# BIA-Report 6/97

# Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1

HVBG
Hauptverband der gewerblichen Berufsgenossenschaften

Autoren: Werner Kleinbreuer, Franz Kreutzkampf
Karlheinz Meffert, Dietmar Reinert
Berufsgenossenschaftliches Institut
für Arbeitssicherheit — BIA
Sankt Augustin

Herausgeber: Hauptverband der gewerblichen
Berufsgenossenschaften (HVBG)
Alte Heerstraße 111, 53754 Sankt Augustin
Telefon: 0 22 41 / 2 31 - 01
Telefax: 0 22 41 / 2 31 - 3 33
— Juli 1997 —

Satz und Layout: HVBG, Abteilung Öffentlichkeitsarbeit

Druck: Druckerei Plump OHG, Rheinbreitbach

ISBN: 3-88383-445-9
ISSN: 0173-0387

# Kurzfassung

Der vorliegende Report stellt die wesentlichen Inhalte der EN 954 „Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze" dar und erläutert die Anwendung der Norm an zahlreichen Beispielen aus den Bereichen Elektromechanik, Fluidtechnik, Elektronik und Rechnertechnik.

Der Zusammenhang mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie wird aufgezeigt, und die möglichen Verfahren zur Risikoabschätzung werden vorgestellt. Auf der Basis dieser Informationen erlaubt der Report die Auswahl der Kategorie für sicherheitsbezogene Teile von Steuerungen an Maschinen. Auf die Anforderungen für die jeweilige Kategorie wird im Detail eingegangen, und da, wo notwendig, finden sich die erforderlichen Hintergrundinformationen zur Umsetzung der Anforderungen in die steuerungstechnische Praxis. In drei umfangreichen Tabellen werden die grundlegenden Sicherheitsprinzipien, die bewährten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile z.T. anwendungsabhängig aufgelistet. Die Beispiele zeigen bis auf die Bauteilebene, wie die Kategorien B bis 4 in den jeweiligen Technologien technisch umgesetzt werden können. Sie geben dabei Hinweise auf die verwendeten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile. Zahlreiche Literaturverweise dienen einem tieferen Verständnis der einzelnen Beispiele.

In zwei Anhängen finden sich sowohl ausführliche elektrische, hydraulische und pneumatische Fehlerlisten als auch mehrere Beispiele für die Risikoabschätzung an Maschinen.

Der Report zeigt, daß die Anforderungen der EN 954-1 in Technik umgesetzt werden können und stellt damit einen ersten Beitrag dar, eine einheitliche Anwendung und Interpretation der Kategorien in Europa zu fördern.

# Abstract

This report describes the main elements of EN 954 "Safety of machinery — safety-related parts of control systems, Part 1: General design principles" and deals with the application of this standard, drawing on numerous examples from electromechanics, fluid technology, electronics and computing.

Information is also provided on the link between EN 954 and the basic safety requirements laid down in the machinery directive, and possible means of risk assessment are also described. On the basis of this information, the report can be used as an aid in the selection of the category of safety-related parts for control systems for machinery. The requirements of each category are covered in detail and, where necessary, the relevant background information regarding the implementation of these requirements for control systems in practice is also provided. Three comprehensive tables depict the fundamental safety principles, those safety principles that have become established and component parts that have proved to be safe. The tables are partly broken down into specific applications. The examples show how categories B to 4 can be implemented in practice, going as far as giving examples of component parts. Information is also provided on the safety principles used and on component parts that have a proven track record in terms of safety. Numerous bibliographical references are also given for readers who want to look into individual examples in more depth.

As well as detailed electric, hydraulic and pneumatic error lists, the two appendices also contain several examples for assessing the risk presented by machinery.

The report shows that the requirements stipulated in EN 954-1 can be implemented in practice and therefore makes an initial contribution to promoting the uniform application and interpretation of categories throughout Europe.

# Résumé

Le compte rendu suivant présente les principaux contenus de la norme EN 954 «Sécurité des machines — Pièces de sécurité dans les commandes, Partie 1: Principes généraux de construction» et explique l'application de la norme à l'aide de nombreux exemples tirés des domaines de l'électromécanique, de la technique des fluides, de l'électronique et le l'informatique.

Le lien avec les exigences de sécurité fondamentales définies dans la directive machines est mis en évidence, les méthodes envisageables pour l'évaluation des risques sont présentées. Sur la base de ces informations, le compte rendu permet de choisir la catégorie des pièces de sécurité dans les commandes de machines. Les exigences des différentes catégories sont exposées en détail et les informations de base sur leur transposition dans la pratique technique sont fournies là où elles sont nécessaires. Trois grands tableaux présentent, partiellement classés par application, les principes de sécurité fondamentaux, les principes de sécurité qui ont fait leurs preuves et les pièces de sécurité confirmées. Les exemples montrent jusqu'au niveau des pièces comment les catégories B à 4 peuvent être mises en pratique dans les différentes technologies. Ils donnent à cet égard des indications sur les principes de sécurité utilisés et sur les pièces de sécurité de fiabilité attestée. De nombreuses indications bibliographiques permettent d'approfondir la compréhension des différents exemples.

Deux annexes contiennent des listes détaillées de défaillances électriques, hydrauliques et pneumatiques, de même que plusieurs exemples d'évaluation des risques sur les machines.

Le compte rendu montre que les exigences de la norme EN 954-1 peuvent être mises en œuvre dans la technique et constitue ainsi une première contribution à une application et à une interprétation homogènes de ces catégories en Europe.

# Resumen

El presente informe da a conocer los contenidos más importantes de la norma europea EN 954 sobre «Seguridad de las máquinas — Piezas en relación a la seguridad de sistemas de control, parte 1: Principios de configuración generales» y explica el empleo de la norma con muy variados ejemplos de los ramos de la electromecánica, la técnica de fluidos, la electrónica y la técnica de ordenadores.

Se muestra la relación con las exigencias de seguridad básicas de la directiva para máquinas y se dan a conocer los posibles procedimientos para el cálculo de riesgos. Mediante estas informaciones, el informe hace posible la selección de la categoría de piezas o elementos relacionados con la seguridad de los sistemas de control de las máquinas. Se hace referencia detallada de las exigencias de cada categoría y, siempre que resulte ello necesario, se cuenta con las informaciones básicas necesarias para la aplicación de las exigencias en la práctica real de la técnica de los sistemas de control. Los principios de seguridad básicos, los principios de seguridad ya aceptados por sus buenos resultados y las piezas de construcción de técnica de seguridad se alistan —en parte de acuerdo a su aplicación— en tres cuadros bien amplios. Los ejemplos muestran hasta al nivel de las piezas de construcción cómo las categorías de B a 4 pueden aplicarse técnicamente a cada una de las tecnologías correspondientes. En estos ejemplos se encuentran indicaciones sobre los principios de seguridad y sobre las piezas de construcción relacionadas a la técnica de seguridad y ya aceptadas por sus buenos resultados. Se ofrece numerosa información bibliográfica para la profundización de los ejemplos individuales mostrados.

En dos anexos se encuentran listas de errores exhaustivas en relación a la electricidad, la hidráulica y la neumática así como varios ejemplos en relación al cálculo de los riesgos propios de las máquinas.

El informe muestra que las exigencias de la norma EN 954-1 pueden tener sus aplicaciones técnicas y en este sentido viene a ser una primera contribución a la promoción de la aplicación unificada y de la interpretación de las categorías en Europa.

# Inhaltsverzeichnis


Seite

**Vorwort** ..... 9

**1 Einleitung** ..... 11

**2 Risikobetrachtung und Abgrenzung der Steuerungen** ..... 15
2.1 Abgrenzung der sicherheitsbezogenen Teile der Steuerung ..... 16
2.2 Identifizierung der Gefährdungen ..... 17
2.3 Risikoabschätzung mit Beschreibung der Risikoparameter ..... 22

**3 Kategorien nach EN 954-1** ..... 31
3.1 Allgemeines ..... 31
3.2 Festlegungen für die jeweiligen Kategorien ..... 33

**4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien** ..... 49
4.1 Grundlegende technologiebezogene Bemerkungen zu den Steuerungsbeispielen ..... 50
4.2 Beispiele für die technologieunabhängige Realisierung der einzelnen Kategorien ..... 60

**5 Schlußbetrachtung** ..... 157

**Literaturverzeichnis** ..... 159

**Anhang A: Beispiele zur Risikoabschätzung an Maschinen** ..... 165
A.1 Der Risikograph ..... 165
A.2 *Beispiele der Anwendung des Risikographen* ..... 168

**Anhang B: Fehlerlisten** (im Original übernommen) ..... 173

# Vorwort

Nach fast achtjähriger Arbeit ist im Frühjahr 1996 die europäische Norm EN 954-1 „Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen, Teil 1 : Allgemeine Gestaltungsgrundsätze" angenommen worden. Die relativ lange Zeit zur Erarbeitung dieser Norm wird verständlich, wenn man bedenkt, daß es sich um einen außerordentlich komplexen Normungsgegenstand handelte, der weder auf europäischer noch auf nationaler Ebene einen Vorläufer hatte, der als Orientierung dienen konnte.

Es galt, eine anwendungsunabhängige Norm (Typ-B-Norm) zu entwickeln, die von anderen Normen im Bereich der Sicherheit von Maschinen (spezielle Maschinen oder Schutzeinrichtungen) in Bezug genommen werden kann, wenn es um die Gestaltung der jeweiligen sicherheitsbezogenen Teile der Steuerung geht. Neben der Unabhängigkeit von der Anwendung war die Unabhängigkeit von der verwendeten Technologie (Elektromechanik, Elektronik, Rechnertechnik, Hydraulik, Pneumatik) eine besondere Zielsetzung im Normungsvorhaben. Gerade diese technologie-übergreifende Sichtweise stellte eine besondere Herausforderung an die Beteiligten aus über zehn europäischen Staaten dar.

Kernstück der europäischen Norm EN 954-1 ist die Festlegung von fünf Kategorien für sicherheitsbezogene Teile von Maschinensteuerungen und Schutzeinrichtungen. Diese Kategorien können unabhängig von der Anwendung und der verwendeten Steuerungstechnologie, lediglich orientiert am vorliegenden Risiko, das von einer Maschine ausgeht, angewendet werden.

Der vorliegende BIA-Report hat zum Ziel, die in EN 954-1 definierten Kategorien zu erläutern und insbesondere anhand zahlreicher Schaltungsbeispiele* die praktische Realisierung in den unterschiedlichsten Technologien beispielhaft aufzuzeigen. Die Erläuterungen und Beispiele sind nicht als offizieller nationaler oder europäischer Kommentar zur EN 954-1 aufzufassen. Vielmehr sind in diesem Report die fast zwanzigjährigen praktischen Erfahrungen des Berufsgenossenschaftlichen Instituts für Arbeitssicherheit — BIA mit der Entwicklung und Beurteilung sicherheitsbezogener Schutz- und Steuereinrichtungen sowie

---

* Ein Teil der in diesem Report zusammengetragenen Schaltungsbeispiele sind vom BIA bereits in anderen Veröffentlichungen publiziert worden. Besonders hinzuweisen ist auf die Loseblattsammlung „BIA-Handbuch", erschienen im Erich Schmidt Verlag, Bielefeld, in dem auch weiterhin die Aktualisierungen und Ergänzungen der Schaltungsbeispiele sowie Kommentierungen zu den Kategorien erfolgen.

die Erkenntnisse aus der langjährigen Mitwirkung in den einschlägigen nationalen, europäischen und internationalen Normungsgremien zusammengetragen.

Mit dieser Zusammenstellung von Schaltungsbeispielen, die sich für die unterschiedlichsten Anwendungen und die damit verbundenen Risiken bewährt haben, soll insbesondere dem Konstrukteur von Maschinen Anregungen und Hilfestellungen für die Auswahl geeigneter Kategorien von Steuerungen sowie für eigene Entwicklungen gegeben werden. Darüber hinaus ist dieser Report ein erster Beitrag, die einheitliche Anwendung und Interpretation der Kategorien in Europa zu fördern.

# 1 Einleitung

Die Richtlinie zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten für Maschinen [1] (kurz Maschinenrichtlinie genannt) trat am 1.1.1993 mit einer Übergangsfrist von zwei Jahren in Kraft. Seit dem 1.1.1995 müssen alle Maschinen, die innerhalb des europäischen Wirtschaftsraumes in Verkehr gebracht werden, den grundlegenden Anforderungen der Maschinenrichtlinie genügen. Als Maschine gilt nach Artikel 1 der oben genannten Richtlinie die Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist, sowie gegebenenfalls von Betätigungsgeräten, Steuer- und Energiekreisen, die für eine bestimmte Anwendung wie Verarbeitung, die Behandlung, die Fortbewegung und die Aufbereitung eines Werkstoffes zusammengefügt sind. Mit der zweiten Änderung dieser Richtlinie vom 22. Juli 1993 [2] fallen auch Sicherheitsbauteile, die vom Hersteller mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion in Verkehr gebracht werden und deren Ausfall oder Fehlfunktion die Sicherheit oder die Gesundheit der Personen im Wirkbereich der Maschine gefährden können, unter den Anwendungsbereich der Maschinenrichtlinie.

Die grundlegenden Anforderungen der Maschinenrichtlinie an Maschinen und Sicherheitsbauteile finden sich im Anhang I der Richtlinie. Neben den allgemeinen Grundsätzen für die Integration der Sicherheit gibt es in diesem Anhang eigene Abschnitte zu den Steuerungen und Befehlseinrichtungen von Maschinen und den Anforderungen an Schutzeinrichtungen. Die grundlegenden Sicherheitsanforderungen bei der Gestaltung von Maschinen und Sicherheitsbauteilen verpflichten den Hersteller, eine Gefahrenanalyse vorzunehmen, um alle mit der Maschine verbundenen Gefahren zu ermitteln. Drei Grundsätze werden genannt, um die mit den einzelnen Gefährdungen verbundenen Unfallrisiken auf ein akzeptables Maß zu reduzieren:

- ☐ die Beseitigung oder Minimierung der Gefahren durch die Konstruktion selbst,
- ☐ das Ergreifen der notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Gefahren und
- ☐ die Unterrichtung der Benutzer gegen Restgefahren.

Nach Artikel 5 läßt die Einhaltung harmonisierter europäischer Normen die Übereinstimmung mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie vermuten. Mehrere europäische Normentwürfe und inzwischen harmonisierte europäische Normen vertiefen bzw. konkretisieren die im Anhang I der Maschinenrichtlinie grundgelegte Philo-

sophie zur Erreichung der Arbeitssicherheit an Maschinen. Die Normenreihe EN 292 [3] behandelt z.B. die Grundbegriffe und allgemeinen Gestaltungsleitsätze für die Sicherheit von Maschinen. Das gesamte Verfahren zur Identifizierung von Gefährdungen sowie zur Risikoeinschätzung und Risikobewertung der einzelnen Gefährdungen wird in der EN 1050 [4] „Leitsätze zur Risikobeurteilung" beschrieben. Auf der Basis dieser beiden grundlegenden Normen beschreibt die EN 954 Teil 1 [5] die erforderliche Risikominderung bei Gestaltung und Aufbau von sicherheitsbezogenen Teilen von Steuerungen und Schutzeinrichtungen. Mit dieser Norm wird erstmals europäisch eine allgemein anwendbare Systematik für Steuerungen von Maschinen und/oder deren Schutzeinrichtungen vorgelegt. Die in der Norm beschriebenen fünf Kategorien sind technologieunabhängig formuliert und werden deshalb von nahezu allen Spezialnormen für die einzelnen Schutzeinrichtungen in Bezug genommen sowie in den maschinenspezifischen Normen erwähnt.

Der vorliegende BIA-Report hat zum Ziel, die in EN 954 Teil 1 [5] definierten Kategorien für sicherheitsbezogene Teile von Steuerungen zu erläutern und insbesondere anhand zahlreicher Lösungen die praktische Realisierung beispielhaft aufzuzeigen. Weder die Erläuterungen noch die Beispiele sind als offizieller nationaler oder europäischer Kommentar zur EN 954-1 aufzufassen. Vielmehr sind im vorliegenden Report die Erfahrungen des Berufsgenossenschaftlichen Instituts für Arbeitssicherheit aus fast zwanzigjähriger Praxis bei der Beurteilung von Schutz- und Steuereinrichtungen der unterschiedlichen Technologien unter Einbeziehung der langjährigen Mitwirkung in den einschlägigen nationalen und europäischen Normungsgremien zusammengetragen.

Im folgenden Kapitel wird der grundlegende Weg von der Gefährdungsanalyse über die Risikobetrachtung zur Auswahl der sicherheitsbezogenen Teile der Steuerungen dargestellt. Ohne die Anforderungen der Norm im Detail zu wiederholen, werden im Kapitel 3 knapp die Kategorien vorgestellt, und auf die Bedeutung der im Anhang des Reports beigefügten Fehlerlisten wird hingewiesen. Das Herzstück des Reports stellt die Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien dar. Geordnet nach den fünf in EN 954-1 festgelegten Kategorien, finden sich konkrete Beispiele in den verschiedenen Technologien (Elektromechanik, Elektronik, Rechnertechnik, Hydraulik, Pneumatik). Es werden sowohl Detailschaltungen als auch Grundprinzipien vorgestellt. Alle Beispiele sind einheitlich gegliedert und enthalten zahlreiche Literaturverweise.

Im Anhang sind neben den Fehlerlisten mehrere Beispiele für die Risikoabschätzung konkreter Gefährdungen an unterschiedlichen Maschinen aufgenommen.

Die Autoren hoffen, daß der vorliegende Report dem Konstrukteur konkrete Hilfen für die Umsetzung der Kategorien sicherheitsbezogener Teile von Steuerungen gibt. Die vorliegende Interpretation der Norm ist in den unterschiedlichsten Anwendungen in der Praxis erprobt, und die Beispiele sind in zahlreichen konkreten Anwendungen technisch umgesetzt worden.

# 2 Risikobetrachtung und Abgrenzung der Steuerungen

In der Europanorm EN 1050 [4] — Leitsätze zur Risikobeurteilung — wird ein iterativer Prozeß zum Erreichen der Sicherheit an einer Maschine beschrieben. In vier Schritten kann danach das Risiko für jede Einzelgefährdung ermittelt werden. Damit ist die Basis für die erforderliche Risikominderung über die in EN 954 [5] dargestellten Kategorien gegeben. Wie in Abbildung 1 zu sehen,

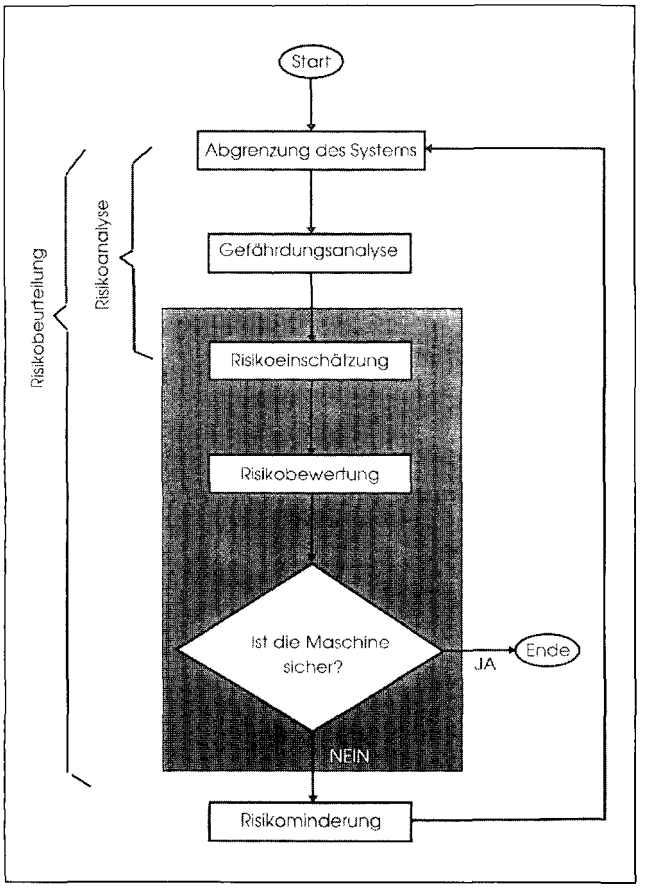



Abbildung 1:
Iteratives Verfahren zum Erreichen von Sicherheit

beginnt der iterative Prozeß mit der Bestimmung der Grenzen einer Maschine. Dabei wird die bestimmungsgemäße Verwendung in allen Situationen festgelegt und beschrieben, aber auch die räumlichen und zeitlichen Grenzen für den Betrieb der Maschine spezifiziert. Im zweiten Schritt werden die einzelnen Gefährdungen an der Maschine identifiziert, und für jede der Gefährdungen über vier verschiedene Risikoelemente wird eine Risikoeinschätzung durchgeführt. Die Risikoeinschätzung, wie sie z.B. durch das in Anhang B der EN 954 [5] beschriebene Verfahren oder aber auch den Risikographen der DIN V 19 250 [6] durchgeführt werden könnte, bildet dann die Grundlage für eine Risikobewertung. Bei all diesen Verfahren ist der Risikovergleich von entscheidender Bedeutung, da die einzelnen Parameter für die Risikobewertung nur durch den Vergleich mit bereits bestehenden Lösungen (Risikobewertungen und Risikominderungen) festgelegt werden können. Auf diese Weise ist über die Risikobewertung eine einigermaßen einheitliche Ermittlung der Kategorie für die sicherheitsbezogenen Teile von Steuerungen möglich.

In den drei folgenden kurzen Abschnitten soll das in EN 292 und EN 1050 beschriebene iterative Verfahren zum Erreichen der Sicherheit auf die sicherheitsbezogenen Teile von Steuerungen angewendet werden.

## 2.1 Abgrenzung der sicherheitsbezogenen Teile der Steuerung

Zur Definition eines sicherheitsbezogenen Teils einer Steuerung verweist die EN 954-1 auf den Anhang A der EN 292 Teil 1. Die Steuerung beginnt danach bei der Komponente, die ein

☐ von der gesteuerten Einrichtung und/oder

☐ vom Benutzer oder

☐ einer anderen zu schützenden Person

gegebenes Eingangssignal so aufbereitet, daß

☐ in Verbindung mit weiteren Eingangssignalen,

☐ der Datenspeicherung und

☐ der logischen Verarbeitung der verschiedenen Eingangssignale

sicherheitsbezogene Ausgangssignale erzeugt werden können. Die Leistungssteuerungselemente (Hauptschütze, Ventile) werden in der Definition der EN 954 ausdrücklich mit zu den sicherheitsbezogenen Teilen einer Steuerung hinzugerechnet. Ebenso fallen Überwachungssysteme unter den Anwendungsbereich der EN 954. Ausgenommen sind, wenn man den Anhang A der EN 292 zugrunde legt, die Antriebselemente, die Kraftübertragungselemente

und Arbeitsteile sowie die trennenden Schutzeinrichtungen selbst.

Aus diesen Bemerkungen wird deutlich, daß nicht nur Logikeinheiten wie speicherprogrammierbare Steuerungen oder Sicherheitsbausteine für die Not-Aus-Verarbeitung unter den Begriff „sicherheitsbezogenes Teil einer Steuerung" fallen, sondern auch vollständige Schutzeinrichtungen wie Schaltmatten mit Signalverarbeitung [7], berührungslos wirkende Schutzeinrichtungen [8], Zweihandschaltungen [9] oder auch Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen [10], soweit sie sicherheitsrelevante Teile von Steuerungen enthalten. Die meisten der für die entsprechenden Schutzeinrichtungen veröffentlichten Normen und Normentwürfe beziehen sich inzwischen auf das Klassifikationsschema der EN 954-1 und definieren unter Nennung der jeweiligen Kategorie abgestufte Anforderungen (häufig Typen genannt) für die jeweilige Schutzeinrichtung. So sind z. B. in der prEN 50 100[1] [8] zur Zeit zwei Typen von berührungslos wirkenden Schutzeinrichtungen genormt, die sich auf die Kategorien 2 und 4 beziehen, während in der EN 574 [9] fünf Typen von Zweihandschaltungen genormt werden, die den Kategorien 1, 3 und 4 zugeordnet werden. Grundsätzlich gilt, daß für alle sicherheitsbezogenen Teile von Steuerungen die entsprechenden Installations- und Betriebsanleitungen mit zur Steuer- oder Schutzeinrichtung gerechnet werden.

## 2.2 Identifizierung der Gefährdungen

Für ein und dieselbe Maschine kann man, je nach betrachteter Funktion und Betriebsart, zu unterschiedlichen Risikoeinschätzungen kommen. Dies bedeutet, daß die geeignete Kategorie für ein sicherheitsbezogenes Teil einer Steuerung von der betrachteten Sicherheitsfunktion abhängt. Es gibt demnach in der Regel keine einheitliche Kategorie für alle Sicherheitsfunktionen an einer Maschine. Um die erforderlichen Kategorien für die Maschinensteuerung festzulegen, ist es notwendig, die verschiedenen Gefährdungen an einer Maschine systematisch zu ermitteln. Zur Identifizierung der Gefährdungen an einer Maschine gibt der Anhang A der EN 1050 [4] durch die Auflistung von 37 Gefährdungsarten mit je bis zu zehn Gefährdungsereignissen bzw. Gefährdungs-

[1] 1997 wird die prEN 50 100 als prEN 61 496 veröffentlicht. Die Änderung der Nummer wurde notwendig, weil diese Norm auch als IEC 61 496 veröffentlicht wird.

situationen eine wertvolle Hilfe. Tabelle 1 zeigt eine Checkliste der wichtigsten Gefährdungen, die im Anhang A von EN 1050 aufgelistet sind. Insbesondere die mechanischen Gefährdungen und die Gefährdungen durch Ausfall/Fehlfunktion können durch eine fehlerhafte Auslegung von sicherheitsbezogenen Teilen von Steuerungen verursacht werden.

Um den Zusammenhang zwischen Gefährdung und dem Ausfall von Schutz- und Steuereinrichtung zu ermitteln, sind in der Literatur zahlreiche Verfahren beschrieben, von denen im folgenden drei kurz erläutert werden sollen.

Bei der Fehlerbaumanalyse [11] geht man von einer bekannten Gefährdung aus und sucht nach allen Ursachen, die zu dieser Gefährdung führen können. Die einzelnen möglichen Fehler werden durch elementar logische Entscheidungen (NICHT, ODER bzw. UND) miteinander verknüpft. Eine logische Null bedeutet „funktionsfähig", während die logische Eins für „ausgefallen" steht. Der Fehlerbaum wird solange verfeinert, bis man zur Ausfallart einer Komponente kommt. Dieser sogenannte Primärausfall kann nicht weiter rückgeführt werden und dient als Eingang in den Fehlerbaum. Abbildung 2 (siehe Seite 20) zeigt ein Beispiel für einen Fehlerbaum für die Gefährdung der Augen durch das von einem Laserscanner (berührungslos wirkende Schutzeinrichtung [12]) ausgesandte Laserlicht zur Personendetektion[2]. Dieses Beispiel ist der Prüfpraxis des BIA entnommen und lehnt sich in der Darstellung an [11] an. Dort wird das Gesamtverfahren im Detail beschrieben, und im Teil 2 der Norm werden auch Hinweise zur quantitativen Fehlerbaumanalyse gegeben. Dieses Verfahren wird qualitativ sehr häufig bis auf Baugruppenebene angewendet.

