 7-38, 7-40
sichere Bewegungssteuerung 4-21, 7-4
sichere Bewegungsüberwachung 7-4, 7-9, 7-26
sichere Bremsenansteuerung (SBC) 7-20
sichere Bremsfunktion 7-20
sichere Dezentralisierung 5-24
sichere Drehrichtung (SDI) 7-35
sichere Geschwindigkeitsüberwachung (SSM) 7-19
sichere Grenzwertvorgabe 7-9
sichere kamerabasierte Lösung 7-41
sichere Kamerasysteme 3-37, 3-81, 4-16, 4-19, 4-20, 7-3
sichere Kommunikation 5-13, 5-15, 6-3, 6-11
sichere Logik 7-24
sichere Nachricht 6-4, 6-5
sichere Steuerungen 5-25, 7-9
sichere Steuerungstechnik 5-11, 5-28, 5-30, 5-31, 5-35, 5-36, 5-37,
sichere Stoppfunktion 7-14, 7-19, 7-28, 7-32
sichere Stoppfunktion an Vertikalachsen 7-30
sichere Trennung 7-4, 7-13
sichere Wiederanlaufsperre 7-14, 7-23
sicherer Beschleunigungsbereich (SAR) 7-17, 7-36, 7-37, 7-38, 7-40
sicherer Betriebshalt (SOS) 7-16, 7-17, 7-36, 7-37, 7-38, 7-40
sicherer Bremsentest (SBT) 7-20
sicherer Geber 5-19, 7-8, 7-40
sicherer Geschwindigkeitsbereich (SSR) 7-18, 7-36, 7-37, 7-38, 7-39, 7-40
sicherer Momentenbereich (STR) 7-19
sicherer Nocken (SCA) 7-19
sicherer Stopp 1 (SS1) 7-12, 7-14, 7-15, 7-16, 7-18
sicherer Stopp 2 (SS2) 7-12, 7-16, 7-17
sicherer Zustand 7-3
sicheres Bestehen 8-12
Sicherheits- und Gesundheitsanforderungen 3-12, 3-14, 3-17
Sicherheitsabschaltung 7-16