Die Ereignisablaufanalyse [13] sucht genau umgekehrt zur Fehlerbaumanalyse die Gefährdungen, die aus einer bestimmten Ursache resultieren. Die jeweiligen Gefährdungen sind dabei das Ergebnis der Ereignisablaufanalyse, während die Primärereignisse den Startpunkt der Ereignisablaufanalyse bilden. Abbildung 3 (siehe Seite 21) zeigt ein Ereignisablaufdiagramm für den Ausfall eines

[2] Bei einem Laserscanner wird Laserlicht durch einen rotierenden Spiegel in die Schutzfeldebene abgelenkt. Grundsätzlich ist es dabei möglich, daß der Laserstrahl die Augen der zu schützenden Person treffen kann. Nur bei entsprechend begrenzter Sendeleistung und einer durch die Rotation des Strahles gewährleisteten kurzen Einwirkdauer auf das Auge ist der Augenschutz gewährleistet. Ob einzelne Bauteilfehler Amplitude oder Einwirkdauer auf das Auge sicherheitskritisch beeinflussen können, wird durch den Fehlerbaum in Abbildung 2 systematisch untersucht.

| Gefährdung | Ereignis | Ja | Nein |
|---|---|---|---|
| mechanisch | Quetschen | | |
| | Scheren/Schneiden | | |
| | Erfassen/Einziehen | | |
| | Stoßen/Stechen | | |
| | Reiben | | |
| | Hochdruckspritzen | | |
| | Wegschleudern von Teilen | | |
| | Rutschen/Stolpern/Stürzen | | |
| elektrisch | direktes Berühren | | |
| | indirektes Berühren | | |
| | Elektrostatik | | |
| | thermische/chemische Vorgänge bei Kurzschluß/Überlastung | | |
| thermisch | Verbrennung/Verbrühung | | |
| | Kälte/Hitze in der Umgebung | | |
| Lärm | Gehörschädigung | | |
| | Streß/Müdigkeit | | |
| | Beeinträchtigung der Kommunikation (Warnsignale) | | |
| Vibration | Nerven- und Gefäßstörungen | | |
| | Durchblutungsstörungen | | |
| | Knochengelenkschäden | | |
| Strahlung | Lichtbogen | | |
| | IR/UV-Strahlung | | |
| | Laser | | |
| | elektromagnetische Strahlung | | |
| | hochfrequente Magnetfelder (Mikrowellen) | | |
| | ionisierende Strahlung | | |
| Stoffe | durch Kontakt oder Einatmen | | |
| | Explosion/Feuer | | |
| | biologisch/mikrobiologisch | | |
| Vernachlässigung der Ergonomie | physiologische Überlastung | | |
| | mentale Überlastung | | |
| | Fehlverhalten (z.B. umgehen) | | |
| Ausfall/Fehlfunktion | Ausfall der Energieversorgung | | |
| | Bauteilausfall (Ausfall der Steuerung) | | |
| | Immission | | |

Tabelle 1:
Checkliste für die Gefährdungsanalyse an Maschinen

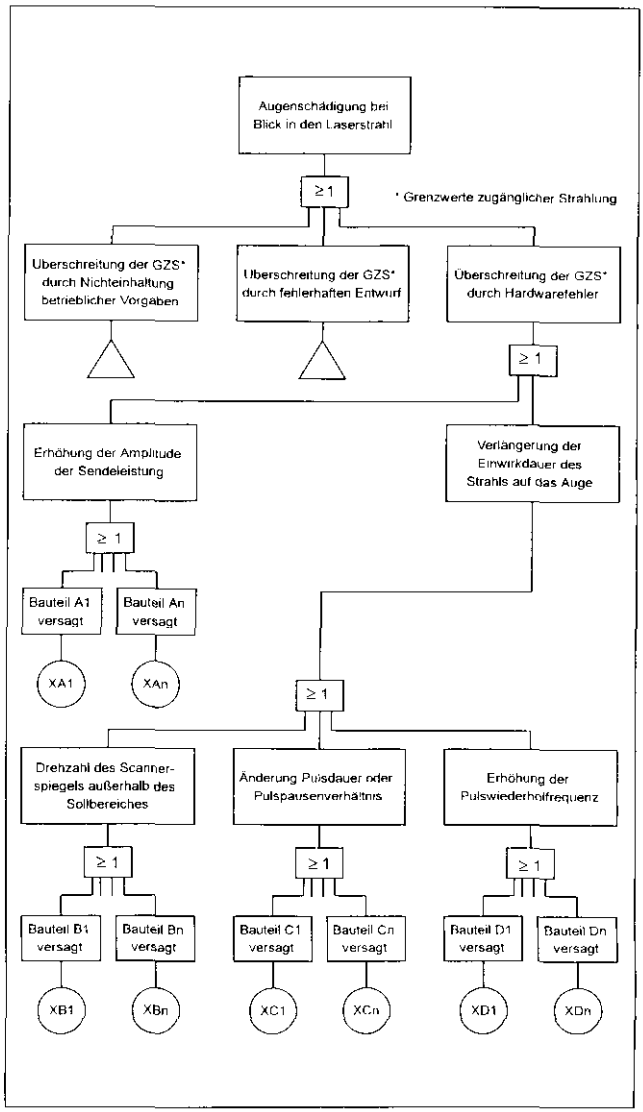



Abbildung 2:
*Fehlerbaumanalyse für* die Gefährdung der Augen durch das Laserlicht eines Laserscanners

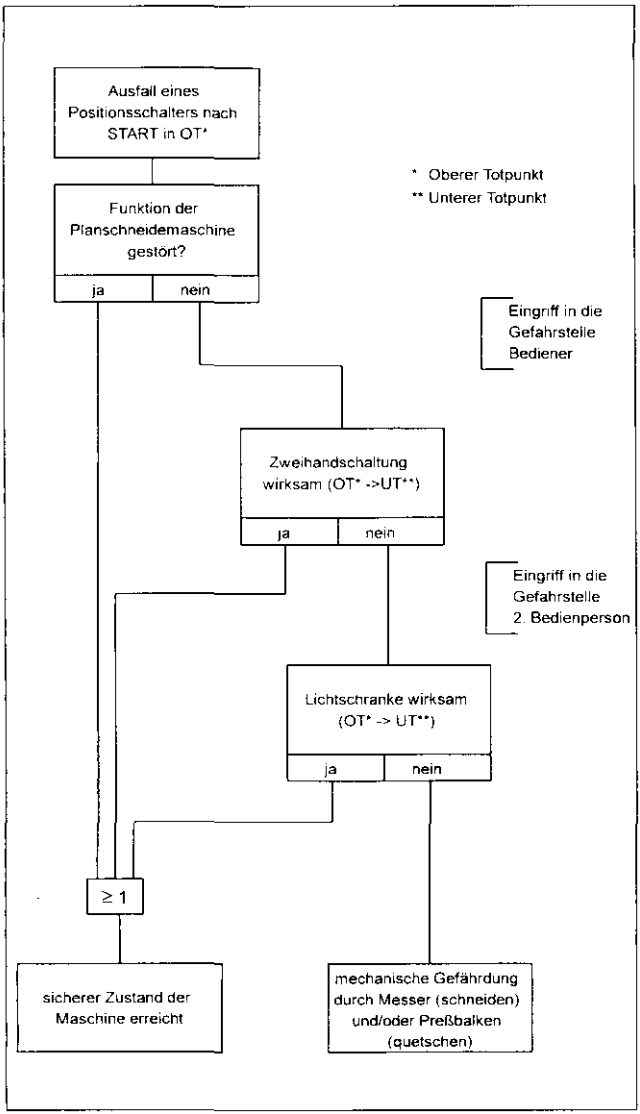



Abbildung 3:
Ereignisablaufanalyse für den Ausfall eines Positionsschalters im oberen Totpunkt an einer Planschneidemaschine

Positionsschalters im oberen Totpunkt an einer Planschneidemaschine[3]. Auch dieses Verfahren läßt sich grundsätzlich quantifizieren, wird für eine Gefährdungsanalyse in der Regel allerdings qualitativ durchlaufen.

Die Ausfalleffektanalyse [14] ist ein Verfahren zur Untersuchung der Ausfallarten aller Komponenten eines Systems und deren Auswirkungen (Effekte auf die sicherheitsbezogenen Teile von Steuerungen). Sie geht von Ausfällen einzelner Komponenten aus und analysiert die dadurch möglichen Gefährdungen. Dieses Verfahren wird sehr häufig angewendet, um konkrete steuerungstechnische Maßnahmen auf ihre Wirksamkeit hin zu untersuchen. Es ist die Basis für die Beurteilung der Kategorien nach EN 954. Tabelle 2 (siehe Seiten 24 und 25) zeigt beispielhaft einen Vordruck für die Ausfalleffektanalyse für verschiedene Ausfallarten eines integrierten Bausteines in einem Lichtgitter.

## 2.3 Risikoabschätzung mit Beschreibung der Risikoparameter

### 2.3.1 Der Begriff des Risikos

Sind alle Gefährdungen für die sicherheitsbezogenen Teile von Steuerungen an der Maschine ermittelt, so muß für jede Gefährdung eine Risikoanalyse durchgeführt werden. Einige Vorbemerkungen zum Begriff des Risikos sollen verdeutlichen, nach welcher Grundphilosophie die EN 1050 dabei vorgeht.

Die Maschinenrichtlinie fordert im Anhang I, daß Unfallrisiken während der voraussichtlichen Lebensdauer der Maschine auszuschließen sind. Da es bei technischen Einrichtungen grundsätzlich kein Nullrisiko[4] geben kann, muß diese Anforderung so interpretiert werden, daß die verbleibenden Restrisiken

[3] Die Sicherheitsfunktionen an einer Planschneidemaschine sind im Anhang A ausführlich beschrieben. Messer und Preßbalken erreichen nach jedem Schnitt die Stellung im oberen Totpunkt und verharren dort, solange kein weiterer Schnitt ausgelöst wird. Diese Stellung muß der Steuerung der Planschneidemaschine über einen Positionsschalter gemeldet werden, damit es nicht zu einem ungewollten Durchlauf von Messer und Preßbalken kommt. Unabhängig vom Positionsschalter ist der Benutzer und eine eventuelle zweite Bedienperson durch eine Zweihandschaltung und ein Lichtgitter geschützt. Eine Gefährdung ist möglich, wenn durch eine falsche Auslegung der Steuerung der Ausfall des Positionsschalters gleichzeitig Zweihandschaltung und Lichtgitter unwirksam macht. Dies wird durch die Ereignisablaufanalyse in Abbildung 3 unmittelbar verdeutlicht.

[4] Nullrisiko meint dabei das völlige Freisein von jeder Art von Risiko.

auf ein Maß reduziert werden müssen, das allgemein akzeptabel ist. Als akzeptabel wird dabei ein Risiko angesehen, wenn es von den Betroffenen im allgemeinen unter Abwägung aller Gesichtspunkte getragen wird. Die Bandbreite akzeptabler Risiken reicht über etwa sieben bis acht Zehnerpotenzen (Abbildung 4) [15]. Eine Vielzahl von Faktoren beeinflußt die Risikoakzeptanz, so daß sich bei objektiv vergleichbaren Risiken verschiedener Herkunft oder Art enorme Unterschiede in der Risikoakzeptanz ergeben können. Die wichtigsten Faktoren und ihr Einfluß auf die Risikoakzeptanz sind in Abbildung 4 schematisch dargestellt. Als markante Orientierungspunkte sind die Risiken für den Tod durch

Abbildung 4:
Abhängigkeit des akzeptablen Risikos von verschiedenen Einflüssen

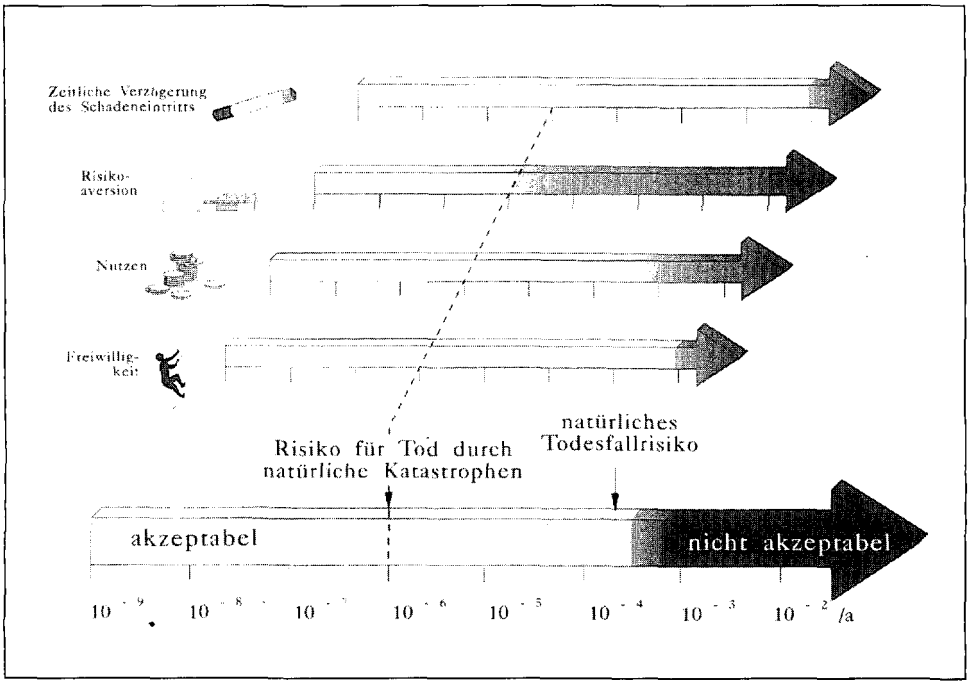


Tabelle 2:
Beispiel für die Ausfalleffektanalyse am Sender eines Lichtgitters

| Ausfalleffektanalyse | | | | Blatt 1 |
|---|---|---|---|---|
| System: Lichtgitter, Typ 4<br>Komponente: Sendeelement; integrierter Baustein U11, 4017 | | | | |
| Ausgangszustand: | | | Ausgangszustand: | |
| Sicherheitsfunktion aufrechterhalten | | | zwei unbemerkte Fehler eingebaut:<br>EF in U13 Kurzschluß Pins 5-12<br>ZF in U13 Kurzschluß Pins 5-7 | |
| 1 | 2 | 3 | 4 | 5 |
| Nr. | Funktionselement | Ausfallart | Schadensbild, mögliche Ursachen | Ausfallerkennung |
| 1.1 | Sendestrahlauswahl | Kurzschluß Pin 1-10 | zufälliger Fehler | keine,<br>Loch im Schutzfeld |
| 1.2 | Sendestrahlauswahl | Kurzschluß aller anderen Pins mit Pins 1 oder 10 | zufällige Fehler | Ausgangsrelais fallen ab |
| 1.3 | Sendestrahlauswahl | Kurzschluß Pin 5-12 | zufälliger Fehler | keine,<br>Loch im Schutzfeld |
| 1.4 | Sendestrahlauswahl | Kurzschluß aller anderen Pins mit Pins 5 oder 12 | zufällige Fehler | Ausgangsrelais fallen ab |
| 1.5 | Sendestrahlauswahl | Kurzschluß aller anderen Pins untereinander | zufällige Fehler | Ausgangsrelais fallen ab |

Tabelle 2
(Fortsetzung):

| Ausfalleffektanalyse | | | | Blatt 1 |
|---|---|---|---|---|
| System: Lichtgitter, Typ 4<br>Komponente: Sendeelement; integrierter Baustein U11, 4017 | | | | |
| Umgebungsbedingungen: | | | | Unterlagen: |
| Raumtemperatur 20 bis 30 °C<br>Luftfeuchtigkeit < 80 %<br>staubfreie Atmosphäre | | | | Schaltpläne<br>Systemspezifikation |
| | 6 | 7 | | 8 |
| Nr. | vorhandene Gegenmaßnahmen | Ausfallauswirkungen auf das System und gegebenenfalls auf seine Umgebung | | Auswirkung Bemerkungen |
| | | Beschreibung | Unterlage | |
| 1.1 | Not-Aus der Maschine durch Benutzer, falls Fehler rechtzeitig bemerkt | Loch im Lichtvorhang, durch Überstrahlung, da zwei Sender an | Prüfprotokoll XXXX Lichtgitter | gefährlicher Ausfall, Fingerschutz nicht mehr gewährleistet, unbemerkt |
| 1.2 | keine, da Fehler bemerkt und sicherer Zustand erreicht | System schaltet in der Reaktionszeit in den sicheren Zustand | Prüfprotokoll XXXX Lichtgitter | Fehler bemerkt, sicherer Zustand erreicht |
| 1.3 | Not-Aus der Maschine durch Benutzer, falls Fehler rechtzeitig bemerkt | Loch im Lichtvorhang, durch Überstrahlung, da zwei Sender an | Prüfprotokoll XXXX Lichtgitter | gefährlicher Ausfall, Fingerschutz nicht mehr gewährleistet, unbemerkt |
| 1.4 | keine, da Fehler bemerkt und sicherer Zustand erreicht | System schaltet in der Reaktionszeit in den sicheren Zustand | Prüfprotokoll XXXX Lichtgitter | Fehler bemerkt, sicherer Zustand erreicht |
| 1.5 | keine, da Fehler bemerkt und sicherer Zustand erreicht | System schaltet in der Reaktionszeit in den sicheren Zustand | Prüfprotokoll XXXX Lichtgitter | Fehler bemerkt, sicherer Zustand erreicht |

natürliche Katastrophen ($10^{-6}$) pro Jahr und für den kleinsten Wert des natürlichen Todesfallrisikos ($3 \times 10^{-4}$) eingetragen. Für die unterschiedliche Risikoakzeptanz sind entscheidend:

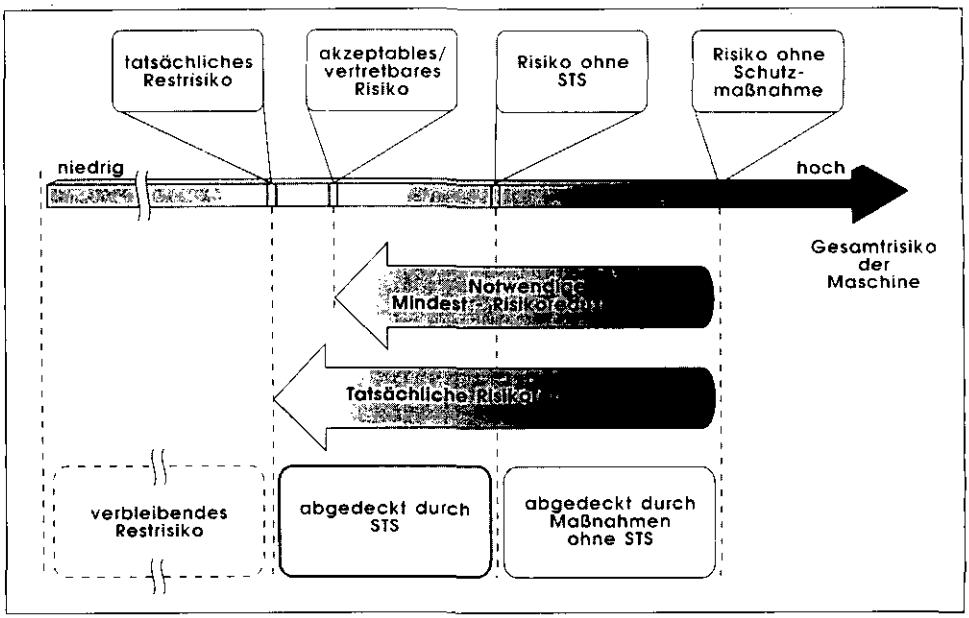
- die Tatsache, ob ein Risiko freiwillig eingegangen oder aufgezwungen wird (Unterschied bis zu drei Zehnerpotenzen),
- der persönliche oder gesellschaftliche Nutzen (bis zu vier Zehnerpotenzen bei gleichem tatsächlichem Risiko),
- die Aversion gegenüber katastrophalen Gefahrenpotentialen (etwa zwei bis drei Zehnerpotenzen geringere Akzeptanz),
- die Diskontierung von Risiken, die hinsichtlich ihrer Auswirkung in der Zukunft liegen (ein bis zwei Zehnerpotenzen höhere Akzeptanz).

Zwischen dem tatsächlichen Risiko, das von einem technischen System ausgeht, und dem Risiko, das für ein System als akzeptabel angesehen werden kann, liegen häufig nicht nur zahlenmäßig Welten. Beide Risiken sind auch völlig verschiedener Natur: Das tatsächliche Risiko ist von Fachleuten ermittelbar; es ist weitgehend durch objektive Gesichtspunkte festgelegt. Das akzeptable Risiko ist eine Konvention der sozialpolitisch Verantwortlichen; es ist also nicht determiniert, sondern stark durch subjektive und gesellschaftliche Gesichtspunkte geprägt. Die Suche nach sicherheitstechnisch befriedigenden Lösungen bedeutet zunächst, diese beiden grundsätzlich unterschiedlichen Risikogrößen zur Deckung zu bringen. Im konkreten Anwendungsfall muß also eine Lösung gewählt werden, die ein tatsächliches Risiko ergibt, das kleiner oder höchstens gleich dem akzeptablen Risiko ist.

Diese Vorbemerkungen erläutern unmittelbar die Grundgedanken, die der EN 1050 zugrundeliegen. Die Norm liefert dabei ein Verfahren, wie man die **Differenz** zwischen dem Risiko ohne Schutzmaßnahme und dem akzeptablen Risiko, in der Norm als „Restrisiko" bezeichnet, bestimmen kann (siehe Abbildung 5).

Dazu geht sie davon aus, daß das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, zusammenfassend durch eine Wahrscheinlichkeitsaussage beschrieben werden kann, die die zu erwartende Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß berücksichtigt. Das Risiko wird also bestimmt durch die beiden Größen „Wahrscheinlichkeit des Eintritts eines möglichen Schadens" (H) und „Ausmaß des möglichen Schadens durch die be-

Abbildung 5:
Der Begriff des akzeptablen Risikos




trachtete Gefährdung" (S). Diese beiden Elemente werden in der Norm in weitere Elemente aufgeteilt und im Anhang der EN 954 in diskrete Stufen zerlegt.

### 2.3.2 Die Risikoelemente

Abbildung 6 (siehe Seite 28) erläutert die durch die Norm EN 1050 definierten vier Risikoelemente. Die Wahrscheinlichkeit des Eintritts eines möglichen Schadens wird durch drei unterschiedliche Risikoelemente charakterisiert:

- die Häufigkeit und Dauer der Gefährdungsexposition (entspricht der Aufenthaltsdauer „A" nach [6]),
- die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses (entspricht der

Eintrittswahrscheinlichkeit des unerwünschten Ereignisses ohne Vorhandensein einer MSR-Schutzeinrichtung „W" nach [6]) und

□ die Möglichkeit zur Vermeidung oder Begrenzung des Schadens (entspricht der Möglichkeit einer Gefahrenabwendung „G" nach [6]).

Jedes dieser die Häufigkeit beschreibenden Risikoelemente wird im Anhang der EN 954 in mehrere diskrete Stufen unterteilt.

Bei der Bestimmung des Risikos muß die Häufigkeit (oder Wahrscheinlichkeit) des Eintritts eines Schadensereignisses mit einem bestimmten Schadensausmaß nicht unbedingt quantifiziert werden. Über qualitative Aussagen für die einzelnen Risikoelemente kann das Risiko der betrachteten Gefährdung charakterisiert werden. Auf diese Weise wird das der Maschine inhärente Risiko ermittelt. In die Bestimmung der Risikoelemente gehen dabei im wesentlichen Erfahrungswerte aus ähnlichen Anwendungen ein. Eine technische Lösung kann nach Bestimmung der Risikoelemente beurteilt werden, indem sie mit der Lösung bei einer Anwendung mit den gleichen Risikoelementen verglichen wird. Die Bewertung der Risikoelemente (siehe auch Anhang A) wird dabei in der Regel branchenspezifisch unterschiedlich vor-

Abbildung 6:
Risikoelemente nach EN 1050

genommen[5], wodurch der Unterschiedlichkeit des akzeptablen Restrisikos Rechnung getragen wird.

Wie man über die Risikoelemente nach EN 1050 **die erforderliche Risikoreduzierung zur Erreichung des akzeptablen Risikos** findet, ist im Anhang A dieses Reports beispielhaft durch die Anwendung des im informativen Anhang B nach EN 954-1 eingeführten Risikographen erläutert.

[5] So wird z.B. bei der Häufigkeit „selten bis öfter" bei Risiken an Maschinen anders interpretiert als in der Prozeßleittechnik.

## 3.1 Allgemeines

Die Anforderungen an sicherheitsbezogene Teile von Steuerungen sind im Rahmen von EN 954-1 [4] durch fünf Kategorien festgelegt. **Die Kategorien stellen eine Einteilung der sicherheitsbezogenen Teile einer Steuerung (STS) in bezug auf ihre Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall dar,** die aufgrund der Zuverlässigkeit und/oder der strukturellen Anordnung der Teile erreicht wird (Tabelle 3, siehe Seite 32). Eine höhere Widerstandsfähigkeit gegenüber Fehlern bedeutet eine höhere mögliche Risikoreduzierung. Die Kategorien sind deshalb grundsätzlich geeignet, durch steuerungstechnische Mittel das Risiko an einer Maschine auf ein akzeptables Maß zu reduzieren.

Kategorie B ist die Basiskategorie, deren Anforderungen auch in den übrigen Kategorien eingehalten werden müssen. In den Kategorien B und 1 wird die Widerstandsfähigkeit gegen Fehler überwiegend durch die Auswahl und Verwendung geeigneter Bauteile erreicht. Beim Auftreten eines Fehlers kann die Sicherheitsfunktion unwirksam sein. Kategorie 1 hat gegenüber Kategorie B eine höhere Widerstandsfähigkeit gegen Fehler durch die Verwendung besonderer, sicherheitstechnisch bewährter Bauteile.

In den Kategorien 2, 3 und 4 wird eine verbesserte Leistungsfähigkeit hinsichtlich der vorgegebenen Sicherheitsfunktion überwiegend durch strukturelle Maßnahmen erreicht. In Kategorie 2 wird die Ausführung der Sicherheitsfunktion in regelmäßigen Abständen (in der Regel durch technische Einrichtungen selbsttätig) überprüft. Zwischen den Testphasen kann beim Auftreten eines Fehlers allerdings die Sicherheitsfunktion ausfallen. Durch geeignete Auswahl der Testintervalle (z.B. einmal pro Schicht) kann bei Anwendung der Kategorie 2 eine geeignete Risikoreduzierung erreicht werden. Bei den Kategorien 3 und 4 kann das Auftreten eines einzelnen Fehlers nicht zum Verlust der Sicherheitsfunktion führen. In Kategorie 4, und, wenn immer in Kategorie 3 in angemessener Weise durchführbar, werden solche Fehler selbsttätig erkannt. In Kategorie 4 ist darüber hinaus die Widerstandsfähigkeit gegenüber einer Anhäufung von unbemerkten Fehlern gegeben.

Bei der Fehlerbetrachtung ist es notwendig, eine Konvention zu treffen, welche Bauteilfehler unterstellt werden und welche begründet ausgeschlossen werden. Hinweise auf die in Betracht zu ziehenden Fehler werden in den nächsten Abschnitten sowie in Anhang B gegeben.

# 3 Kategorien nach EN 954-1

Tabelle 3:
Anforderungen der Kategorien sicherheitsbezogener Teile von Maschinensteuerungen (nach [5])

| Kategorie | Anforderungen (Kurzfassung) | Systemverhalten | Prinzip |
|---|---|---|---|
| B | Die sicherheitsbezogenen Teile von Steuerungen und/oder ihre Schutzeinrichtungen als auch ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert werden, daß sie den zu erwartenden Einflüssen standhalten. | Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. | überwiegend durch die Auswahl von Bauteilen charakterisiert |
| 1 | Die Anforderungen von B müssen erfüllt sein.<br>Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden. | Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B. | |
| 2 | Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein.<br>Die Sicherheitsfunktion muß in geeigneten Zeitabständen durch die Maschinensteuerung geprüft werden. | Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Prüfungen führen.<br>Der Verlust der Sicherheitsfunktion wird durch die Prüfung erkannt. | überwiegend durch die Struktur charakterisiert |
| 3 | Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein.<br>Sicherheitsbezogene Teile müssen so gestaltet sein, daß<br>1. ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und,<br>2. wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird. | Wenn der einzelne Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten.<br>Einige, aber nicht alle Fehler werden erkannt.<br>Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen. | |
| 4 | Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein.<br>Sicherheitsbezogene Teile müssen so gestaltet sein, daß<br>1. ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und<br>2. der einzelne Fehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt wird, oder, wenn dies nicht möglich ist, darf eine Anhäufung von Fehlern dann nicht zum Verlust der Sicherheitsfunktion führen. | Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten. Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern. | |

Systematische Fehler[1] werden in der EN 954-1 kaum angesprochen. Nur in den Kategorien 3 und 4 weist der Satz „Fehler gemeinsamer Ursache müssen berücksichtigt werden" auf einen Typ systematischer Fehler, den Common-Mode-Fehler[2], hin. In der Kategorie 4 werden als Maßnahmen beispielhaft die Diversität und der Einsatz spezieller Prüfverfahren bei der Validierung der Kategorie als *Mittel gegen systematische* Fehler erwähnt. Grundsätzlich läßt sich sagen, daß natürlich viele der grundlegenden und der bewährten Sicherheitsprinzipien gegen systematische Fehler wirken (siehe Tabelle 4, Seiten 34 bis 36, und Tabelle 6, Seiten 41 bis 43).

## 3.2 Festlegungen für die jeweiligen Kategorien

### 3.2.1 Kategorie B

Die sicherheitsbezogenen Teile von Steuerungen müssen nach den zutreffenden Normen unter Verwendung der grundlegenden Sicherheitsprinzipien für die bestimmte Anwendung so gestaltet, konstruiert, ausgewählt, zusammengestellt und kombiniert werden, daß sie

- ☐ den erwarteten Betriebsbeanspruchungen (z.B. Zuverlässigkeit hinsichtlich ihres Schaltvermögens und ihrer Schalthäufigkeit),
- ☐ dem Einfluß des im Arbeitsprozeß verwendeten Materials (z.B. Reinigungsmittel in einer Waschmaschine),
- ☐ anderen relevanten äußeren Einflüssen (z.B. mechanischen Erschütterungen, externen elektromagnetischen Feldern, Unterbrechungen oder Störungen der Energieversorgung)

standhalten können.

Diese allgemeinen Grundsätze lassen sich in den in Tabelle 4 aufgeführten grundlegenden Sicherheitsprinzipien allgemein und technologiebezogen darstellen. *Die allgemeinen grundlegenden* Sicherheitsprinzipien gelten dabei vollständig für alle Technologien, während die technologiebezogenen Prinzipien zusätzlich für die jeweilige Technologie erforderlich sind. Da die Kategorie B eine Basiskategorie für jede der anderen Kategorien darstellt (siehe Tabelle 3), sind die grundlegenden Sicherheitsprinzipien generell bei der Konstruktion sicherheitsrelevanter Teile von Steuerungen (STS) und/oder Schutzeinrichtungen anzuwenden.

---

[1] Systematische Fehler können sich irgendwann im Laufe des Produktlebenszyklus in das Produkt einschleichen.

[2] Common-Mode-Fehler sind diejenigen Fehler, die ein mehrkanaliges System versagen lassen.

Tabelle 4:
Grundlegende Sicherheitsprinzipien für die Gestaltung sicherheitsbezogener Teile von Steuerungen
Teil 1

| Prinzip | Beschreibung | wichtige Kriterien |
|---|---|---|
| **Allgemein** | | |
| Ausreichende Dimensionierung aller Bauteile | Alle Bauteile wurden so ausgewählt, daß sie den erwarteten Betriebsbeanspruchungen genügen. | ☐ Schaltvermögen, Schalthäufigkeit<br>☐ Spannungsfestigkeit<br>☐ Druckhöhe, dynamisches Druckverhalten, Volumenstrom<br>☐ Temperatur und Viskosität der Druckflüssigkeit<br>☐ Art und Zustand der Druckflüssigkeit bzw. der Druckluft |
| Beständigkeit gegen relevante äußere Einflüsse | Die sicherheitsbezogenen Teile von Steuerungen (STS) sind so ausgelegt, daß sie ihre Funktion auch unter für die Anwendung üblichen äußeren Einflüssen ausführen können. | ☐ mechanische Einflüsse (Schock, Vibration)<br>☐ klimatische Einflüsse (Temperatur, Luftfeuchte)<br>☐ Dichtigkeit des Gehäuses (IP-Schutz)<br>☐ EMV (Felder, leitungsgebundene Störungen) |
| Ruhestromprinzip (positive Signalgabe zum Starten) | Die sicherheitsbezogene Schaltstellung der STS wird durch Wegnahme des Steuersignals (elektrische Spannung, Druck), also durch Energieabschaltung, erreicht. | ☐ Sicherer Zustand bei Unterbrechung<br>☐ Ventile mit wirksamen Federn in der Fluidtechnik |
| Beherrschung von Energieänderungen, Energieausfall und Energiewiederkehr | Bei Änderungen in der Energieversorgung (Spannung oder Druck) dürfen die STS keine unerwarteten Reaktionen initiieren. | ☐ Störungen der Stromversorgung<br>☐ Druckänderungen/Druckausfall |
| Beachtung der zutreffenden technischen Regeln | Die im Zusammenhang mit der Anwendung zutreffenden technischen Regeln sind zu beachten. | ☐ Vollständigkeit<br>☐ Korrektheit |
| Qualitätssichernde Maßnahmen während der Fertigung | Allgemeine qualitätssichernde Maßnahmen, z. B. nach EN 45 000, gewähren eine gleichbleibende Produktqualität der STS. | ☐ Reproduzierbarkeit bei der Produktion |
| Verständliche und vollständige Installations-, Inbetriebnahme-, Betriebs- und Wartungsanleitungen | Zur Installation, zur Inbetriebnahme, zum Betrieb und zur Wartung von STS sind gut strukturierte und allgemein verständliche Anleitungen vorhanden. | ☐ Vollständigkeit<br>☐ Verständlichkeit<br>☐ Korrektheit |
| Formalisierung des Änderungsgeschehens | Alle Änderungen in STS sind zu dokumentieren und die Auswirkungen auf nicht geänderte Teile der STS zu protokollieren. Freigabe der geänderten STS erst nach erfolgreicher Abnahme. | ☐ Korrektheit der Änderungen<br>☐ Rückwirkungsfreiheit auf nicht geänderte Teile |

Tabelle 4:
Grundlegende Sicherheitsprinzipien für die Gestaltung sicherheitsbezogener Teile von Steuerungen
Teil 2

| Prinzip | Beschreibung | wichtige Kriterien |
|---|---|---|
| **Fluidtechnik** | | |
| Druckbegrenzung im System | Der Anstieg des Druckes in einem System oder in Teilen von Systemen über ein festgelegtes Niveau hinaus ist in der Regel durch ein oder mehrere Druckbegrenzungsventile verhindert. In pneumatischen Sytemen werden dazu vorwiegend Druckregelventile mit Sekundärentlüftung eingesetzt. | ☐ Dimensionierung<br>☐ Anordnung im System (Anzahl)<br>☐ Ausführung |
| Filtration des Druckmediums (Druckflüssigkeit, Druckluft) | Die bezogen auf die verwendeten Bauteile vom Hersteller angegebene erforderliche Reinheitsklasse des Druckmediums während des Betriebes ist unter Berücksichtigung der jeweiligen Anwendung durch eine geeignete Einrichtung (meist Filter) erreicht. In der Pneumatik ist dazu auch eine ausreichende Entwässerung der Druckluft erforderlich. | ☐ Dimensionierung<br>☐ Art der Druckflüssigkeit/Zustand der Druckluft<br>☐ Anforderungen der Bauteilhersteller<br>☐ Umgebungs- und Einsatzbedingungen<br>☐ Anordnung im fluidtechnischen System |
| Verhinderung von Schmutzeinzug | Das Eindringen von Verschmutzung in das fluidtechnische System ist in offenen Hydrauliksystemen insbesondere durch ein wirksames Belüftungsfilter verhindert. In Pneumatiksystemen sind zu diesem Zweck (Unterdruck) Abluftfilter (Filter-Schalldämpfer-Kombination) eingesetzt. | ☐ Dimensionierung<br>☐ Anforderungen der Bauteilhersteller<br>☐ Umgebungs- und Einsatzbedingungen<br>☐ Ausströmrichtung der Abluft |
| Trennung von der Energiezufuhr (wenn die Energiezufuhr nicht für die Sicherheitsfunktion erforderlich ist, wie z.B. bei Spanneinrichtungen) | Die Trennung von der Energie und Ableitung der Restenergie (wenn erforderlich) ist durch geeignete Hauptbefehlseinrichtungen (z.B. Absperrventile) ermöglicht. | ☐ Zuverlässige Trennung/gefahrlose Ableitung (auch bei Speichern)<br>☐ Erkennbarkeit der Schaltstellung und des Betriebszustandes |

Tabelle 4:
Grundlegende Sicherheitsprinzipien für die Gestaltung sicherheitsbezogener Teile von Steuerungen
Teil 3

| Prinzip | Beschreibung | wichtige Kriterien |
|---|---|---|
| **Rechnertechnik** | | |
| Einfache Funktionsprüfung | Die sicherheitstechnischen Funktionen sind zu überprüfen. | ☐ normale Funktions- und Bedienungsabläufe<br>☐ Repräsentanz der Tests |
| Übertragungsprotokolle mit zeitlicher Sequenzüberwachung bei der Datenübertragung über Busse | Bei der Übertragung von Nutzdaten wird die Einhaltung einer Übermittlungsvorschrift (z.B. Paritätsbit) überwacht. | ☐ Korrektheit der Datenübermittlung |
| Taktüberwachung mittels Watch-Dog | Ein Zeitglied wird periodisch vom Programm zurückgesetzt. Reagiert das Programm nicht mehr mit einem Zurücksetzen, werden die STS über das Zeitglied in einen definierten Zustand gebracht. | ☐ Überwachung des Programmablaufes |
| Technischer Änderungsschutz (ROM, EPROM) | Eine Änderung der sicherheitsrelevanten Software durch Unbefugte wird durch technische Maßnahmen verhindert. | ☐ keine Änderung durch Unbefugte |
| Minimierung von Realzeiteinflüssen | Echtzeiteinflüsse im Programm erschweren die Analyse und können bestimmte Eigenschaften eines Programms unberechenbar machen. Es sollen deshalb möglichst wenige Interrupts und Nebenläufigkeiten (Multi-Tasking) existieren. Die zyklische Erfassung von Prozeßzuständen soll in fester Reihenfolge geschehen. Regeln für die Zulassung von Interrupts sind aufzustellen. | ☐ Analysierbarkeit der Software<br>☐ Änderungsfreundlichkeit von Software |
| Strukturierte Programmierung | Durch diese Methode werden der Steuerfluß bei Programmen und der Datenfluß dieser Programme transparent konstruiert. Vermieden werden dadurch nicht-systematische, komplexe und unübersichtliche Programmstrukturen. | ☐ Prüfbarkeit, Verständlichkeit<br>☐ Anpaßbarkeit<br>☐ Instandhaltbarkeit<br>☐ Portabilität |

Für die Bauteile, die mit Kategorie B übereinstimmen, sind keine weitergehenden besonderen sicherheitstechnischen Maßnahmen erforderlich[3].

### 3.2.2 Kategorie 1

Zusätzlich zu den grundlegenden Sicherheitsprinzipien müssen sicherheitsbezogene Teile der Kategorie 1 unter Verwendung sicherheitstechnisch bewährter Bauteile und Prinzipien gestaltet und konstruiert werden.

Ein sicherheitstechnisch bewährtes Bauteil für eine sicherheitsbezogene Anwendung ist ein Bauteil, das

☐ in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen mit Erfolg verwendet worden ist oder

☐ unter Anwendung von Prinzipien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen gezeigt haben.

Tabelle 5 (siehe Seite 40) gibt eine Übersicht über bekannte sicherheitstechnisch bewährte Bauteile in der Elektrotechnik sowie über Bauteile aus der Fluidtechnik, die sicherheitstechnisch bewährte Bauteile sein können.

Anforderungen an die Konstruktion und Ausführung sicherheitstechnisch bewährter Ventile sowie an den Zustand des beteiligten Druckmediums wurden bisher noch nicht festgelegt. Daher können in der Regel nur die Ventilhersteller und/oder die Anwender aufgrund ihrer Praxiserfahrungen sicherheitstechnisch bewährte Ventile für definierte Anwendungen benennen. Ein sicherheitstechnisch bewährtes Ventil ist insbesondere ein Ventil mit einer ausreichend hohen sicherheitsbezogenen Zuverlässigkeit bei Praxisbedingungen. Diese Zuverlässigkeit bezieht sich nur auf die Schaltfunktion in die sicherheitsrelevante Stellung. Ein solches Ventil muß die bauteilspezifischen grundlegenden und bewährten Sicherheitsprinzipien in den Tabellen 4 und 6 erfüllen. Die Filtration für ein sicherheitstechnisch bewährtes Ventil muß gezielt vorgenommen werden. Bei niedrigem Risiko in Verbindung mit einfachen Anlagen kann für die notwendige Filtration das in der Anlage stets vorhandene Systemfilter ausreichend sein. Bei einem höheren Risiko sowie bei komplexen Anlagen sollte die Filtration unmittelbar vor dem relevanten Ventil bzw. den relevanten Ventilen durch ein Vollstrom-Druckfilter realisiert werden (in den Beispielen

[3] Wenn ein Bauteilausfall auftritt, kann er zum Verlust der Sicherheitsfunktion führen.

von Kapitel 4 mit DF bezeichnet). Der Verschmutzungsgrad des Filters ist zu überwachen. In pneumatischen Anlagen kann darüber hinaus bei größeren Leitungssystemen, mehreren Verbrauchern und bei Ventilen, die eine höhere Filterfeinheit als andere Bauteile in der Anlage erfordern, ein Vollstrom-Druckfilter unmittelbar vor den relevanten Ventilen notwendig sein.

Um das Ventil von der Zylinderseite kommend weitgehend vor Verschmutzung im Druckmedium zu schützen, sind gezielte Maßnahmen an den Kolbenstangen der Hydraulik-/Pneumatikzylinder (wie z.B. wirksame Abstreifer) notwendig. In pneumatischen Steuerungen ist desweiteren zu beachten, daß durch Abluft-Öffnungen Verschmutzung in das System eingezogen werden kann. Deshalb sind Abluft-(Entlüftungs-)Öffnungen (z.B. an Ventilen) mit wirksamen Filtern, sogenannten Filter-Schalldämpfer-Kombinationen, zu versehen.

Für die Elektronik und die Rechnertechnik sind derzeit ebenfalls keine sicherheitstechnisch bewährten Bauteile bekannt. Die im folgenden ausführlich beschriebene Maßnahme der Betriebsbewährtheit dient nach [17] dem Nachweis, daß die verwendeten Komponenten, wie z.B. auch Software, ausreichend frei von systematischen Entwurfsfehlern sind. Die Betriebsbewährtheit klassifiziert damit aber noch nicht einen Hardwarebaustein zum bewährten Bauteil, da unabhängig von systematischen Fehlern für ein Bauteil auch die zufällige Fehlerrate sehr gering sein muß [16][4]. Die Betriebsbewährtheit sagt aus, daß beim Einsatz einer Betrachtungseinheit, die im wesentlichen unverändert über einen ausreichenden Zeitraum in zahlreichen verschiedenen Anwendungen betrieben wurde, keine oder nur unwesentliche Fehler festgestellt wurden [17]. Nach [17] liegt eine Betriebsbewährtheit dann vor, wenn bei unveränderter Spezifikation:

- 10 Systeme in unterschiedlichen Anwendungen und
- $10^4$ Betriebsstunden mit
- mindestens jedoch einem Jahr Betriebsdauer vorlagen und
- keine bzw. keine sicherheitsrelevanten Fehler gefunden wurden.

[4] Der IEC-Entwurf 1508 klassifiziert die Zielvorgaben für ein sicherheitsrelevantes System in der Kategorie 1 mit einer Wahrscheinlichkeit für einen Ausfall von $10^{-1}$ bis $10^{-2}$ pro Anforderung für Systeme mit niedriger Anforderungsrate und einer Wahrscheinlichkeit für einen gefährlichen Ausfall pro Jahr von $10^{-1}$ bis $10^{-2}$ für sicherheitsrelevante Systeme mit kontinuierlicher oder hoher Anforderungsrate. Für die Kategorien 3 und 4 sinkt dieser Grenzwert für die Wahrscheinlichkeit jeweils um eine Zehnerpotenz.

☐ Die statistische Aussagesicherheit muß 95 % betragen.

Der Nachweis erfolgt durch Dokumentation des Herstellers bzw. Betreibers. Die Dokumentation muß mindestens enthalten: eine genaue Bezeichnung des Systems und dessen Komponenten einschließlich der Versionsstände für Hard- und Software, den Anwender und Anwendungszeitraum, die Betriebsstunden, ein Verfahren zur Auswahl der zum Nachweis herangezogenen Systeme und Anwendungsfälle und ein Verfahren zur Fehlerermittlung und Erfassung sowie Fehlerbeseitigung [17]. Insbesondere für Software oder komplexe elektronische Systeme kann auf diese Weise eine Betriebsbewährtheit bezüglich systematischer Fehler nachgewiesen werden. Für höhere Kategorien ist eine entsprechend höhere Betriebsstundenzahl erforderlich [16].

Bei einigen bewährten Bauteilen können bestimmte für die Beurteilung herangezogene Fehler auch ausgeschlossen werden, weil bekanntermaßen die Fehlerrate für diese Ausfallart sehr gering ist (z.B. bei zwangläufigem Öffnen der Schalter das Nichtöffnen in der Kategorie 3). Derartige Fehlerausschlüsse sind in den Fehlerlisten im Anhang B dieses Reports technologieabhängig beschrieben.

Die Entscheidung, ein bestimmtes Bauteil als sicherheitstechnisch bewährt zu akzeptieren, hängt von dem Anwendungsfall ab.

Bewährte Sicherheitsprinzipien sind z.B.

☐ Vermeidung von bestimmten Fehlern (z.B. Vermeidung des Kurzschlusses durch Abstand)

☐ Verringerung der Wahrscheinlichkeit von Fehlern (z.B. durch Überdimensionierung) oder Beanspruchung der Bauteile unterhalb der Bemessungsgrenze

☐ Festlegen der Ausfallrichtung eines Fehlers

☐ frühzeitige Fehlererkennung (z.B. Erdschlußerkennung)

☐ Einschränken der Folgen eines Fehlers

Tabelle 6 zeigt heute bekannte bewährte Sicherheitsprinzipien allgemeiner und technologieabhängiger Art. Die Prinzipien sind zum Teil sehr allgemein gefaßt und werden z.T. in Abhängigkeit von der Kategorie eingesetzt. Das Prinzip der selbsttätigen Überwachung findet sich als bewährtes Prinzip z.B. in den Kategorien 3 und 4, während der weg- oder zeitbegrenzte Tippbetrieb ein anwendungsabhängiges Prinzip darstellt. Das Prinzip „Steuerung mit Selbsthaltung" dagegen ist sehr

| Sicherheitstechnisch bewährte Bauteile | Ziel/Funktion |
|---|---|
| **Elektrotechnik** | |
| Sicherung/Automat | Abschaltung bei Kurzschluß/Erdschluß |
| mechanischer Positionsschalter mit Personenschutzfunktion mit zwangläufig betätigtem Öffner EN 60 947-5-1, Kap. 3) | Unterbrechung der Steuerspannung bei Betätigung |
| formschlüssige Zuhaltung (siehe EN 1088) | Verhinderung des gefährlichen Zugriffs |
| zwangläufig betätigter Nockenschalter | Betätigen von Schaltkontakten |
| Steuerschütze nach EN 60947-4-1<br>Leistungsschütze[5] | Abfall bei Entregung |
| NOT-AUS-Taster/Seilzugschalter mit zwangläufig betätigtem Öffner EN 60 947-5-1, Kap. 3) | Unterbrechung der Steuerspannung bei Betätigung |
| Aderleitung bei Verlegung im Schaltschrank<br>Mantelleitung bei geschützter Verlegung im Maschinenrahmen | Vermeidung von Leitungsschluß |
| Tipptaster<br>mechanisch betätigter Zustimmungsschalter (siehe EN 292) | Unterbrechung der Steuerspannung beim Loslassen |
| Klemmen im Schaltschrank/Klemmkasten in der Maschine (bei ausreichender Schutzart) | Vermeidung von Querschlüssen |
| **Fluidtechnik[6]** | |
| Wegeventile mit diskreten Schaltstellungen (Schieber- und Sitzventile)<br>Stetig-Wegeventile | Einnahme der sicherheitsbezogenen Schaltstellung durch wirksame, dauerfeste Federn bei Unterbrechung der Steuerenergie |
| Sperrventile (Rückschlagventile, gesteuerte Rückschlagventile) | Verhinderung des Durchflusses in der gesperrten Richtung |
| Stromventile (Drosseln und Blenden) als fester fluidtechnischer Widerstand | Beibehaltung des eingestellten Volumenstroms |
| Druckventile im sicherheitsbezogenen Teil der Steuerung<br>Druckschalter, Drucksensoren | vorgesehene Funktion bei Über- oder Unterschreiten von Drücken |
| mechanisch formschlüssig betätigte Ventile (zwangläufig betätigt)<br>Handhebelventile mit Federrückstellung bzw. Federzentrierung | Unterbrechung des Volumenstroms bzw. des Steuersignals |
| Leitungen im sicherheitsbezogenen Teil der Steuerung und zum Verbraucher | Dichtigkeit, Bruchfestigkeit |

[5] Während bei Steuer- und Leistungsschützen kein Zweifel besteht, daß diese bei fehlender Steuerspannung nicht anziehen (Fehlerausschluß), ist die Frage, ob diese Schütze bezüglich ihres Abfalls bei Entregung als „bewährtes Bauteil" zu betrachten sind, teilweise umstritten. Nach Auffassung der Autoren kann bei diesen Schaltgeräten zwar kein Fehlerausschluß gemacht werden, eine Einstufung als „bewährtes Bauteil" ist jedoch möglich bzw. gerechtfertigt. Andernfalls müßte z.B. entgegen langjähriger Praxis eine Stellungsüberwachung einer beweglichen Schutzeinrichtung mit nur einem Leistungsschütz für die Abschaltung der gefahrbringenden Bewegung in Kategorie B eingestuft werden.

[6] Hier sind Bauteile aufgeführt, die sicherheitstechnisch bewährte Bauteile sein können, da z.Z. in der Fluidtechnik nur im konkreten Einzelfall sicherheitstechnisch bewährte Bauteile genannt werden können.

Tabelle 5:
Sicherheitstechnisch bewährte Bauteile für die Gestaltung sicherheitsbezogener Teile von Steuerungen

Tabelle 6:
Bewährte Sicherheitsprinzipien für die Gestaltung sicherheitsbezogener Teile von Steuerungen
Teil 1

| Prinzip | Beschreibung | Ziel |
|---|---|---|
| Allgemein | | |
| Steuerung mit Selbsthaltung | Diese Art der Steuerung geht bei einem kurzzeitigen Befehl z.B. durch Tipptaster in Selbsthaltung und behält diese solange bei, wie Steuerenergie (Spannung, Druck) vorhanden ist. | Schutz<br>☐ gegen unerwarteten Wiederanlauf<br>☐ nach Energieausfall und -wiederkehr |
| Abstand/Isolation | Es werden ausreichende Kriech- und Luftstrecken verwendet sowie geeignete Isolierstoffe und -stärken eingesetzt. | Vermeiden von Kurzschlüssen |
| Erden von Steuerkreisen | Es erfolgt eine einseitige Verbindung von Steuerstromkreisen mit dem Schutzleitersystem (siehe EN 60 204-1, Abs. 9.1.4) | Fehlererkennung bei Erdschluß |
| Drehmoment-/Kraftbegrenzung (reduzierter Druck) | Kräfte, die zu einer Gefahr führen können, werden durch z.B. elektrische, mechanische oder fluidtechnische Einrichtungen reduziert. | Risikominderung durch verbesserte Gefahrenabwehr |
| Wegbegrenzter Tippbetrieb | Bei einer Bewegung wird der Weg auf einen zulässigen Wert im Tippbetrieb begrenzt. | |
| Zeitbegrenzter Tippbetrieb | Bei einer Bewegung wird die Zeit der Bewegung auf einen zulässigen Wert im Tippbetrieb begrenzt. | |
| Reduzierte Drehzahl/Geschwindigkeit (reduzierter Volumenstrom) | Bei einer Bewegung wird die Drehzahl bzw. die Geschwindigkeit auf einen zulässigen Wert im Tippbetrieb begrenzt. | |
| Überdimensionierung (Unterbeanspruchung) | Alle Betriebsmittel werden unter Nennwert beansprucht. | Reduzierung der Ausfallwahrscheinlichkeit |
| Anlauftestung | Die Schutzfunktion wird vor dem Ingangsetzen einer gefahrbringenden Bewegung zwangsläufig überprüft. | Fehlererkennung vor Ingangsetzen |
| Selbsttätige/automatische Überwachung | Fehler von Bauteilen werden durch die Überwachung frühzeitig erkannt. | Frühzeitige Fehleraufdeckung |
| Hardwarediversität | Technische Einrichtungen sind in Art und Ausführung unterschiedlich aufgebaut. | Vermeidung von Fehlern gleicher Ursache |
| Verwendung von Standardschaltungen | Standardschaltungen sind Schaltungen für spezielle Einsatzfälle, deren Verhalten im Fehlerfall geprüft wurde und die sich in der Praxis bewährt haben. | Sicherheitsfunktion durch bewährte bzw. geprüfte Einrichtungen |
| Verwendung von geprüften Bausteinen (z. B. Kontrollgeräten) | Geprüfte Bausteine sind fabrikfertige Geräte, die besondere nachgewiesene Anforderungen erfüllen. | |
| Öffner-Schließer-Kombination | Es handelt sich um die Anordnung von zwei mechanischen Positionsschaltern an einer Schutzeinrichtung mit prinzipverschiedener Betätigung. In jeder Stellung der Schutzeinrichtung ist stets ein Schalter betätigt und der andere nicht betätigt. | ☐ Aufrechterhaltung der Sicherheitsfunktion von mechanischen Positionsschaltern bei Einzelfehler in der Mechanik<br>☐ Entfernen der Schutzeinrichtung wird erkannt |

Tabelle 6:
Bewährte Sicherheitsprinzipien für die Gestaltung sicherheitsbezogener Teile von Steuerungen
Teil 2

| Prinzip | Beschreibung | Ziel |
|---|---|---|
| **Elektromechanik** | | |
| Zwangsführung von Kontakten | Zwangsführung ist eine mechanische Verbindung von Kontakten in Schützen und Relais, die auch im Fehlerfall verhindert, daß Öffner und Schließer gleichzeitig geschlossen sein können. | Überwachung von Steuerschützen |
| Gegenseitige Verriegelung | Mehrere Relais/Schütze sind so miteinander verschaltet, daß auf Grund der Zwangsführung bei einem Fehler in einem Bauteil andere Bauteile nicht mehr betätigt werden können. | Verhinderung von nicht gewollten Zuständen |
| Zwangläufige/formschlüssige Betätigung | Es handelt sich um eine zuverlässige Betätigung durch starre, mechanische Teile ohne kraftschlüssige und federnde Verbindungen. | Sichere Betätigung, z.B. bei mechanischen Positionsschaltern |
| **Elektronik/Rechnertechnik** | | |
| Dynamische Techniken | Alle sicherheitsrelevanten Signale ändern regelmäßig ihren Zustand, so daß statische Fehler automatisch eine sicherheitsgerichtete Funktion einleiten. | Frühzeitige Aufdeckung und Beherrschung statischer Bauteilfehler |
| Trennung der elektrischen Energieleitungen von den Informationsleitungen | Eine räumliche Trennung führt insbesondere bei empfindlichen Analogsignalen zu einer Erhöhung der Störfestigkeit. | Kein kapazitives oder induktives Übersprechen von elektrischen Energieleitungen auf Signalleitungen |
| Antivalente Signalführung | Bei der Verarbeitung redundanter Signale nutzt der eine Kanal eine logische 1, wenn der andere eine logische 0 benutzt und umgekehrt. | Erhöhung der Störfestigkeit gegenüber Common-mode-Fehlern |
| Fehlererkennung über den technischen Prozeß | Fehler werden über bestimmte Erwartungshaltungen, die durch den technischen Prozeß vorgegeben sind, aufgedeckt. Eine Lokalisierung des Fehlers ist dabei meist nicht möglich. | Frühzeitige Fehlererkennung |
| Plausibilitätskontrollen | Plausibilitätskontrollen dienen dazu, bei nicht zugelassenen, unüblichen bzw. außerhalb der spezifizierten Werte liegenden Eingaben und Zuständen eine definierte Reaktion zu erzielen. | Definierte Reaktion<br>☐ bei fehlerhaften Benutzervorgaben und<br>☐ bei Bauteilausfällen |
| Einsatz eines externen Watchdogs | Bei einem Watchdog handelt es sich um eine zeitliche Programmlaufüberwachung, bei der ein externes Bauelement in regelmäßigen Zeitabständen vom Mikrorechner Signale erwartet. Bleiben diese Signale aus, so hat der Watchdog über einen zweiten unabhängigen Abschaltpfad die Möglichkeit, eine sicherheitsgerichtete Reaktion einzuleiten. | Definierte Reaktion bei fehlerhaftem Programmablauf |

Tabelle 6:
Bewährte Sicherheitsprinzipien für die Gestaltung sicherheitsbezogener Teile von Steuerungen
Teil 3

| Prinzip | Beschreibung | Ziel |
|---|---|---|
| **Fluidtechnik** | | |
| Positive Überdeckung | Es ist eine ausreichend große positive Überdeckung an zu sperrenden Anschlüssen bei Schieberventilen vorhanden. | ☐ Anhalten von gefahrbringenden Bewegungen<br>☐ Verhinderung eines ungewollten Anlaufs |
| Formschlüssige Krafteinwirkung | Die Betätigungskräfte wirken direkt (zwangläufig) auf die bewegten Teile, d.h. ohne kraftschlüssige Verbindungen. | Zuverlässige Betätigung der bewegten Teile |
| Gezielte Auswahl von Werkstoffen und Werkstoffpaarungen | Diese Auswahl erfolgt unter Berücksichtigung der Eigenschaften der Druckflüssigkeit aufgrund von entsprechenden Erfahrungen und/oder gezielten Untersuchungen. | Reduzierung der Ausfallwahrscheinlichkeiten |
| Eingrenzung von Betriebsdaten | Im wesentlichen werden Betriebstemperaturbereich und Betriebsviskositätsbereich der Druckflüssigkeit eingegrenzt. | |
| Überwachung der Druckflüssigkeit | Es erfolgt eine regelmäßige Überwachung des Zustandes der Druckflüssigkeit, z.B. durch Probenentnahme. | |

allgemein für alle Kategorien einsetzbar. Aus diesen Überlegungen wird deutlich, daß die bewährten Prinzipien anders als die grundlegenden Sicherheitsprinzipien nicht immer alle angewendet werden können, sondern technologie-, anwendungs- oder kategoriespezifisch sind.