9.1 Stichwortverzeichnis

Sicherheitsabstand.....3-28, 4-6, 4-15, 4-16, 4-17, 7-16, 7-42
Sicherheitsanforderungen 2-22, 3-9, 3-12, 3-14, 3-17, 3-40, 3-41, 3-42, 3-43, 3-44, 3-48, 3-51, 3-53, 3-72, 5-12, 5-14, 5-22, 5-40, 7-12, 7-25, 8-55, 8-56
Sicherheitsbauteil 3-6, 3-11, 3-40, 3-44, 3-48, 3-74, 8-23, 8-28, 8-56
Sicherheitserwartung..... 2-6, 2-7, 2-8, 2-10, 2-19, 2-20
Sicherheitsfunktionen 3-9, 3-24, 3-27, 3-29, 3-38, 3-54, 3-60, 3-61, 3-63, 3-68, 3-69, 3-70, 3-71, 3-72, 3-73, 5-3, 5-4, 5-6, 5-9, 5-11, 5-19, 5-21, 5-26, 5-32, 5-36, 5-37, 7-3, 7-6, 7-7, 7-10, 7-11, 7-12, 7-13, 7-14, 7-15, 7-16, 7-17, 7-18, 7-19, 7-20, 7-21, 7-23, 7-24, 7-25, 7-26, 7-28, 7-29, 7-30, 7-31, 7-33, 7-36, 7-37, 7-38, 7-39, 7-40, 7-41, 7-42, 8-9, 8-60
sicherheitsgerichtete Kommunikation 6-3, 6-4, 6-5, 6-7, 6-11
Sicherheitsgrund- und Sicherheitsfachgrundnormen 7-28
Sicherheitshinweise.....2-16, 8-19
Sicherheitsintegrität..... 7-8, 7-9, 7-11, 7-13, 7-23
Sicherheitskategorie.....4-20, 7-6
Sicherheitskennwerte.....7-36
Sicherheitskette.....5-4, 5-18, 7-13, 8-31
Sicherheitsprinzipien 3-23, 3-69, 3-74, 8-26, 8-58, 8-59, 8-60, 8-61, 8-62
sicherheitsrelevante Übertragungsfunktion.....6-4
Sicherheitsschalter mit integrierter Fehlererkennung 4-13
Sicherheitsschaltgeräte.....3-33, 4-13, 4-15, 4-18, 5-3, 5-4, 5-5, 5-6, 5-7, 5-8, 5-9, 5-10, 5-11, 5-12, 5-13, 5-23, 5-25, 7-23, 7-24, 7-27, 7-36, 8-29, 8-30, 8-32, 8-33
Sicherheitsstandard 2-6, 2-8, 2-10
Sicherheitssteuerungen.....3-33, 3-60, 3-61, 3-63, 3-73, 5-4, 5-12, 5-15, 5-21, 5-22, 5-24, 5-25, 5-28, 5-30, 5-31, 5-32, 5-33, 5-35, 5-36, 6-3, 6-7, 6-12, 7-3, 7-14, 7-23, 7-24, 7-28
sicherheitswidriges Verhalten.....4-24
Sicherungsmaßnahmen.....2-6, 2-7
Sin/Cos-Geber: $\sin^2+\cos^2=1$ 7-40
Sinus-/Cosinus-Motorgeber.....7-26
Sistema.....3-75
Softwaretool 5-11, 5-32, 5-38
Sollwert-Vorgabe.....7-6
Sorgfaltsmaßnahmen 2-6
speicherprogrammierbare Steuerung (SPS).....5-3
Spannungsfreiheit 5-4, 5-10
Spezifikationen 2-7, 2-19, 3-14, 3-63, 3-70
SPDO.....6-12
Spitzenstrom I_S.....4-15
SPS-Steuerung.....5-21, 5-33
SRCF 3-70
Standardgeber.....7-8, 7-36, 7-37, 7-38
Standards Australia 3-49
Standardsensoren 7-38 7-39
statistische Methoden 3-24, 3-29
Stellgröße 7-5, 7-6
Stellteile.....4-20, 4-24
Stellventil 5-20
Steuerkreispläne.....3-14
Steuerung (SRP/CS).....7-28
Steuerungssystem..... 3-20, 3-29, 3-33, 3-67, 4-11, 5-21, 5-22, 5-27, 5-29, 5-39, 6-6, 7-11
Steuerungstechnik 5-3, 5-22, 5-24, 5-29
Stillsetzen 4-5, 4-11, 5-4, 7-12, 7-14, 7-15, 7-16, 7-20
Stillstand..... 3-54, 5-10, 5-19, 7-3, 7-12, 7-14, 7-15, 7-16, 7-42, 8-60
Stillstandserkennung.....7-15, 7-16
Stillstandsposition 7-16, 7-17
Stillstandsschwelle.....7-12
stochastische Gefährdungen 8-8, 8-12, 8-15
Stopp-Funktion 7-12, 7-14, 7-19, 7-28 7-29, 7-30, 7-32, 7-34, 7-35
Stopp-Kategorie.....7-12, 8-30
Störfestigkeit 3-36
Störfestigkeitsanforderungen 3-36
Stöselhub 5-31
Strömungsformen.....8-41
strukturelle Methoden 3-24, 3-29
Synchronisation.....7-16
Subscriber 6-7, 6-10, 6-14
Systembetrachtung 3-26, 3-31, 7-22 7-23, 7-24, 7-25, 7-26, 7-27

T

technische Dokumentation.....3-6, 3-14
technische Spezifikationen.....2-7, 3-14
Teilmaschinen.....3-10
Telegramm 6-3, 6-4, 6-11
Telegrammaufbau.....6-12
TGA/DATECH 3-78
Tippbetrieb 7-3, 7-18, 8-59
Tippfunktion 7-18, 7-33, 7-34
T_m Gebrauchsdauer.....5-26
t_{multi}.....7-42
Topologie.....6-8
Top-down 3-70

9.1 Stichwortverzeichnis

Tore ... 3-19
trennende Schutzeinrichtungen ... 4-4, 4-5, 4-6, 4-8, 4-9, 4-11, 4-14, 4-16, 4-27, 4-28, 8-17
t_{rampe} ... 7-42
$t_{reak} = t_{multi} + t_{PMC} + t_{rampe}$ ... 7-42
$t_{reak} = t_{PMC} + t_{rampe}$ ... 7-42
TÜV ... 5-11, 5-30
Typ C ... 3-80
t_{zyklus} ... 7-31, 7-34