Generell läßt sich sagen, daß die Wahrscheinlichkeit eines gefährlichen Ausfalls in der Kategorie 1 geringer ist als in der Kategorie B. Folglich ist der Verlust der Sicherheitsfunktion weniger wahrscheinlich[7].

Zu den bewährten Sicherheitsprinzipien gibt es bisher in der Fluidtechnik keine Festlegungen. Diese Sicherheitsprinzipien

[7] Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.

betreffen sowohl die Bauteile wie auch das Druckmedium. In der Tabelle 6, Teil 3, sind die nach unserer Auffassung wichtigsten bewährten Sicherheitsprinzipien für die Fluidtechnik aufgeführt, die, abhängig vom Anwendungsfall, nicht immer alle gleichzeitig realisiert werden können.

### 3.2.3 Kategorie 2

Die Anforderungen von Kategorie B müssen erfüllt sein. Außerdem sind bewährte Sicherheitsprinzipien einzusetzen. Zusätzlich müssen die sicherheitsbezogenen Teile der Steuerung in der Kategorie 2 in geeigneten Zeitabständen durch die Maschinensteuerung willensunabhängig geprüft werden (siehe Tabelle 3). Die Prüfung der Sicherheitsfunktionen muß

- beim Anlauf der Maschine und/oder vor Einleiten eines gefährlichen Zustandes,
- periodisch während des Betriebes, wenn die Risikoanalyse und die Betriebsart zeigen, daß dies notwendig ist,

erfolgen. Diese Prüfung kann automatisch oder manuell eingeleitet werden. Ein positives Prüfergebnis ist allerdings Voraussetzung für den Start oder den Weiterlauf der Maschine. Jede Prüfung der Sicherheitsfunktion muß entweder den Betrieb zulassen, wenn keine Fehler erkannt wurden, oder bei Fehlererkennung einen Ausgang für die Einleitung angemessener Steuerungsmaßnahmen erzeugen[8]. Die Prüfung selbst darf nicht zu einem gefährlichen Zustand führen. Nach Erkennung eines Fehlers muß ein sicherer Zustand bis zur Behebung des Fehlers aufrechterhalten werden. Die Prüfeinrichtung darf getrennt oder als Bestandteil des sicherheitsbezogenen Teiles der Steuerung vorgesehen sein, das die Sicherheitsfunktion ausführt.

In einigen Fällen ist Kategorie 2 nicht anwendbar, da sich die Prüfung der Sicherheitsfunktionen nicht bei allen Bauteilen, z.B. Druckschalter oder Temperatursensoren, durchführen läßt. Die Kategorie 2 kann im allgemeinen mit elektroni-

[8] In der neuesten Ausgabe der Norm wird diese Anforderung abgeschwächt, wenn es heißt: Wenn die Einleitung eines sicheren Zustandes nicht möglich ist, z.B. Verschweißen des Kontaktes beim Endschalter, muß der Ausgang eine Warnung vor der Gefährdung vorsehen. Im BIA wurde die Kategorie 2 bis heute schärfer ausgelegt und ein zweiter unabhängiger Abschaltweg gefordert. Nur durch den zweiten unabhängigen Abschaltweg ist die zusätzliche Forderung, den sicheren Zustand bis zur Behebung des Fehlers aufrechtzuerhalten, erfüllbar. Diese Widersprüchlichkeit muß u.E. vom Normensetzer selbst beseitigt werden, bevor der zweite unabhängige Abschaltweg durch eine Warnung ersetzt werden kann.

schen Techniken realisiert werden, z.B. in Schutzeinrichtungen oder bestimmten Steuerungen.[9] Dabei muß allerdings gewährleistet sein, daß Prüfeinrichtung und STS nicht durch einen einzigen in Anhang B aufgeführten Fehler gemeinsam ausfallen können (z.B. indem sie **nicht** in einer einzigen speicherprogrammierbaren Steuerung implementiert sind).

### 3.2.4 Kategorie 3

Die Anforderungen von Kategorie B müssen erfüllt sein. Außerdem sind bewährte Sicherheitsprinzipien einzusetzen. Zusätzlich müssen die sicherheitsbezogenen Teile der Kategorie 3 so gestaltet werden, daß ein einzelner Fehler nach Fehlerliste in Anhang B in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt (siehe Tabelle 3). Fehler gemeinsamer Ursache müssen berücksichtigt werden, wenn die Wahrscheinlichkeit für das Auftreten eines Fehlers groß ist. Wann immer in angemessener Weise durchführbar, muß der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

Die Anforderung für die Erkennung einzelner Fehler bedeutet nicht, daß alle Fehler erkannt werden. Daher kann die Anhäufung unentdeckter Fehler für bestimmte Maschinen u.U. zu einem unbeabsichtigten Ausgangssignal und zu einem gefährlichen Zustand an der Maschine führen. Typische Beispiele für durchführbare Maßnahmen zur Fehlererkennung sind die Abfrage der zwangsgeführten Relaiskontakte oder die Überwachung von redundanten elektrischen Ausgängen. Falls aufgrund der Technologie und Anwendung notwendig, sollte der Typ-C-Normensetzer weitere Einzelheiten im Hinblick auf die Fehlererkennung angeben. „Wann immer in angemessener Weise durchführbar" bedeutet, daß die erforderlichen Maßnahmen zur Fehlererkennung und der Umfang, in dem diese umgesetzt werden, hauptsächlich von den Folgen eines Ausfalls und von der Wahrscheinlichkeit des Auftreten eines Unfalls innerhalb der Anwendung abhängt. Die verwendete Technologie beeinflußt die Möglichkeiten der Einbeziehung der Fehlererkennung.[10]

---

[9] Dieses Systemverhalten läßt zu, daß
☐ das Auftreten eines Fehlers zum Verlust der Sicherheitsfunktion zwischen den Prüfungen führt,
☐ der Verlust der Sicherheitsfunktion in der Regel rechtzeitig bei der Prüfung erkannt wird.

[10] Dieses Systemverhalten läßt zu, daß
☐ beim Auftreten eines einzelnen Fehlers die Sicherheitsfunktion immer erhalten bleibt,
☐ einige, aber nicht alle Fehler erkannt werden,
☐ *die Anhäufung unerkannter Fehler zum Verlust* der Sicherheitsfunktion führen kann.

### 3.2.5 Kategorie 4

Die Anforderungen von Kategorie B müssen erfüllt sein. Außerdem sind bewährte Sicherheitsprinzipien einzusetzen. Zusätzlich müssen sicherheitsbezogene Teile von Steuerungen der Kategorie 4 so gestaltet werden, daß (siehe auch Tabelle 3)

☐ ein einzelner Fehler (siehe Anhang B dieses Reports) in jedem dieser sicherheitsbezogenen Teile nicht zum Verlust von Sicherheitsfunktionen führt und

☐ der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird, z.B. unmittelbar beim Einschalten oder am Ende eines Maschinenzyklus. Falls diese Erkennung nicht möglich ist, darf die Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen.[11]

Ist die Erkennung bestimmter Fehler aufgrund der Technologie oder Schaltungstechnik nicht wenigstens bei der nächsten Prüfung möglich, muß das Auftreten weiterer Fehler angenommen werden. In diesem Fall darf die Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen. Die Fehlerbetrachtung darf abgebrochen werden, wenn die Wahrscheinlichkeit des Auftretens weiterer Fehler als ausreichend gering angesehen werden kann.[12]

Die Fehlerbetrachtung darf auf zwei kombinierte Fehler beschränkt werden, wenn

☐ die Fehlerraten der Bauteile niedrig sind und

☐ die kombinierten Fehler überwiegend unabhängig voneinander auftreten und

☐ die Sicherheitsfunktion nur dann ausfällt, wenn die Fehler in einer bestimmten Reihenfolge auftreten.

Beim Auftreten weiterer Fehler als Ergebnis eines ersten einzelnen Fehlers müssen der erste Fehler und alle sich daraus ergebenden Fehler als ein einzelner Fehler betrachtet werden. Fehler gemeinsamer Ursache müssen berücksichtigt werden, z.B. durch Anwendung von Diversität oder spezieller Verfahren, um solche Fehler zu erkennen.

---

[11] Dieses Systemverhalten läßt zu, daß
☐ bei Auftreten der Fehler die Sicherheitsfunktion immer erhalten bleibt,
☐ die Fehler rechtzeitig erkannt werden, um den Verlust der Sicherheitsfunktion zu verhindern.

[12] Nach den im BIA gewonnenen Erkenntnissen kann die Fehlerhäufung nach dem dritten Fehler technologieunabhängig abgebrochen werden.

Im Falle komplexer Schaltungsstrukturen (z.B. Mikroprozessoren, vollständige Redundanzen) wird die Fehlerbetrachtung im allgemeinen auf der Strukturebene durchgeführt, d.h. auf Baugruppen basierend.

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

Geordnet nach den fünf Kategorien, sind in diesem Kapitel Beispiele für die technische Realisierung zusammmengestellt. Die grundlegenden Sicherheitsprinzipien werden bei der Beschreibung der Beispiele vorausgesetzt und nicht mehr eigens aufgeführt (siehe Kapitel 3).

Jedes Schaltungsbeispiel wird durch die vier Abschnitte erläutert:

- ☐ Funktionsbeschreibung,
- ☐ konstruktive Merkmale,
- ☐ Anwendung und
- ☐ weiterführende Literatur.

Im Abschnitt „**Funktionsbeschreibung**" werden aufbauend auf einer Schaltungsskizze die wesentlichen sicherheitstechnischen Funktionen kurz beschrieben. Das Verhalten im Fehlerfall wird erläutert. Maßnahmen zur Fehlererkennung werden erwähnt.

Unter dem Stichwort „**Konstruktive Merkmale**" sind die Besonderheiten beim Aufbau des jeweiligen Beispieles aufgelistet. Insbesondere werden die bewährten Sicherheitsprinzipien und die Verwendung bewährter Bauteile dort aufgeführt.

Im Abschnitt „**Anwendung**" wird auf die mögliche Risikoreduzierung eingegangen, die durch den Einsatz der Kategorie erreicht werden kann. Eine Entscheidung über die Anwendung muß letztlich anwendungsabhängig erfolgen. Die Bemerkungen sind deshalb in den Beispielen nur als Empfehlung anzusehen.

Die Beschränkung der Beispiele auf maximal drei Seiten macht den Hinweis auf „**Weiterführende Literatur**" notwendig. In der Regel enthält dieser Abschnitt eine Veröffentlichung im Zusammenhang mit dem erwähnten Beispiel. Dort kann auch die Funktion im Detail nachgelesen werden.

Die Beispiele stellen **keine verbindliche Interpretation** der Kategorien dar. Vielmehr sind diese Beispiele von den Autoren aufgrund der langjährigen Erfahrungen mit sicherheitsbezogenen Maschinensteuerungen und der Mitwirkung in den nationalen und europäischen Normungsgremien zusammengestellt worden, um dem Konstrukteur eine wirksame Hilfestellung für eigene Entwicklungen zu geben.

Für jede Technologie werden in den folgenden technologiebezogenen Abschnitten einige grundlegende Bemerkungen zum Verständnis der Beispiele und zur Umsetzung der Kategorien gegeben.

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## 4.1 Grundlegende technologiebezogene Bemerkungen zu den Steuerungsbeispielen

### 4.1.1 Elektromechanische Steuerungen

In den elektromechanischen Steuerungen werden in erster Linie Bauteile in Form von Schaltern bzw. Befehlsgeräten (z.B. Positionsschalter, Wahlschalter, Taster) und Schaltgeräten (Steuerschütze, Relais, Leistungsschütze) eingesetzt. Diese Geräte besitzen eindeutige Schaltstellungen. Ohne Betätigung von außen oder elektrische Ansteuerung ändern sie in der Regel ihren Schaltzustand nicht. Bei bestimmungsgemäßer Verwendung und entsprechender Auswahl sind sie weitgehend unempfindlich gegenüber Umgebungseinflüssen wie Feuchtigkeit, Temperatur sowie elektrischen und elektromagnetischen Störeinflüssen. Das unterscheidet sie zum Teil erheblich von elektronischen Betriebsmitteln (siehe auch Absatz 4.1.3). Durch geeignete Auswahl, Dimensionierung und Anordnung kann auf die Haltbarkeit und das Ausfallverhalten Einfluß genommen werden. Das gilt auch für die verwendeten Leitungen bei entsprechender Verlegung innerhalb und außerhalb der elektrischen Einbauräume.

Aus vorstehenden Gründen entsprechen in den meisten Fällen die elektromechanischen Bauteile den „grundlegenden Sicherheitsprinzipien" und sind auch in vielen Fällen als „sicherheitstechnisch bewährte Bauteile" zu betrachten. Diese Aussage gilt jedoch nur, wenn die Anforderungen der EN 60 204-1 [18] für die elektrische Ausrüstung der Maschine/Anlage berücksichtigt wurden. In einigen Fällen sind auch Fehlerausschlüsse möglich, z.B. bei einem Steuerschütz in bezug auf das Anziehen bei fehlender Steuerspannung oder das Nicht-Öffnen eines zwangläufig betätigten Öffners bei einem Schalter nach EN 60 947-5-1, Kapitel 3 [19], siehe auch Anhang B.

Da die Kategorie B die Einhaltung zutreffender Normen erfordert und in der grundlegenden Norm [18] für elektromechanische sicherheitsrelevante Teile von Steuerungen wesentliche „sicherheitstechnisch bewährte Prinzipien" vorgeschrieben werden, unterscheidet sich die Kategorie B für diese Technologie nicht von der Kategorie 1. Bei den Schaltungsbeispielen werden deshalb in diesem Report keine elektromechanischen Steuerungen in der Kategorie B vorgestellt.

### 4.1.2 Fluidtechnische Steuerungen

Bei fluidtechnischen Anlagen ist als „sicherheitsbezogener Teil der Steuerung" insbesondere der Ventilbereich zu be-

trachten, und zwar die Ventile, die gefahrbringende Bewegungen oder Zustände steuern. Bei hydraulischen Anlagen (siehe Abbildung 7) sind außerdem die Maßnahmen zur Druckbegrenzung im System (VDB) und zur Filtration der Druckflüssigkeit (RF) in diesem Zusammenhang zu sehen. Die in Abbildung 7 dargestellten Bauteile LF, N und T sind in den meisten hydraulischen Anlagen vorhanden und insbesondere für den Zustand der Druckflüssigkeit und damit für die Ventilfunktionen von großer Bedeutung. Das auf dem Flüssigkeitsbehälter angeordnete Belüftungsfilter LF verhindert das Eindringen von äußerer Verschmut-

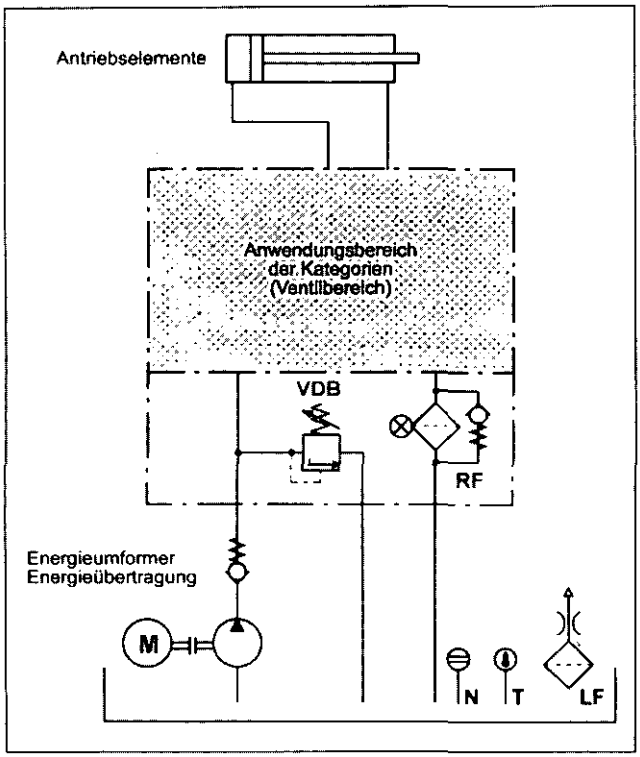



Abbildung 7:
Anwendungsbereich der Kategorien bei hydraulischen Anlagen

zung. Die Niveauanzeige N bewirkt die Einhaltung des Flüssigkeitsspiegels in vorgegebenen Grenzen. Die Temperaturanzeige T symbolisiert geeignete Maßnahmen zur Begrenzung des Betriebstemperatur-Bereiches und damit des Betriebsviskositäts-Bereiches der Druckflüssigkeit. Bei Bedarf müssen Einrichtungen zur Kühlung und/oder Heizung in Verbindung mit einer Temperaturregelung eingesetzt werden (siehe hierzu auch Tabelle 6, Teil 3).

Die Antriebselemente sowie die Bauteile der Energieumformung und der Energieübertragung sind bei fluidtechnischen Anlagen in der Regel außerhalb des Anwendungsbereiches der Kategorien.

Bei pneumatischen Anlagen (siehe Abbildung 8) sind die Bauteile gegen Gefährdungen bei Energieänderungen und die sogenannte Wartungseinheit zur Aufbereitung der Druckluft in sicherheitstechnischem Zusammenhang mit dem Ventilbereich zu sehen. Um mögliche Energieänderungen sicherheitstechnisch zu beherrschen, wird häufig ein Entlüftungsventil zusammen mit einem Druckschalter eingesetzt. In den Schaltungsbeispielen des Abschnittes 4.2 sind diese Bauteile mit EV (Entlüftungsventil) und mit DS (Druckschalter) bezeichnet. Die Wartungseinheit (siehe Abbildung 8) besteht in der Regel aus einem Handabsperrventil HV, einem Filter mit Wasserabscheider FW, wobei der Verschmutzungsgrad des Filters überwacht wird, und einem Druckregelventil VDR (mit ausreichend dimensionierter Sekundärentlüftung).

Die in Abschnitt 4.2 beispielhaft dargestellten fluidtechnischen Schaltungen enthalten außer dem sicherheitsbezogenen Steuerungsteil nur noch die zusätzlichen Bauteile, die zum Verständnis der fluidtechnischen Anlage notwendig sind oder einen direkten steuerungstechnischen Bezug haben. Die Gesamtheit der Anforderungen, die von fluidtechnischen Anlagen erfüllt werden müssen, sind aus [20] und [21] zu entnehmen. Als weitere zutreffende Normen sind [22] bis [25] zu nennen.

Die meisten Steuerungsbeispiele stellen elektro-hydraulische bzw. elektro-pneumatische Steuerungen dar. Verschiedene Sicherheitsanforderungen werden bei diesen Steuerungen durch den elektrischen Steuerungsteil ausgeführt, so z.B. die Anforderungen zur Beherrschung von Energieänderungen in elektro-hydraulischen Steuerungen.

Die geforderte Sicherheitsfunktion ist bei allen Steuerungsbeispielen das Anhalten einer gefahrbringenden Bewegung oder die Umkehrung der Bewegungsrichtung. Die Verhinderung eines unerwarteten Anlaufs ist implizit enthalten.

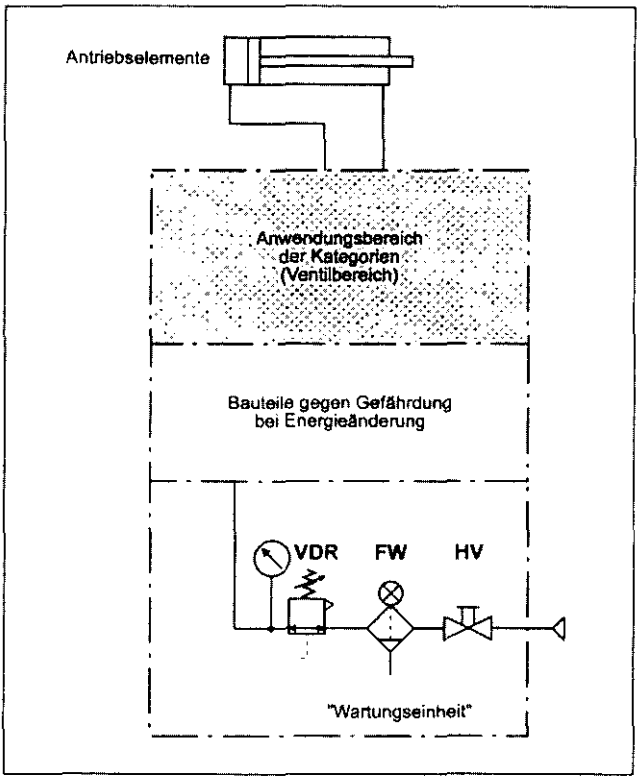



Abbildung 8:
Anwendungsbereich der Kategorien bei pneumatischen Anlagen

Fluidtechnische Steuerungen werden üblicherweise in den Kategorien 1, 3 oder 4 ausgeführt, die Anwendung der Kategorie 2 ist ebenfalls realisierbar. Da die Kategorie B bereits die Einhaltung der zutreffenden Normen und der grundlegenden Sicherheitsprinzipien erfordert, unterscheiden sich fluidtechnische Steuerungen der Kategorien B und 1 im wesentlichen nicht durch den Steuerungsaufbau, sondern nur durch die höhere, sicherheitsbezogene Zuverlässigkeit der relevanten Ventile. Aus diesem Grund werden in diesem Report keine fluidtechnischen Steuerungen in der Kategorie B vorgestellt.

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

Im folgenden sind mit dem Begriff „pneumatische/hydraulische Steuerungen" nur die sicherheitsbezogenen Teile von pneumatischen/hydraulischen Steuerungen erfaßt.

### 4.1.3 Elektronische Steuerungen

In der Regel sind elektronische Bauteile gegenüber äußeren Umgebungseinflüssen empfindlicher als elektromechanische Komponenten. Werden keine besonderen Maßnahmen ergriffen, können elektronische Bauelemente im negativen Temperaturbereich deutlich eingeschränkter eingesetzt werden als elektromechanische Bauelemente. Zusätzlich gibt es Umgebungseinflüsse, die beim Einsatz elektromechanischer Schaltglieder fast bedeutungslos waren, aber in Elektroniksystemen ein zentrales Problem darstellen. Gemeint sind alle elektromagnetischen Störeinflüsse, Fremdfelder und dergleichen, die über Leitungen oder über elektromagnetische Felder in Elektroniksysteme eingekoppelt werden. Gegen derartige Einflüsse sind erhebliche Maßnahmen notwendig, um eine für die Praxis ausreichende Störfestigkeit zu erzielen.

Bei elektronischen Bauelementen sind kaum Fehlerausschlüsse möglich. Dies hat zur Folge, daß grundsätzlich nicht die Konstruktion eines bestimmten Bauelementes die Sicherheit gewährleisten kann, sondern nur bestimmte Schaltungskonzepte sowie die Anwendung entsprechender Maßnahmen zur Fehlerbeherrschung. Aus diesem Grund gibt es keine elektronischen Systeme mit der Kategorie 1.

Ein weiterer Punkt, der sicherheitstechnisch von Bedeutung ist, hängt mit dem zuvor Genannten unmittelbar zusammen: Das Ausfallverhalten elektronischer Bauelemente ist in der Regel sicherheitskritischer als das elektromechanischer Komponenten. Dies soll an einem Beispiel erläutert werden: Wenn ein Schütz elektrisch nicht angesteuert wird, d.h., wenn seine Spule nicht vom Strom durchflossen wird, gibt es keinen Grund, warum sich die Kontakte des Schützes schließen sollten. Das bedeutet, daß ein ausgeschaltetes Relais oder Schütz sich durch einen internen Fehler nicht selbständig einschaltet. Anders ist das bei den meisten elektronischen Bauteilen, z.B. dem Transistor. Ist ein Transistor gesperrt, d.h. es fließt kein ausreichend hoher Basisstrom, so ist es trotzdem nicht ausgeschlossen, daß durch einen internen Fehler der Transistor plötzlich ohne äußere Einwirkung leitfähig wird und somit unter Umständen eine gefährliche Bewegung einleitet. Auch dieser sicherheitstechnische Nachteil elektronischer Bauelemente muß

durch ein entsprechendes Schaltungskonzept beherrscht werden.

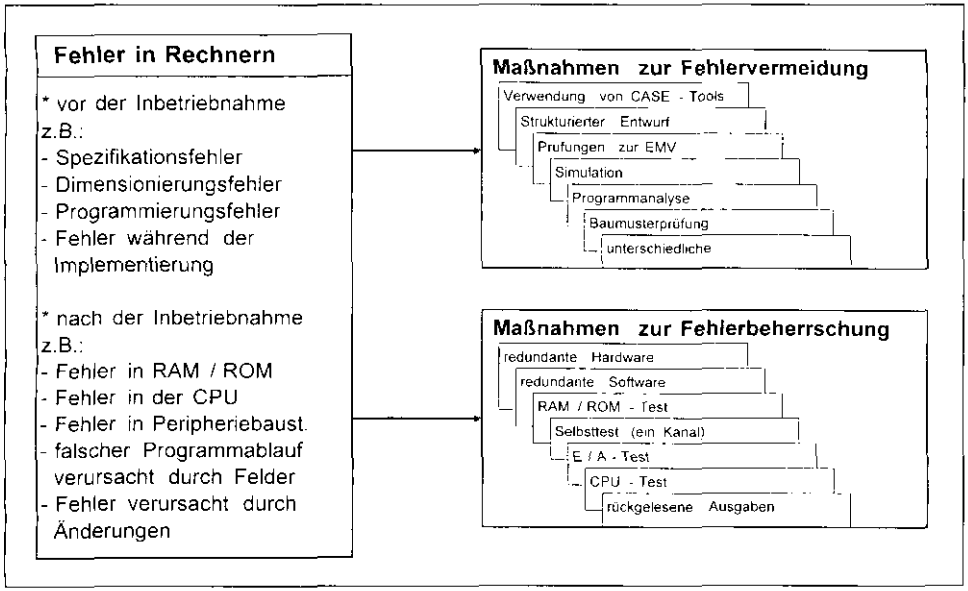
Insbesondere beim Einsatz hochintegrierter Bausteine ist es teilweise nicht mehr möglich, zu Beanspruchungsbeginn, d.h. zum Zeitpunkt der Übergabe der Anlage an den Kunden, nachzuweisen, daß die Anlage völlig fehlerfrei ist. Schon auf der Bauelementeebene ist dieser Nachweis selbst durch die Hersteller der integrierten Schaltkreise u.U. nicht mehr 100prozentig durchführbar. An diesem Punkt greifen die in neueren Normentwürfen [16] beschriebenen fehlervermeidenden Maßnahmen, die, wenn sie entsprechend der Steuerungskategorie durchgeführt werden, nach dem heutigen Stand der Regeln der Technik ausreichen, um die geforderte Sicherheit zu Beanspruchungsbeginn zu gewährleisten.