U

Überdruck ... 2-16, 8-38
Überfunktionalität ... 4-27
Übergangsfristen ... 3-3, 3-5, 3-17, 3-48
Übertragungsfunktion ... 6-4
Überwachungsfunktion ... 5-4, 5-18, 5-22, 5-28, 7-16, 7-18, 7-25, 7-36, 7-37, 7-38, 7-39, 7-40
UDP/IP-basierte Kommunikation ... 6-9
UDP/IP-Kommunikation ... 6-8
UL ... 3-18
Umbau ... 2-17, 3-8, 8-36
Umgehen von Schutzeinrichtungen ... 4-20, 4-22, 4-24
Umgebungsanforderungen ... 3-73
Umgehungsmöglichkeit ... 3-36, 4-17, 4-18
Umrichter ... 4-21, 6-8, 7-4, 7-5, 7-6, 7-25, 7-31
unerwarteter Anlauf ... 3-19, 4-11, 4-21, 7-14, 8-27, 8-55
ungewollter Wiederanlauf ... 4-21
unmittelbare Sicherheitstechnik ... 8-15, 8-16
Unterbrechung ... 5-4, 5-37, 7-6, 7-12, 8-16
unvollständige Maschine ... 3-6
U_{Pmax} ... 4-15
UVG-Bundesgesetz ... 3-80

V

V-Modell ... 3-62, 3-66, 3-72
Validierung ... 3-9, 3-14, 3-19, 3-24, 3-57, 3-59, 3-62, 3-67, 3-68, 3-69, 3-70, 3-71, 3-72, 3-73, 3-74, 3-75, 4-11, 5-26
Validierung von Sicherheitsfunktionen ... 3-29, 3-71, 3-72
VCI-Regeln ... 2-11
VDE- oder ETSI-Normen ... 2-11
VDE-Empfehlungen ... 2-7, 2-11
VDE-Richtlinien ... 2-11
Ventilansteuerung ... 5-32
Ventile mit definierter Schaltstellung ... 8-56
Ventilquerschnitt ... 8-45
Verdrahtungsaufwand ... 5-7, 5-8, 5-9, 5-14, 7-12, 7-23, 7-25
Verfälschung von Nachrichten ... 6-4
Verjährung ... 2-12
Verkehrssicherungspflicht ... 2-14
Verknüpfungslogik ... 5-8
Verletzung, Schwere der ... 3-25
Verlust von Nachrichten ... 6-4
Vermutungswirkung ... 3-3, 3-4, 3-24, 3-29
Verriegelung ... 4-4, 4-5, 4-9, 4-11, 4-24, 4-25, 4-27, 4-29, 5-28, 8-55
Verriegelungseinrichtung ... 3-19, 3-36, 4-5, 4-7, 4-23
Verriegelungskonzept für Sonderbetriebsarten ... 4-25
Verschaltung ... 5-3, 5-7
Verschraubungen ... 8-25, 8-26, 8-36
Verschuldenshaftung ... 2-13, 2-14, 2-15, 2-16, 2-17, 2-18, 2-19, 2-20, 2-21
Verstellpumpe ... 8-43
Vertikalachsen ... 7-14, 7-25, 7-30
vertragliche Haftung ... 2-4
Verwenderkreis ... 2-8
Verzögerung von Nachrichten ... 6-4
Viskosität ... 8-22, 8-41, 8-42, 8-43, 8-56, 8-58
Visualisierung ... 5-27, 5-29
Vollständiges Antriebsmodul/ Complete Drive Module (CDM) ... 7-10

W

Warenvertrieb (cross border business) ... 2-4
Warnhinweise ... 2-15, 2-16, 2-19
Warnung ... 2-16, 2-17, 2-20
Wartungseinheit ... 8-24, 8-27, 8-29, 8-36
Wechselrichter ... 7-5, 7-6
Wellenbruch ... 5-18
wesentliche Änderung ... 3-8
wesentliche Veränderung ... 3-8
Wiederanlauf ... 4-18, 4-21, 5-12, 7-6, 7-23, 8-54
Wiederholung von Nachrichten ... 6-3, 6-4

Z

Zahnradpumpe ... 8-52, 8-54
Zeiterwartung (timeout) ... 6-4
Zeitverzögerung ... 7-15, 7-16
Zertifizierungspflicht ... 3-45, 3-47
Zugang ... 3-7, 3-54, 4-3, 4-4, 4-5, 4-8, 4-9, 4-16, 4-18, 7-17, 7-31, 7-41
zugangsbeschränkende verstellbare Schutzeinrichtungen ... 4-5
Zugriff ... 4-9, 5-40, 8-17
Zuhaltung ... 3-36, 4-5, 4-9, 4-11
zusammengesetzte Maschinen ... 3-6
Zustimmprinzip ... 5-24

9.1 Stichwortverzeichnis

Zustimmschalter.....5-7, 7-34
Zweihand.....5-6
Zweihandschaltungen ... 3-19, 4-17, 4-20, 8-17, 8-25
Zweihandsteuerung.....4-20
Zweizylindersteuerungen
mit elektrischen Ventilen.....8-47
Zwischenkreis..... 7-5, 7-6, 7-23
zyklischer Datenkanal.....6-11

9.2 Haftungsausschluss

Wir haben unser Sicherheitskompendium sehr sorgfältig zusammengestellt. Es enthält Informationen über unser Unternehmen sowie über unsere Produkte. Alle Angaben haben wir nach dem heutigen Stand der Technik und bestem Wissen und Gewissen gemacht. Dennoch können wir für die Richtigkeit und Vollständigkeit der Angaben, sofern uns nicht der Vorwurf grober Fahrlässigkeit trifft, keine Haftung übernehmen, da sich trotz aller Sorgfalt Fehler nicht vollständig vermeiden lassen. Insbesondere haben die Angaben nicht die rechtliche Qualität von Zusicherungen oder zugesicherten Eigenschaften. Für Hinweise auf Unstimmigkeiten sind wir dankbar.

© 2017 by Pilz GmbH & Co. KG, Ostfildern
5., überarbeitete und erweiterte Auflage

Sach-Nr.: 775740
8-8-1-0-100, Printed in Germany

Support

Technische Unterstützung von Pilz erhalten Sie rund um die Uhr.

Amerika
Brasilien
+55 11 97569-2804
Kanada
+1 888-315-PILZ (315-7459)
Mexiko
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asien
China
+86 21 60880878-216
Japan
+81 45 471-2281
Südkorea
+82 31 778 3300

Australien
+61 3 95600621

Europa
Belgien, Luxemburg
+32 9 3217575
Deutschland
+49 711 3409-444
Frankreich
+33 3 88104000
Großbritannien
+44 1536 462203
Irland
+353 21 4804983
Italien, Malta
+39 0362 1826711
Niederlande
+31 347 320477
Österreich
+43 1 7986263-0
Schweiz
+41 62 88979-30
Skandinavien
+45 74436332
Spanien
+34 938497433
Türkei
+90 216 5775552

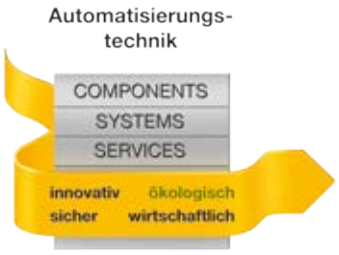
Unsere internationale Hotline erreichen Sie unter:
+49 711 3409-444
support@pilz.com

Haben Sie Fragen zur Maschinensicherheit?
Pilz antwortet auf www.wissen-maschinensicherheit.de

Pilz entwickelt umweltfreundliche Produkte unter Verwendung ökologischer Werkstoffe und energiesparender Techniken. In ökologisch gestalteten Gebäuden wird umweltbewusst und energiesparend produziert und gearbeitet. So bietet Pilz Ihnen Nachhaltigkeit mit der Sicherheit, energieeffiziente Produkte und umweltfreundliche Lösungen zu erhalten.

Energy saving by Pilz

BLUEcoMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative



Überreicht durch:

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Deutschland
Telefon: +49 711 3409-0, Telefax: +49 711 3409-133
E-Mail: info@pilz.com, Internet: www.pilz.com

In vielen Ländern sind wir durch Handelspartner vertreten. Nähere Informationen entnehmen Sie bitte unserer Homepage www.pilz.com oder nehmen Sie Kontakt mit unserem Stammhaus auf.

PILZ
THE SPIRIT OF SAFETY

8-8-de-3-138, 2017-12 Printed in Germany