### 4.1.4 Rechnersteuerungen

Analysiert man das Fehlverhalten mikroprozessorgesteuerter Sicherheitseinrichtungen, so stellt man fest, daß oft nicht die zufälligen Bauteilausfälle die Ursachen für das Versagen gewesen sind, sondern besondere Zustände während des Betriebes, die der Programmierer nicht berücksichtigt hat. Eine weitere Fehlerquelle sind die nicht unmittelbar einsichtigen Auswirkungen von Programmänderungen bei der Systempflege.
Aus diesen Bemerkungen folgt, daß es insbesondere bei mikroprozessorgesteuerten Maschinen Fehler geben kann, die während der Entwicklung des Systems gemacht worden sind, aber erst während des Betriebes zu einer gefährlichen Situation führen können. Maßnahmen gegen solche Fehler müssen deshalb schon im Entwicklungsprozeß der Sicherheitseinrichtung wirksam sein. Genau an diesem Punkt setzt die Vornorm zur Rechnersicherheit [17] und der Normentwurf IEC 1508 [16] an, wenn sie fehlervermeidende und fehlerbeherrschende Maßnahmen unterscheiden (Abbildung 9, siehe Seite 56). Maßnahmen zur Fehlervermeidung werden durch Hersteller und Prüfstelle während der Konzeptphase, des Entwicklungs-, Installations- und Änderungsprozesses ergriffen, um bestimmte Fehler erst gar nicht zu machen bzw. im Prozeß aufzudecken und zu korrigieren. Maßnahmen zur Fehlerbeherrschung sind Hardware- und Softwarebausteine, die im wesentlichen im Betrieb auftretende Fehler erkennen und sicherheitsgerichtete Reaktionen des Rechnersystems veranlassen.

Die in [17] aufgeführten Einzelmaßnahmen zur Fehlerbeherrschung und Fehlervermeidung sind in ihrer Wirksamkeit bewertet. Eine Tabelle legt fest, bei welcher Anforderungsklasse nach [6] welche

Abbildung 9:
Fehlervermeidende und fehlerbeherrschende Maßnahmen




Wirksamkeit bezüglich der möglichen Fehler gefordert wird (siehe Tabelle 7).

Die in [17] für die einzelnen Anforderungsklassen geforderten Maßnahmenkataloge lassen die in Tabelle 8 (siehe Seite 58) dargestellte Zuordnung zwischen den Sicherheitsniveaus der Vornorm für Rechnersicherheit, den in [16] genormten sog. „Safety Integrity Levels" und den in [5] genormten Kategorien erkennen. Die in Tabelle 8 unter der Spalte „Kurzbeschreibung" aufgelisteten Beschreibungen finden sich in vielen älteren nationalen und internationalen Normen für Maschinen. Mit Hilfe von Tabelle 8 läßt sich für jede der Kategorien eine Anforderung an die Wirk-

samkeit der zu treffenden Maßnahmen gegenüber den beschriebenen Fehlertypen in mikroprozessorgesteuerten Systemen unter Anwendung von Tabelle 7

Tabelle 7:
Wirksamkeit von Maßnahmen gegenüber Fehlern in Abhängigkeit von der Anforderungsklasse nach [17]

| Versagen bedingt durch | | Sicherheitstechnische Maßnahmen entsprechend den Anforderungsklassen 1 2 3 4 5 6 7 8 |
|---|---|---|
| Zufallsfehler in der Hardware | Einfachfehler | Maßnahmen der Fehlerbeherrschung: einfach \| mittel \| hoch |
| | | Die Wirksamkeit muß durch Maßnahmen auf Systemebene und/oder unterhalb der Systemebene insgesamt erreicht werden. |
| | Mehrfachfehler durch Fehlerhäufung (statistisch) | Maßnahmen der Fehlerbeherrschung: einfach \| mittel \| hoch |
| | | *Die Wirksamkeit muß durch Maßnahmen auf* Systemebene und/oder unterhalb der Systemebene und/oder durch nichttechnische Maßnahmen insgesamt erreicht werden. |
| systematische Fehler mit Common-Mode-Fehler | in der Hardware | Maßnahmen der Fehlervermeidung: Basismaßnahmen \| einfach \| mittel \| hoch |
| | | Maßnahmen der Fehlerbeherrschung: einfach \| hoch |
| | in der Software | Maßnahmen der Fehlervermeidung: Basismaßnahmen \| einfach \| mittel \| hoch |
| | | Maßnahmen der Fehlerbeherrschung: einfach \| mittel \| hoch |
| Handhabungsfehler, Bedienfehler, Manipulation | | Maßnahmen der Fehlervermeidung: Basismaßnahmen \| einfach \| hoch |
| | | Maßnahmen der Fehlerbeherrschung: Basismaßnahmen \| einfach \| hoch |
| Fehler durch Betriebs- und Umgebungseinflüsse | | Maßnahmen der Fehlervermeidung: Basismaßnahmen \| einfach \| mittel \| hoch |
| | | Maßnahmen der Fehlerbeherrschung: Basismaßnahmen \| einfach \| hoch |
| einfach/mittel/hoch = Bezeichnung der Wirksamkeit der Maßnahmen | | |

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

zuordnen. Die Wirksamkeit der verschiedenen Einzelmaßnahmen für Rechnersysteme ist in den Anhängen von [16] bzw. [17] bezeichnet.

Zufällige Fehler in rechnergesteuerten sicherheitsbezogenen Steuerungen lassen sich im wesentlichen durch die Struktur der Gesamtschaltung beherrschen. So führt eine zweikanalige Struktur z.B. dazu, daß auch bei einem nicht erkannten Fehler in einem Kanal die Sicherheitseinrichtung noch sicher arbeiten kann. Diese sog. Maßnahmen auf Systemebene [17] bzw. Architekturen [16] helfen Fehler zu tolerieren. Will man dagegen Fehler in den einzelnen Rechnerkomponenten rechtzeitig aufdecken, so sind Maßnahmen unterhalb der Systemebene zu ergreifen. Solche Maßnahmen sind z.B. Tests für die einzelnen Befehle der Zentraleinheit oder Algorithmen, die eine Aussage über die Veränderung des Programms im Festwertspeicher erlauben. Sowohl die zu ergreifenden Maßnahmen auf Systemebene als auch die unterhalb der Systemebene werden durch die geforderte Kategorie bestimmt.

Die Maßnahmen zur Fehlerbeherrschung können nicht verhindern, daß z.B. Programmfehler, die in der Software beider Rechnersysteme gemacht worden sind und die sich deshalb auf beide Teilsysteme zur gleichen Zeit auswirken, zu einer Gefährdung führen können. Zusätzlich zu den fehlerbeherrschenden Maßnahmen ist deshalb eine Reihe von fehlervermeidenden Maßnahmen während des Entwicklungsprozesses zu ergreifen.

| Kategorie nach [5] | Anforderungsklasse nach [6] | Safety Integrity Level nach [16] | Kurzbeschreibung |
|---|---|---|---|
| B | 1 | – | Steuerungen gemäß dem Stand der Technik |
| 2 | 2/3 | 1 | Testung |
| 3 | 4 | 2 | Einfehlersicherheit mit partieller Fehlererkennung |
| 4 | 5/6 | 3 | Selbstüberwachung |
| – | 7/8 | 4 | im Maschinenschutz nicht von Bedeutung |

Tabelle 8:
Zusammenhang zwischen Kategorien, Anforderungsklassen und Safety Integrity Levels

Abbildung 10 und Abbildung 11 (siehe Seite 60) listen beispielhaft eine Reihe von Maßnahmen zur Fehlervermeidung für die Kategorien B bis 4 auf. Für die Kategorie 4 sind jeweils alle Maßnahmen zu ergreifen, während für die Anforderungen aus Kategorie 3 alle diejenigen außer den ab Kategorie 4 geforderten Maßnahmen von Bedeutung sind. Für die Kategorie 2 und 1 verbleiben nur

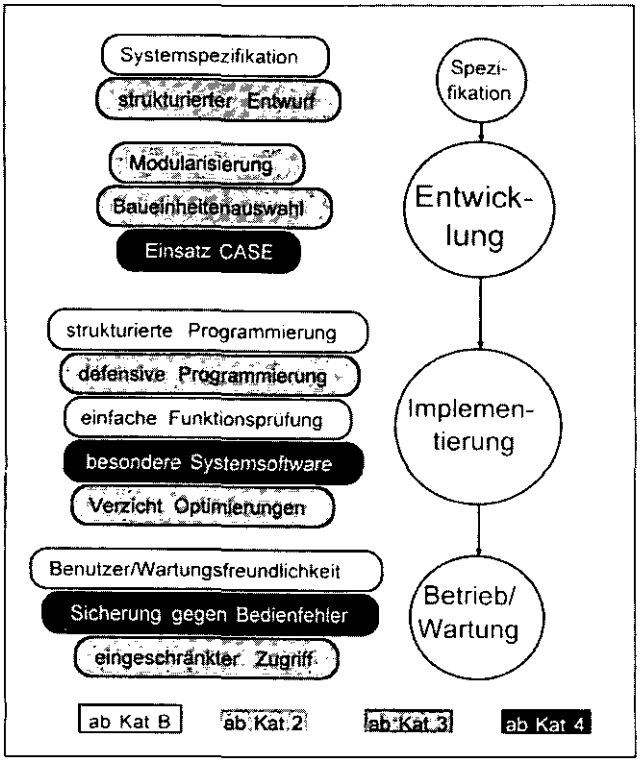



Abbildung 10:
Vom Hersteller zu ergreifende Maßnahmen zur Fehlervermeidung

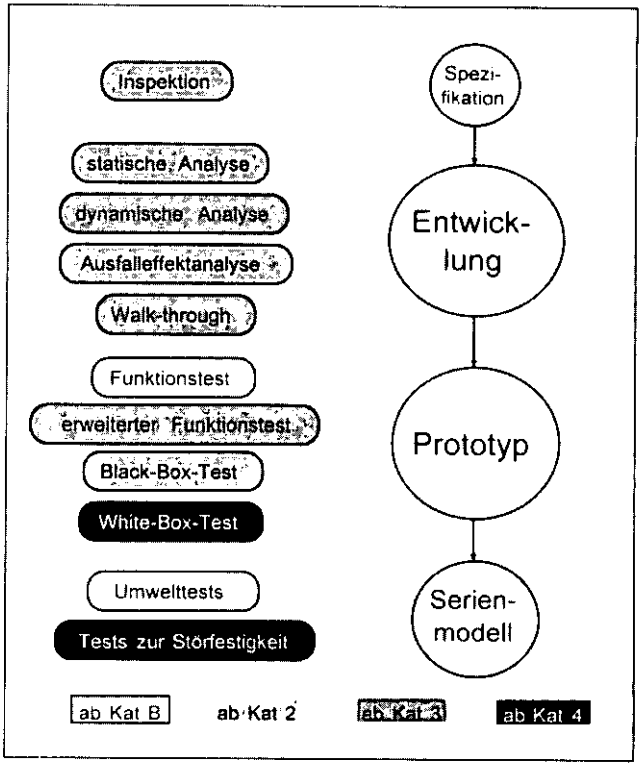



Abbildung 11:
Von der prüfenden Stelle zu ergreifende Maßnahmen zur Fehlervermeidung

noch diejenigen fehlervermeidenden Maßnahmen, die ab Kategorie 2 erforderlich sind. Für die Kategorie B sind nur wenige fehlervermeidende Maßnahmen zu ergreifen. Sie entsprechen den grundlegenden Sicherheitsprinzipien nach EN 954.

## 4.2 Beispiele für die technologieunabhängige Realisierung der einzelnen Kategorien

Die folgenden Schaltungsbeispiele erläutern die Umsetzung der Kategorien jeweils spezifisch für die jeweilige Tech-

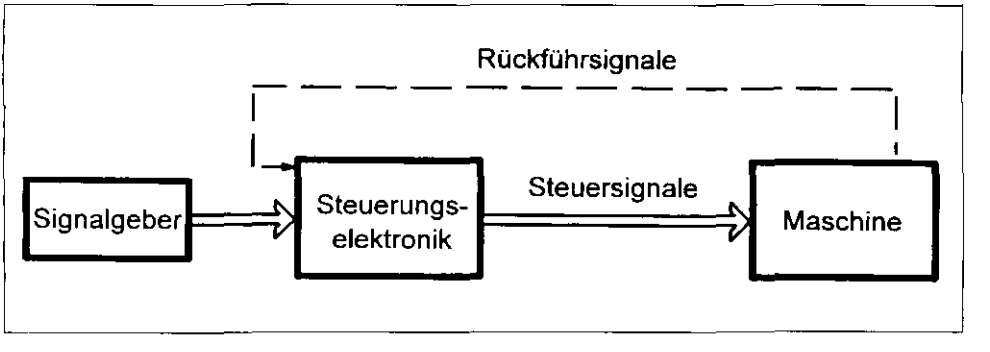
nologie. Auf dieser Basis ist sowohl die Entwicklung von sicherheitsbezogenen Teilen von Steuerungen als auch deren Validierung möglich.

Die folgenden Beispiele entstammen der langjährigen Erfahrung des BIA mit der Entwickung und Prüfung von sicherheitsbezogenen Maschinensteuerungen, ohne auf herstellerspezifische Realisierungsvorschläge einzugehen. Sie wurden z.T. bereits in verschiedenen Veröffentlichungen der Allgemeinheit vorgestellt, sind in diesem Zusammenhang allerdings erstmalig zusammenhängend und in bezug auf die Umsetzung der Kategorien dargestellt. Als Hauptquelle sei auf das BIA-Handbuch hingewiesen, das vom Erich Schmidt Verlag herausgegeben und als Loseblattsammlung ständig aktualisiert und ergänzt wird.

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektroniksteuerungen
## Beispiel für EN 954 — Kategorie B

Abbildung 12:
Elektronische Steuerung nach EN 954 — Kategorie B
zur Steuerung von gefahrbringenden Bewegungen



*Funktionsbeschreibung:*

☐ Gefahrbringende Bewegungen oder Zustände werden durch eine einkanalige integrierte Logik in Abhängigkeit vom Sensor gesteuert.

☐ Die Sicherheitsfunktion läßt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.

☐ Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

**Konstruktive Merkmale:**

☐ Die Reaktion wird durch die einkanalige Logik zurückgelesen, und bei fehlender Plausibilität wird eine Warnung gegeben und eine Abschaltreaktion eingeleitet.

☐ Die Steuerung ist gegenüber üblichen industriellen Umgebungseinflüssen (Schock, Vibration, Temperatur, EMV) ertüchtigt.

**Anwendung:**

☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich, relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann und in Verbindung mit zusätzlichen, z.B. organisatorischen Maßnahmen.

**Weiterführende Literatur:**

☐ *Jürs, H.; Reinert, D.*: Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 1

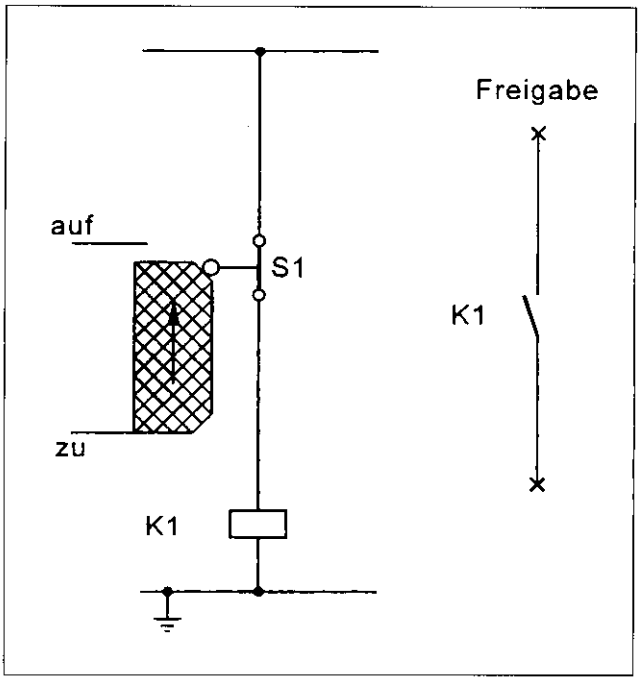



Abbildung 13:
Elektromechanische Steuerung nach EN 954 — Kategorie 1
Stellungsüberwachung beweglicher Schutzeinrichtungen

**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Hilfsschütz K1 unterbrochen bzw. verhindert.
- ☐ Die Sicherheitsfunktion läßt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- ☐ Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.
- ☐ Ein Entfernen der Schutzeinrichtung wird nicht bemerkt.

**Konstruktive Merkmale:**

- ☐ Als bewährte Prinzipien werden das Ruhestromprinzip und die Erdung des Steuerkreises verwendet.
- ☐ Der Schalter S1 ist ein zwangsöffnender Positionsschalter entsprechend EN 1088. Der Öffnerkontakt muß mechanisch zwangläufig unterbrechen, wenn die Schutzeinrichtung sich nicht in Schutzstellung befindet.
- ☐ Die Stellungsüberwachung erfolgt durch ein Hilfsschütz in bewährter Technik.
- ☐ Betätigungselemente und Positionschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden.
- ☐ Der Betätigungshub für den Positionsschalter erfolgt nach Herstellerangabe.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

- ☐ *Kreutzkampf, F.; Hertel, W.*: Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X/91. Erich Schmidt Verlag, Bielefeld
- ☐ *Kreutzkampf, F.; Becker, K.*: Verriegelung beweglicher Schutzeinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 210. In: BIA-Handbuch 1. Lfg. IX/85. Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 1

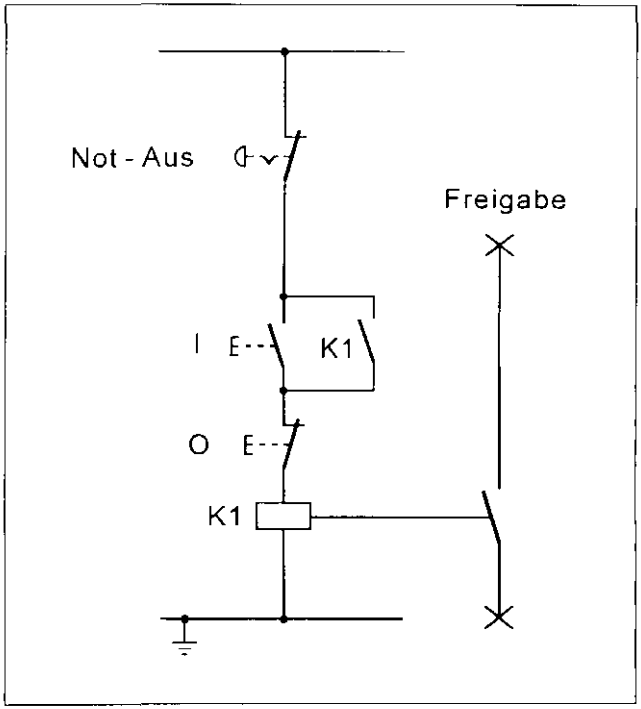



Abbildung 14:
Elektromechanische Steuerung nach EN 954 — Kategorie 1
Not-Aus-Einrichtung

**Funktionsbeschreibung:**

☐ Gefahrbringende Bewegungen oder Zustände werden bei Betätigung der Not-Aus-Einrichtung durch Hilfsschütz K1 und Unterbrechung der Steuerspannung abgeschaltet.

☐ *Die Sicherheitsfunktion läßt sich nicht bei allen Bauteilausfällen aufrechterhalten* und hängt von der Zuverlässigkeit der Bauteile ab.

☐ *Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.*

**Konstruktive Merkmale:**

☐ Als bewährte Prinzipien werden das Ruhestromprinzip und die Erdung des Steuerkreises verwendet.

☐ Befehlsgerät und Stellteil arbeiten nach dem Prinzip der Zwangsbetätigung (EN 418).

☐ Die Signalverarbeitung erfolgt durch ein Hilfsschütz in bewährter Technik.

**Anwendung:**

☐ Bei niedrigen Risiken, z.B. wenn sofortiges Abschalten der Energiezufuhr nicht zu gefährlichen Zuständen führt (Stop-Kategorie 0 nach EN 60 204-1).

Anmerkung:

Die Anwendung ist auch möglich bei Maschinen, bei denen die Wahrscheinlichkeit des Auftritts von Gefahren durch geeignete Maßnahmen verringert ist. Solche Maßnahmen können z.B. Schutzeinrichtungen mit entsprechender Steuerungskategorie oder Abdecken bzw. Kapselung von Gefahrstellen sein.

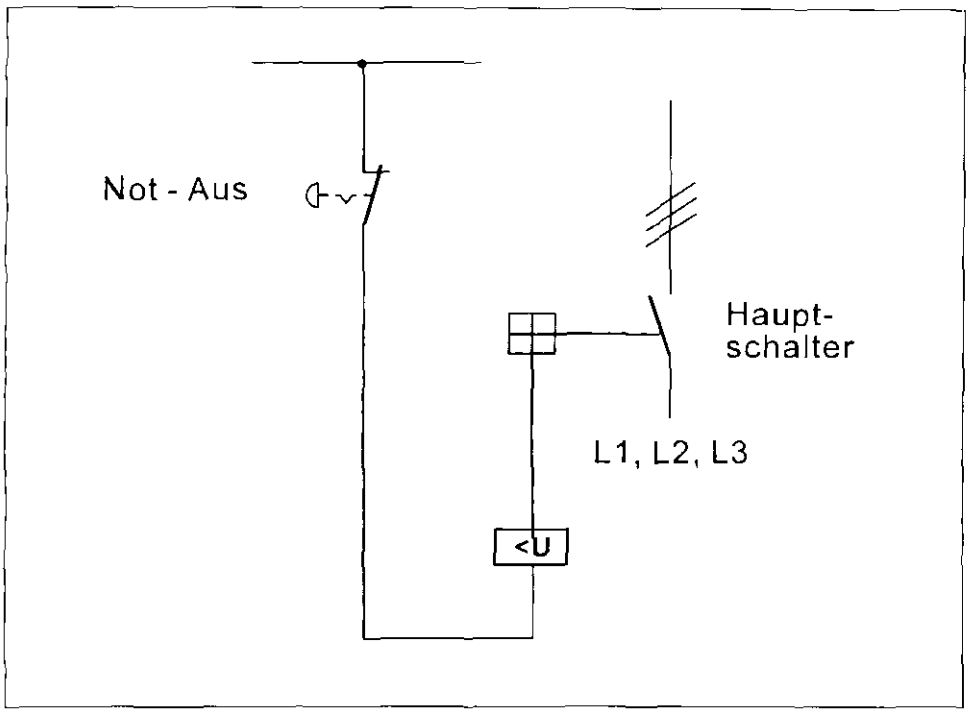
**Weiterführende Literatur:**

☐ *nicht bekannt*

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 1

Abbildung 15:
Elektromechanische Steuerung nach EN 954 — Kategorie 1
Not-Aus-Einrichtung auf Unterspannungsauslöser des Hauptschalters wirkend



**Funktionsbeschreibung:**

☐ Gefahrbringende Bewegungen oder Zustände werden bei Betätigung der Not-Aus-Einrichtung durch Ausschalten des Hauptschalters durch Unterspannungsauslöser unterbrochen.

☐ Die Sicherheitsfunktion läßt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.

☐ Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

*Konstruktive Merkmale:*

☐ Als bewährtes Prinzip wird das Ruhestromprinzip des Unterspannungsauslösers verwendet.

☐ Befehlsgerät und Stellteil arbeiten nach dem Prinzip der Zwangsbetätigung (EN 418).

☐ Es wird die Spannungsversorgung der ganzen Maschine abgeschaltet.

**Anwendung:**

☐ Bei niedrigen Risiken, z.B. wenn sofortiges Abschalten der Energiezufuhr nicht zu gefährlichen Zuständen führt (Stop-Kategorie 0 nach EN 60 204-1).

☐ Die Anwendung ist auch möglich bei Maschinen, bei denen die Wahrscheinlichkeit des Auftritts von Gefahren durch geeignete Maßnahmen verringert ist. Solche Maßnahmen können z. B. Schutzeinrichtungen mit entsprechender Steuerungskategorie oder Abdecken bzw. Kapselung von Gefahrstellen sein.

**Weiterführende Literatur:**

☐ *nicht bekannt*

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 1

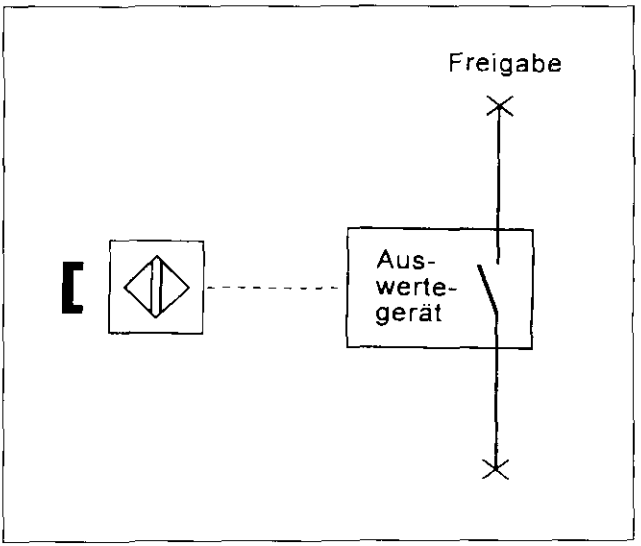



Abbildung 16:
Elektromechanische Steuerung nach EN 954 — Kategorie 1
Stellungsüberwachung beweglicher Schutzeinrichtungen durch berührungslos wirkenden Positionsschalter für Sicherheitsfunktionen

**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Auswertegerät eines berührungslos wirkenden Positionsschalters nach DIN VDE 0660 Teil 209 unterbrochen bzw. verhindert.
- ☐ Die Sicherheitsfunktion ist vergleichbar mit mechanischen Positionsschaltern nach EN 1088.
- ☐ Die Sicherheitsfunktion wird durch das Auftreten von Einfachfehlern nicht beeinflußt. Bei geeigneter Ausführung der Gebereinheiten, Leitungen und Auswertegeräte kann die Sicherheitsfunktion noch erweitert werden.
- ☐ Ein Entfernen der Schutzeinrichtung wird bemerkt.

**Konstruktive Merkmale:**

- ☐ In der Auswerteeinheit werden die Schaltzustände von unterschiedlichen Sensoren (Reed-Kontakte) ausgewertet. Der Schaltvorgang wird durch Veränderung magnetischer, elektromechanischer, optischer, akustischer oder anderer Felder ausgelöst.
- ☐ Die sichere Funktion kann nicht durch Umgehen auf einfache Weise aufgehoben werden; z.B. durch Verwendung codierter Betätigungsmagnete.

Anwendung:

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrenbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann. Außerdem dort, wo berührungslos wirkende Systeme wegen der fehlenden Mechanik und der hohen Schutzart Vorteile bringen.

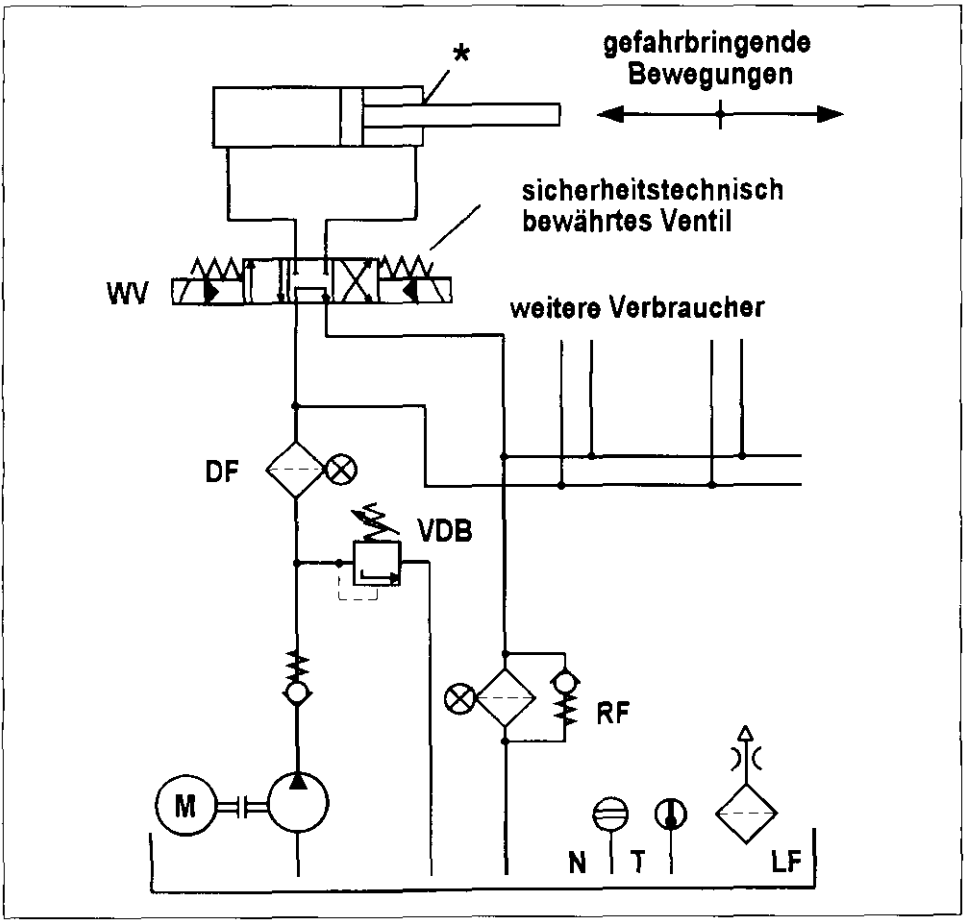
**Weiterführende Literatur:**


- ☐ *Börner, F., H.-G. Foermer und K. Meffert:* Magnetschalter in Sicherheitskreisen. BIA-Report 4/89. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitssicherheit — BIA, Sankt Augustin
- ☐ *Börner, F.; K. Meffert:* Berührungslos wirkende Positionsschalter für Sicherheitsfunktionen, Positivliste. Sicherheitstechnisches Informations- und Arbeitsblatt 545 213. In: BIA-Handbuch 22. Lfg. V/94. Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 1

Abbildung 17:
Elektro-hydraulische Steuerung nach EN 954 — Kategorie 1, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden durch ein sicherheitstechnisch bewährtes Wegeventil WV gesteuert.
- ☐ Der Ausfall des Wegeventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- ☐ Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

**Konstruktive Merkmale:**

- ☐ Bei WV handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- ☐ Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- ☐ Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil (ausreichend hohe Zuverlässigkeit) erfolgt bei Bedarf durch den Hersteller/ Anwender.
- ☐ Als gezielte Maßnahmen zur Erhöhung der Zuverlässigkeit des Wegeventils sind ein Druckfilter DF vor dem Wegeventil und geeignete Maßnahmen gegen Schmutzeinzug durch die Kolbenstange am Zylinder (z.B. wirksamer Abstreifer an der Kolbenstange, siehe ✳) vorgesehen.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

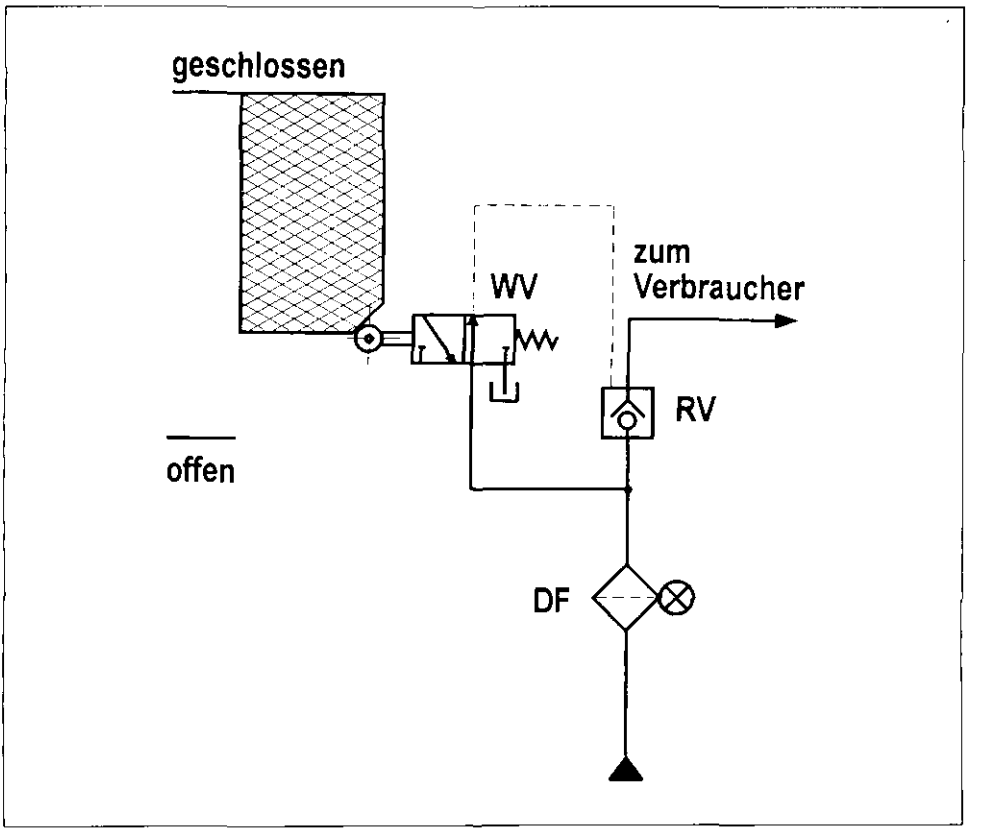
**Weiterführende Literatur:**

- ☐ *Kleinbreuer, W.*: Anwendung der Kategorien nach pr EN 954-1 auf fluidtechnische Steuerungen. O+P „Ölhydraulik und Pneumatik" 38 (1994) Nr. 9
- ☐ *Kleinbreuer, W.*: Application of the categories laid down in prEN 954-1 to fluid technology control systems. HEALTH AND SAFETY EXECUTIVE LANGUAGE SERVICE, Transl. No.: 15214 B, Information Centre, Broad Lane, Sheffield S37HQ, GB

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 1

Abbildung 18:
Hydraulische Steuerung nach EN 954 — Kategorie 1,
Verriegelung beweglich trennender Schutzeinrichtung (Schließsicherung)



**Funktionsbeschreibung:**

- ☐ Die Verriegelung beweglich trennender Schutzeinrichtung wird durch einen „hydraulischen Positionsschalter" WV überwacht. Dieser gibt einen Steuerbefehl an das Sperrventil RV. Beide Ventile sind sicherheitstechnisch bewährte Bauteile.
- ☐ Die Energiezufuhr (hydraulisch) erfolgt nur bei geschlossener Schutzeinrichtung.
- ☐ Der Ausfall des Sperrventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Sperrventils ab.
- ☐ Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

**Konstruktive Merkmale:**

- ☐ Bei WV handelt es sich um einen hydraulischen Positionsschalter (Rollenhebelventil) mit zwangläufiger Betätigung durch eine beweglich trennende Schutzeinrichtung, entsprechend EN 1088.
- ☐ Die sicherheitsgerichtete Schaltstellung an RV wird durch Wegnahme des Steuersignals erreicht.
- ☐ Die Bestätigung für die Ventile als sicherheitstechnisch bewährte Bauteile (ausreichend hohe Zuverlässigkeit) erfolgt bei Bedarf durch den Hersteller/Anwender.
- ☐ Als gezielte Maßnahme zur Erhöhung der Zuverlässigkeit ist ein Druckfilter DF vor den Ventilen vorgesehen.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

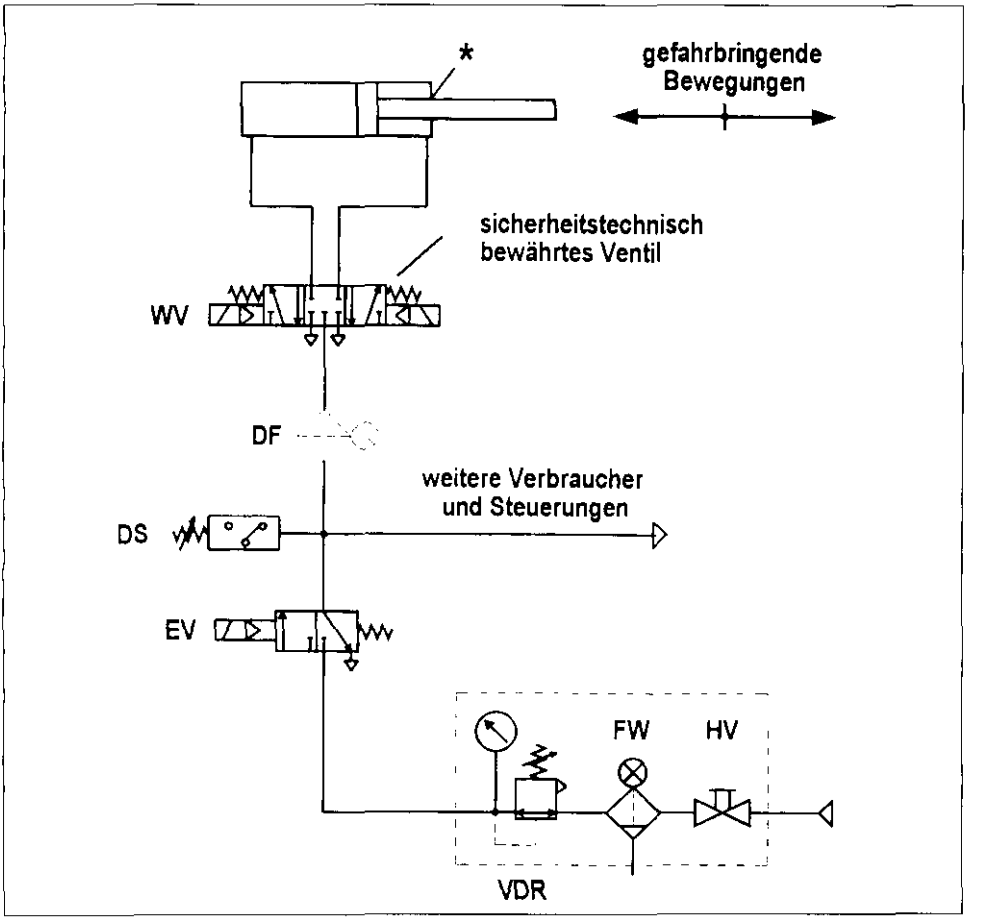
**Weiterführende Literatur:**


- ☐ *Kleinbreuer, W.*: Anforderungen an hydraulische und pneumatische Maschinensteuerungen. Sichere Chemiearbeit (1992) Nr. 2 und Nr. 3
- ☐ EN 1088: Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 1

Abbildung 19:
Elektro-pneumatische Steuerung nach EN 954 — Kategorie 1, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden durch ein sicherheitstechnisch bewährtes Wegeventil WV gesteuert.
- ☐ Der Ausfall des Wegeventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- ☐ Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

**Konstruktive Merkmale:**

- ☐ Bei WV handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- ☐ Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- ☐ Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil (ausreichend hohe Zuverlässigkeit) erfolgt bei Bedarf durch den Hersteller/ Anwender.
- ☐ Als gezielte Maßnahmen zur Erhöhung der Zuverlässigkeit des Wegeventils sind ein Druckfilter DF (eventuell bei umfangreichen Leitungssystemen notwendig) vor dem Wegeventil und geeignete Maßnahmen gegen Schmutzeinzug durch die Kolbenstange am Zylinder (z.B. wirksamer Abstreifer an der Kolbenstange, siehe *) vorgesehen.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

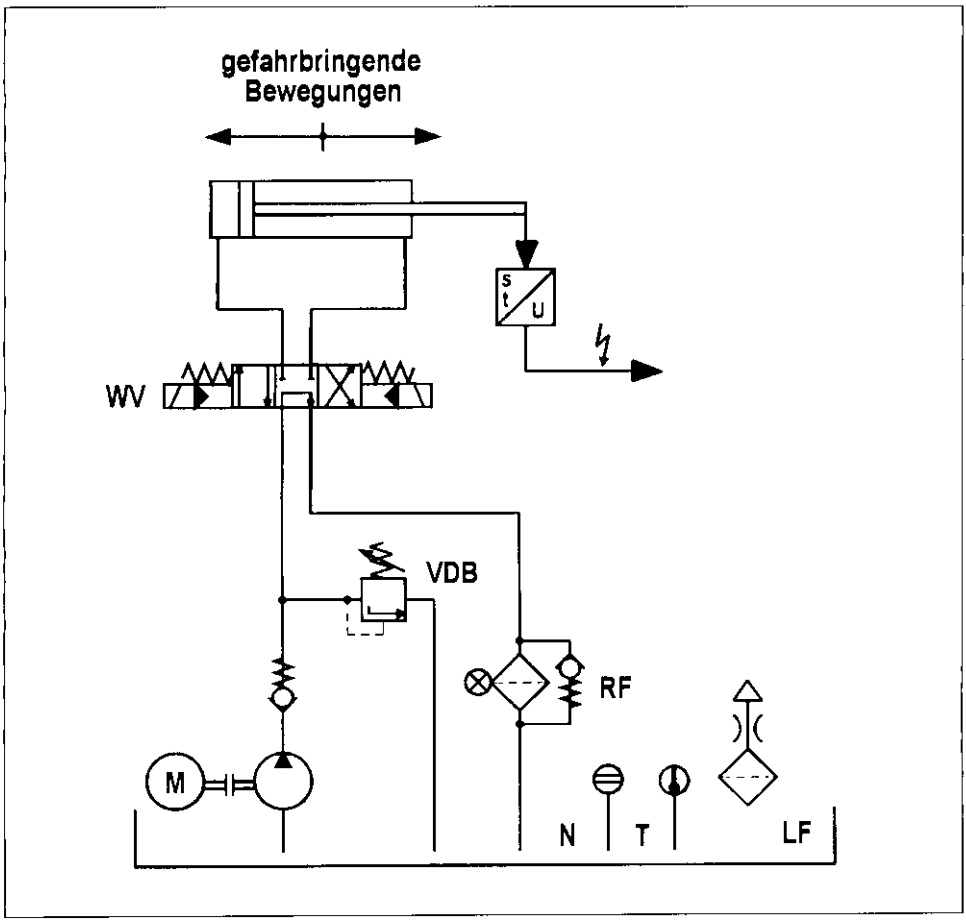
**Weiterführende Literatur:**


- ☐ *Kleinbreuer, W.*: Anwendung der Kategorien nach pr EN 954-1 auf fluidtechnische Steuerungen. O+P „Ölhydraulik und Pneumatik" 38 (1994) Nr. 9
- ☐ *Kleinbreuer, W.*: Application of the categories laid down in prEN 954-1 to fluid technology control systems. HEALTH AND SAFETY EXECUTIVE LANGUAGE SERVICE, Transl. No.: 15214 B, Information Centre, Broad Lane, Sheffield S37HQ, GB

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 2

Abbildung 20:
Elektro-hydraulische Steuerung nach EN 954 — Kategorie 2, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden durch ein Wegeventil WV gesteuert.
- ☐ Der Ausfall des Wegeventils zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- ☐ Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion in geeigneten Zeitabständen. Das Erkennen des Ausfalls des Wegeventils führt z.B. zum Abschalten der Maschine.
- ☐ Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.

**Konstruktive Merkmale:**

- ☐ Bei WV handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.
- ☐ Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- ☐ Die Testung erfolgt z.B. durch Überprüfung des Weg-/Zeitverhaltens der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einkanaliger SPS.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

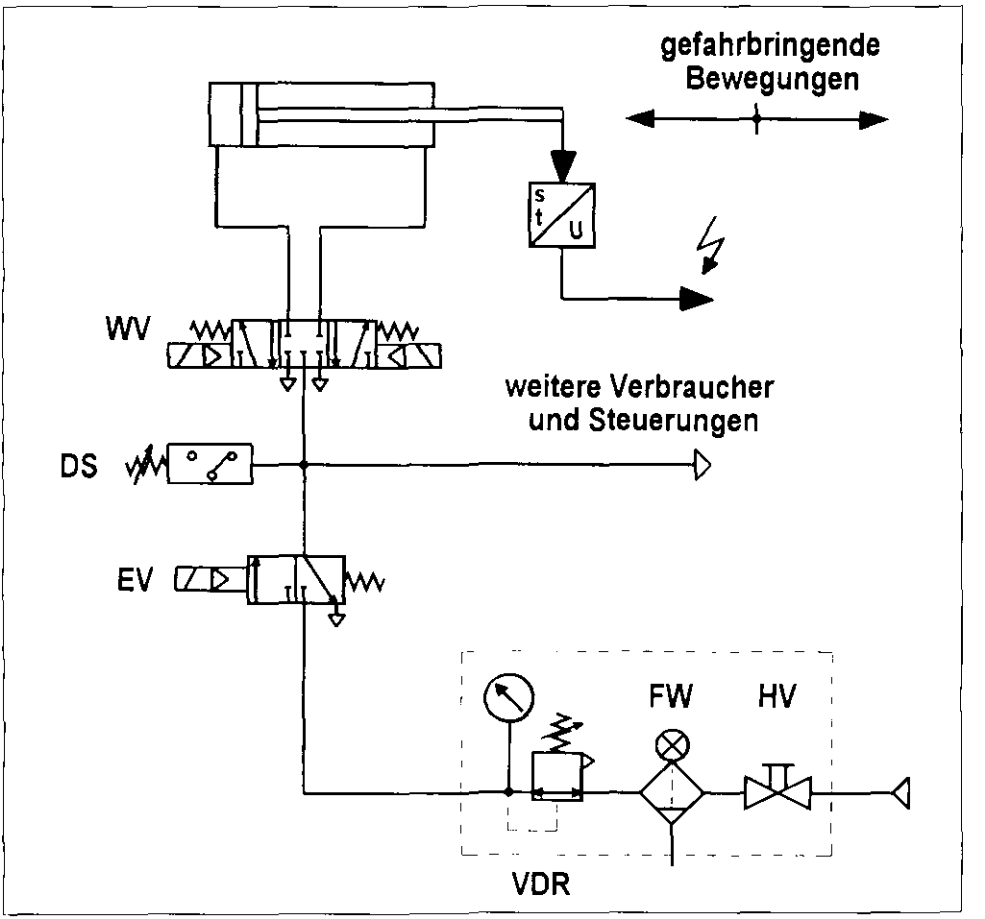
**Weiterführende Literatur:**

- ☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 2

Abbildung 21:
Elektro-pneumatische Steuerung nach EN 954 — Kategorie 2, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

☐ Gefahrbringende Bewegungen oder Zustände werden durch ein Wegeventil WV gesteuert.

☐ Der Ausfall des Wegeventils zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.

☐ Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion in geeigneten Zeitabständen. Das Erkennen des Ausfalls des Wegeventils führt z.B. zum Abschalten der Maschine.

☐ Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.

**Konstruktive Merkmale:**

☐ Bei WV handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.

☐ Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.

☐ Die Testung erfolgt z.B. durch Überprüfung des Weg-/Zeitverhaltens der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einkanaliger SPS.

**Anwendung:**

☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

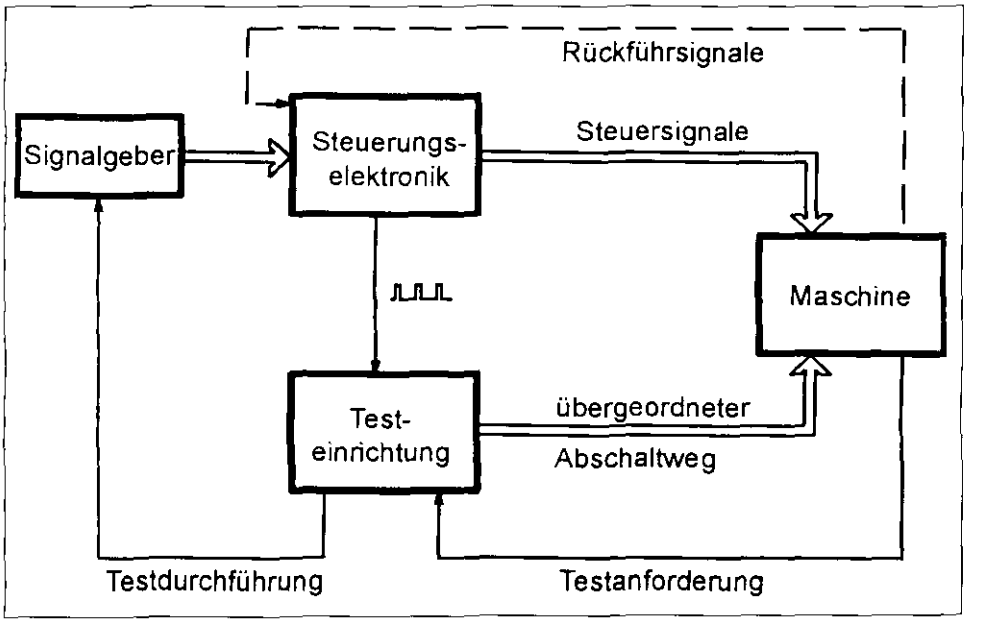
**Weiterführende Literatur:**

☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektroniksteuerungen
## Beispiel für EN 954 — Kategorie 2

Abbildung 22:
Elektroniksteuerung nach EN 954 — Kategorie 2
Grobstruktur der Steuerung



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden in Abhängigkeit vom Signalgeber gesteuert.
- ☐ *Eine zwangsweise Testung der Sicherheitsfunktion* (durch eigene von der Steuerungselektronik unabhängige Hardware) erfolgt entweder beim Start der Maschine oder zyklisch.
- ☐ Während des Tests wird die sicherheitstechnische Funktion vollständig überprüft, d.h. zum Testzeitpunkt wird eine Freigabe der gefahrbringenden Bewegung verhindert.
- ☐ Die Test- oder die Sicherheitsfunktion muß bei einem einzelnen Bauteilausfall erhalten bleiben.
- ☐ Ein Ausfall der Sicherheitsfunktion wird beim nächsten Test aufgedeckt.

**Konstruktive Merkmale:**

- ☐ Der zweite unabhängige Abschaltweg ermöglicht eine Abschaltung, auch wenn der normale Abschaltweg ausgefallen ist.
- ☐ Es werden keine zusätzlichen Anforderungen an die Testeinrichtung (ein Ausfall muß nicht bemerkt werden) gestellt.
- ☐ Der Test umfaßt Signalgeber und Abschalteinrichtung.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann. Ein Stillsetzen der gefahrbringenden Bewegungen oder Zustände muß regelmäßig prozeßbedingt möglich sein.

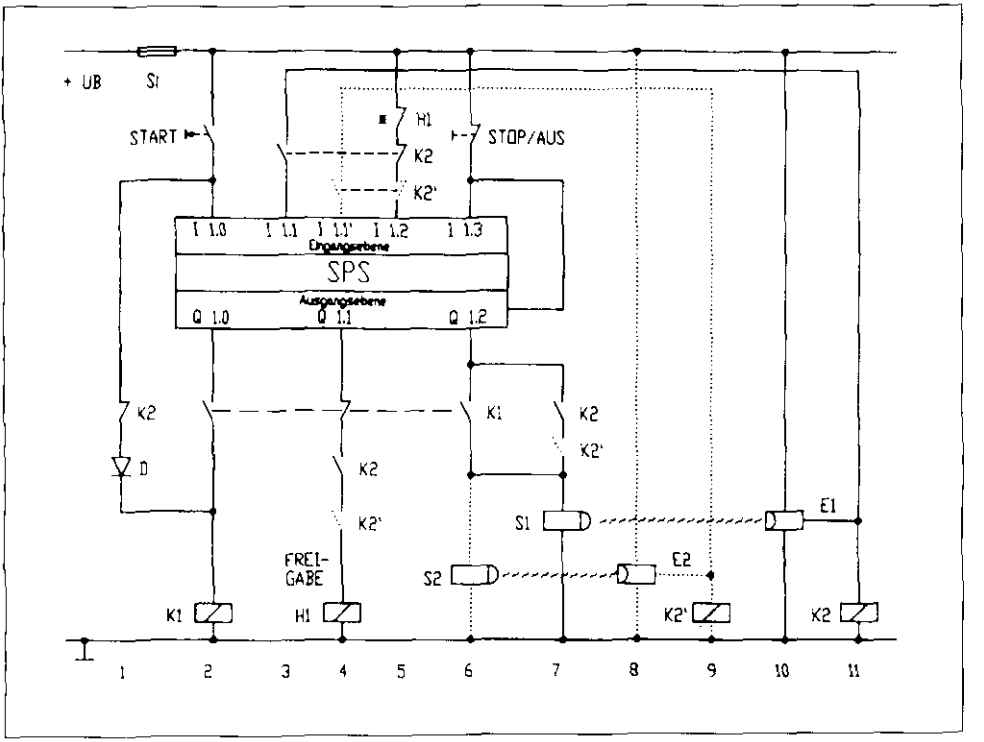
**Weiterführende Literatur:**

- ☐ *Jürs, H.; Reinert, D.*: Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93 Erich Schmidt Verlag, Bielefeld
- ☐ *Grigulewitsch, W.; Reinert, D.*: Lichtschranken mit Testung. Sicherheitstechnisches Informations- und Arbeitsblatt 330 228. In: BIA-Handbuch 22. Lfg. V/94 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 2

Abbildung 23:
Rechnersteuerung nach EN 954 — Kategorie 2
Sicherheitslichtschranke realisiert durch eine Standard-SPS



**Funktionsbeschreibung:**

- ☐ Bei einer Lichtstrahlunterbrechung in der Lichtschranke S1/E1 (bzw. S2/E2) erfolgt eine redundante Abschaltung von gefahrbringenden Bewegungen oder Zuständen durch den SPS-Ausgang Q1.1 und das Relais/Schütz K2.
- ☐ Die Testung der Sicherheitsfunktion der Lichtschranke erfolgt nach dem Drücken der START-Taste durch *softwaregesteuertes Ausschalten des Lichtschranken-Senders* mittels SPS-Ausgang Q 1.2 und Überwachen der Empfängerreaktion durch die SPS-Eingänge I 1.1 und I 1.2
- ☐ Die Detektion eines Lichtschrankenausfalls oder einer fehlerhaften Abfallverzögerung erfolgt durch die Software.
- ☐ *Während des Tests ist die FREIGABE aufgehoben.*

**Konstruktive Merkmale:**

- ☐ Es müssen spezielle Lichtschranken mit ausreichenden optischen Eigenschaften nach EN 61 496 verwendet werden.
- ☐ K1 und K2 sind Relais mit zwangsgeführten Kontakten.
- ☐ Mit nur einem zusätzlichen SPS-Eingang pro Lichtschranke können mehrere Sende-/Empfangssysteme kaskadiert und überwacht werden.

**Anwendung:**

- ☐ Bei niedrigen Risiken, z.B. bei seltenem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch *andere Maßnahmen noch* abgewendet werden kann. Der Anlauftest der Lichtschranke muß an den regelmäßigen Start der gefahrbringenden Bewegung (Zustand) anbindbar sein.

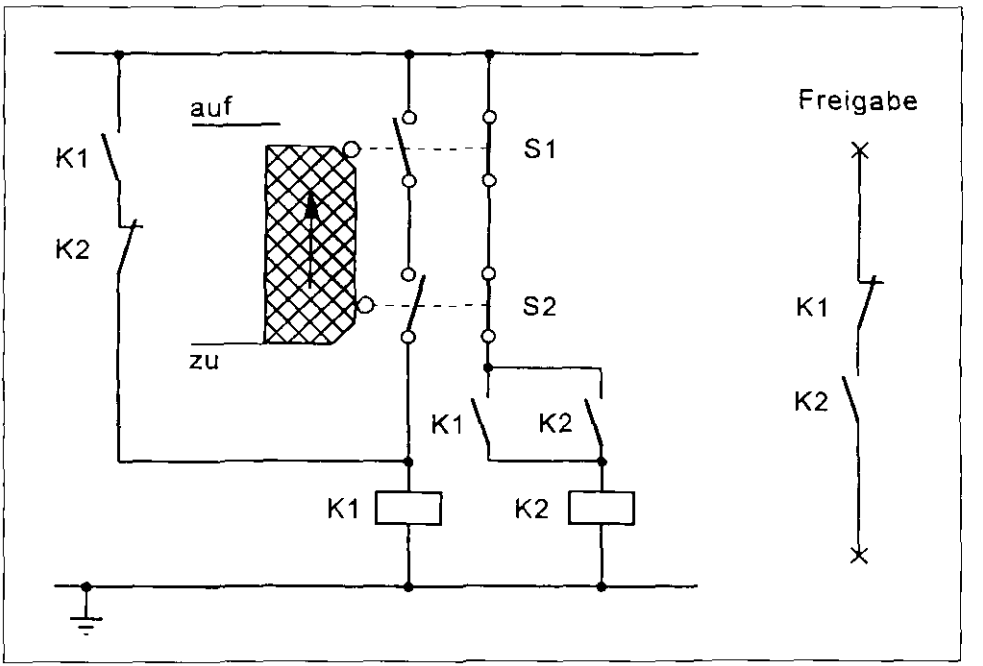
**Weiterführende Literatur:**


- ☐ *Grigulewitsch, W.; Reinert, D.:* Lichtschranken mit Testung. Sicherheitstechnisches Informations- und Arbeitsblatt 330 228. In: BIA-Handbuch 22. Lfg. V/94 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 24:
Elektromechanische Steuerung nach EN 954 — Kategorie 3
Stellungsüberwachung beweglicher Schutzeinrichtungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Öffner-Schließer-Kombination unterbrochen bzw. verhindert.
- ☐ Die Freigabe erfolgt nur, wenn die Schutzeinrichtung geöffnet und danach wieder geschlossen wird.
- ☐ Das Entfernen der Schutzeinrichtung wird (durch S2) unmittelbar erkannt.
- ☐ Beim Auftreten eines Bauteilausfalles bleibt die Sicherheitsfunktion erhalten.
- ☐ Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung.
- ☐ Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschieden betätigten Positionsschaltern (Öffner-Schließer-Kombination) erkannt.
- ☐ Wenige Fehler werden nicht erkannt (Nicht-Abfallen des Steuerschützes K2 bei Entregung; Nicht-Unterbrechung der Kontakte in S1 oder S2). Die Anhäufung derartiger Fehler kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ Der Schalter S1 ist ein zwangsöffnender Positionsschalter entsprechend EN 1088.
- ☐ Der Schalter S2 und die Steuerschütze K1/K2 haben zwangsgeführte Kontakte.
- ☐ Die Zuleitungen zu den Positionsschaltern sind getrennt verlegt.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

- ☐ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X/91 Erich Schmidt Verlag, Bielefeld
- ☐ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen zur Stellungsüberwachung beweglicher Schutzeinrichtungen. BIA-Report 3/89

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 3

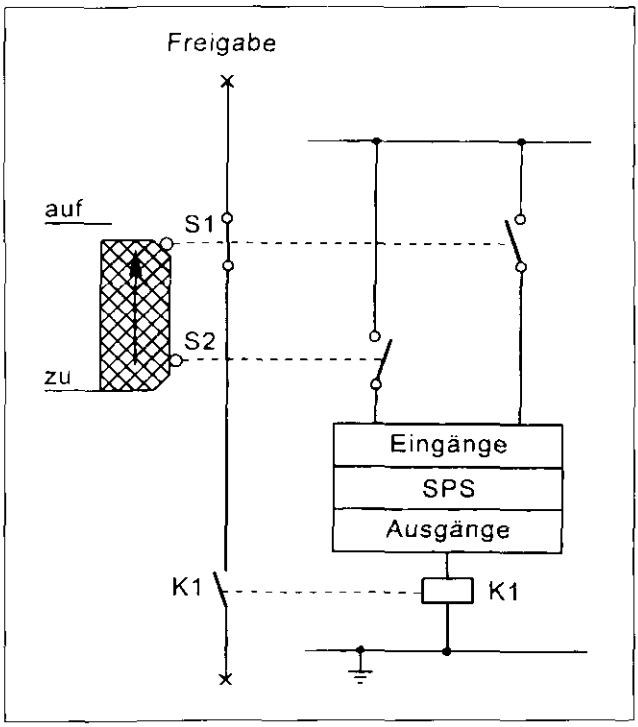



Abbildung 25:
Elektromechanische Steuerung nach EN 954 — Kategorie 3
Stellungsüberwachung beweglicher Schutzeinrichtungen

**Funktionsbeschreibung:**

☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Öffner-Schließer-Kombination unterbrochen bzw. verhindert.

☐ Beim Auftreten eines Bauteilausfalles bleibt die Sicherheitsfunktion erhalten.

☐ Bauteilausfälle in S1 und S2 werden durch die SPS erkannt und führen zur Betriebshemmung durch K1.

☐ Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschieden betätigten Positionsschaltern (Öffner-Schließer-Kombination) erkannt.

☐ Fehler in der SPS und K1 werden nicht erkannt. Ein weiterer Fehler (z.B. Versagen von S1) führt zum Verlust der Sicherheitsfunktion.

**Konstruktive Merkmale:**

☐ Der Schalter S1 ist ein zwangsöffnender Positionsschalter entsprechend EN 1088.

☐ Die Zuleitungen zu den Positionsschaltern sind getrennt verlegt, oder es erfolgt eine geschützte Leitungsverlegung.

**Anwendung:**

☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

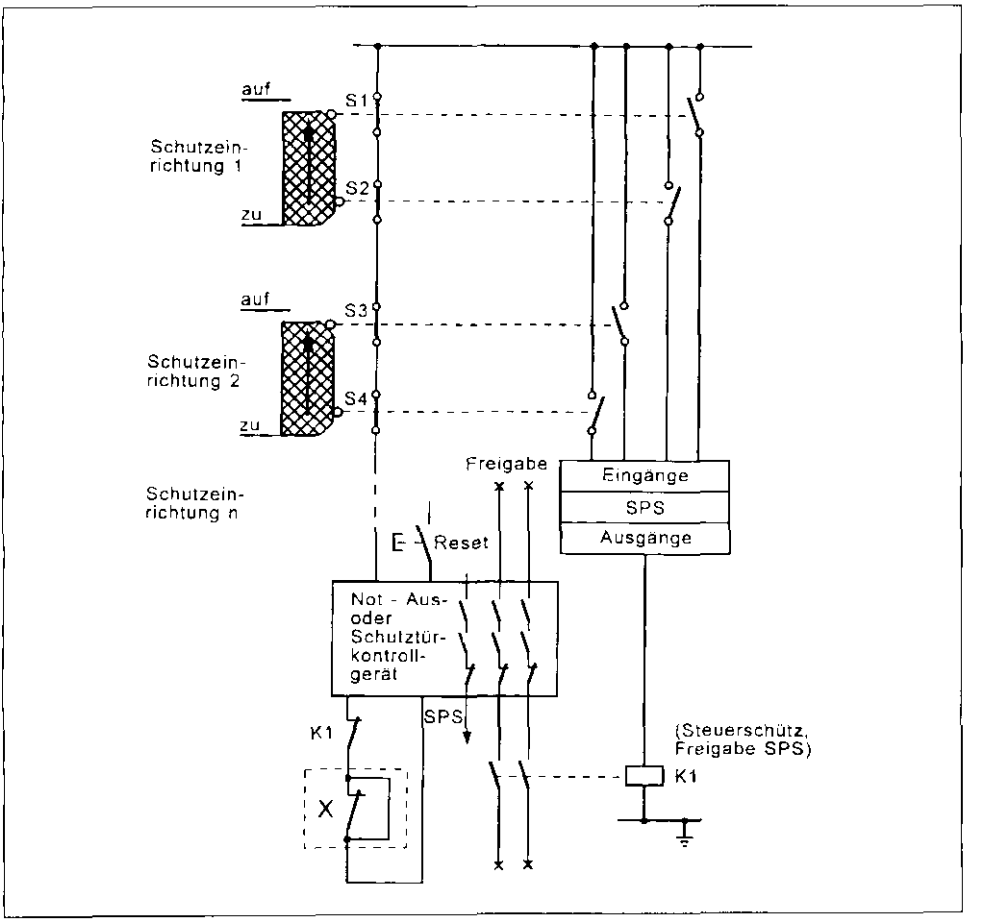
**Weiterführende Literatur:**

☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 26:
Elektromechanische Steuerung nach EN 954 — Kategorie 3
Stellungsüberwachung beweglicher Schutzeinrichtungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Öffner-Schließer-Kombination unterbrochen bzw. verhindert.
- ☐ Beim Auftreten eines Bauteilausfalles bleibt die Sicherheitsfunktion erhalten.
- ☐ Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung.
- ☐ Auch Fehler in den Leistungsschützen K2 und K3 werden erkannt.
- ☐ Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschiedenen betätigten Positionsschaltern (Öffner-Schließer-Kombination) erkannt.
- ☐ Einige, wenige Fehler werden nicht erkannt (z.B. Nicht-Unterbrechung der Kontakte in S1 bis S4).
- ☐ Es können mehrere Schutzeinrichtungen hintereinander geschaltet werden (Kaskadierung).

**Konstruktive Merkmale:**

- ☐ Die Schalter S1 und S3 sind zwangsöffnende Positionsschalter entsprechend EN 1088.
- ☐ Die Schalter S2/S4 und die Schütze K1/K2/K3 haben zwangsgeführte Kontakte.
- ☐ Die Zuleitungen zu den Positionsschaltern sind getrennt verlegt, oder es erfolgt eine geschützte Leitungsverlegung.
- ☐ Das Not-Aus- oder Schutztürkontrollgerät entspricht Kategorie 4.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

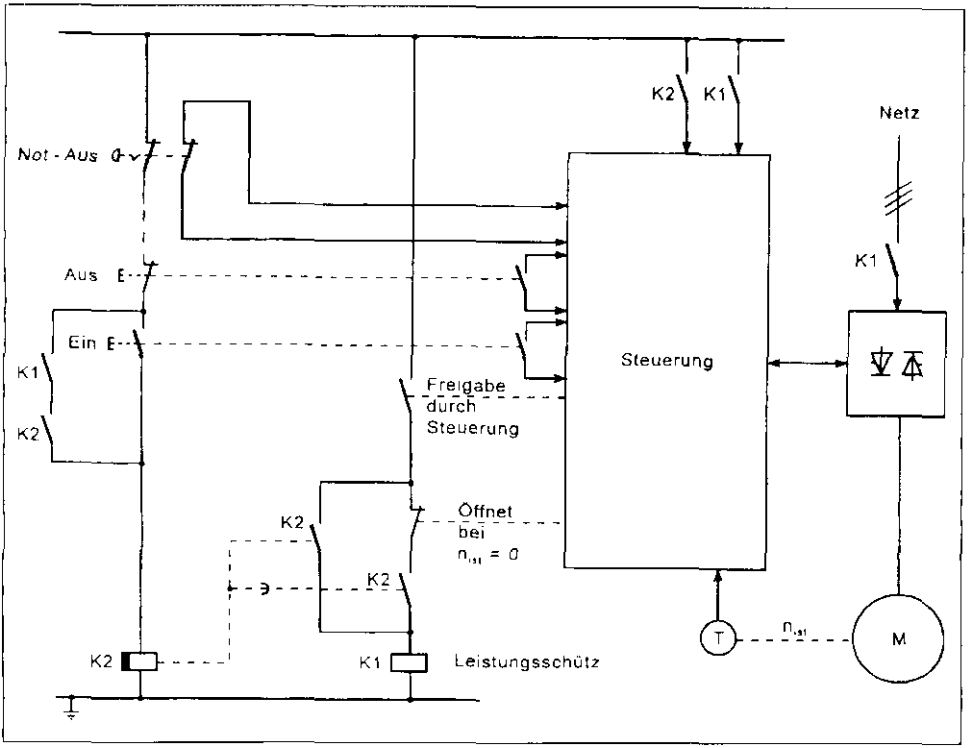
**Weiterführende Literatur:**

- ☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele *für die einzelnen Kategorien*

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 27:
Elektromechanische Steuerung nach EN 954 — Kategorie 3
Not-Aus-Einrichtung für Umrichter mit Nutzbremsung durch Energierückspeisung



**Funktionsbeschreibung:**

- ☐ Nach Betätigen der Not-Aus-Einrichtung wird der Antrieb durch Energierückspeisung abgebremst. Das Leistungsschütz K1 muß so lange eingeschaltet bleiben, bis der Antrieb steht. Bei $n_{ist}$ gleich Null wird das Leistungsschütz durch die Stillstandsmeldung des Umrichters abgeschaltet.
- ☐ Sollte diese Abschaltung nicht wirken, erfolgt spätestens nach der üblichen Bremszeit eine Abschaltung durch den verzögerten Kontakt von K2.

**Konstruktive Merkmale:**

- ☐ Die Not-Aus-Einrichtung ist zweipolig aufgebaut. Über einen Öffnerkontakt wird die Bremsung eingeleitet und der Antrieb zum Stillstand gebracht (Stop-Kategorie 2 nach EN 60 204-1). Über den anderen Öffner der Not-Aus-Einrichtung werden K2 und das Leistungsschütz K1 verzögert abgeschaltet (Stop-Kategorie 1 nach EN 60 204-1).
- ☐ Durch die Not-Aus-Einrichtung erfolgt auf unterschiedliche Weise ein redundantes Stillsetzen des Antriebes. Je nachdem, an welcher Stelle ein Fehler auftritt, wird entweder der Antrieb nicht abgebremst, jedoch durch K2 und K1 verzögert abgeschaltet, oder nach der Abbremsung durch den Umrichter erfolgt keine Trennung der Energieversorgung durch K1.
- ☐ Durch die Steuerung können die meisten Fehler erkannt werden und ein Anlauf des Antriebs kann verhindert werden.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann. Nur einsetzbar beim Einsatz von Umrichtern mit Nutzbremsung (Stop-Kategorie 1), bei denen bei Not-Aus-Betätigung der Ausfall der elektronischen Bremse im Fehlerfall toleriert werden kann.

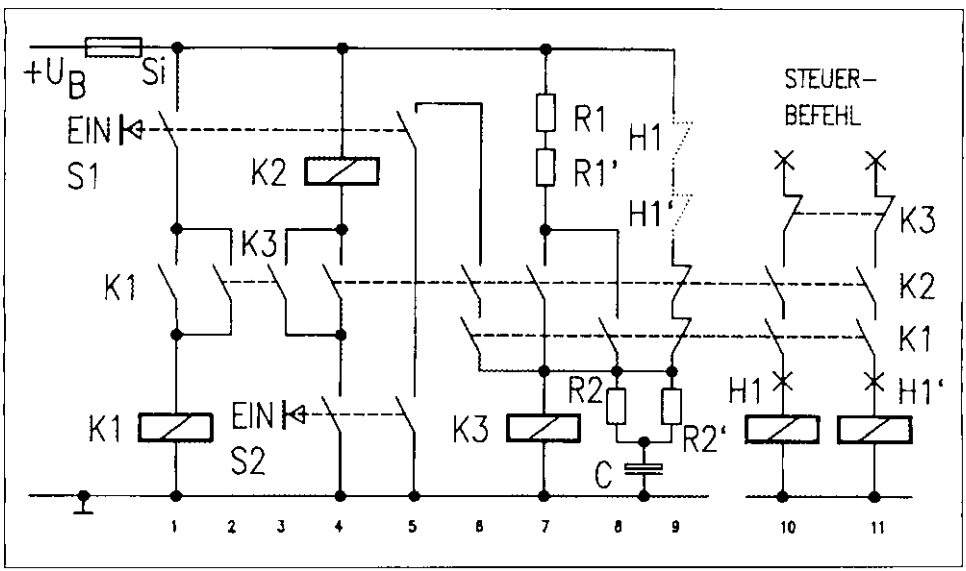
**Weiterführende Literatur:**

- ☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 28:
Elektromechanische Steuerung nach EN 954 — Kategorie 3
Zweihandschaltung in kontaktbehafteter Technik nach EN 574 Typ II ohne Zeitvorgabe für eine synchrone Betätigung



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung oder Zustand kann nur durch die Betätigung beider Befehlsgeber S1 und S2 (Strompfad 1, 4 und 5) eingeleitet werden, indem nach dem Anzug von K1 und K2 über die Pfade 5 und 6 K3 abfällt und damit der Steuerbefehl gegeben wird.

- ☐ Die Rücknahme auch nur eines Eingangsbefehles durch S1 oder S2 führt, da K3 bei Befehlsgabe abgefallen ist, über K1 oder K2 unmittelbar zur Rücknahme des Steuerbefehles (siehe Strompfad 10 und 11).

- ☐ Die Rückstellkontrolle wird realisiert über K3 (Strompfade 2 und 3) und die beiden Öffner von K1 und K2 in Strompfad 9.

- ☐ Eine Einhandschaltung ist bei Auftreten eines Fehlers nicht möglich. Im Ruhezustand ist K3 angezogen und bereitet in den Strompfaden 2 und 3 die Ansteuerung für K1 und K2 vor. Gleichzeitig sperrt K3 die Ausgabe eines Steuerbefehles im Ausgangskreis. Falls eines der Relais K1 oder K2 nach Rücknahme eines Eingabebefehles nicht abfällt, bleibt über R1/R1' auch K3 abgefallen.

**Konstruktive Merkmale:**

- ☐ Die versetzte Spulenanordnung von K1 und K2 deckt Kurzschlüsse in der Leitungsführung zu den Befehlsgebern mit Hilfe der Sicherung Si auf.

- ☐ Für beide Befehlsgeber sind Taster mit Doppelkontakten vorgesehen, damit auch beim Nichtöffnen eines Kontaktes eine gewollte Betätigung der Tasten Voraussetzung für einen gültigen Steuerbefehl bleibt.

- ☐ K3 ist zur Überbrückung von Kontaktumschaltzeiten der Relais K1 und K2 abfallverzögert beschaltet. Die Widerstände R2/R2' begrenzen den Einschaltstrom des Kondensators C auf ca. 0,5A.

- ☐ K1—K3, H1/H1' sind Relais bzw. Schütze mit zwangsgeführten Kontakten.

- ☐ Für die sichere Funktion der Schaltung sind alle Relais-/Schützspulen mit Funkenlöschgliedern versehen worden.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

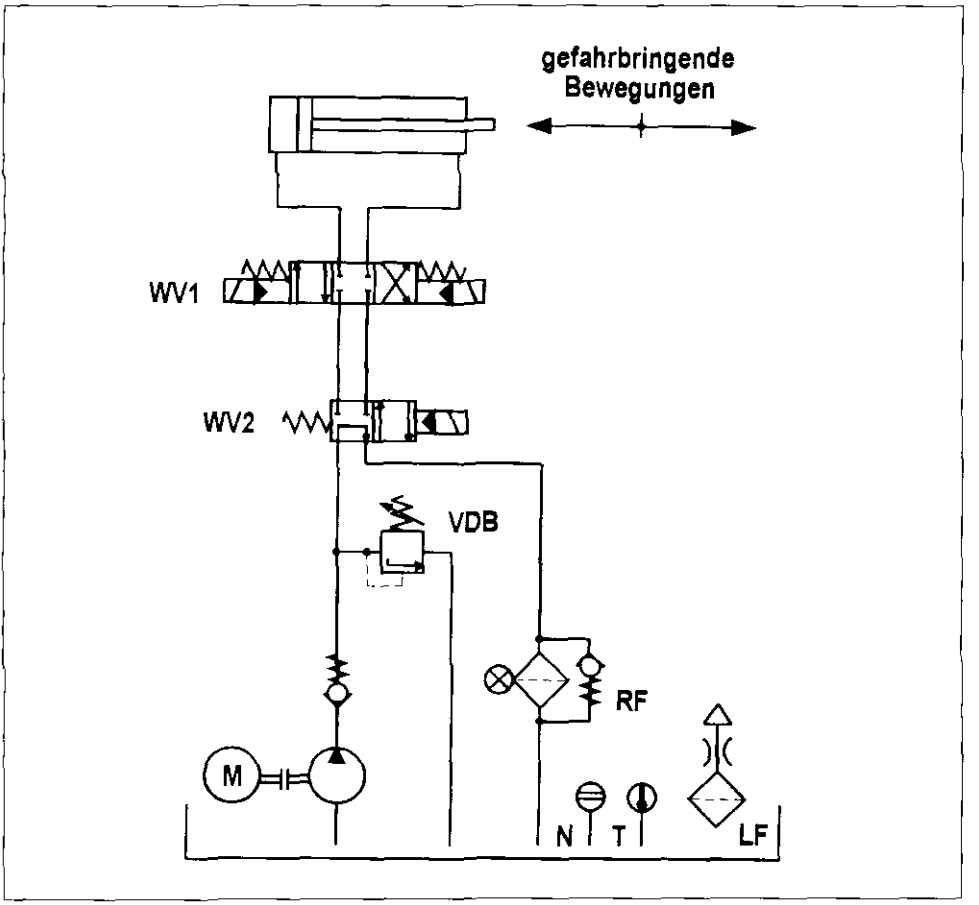
**Weiterführende Literatur:**


- ☐ *Grigulewitsch, W.; Reinert, D.*: Zweihandschaltungen nach Anforderungsstufe II in DIN 24 980. Sicherheitstechnisches Informations- und Arbeitsblatt 330 229. In: BIA-Handbuch 17. Lfg. X/91 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 29:
Elektro-hydraulische Steuerung nach EN 954 — Kategorie 3, ohne Fehlererkennungsmaßnahmen, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

☐ Gefahrbringende Bewegungen oder Zustände werden durch zwei Wegeventile (WV1 und WV2) gesteuert.

☐ Der Ausfall eines Wegeventils führt nicht zum Verlust der Sicherheitsfunktion.

☐ Beide Wegeventile werden zyklisch angesteuert.

☐ Es sind (entsprechend einer Risikobewertung) keine Maßnahmen zur Fehlererkennung vorgesehen. Einige Fehler werden funktionsbedingt erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

*Konstruktive Merkmale:*

☐ Beide Wegeventile (WV1 und WV2) haben eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung bzw. -rückstellung.

☐ Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.

**Anwendung:**

☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

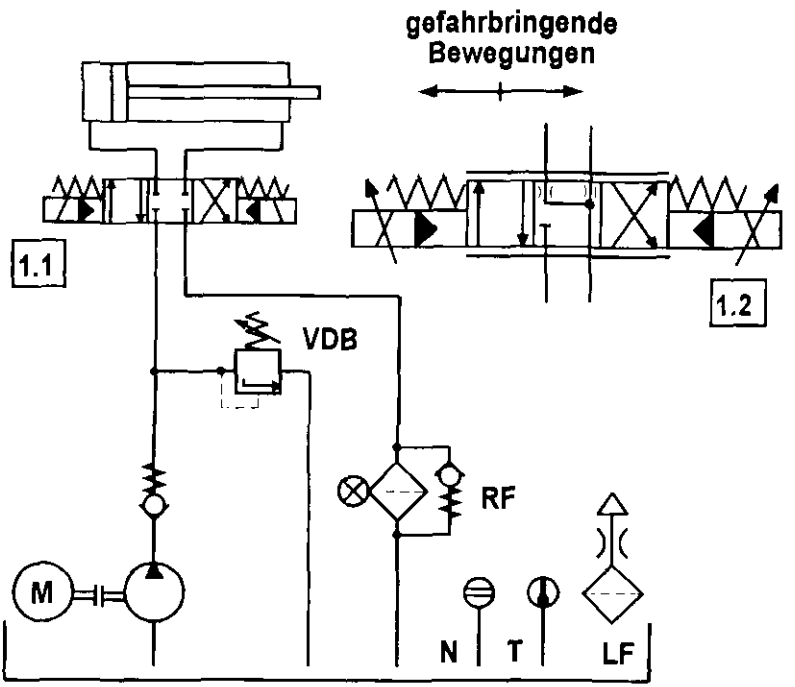
**Weiterführende Literatur:**

☐ *Kleinbreuer, W.*: Konstruierte Sicherheit, Anforderungen an hydraulische und pneumatische Maschinensteuerungen. fluid (1992) Nr. 11/12

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 30:
Elektro-hydraulische Steuerung nach EN 954 — Kategorie 3, zur Steuerung von gefahrbringenden Bewegungen




1.1 Für die Kategorie 3 geeignetes Ventil und Abschaltung des Pumpen-Antriebsmotors mit einem geeigneten Leistungsschütz.

1.2 Für die Kategorie 3 nicht geeignetes Ventil, aber Abschaltung des Pumpen-Antriebs - motors entsprechend Kategorie 3.

**Funktionsbeschreibung:**

- ☐ *Gefahrbringende Bewegungen oder Zustände werden durch ein Wegeventil und* Abschalten des Pumpen-Antriebsmotors (Lösung 1.1) bzw. durch redundantes Abschalten des Pumpen-Antriebsmotors gesteuert (Lösung 1.2).
- ☐ *Ein Bauteilausfall (Wegeventil oder Leistungsschütz bzw. eines der beiden* Leistungsschütze) führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ Alle genannten Bauteile werden zyklisch angesteuert.
- ☐ Es sind (entsprechend einer Risikobewertung) im hydraulischen Steuerungsteil keine Maßnahmen zur Fehlererkennung vorgesehen. Einige Fehler werden funktionsbedingt erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ Das Wegeventil 1.1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. Das Wegeventil 1.2 ist für die Kategorie 3 nicht geeignet (z.B. Servoventil mit Null-Überdeckung).
- ☐ Der sicherheitsgerichtete Zustand wird bei beiden Lösungen jeweils durch Wegnahme des Steuersignals erreicht.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

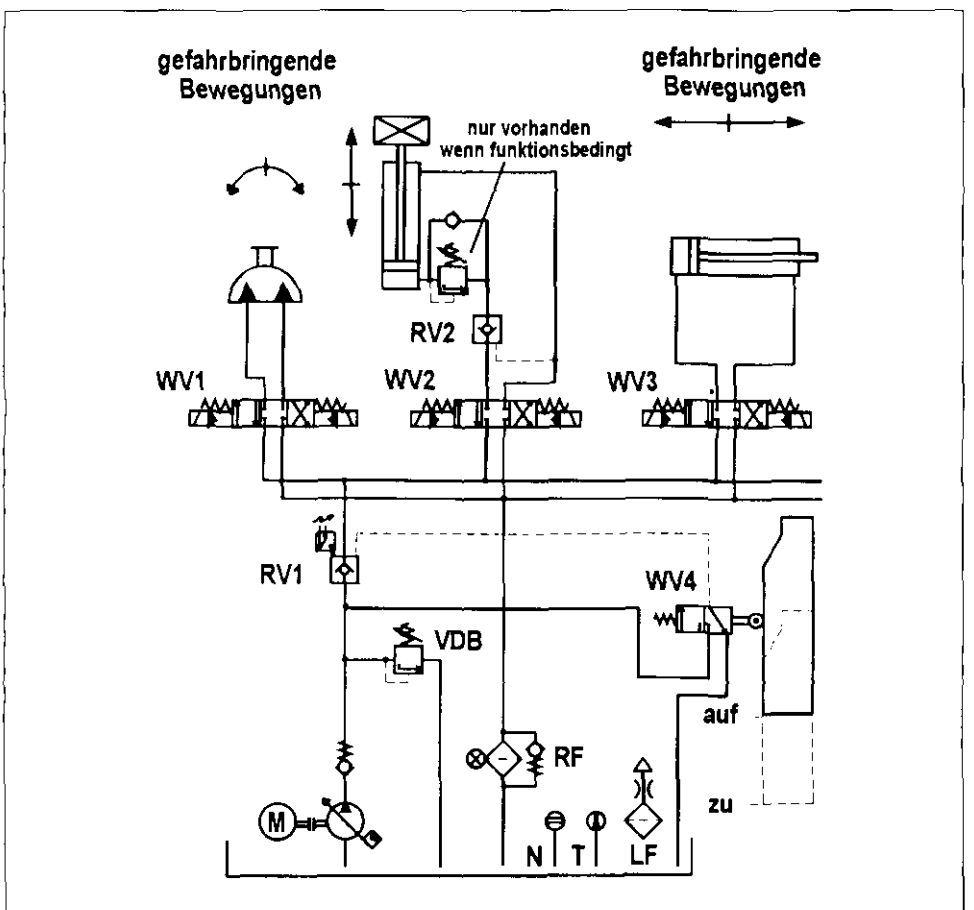
**Weiterführende Literatur:**

- ☐ *Kleinbreuer, W.*: Hydraulische und pneumatische Maschinensteuerungen mit abgestuften sicherheitstechnischen Maßnahmen für den Fehlerfall (Allgemeine Anforderungen, Schaltungsbeispiele, Fehlerliste). 16. Internationales Kolloquium, Berichtsband S. 69-76, Hrsg.: ISSA, Heidelberg

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 31:
*Elektro-hydraulische Steuerung nach EN 954 — Kategorie 3, mit Fehlererkennungsmaßnahme, zur Steuerung von gefahrbringenden Bewegungen*



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden durch jeweils zwei Wegeventile gesteuert (RV1 jeweils mit einem WV wirkend). Es existiert ein zusätzliches Sperrventil RV2 gegen eine Schließbewegung durch Massenkräfte.
- ☐ Der Ausfall eines von jeweils zwei der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ WV1 bis WV3 werden zyklisch angesteuert, RV1 schließt nur bei Öffnen der beweglich trennenden Schutzeinrichtung.
- ☐ Eine Maßnahme zur Fehlererkennung ist nur an RV1 vorgesehen. An den nicht überwachten Ventilen werden einige Fehler funktionsbedingt erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ Die Wegeventile WV1 bis WV3 haben Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. RV1 ist mit elektrischer Stellungsüberwachung ausgeführt, da RV1 nicht zyklisch schaltet.
- ☐ Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals (elektrisch bzw. hydraulisch) erreicht.
- ☐ Die Signalverarbeitung der elektrischen Stellungsüberwachung erfolgt z.B. in einer einkanaligen SPS.

**Anwendung:**

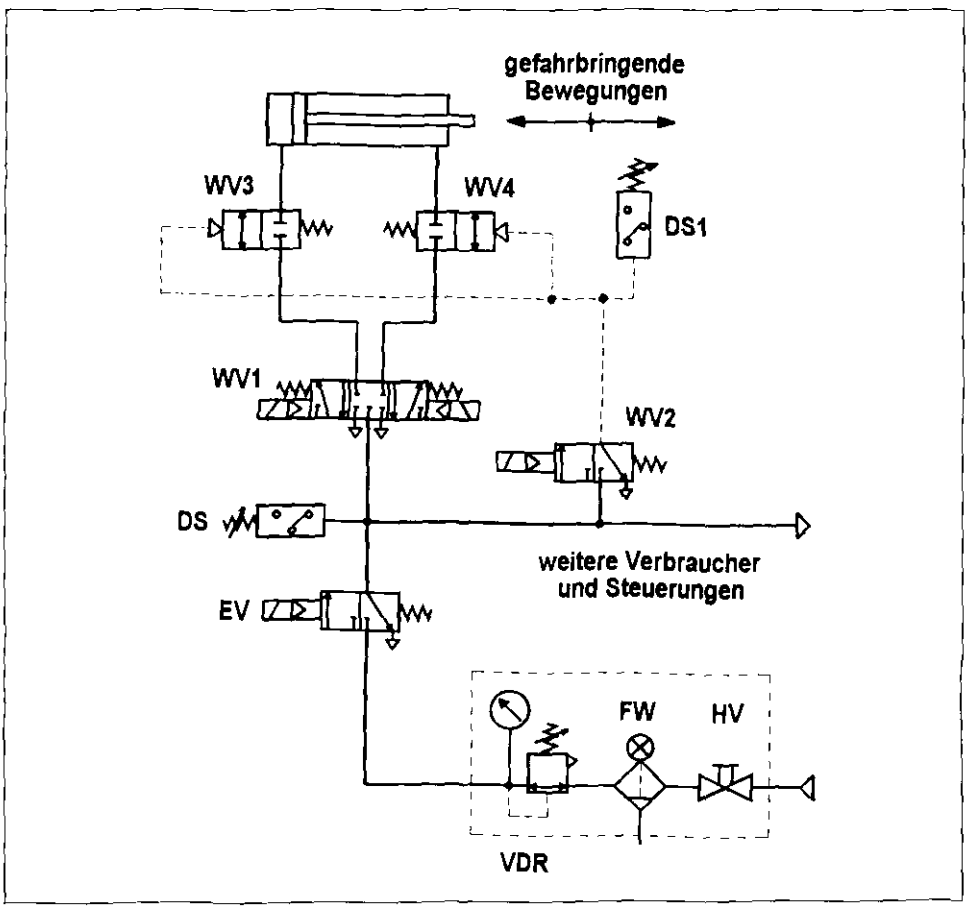
- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

- ☐ *Kleinbreuer, W.:* Hydraulische und pneumatische Maschinensteuerungen mit abgestuften sicherheitstechnischen Maßnahmen für den Fehlerfall (Allgemeine Anforderungen, Schaltungsbeispiele, Fehlerliste). 16. Internationales Kolloquium, Berichtsband S. 69-76, Hrsg.: ISSA, Heidelberg

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 32:
Elektro-pneumatische Steuerung nach EN 954 — Kategorie 3, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

- ☐ *Gefahrbringende Bewegungen oder Zustände werden durch jeweils zwei Wegeventile gesteuert (WV1 und WV3 bzw. WV1 und WV4).*
- ☐ Der Ausfall eines Wegeventils führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ Alle Wegeventile werden zyklisch angesteuert.
- ☐ Die Funktion des Vorsteuerventils WV2 wird durch den Druckschalter DS1 überwacht. An den nicht überwachten Ventilen werden einige Fehler funktionsbedingt erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ Das Wegeventil WV1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.
- ☐ Die Sperrventile WV3 und WV4 sind möglichst im Zylinder eingeschraubt und vorgesteuert über das Ventil WV2.
- ☐ Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- ☐ *Die Signalverarbeitung der Drucküberwachung (DS1) erfolgt z.B. in einer einkanaligen SPS.*

**Anwendung:**

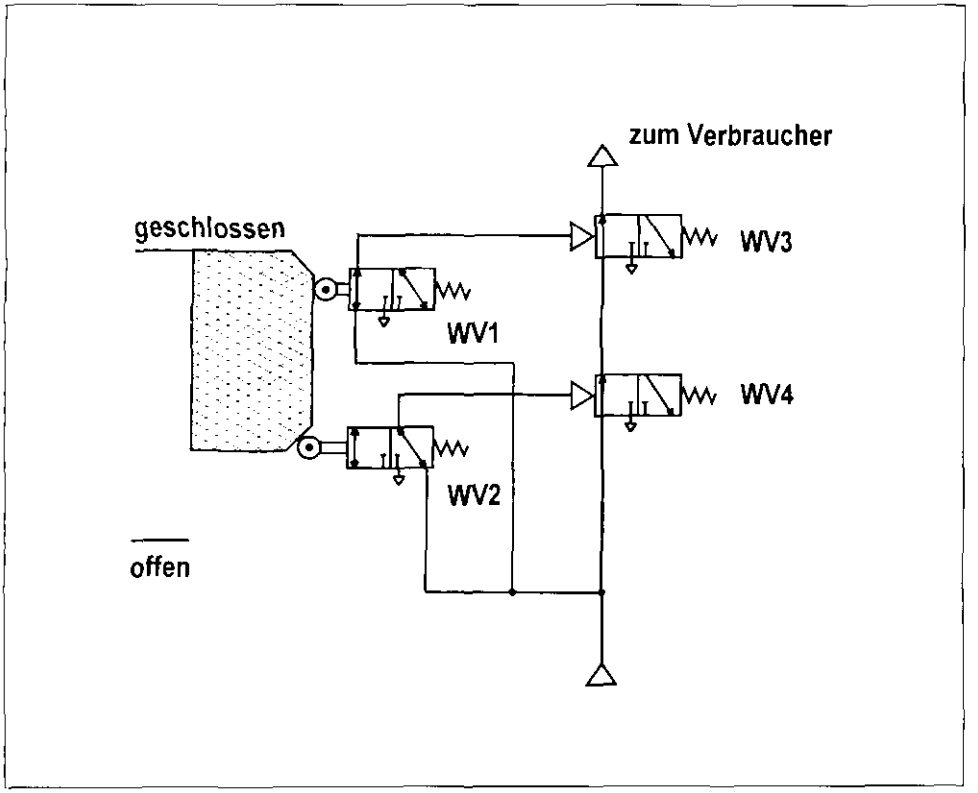
- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

- ☐ *Kleinbreuer, W.:* Konstruierte Sicherheit, Anforderungen an hydraulische und pneumatische Maschinensteuerungen. fluid (1992) Nr. 11/12

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 33:
Pneumatische Steuerung nach EN 954 — Kategorie 3,
Verriegelung beweglich trennender Schutzeinrichtung



**Funktionsbeschreibung:**

- ☐ Die Verriegelung der beweglich trennenden Schutzeinrichtung erfolgt durch zwei „pneumatische Positionsschalter" (WV1 und WV2). Diese geben jeweils einen Steuerbefehl an die Wegeventile WV3 und WV4.
- ☐ Energiezufuhr (pneumatisch) erfolgt nur bei geschlossener Schutzeinrichtung.
- ☐ Der Ausfall eines Wegeventils führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ Es sind (entsprechend einer Risikobewertung) keine Maßnahmen zur Fehlererkennung vorgesehen. Einige Fehler werden funktionsbedingt erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ WV2 ist ein pneumatischer Positionsschalter mit zwangläufiger Betätigung durch die beweglich trennende Schutzeinrichtung, entsprechend EN 1088.
- ☐ Die sicherheitsgerichtete Schaltstellung der Wegeventile WV3 und WV4 wird durch Wegnahme der Steuersignale erreicht.

**Anwendung:**

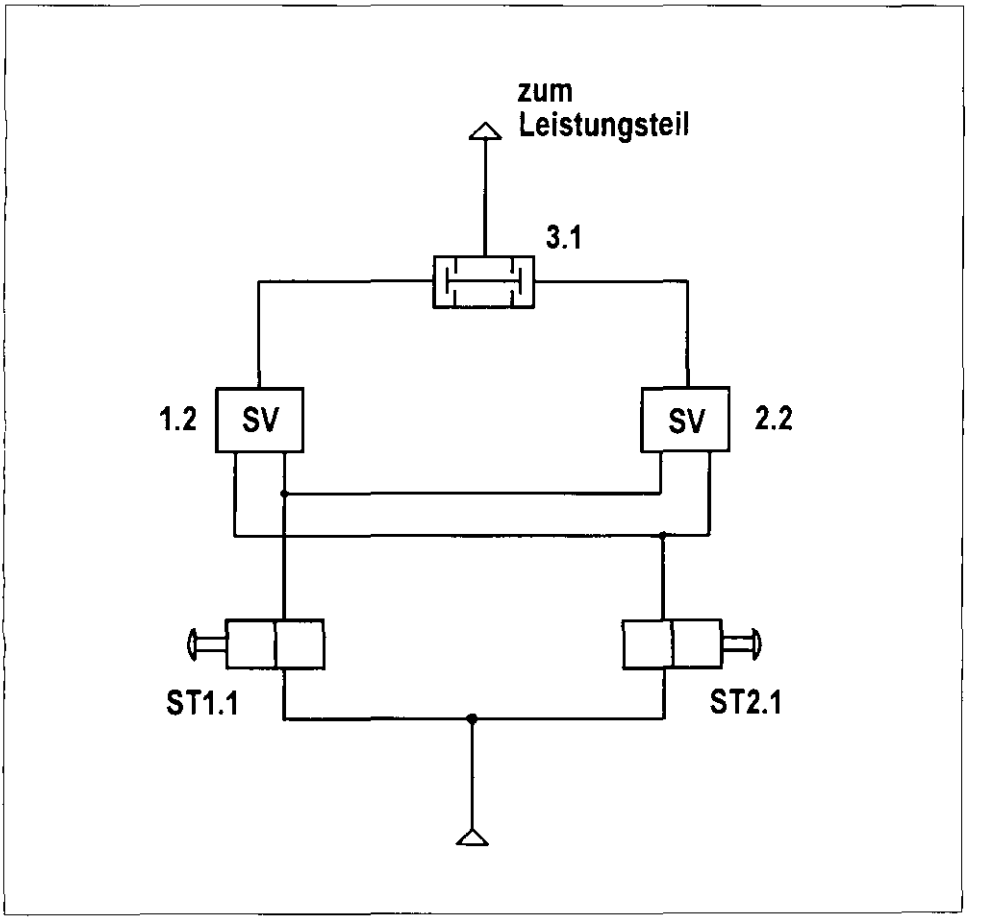
- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**


- ☐ *Kleinbreuer, W.*: Anforderungen an hydraulische und pneumatische Maschinensteuerungen. Sichere Chemiearbeit (1992) Nr. 2 und Nr. 3
- ☐ *EN 1088: Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung* mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 34:
Pneumatische Steuerung nach EN 954 — Kategorie 3,
für Zweihandsteuerung, realisiert durch zwei „handelsübliche Zweihandbausteine"



**Funktionsbeschreibung:**

- ☐ *Gefahrbringende Bewegungen oder Zustände werden durch synchrone* Betätigung der Stellteile ST1.1 und ST2.1 über die Signalverarbeitungen SV von einem Steuersignal am Ausgang des UND-Gliedes 3.1 gesteuert.
- ☐ *Der Ausfall einer Signalverarbeitung SV führt nicht zum Verlust der Sicherheits*funktion.
- ☐ Es sind (entsprechend einer Risikobewertung) keine Maßnahmen zur Fehlererkennung vorgesehen. *Einige Fehler werden funktionsbedingt erkannt. Die Anhäufung* unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

***Konstruktive Merkmale:***

- ☐ Die pneumatischen Signalverarbeitungen SV1.2 und SV2.2 bestehen aus „handelsüblichen Zweihandbausteinen".
- ☐ Die sicherheitsgerichtete Schaltstellung der pneumatischen Bauteile wird durch Wegnahme der Steuersignale erreicht.
- ☐ Die Signalverarbeitungen SV1.2 und SV2.2 erfüllen die Anforderungen bzgl. der Beziehung zwischen Eingangssignalen und Ausgangssignal, Beendigung des Ausgangssignals, erneutes Erzeugen des Ausgangssignals und synchroner Betätigung nach EN 574.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

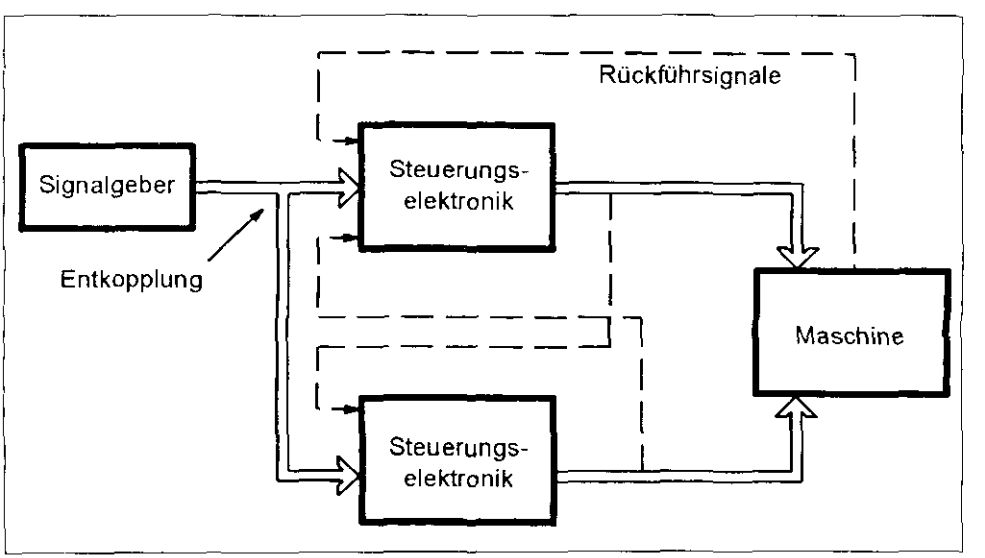
**Weiterführende Literatur:**


- ☐ *Kleinbreuer, W., und Kühlem, W.*: Pneumatische Zweihandschaltungen, Technische Realisierung und Ergebnisse von experimentellen Untersuchungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 242. In: BIA-Handbuch 18.Lfg. VI/92 Erich Schmidt Verlag, Bielefeld
- ☐ EN 574: Sicherheit von Maschinen, Zweihandschaltungen, Funktionelle Aspekte — Gestaltungsleitsätze

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektroniksteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 35:
Elektroniksteuerung nach EN 954 — Kategorie 3
Grobstruktur der Steuerung



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden von zwei Kanälen unabhängig voneinander aber in Abhängigkeit vom Signalgeber gesteuert.
- ☐ Eine Fehlererkennung wird für die Peripherieelemente durchgeführt.
- ☐ Eine Ungleichheit in den Ausgangssignalen oder eine Fehlererkennung in den Peripherieelementen führt zum Auslösen der Sicherheitsfunktion.

**Konstruktive Merkmale:**

- ☐ Die Maschinenreaktion wird auf ihr sicherheitstechnisches Verhalten über die Rückführsignale überwacht.
- ☐ Eine Rückführung der Maschinenreaktion durch zwangsgeführte Kontakte ist möglich.
- ☐ Abhängig von der Maschinenreaktion lassen sich häufig zahlreiche Plausibilitätskontrollen zur Fehlererkennung nutzen.
- ☐ Statische Signalgeber müssen ebenfalls redundant ausgeführt werden.
- ☐ Bei der Verdrahtung der Signalgeber in beide Kanäle ist darauf zu achten, daß die Eingänge so entkoppelt (z.B. durch Entkopplungsdioden) werden, daß ein Fehler in einem Kanal nicht den anderen Kanal in gleicher Weise ausfallen läßt.

**Anwendung:**

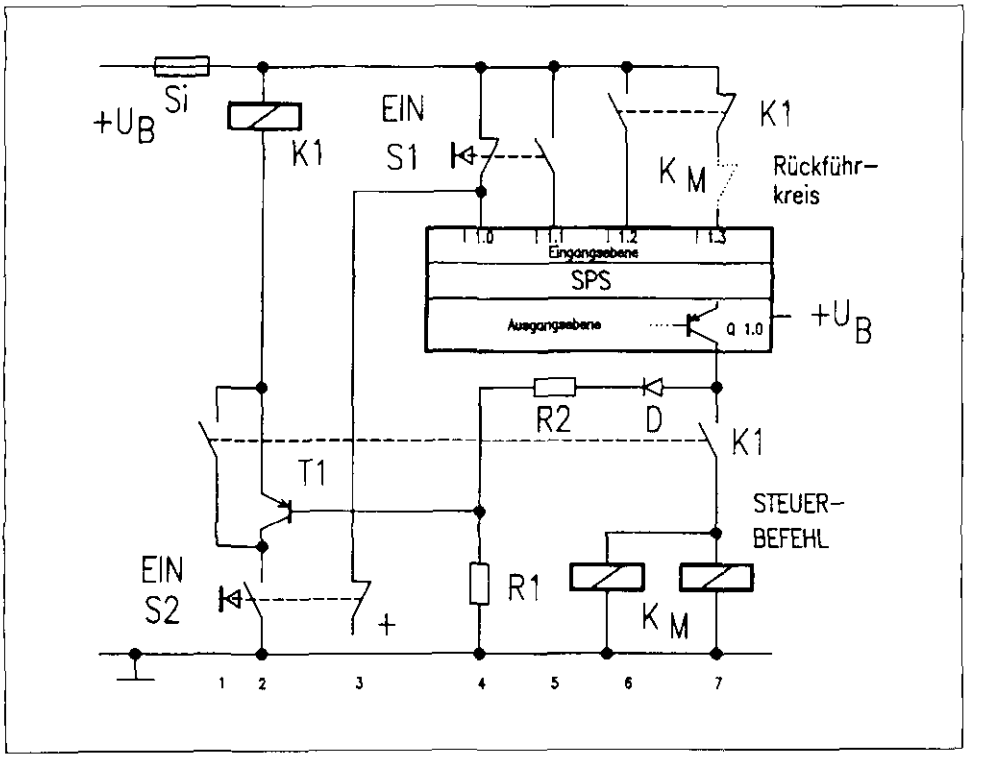
- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**


- ☐ *Jürs, H.; Reinert, D.*: Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93 Erich Schmidt Verlag, Bielefeld
- ☐ *Grigulewitsch, W.; Meffert, K.*: Redundante Schaltungstechniken. Sicherheitstechnisches Informations- und Arbeitsblatt 330 226. In: BIA-Handbuch 10. Lfg. X/88 Erich Schmidt Verlag, Bielefeld

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 36:
Rechnersteuerung nach EN 954 — Kategorie 3
Zweihandschaltung realisiert durch eine Standard-SPS nach EN 574 Typ II
ohne Zeitvorgabe für eine synchrone Betätigung



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung oder Zustand kann nur durch die Betätigung beider Befehlsgeber S1 und S2 eingeleitet werden, indem K1 in Selbsthaltung gebracht und Q 1.0 eingeschaltet wird (die Zweihandbedingung wird ausschließlich durch die Software realisiert).
- ☐ Vor dem Drücken der Befehlsgeber S1 und S2 ist der Ausgang Q 1.0 auf LOW-Potential geschaltet und K1 entregt. Eine Steuerbefehlsgabe ist somit redundant verhindert.
- ☐ Ein fehlerhaftes HIGH-Potential an Q 1.0 führt nach dem Loslassen von S2 zum bleibenden Abfall von K1 — Transistor T1 sperrt — und verhindert sowohl das Anstehen eines Steuerbefehls als auch eine nochmalige Steuerbefehlsgabe beim erneuten Betätigen von S2.
- ☐ Durch keinen Fehler nach Fehlerliste ist eine Einhandschaltung möglich.
- ☐ Eine fast vollständige Fehlererkennung in den Peripherieelementen wird durch die Eingänge I 1.1, I 1.2 und I 1.3 erreicht.

**Konstruktive Merkmale:**

- ☐ Für beide Befehlsgeber sind Taster mit Doppelkontakten vorgesehen, damit auch beim Nichtöffnen eines Kontaktes eine gewollte Betätigung der Tasten Voraussetzung für einen gültigen Steuerbefehl bleibt. Das mechnische Versagen eines der Befehlsgeber wird über die Rückstellkontrolle aufgedeckt.
- ☐ K1 ist ein Relais mit zwangsgeführten Kontakten.
- ☐ Für die sichere Funktion der Schaltung sind alle Relais-/Schützspulen mit Funkenlöschgliedern versehen worden.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

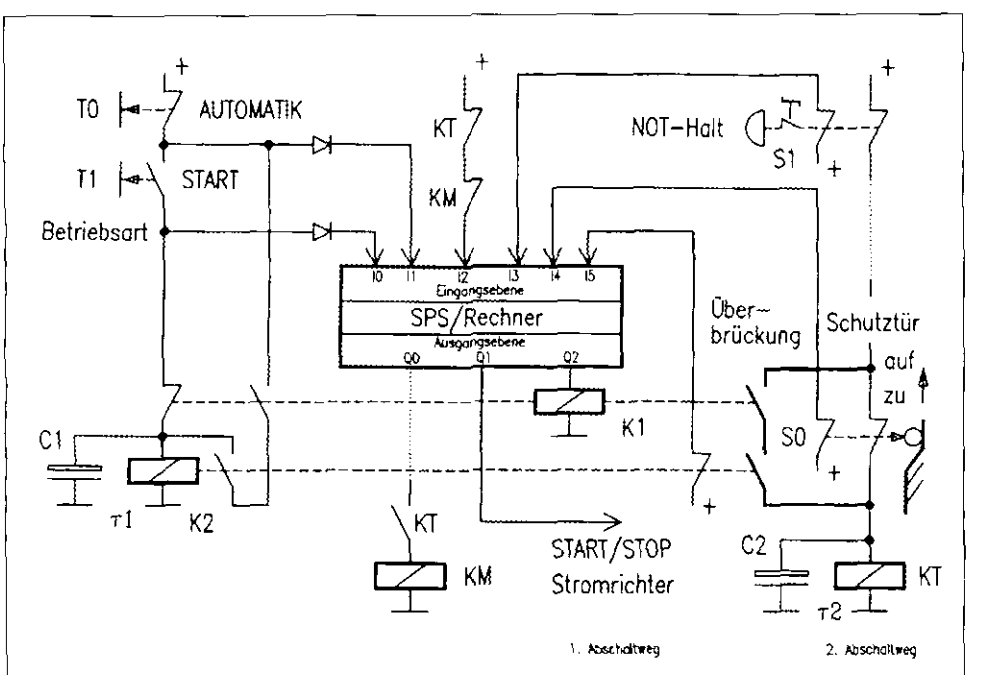
**Weiterführende Literatur:**


- ☐ *Grigulewitsch, W.; Reinert, D.*: Zweihandschaltungen nach Anforderungsstufe II in DIN 24 980. Sicherheitstechnisches Informations- und Arbeitsblatt 330 229. In: BIA-Handbuch 17. Lfg. X/91 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 37:
Rechnersteuerung nach EN 954 — Kategorie 3
Dauerhafte Überbrückung eines Schutztürkontaktes im Einrichtbetrieb bei Verwendung einer Standard-SPS, z.B. beim Tippen mit sicher reduzierter Geschwindigkeit



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter mit Hilfe einer speicherprogrammierbaren Steuerung (SPS) und einer separaten Hardware verhindert bzw. unterbrochen. Der zwangsöffnende Positionsschalter S0 ist dann betätigt und das Relais/Schütz KT wird verzögert entregt. Mit dem Abfall von KT ist das Entregen des Netzschützes KM und damit die Unterbrechung der Energiezufuhr zum Antrieb des im Bild nicht dargestellten Stromrichters verbunden.
- ☐ Die Überbrückung des Öffnerkontaktes S0, der das Entregen des Relais/Schützes KT bewirkt, wird redundant vorgenommen, nämlich zum einen SPS-gesteuert (Ausgang Q2) mit dem Relais K1, zum anderen unabhängig von der SPS mit dem Relais K2.
- ☐ Voraussetzung für das Tippen mit sicher reduzierter Geschwindigkeit ist das Abgefallensein der Schütze KT und KM und die geöffnete Schutztür. Bei betätigtem START-Taster T1 erreicht K2 nur dann die Selbsthaltung, wenn K1 SPS-gesteuert zuerst abgefallen ist und anschließend innerhalb einer Zeitvorgabe $\tau 1$ angezogen hat. Erst wenn beide Relais zum Anzug gekommen sind, ist die Überbrückung des Schutztürüberwachungskontaktes S0 erreicht und die START-Taste T1 kann losgelassen werden. Mit dem Anzug des Schützes KT kann dann auch das Netzschütz KM erregt werden. Dies ist die Vorbedingung für das Auslösen einer Maschinenbewegung durch das Setzen des SPS-Ausganges Q1 (START-Signal für Stromrichter).
- ☐ Eine Fehlererkennung wird für die Peripherieelemente K1, K2, KT und KM über die SPS-Software durchgeführt und führt zur Betriebshemmung. Eine dauerhafte Überbrückung der Schutztür ist dadurch wirksam verhindert.

**Konstruktive Merkmale:**

- ☐ Der Schalter S0 ist ein zwangsöffnender Positionsschalter entsprechend EN 1088.
- ☐ Die Relais K1, K2, KT und KM haben zwangsgeführte Kontakte.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

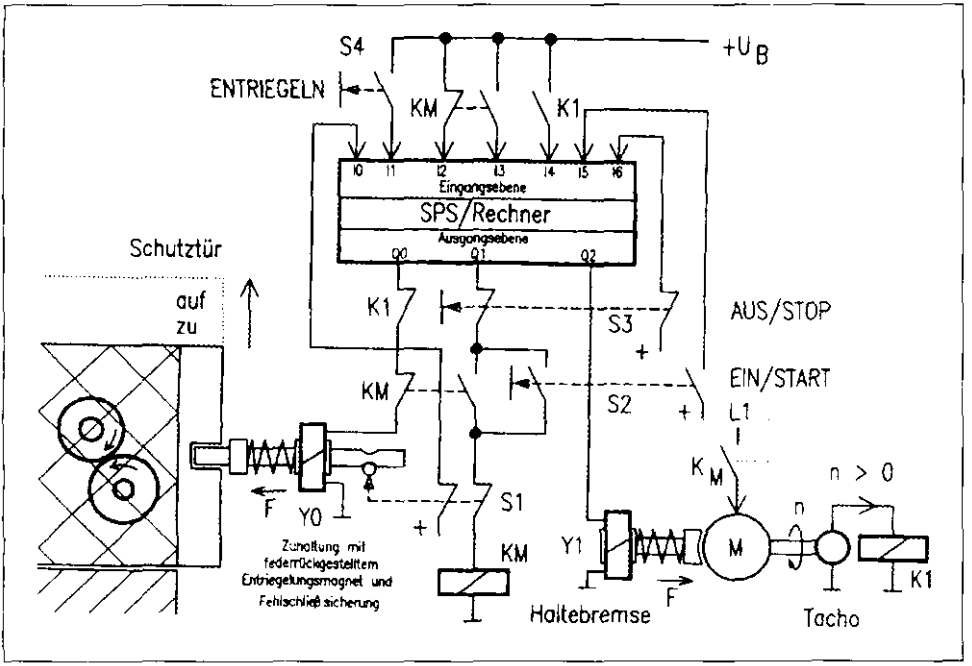
**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 38:
Rechnersteuerung nach EN 954 — Kategorie 3
Zuhaltung einer Schutztür mit einer Standard-SPS




**Funktionsbeschreibung:**

- Voraussetzung für das Ingangsetzen einer gefahrbringenden Maschinenbewegung ist die geschlossene Schutztür. Ein Öffnen der Tür ist nur möglich durch Ziehen des Bolzens bei erregtem Entriegelungsmagnet Y0.
- Die Stellungsüberwachung des Sperrbolzens erfolgt allein über den zwangsöffnenden Positionsschalter S1. Ein Öffnerkontakt S1 wird direkt durch die SPS über den Eingang I0 abgefragt. Der andere Öffnerkontakt wirkt unmittelbar auf das Motorschütz KM, dessen Schließer- und Öffnerkontakt jeweils auf einen Eingang der SPS (I2/I3) geführt sind.
- Beim Betätigen des EIN/START-Tasters S2 aktiviert die SPS über den Eingang I5 zuerst den zum Lösen der Haltebremse zuständigen Ausgang Q2, danach erfolgt die Ansteuerung des Motorschützes KM durch Setzen des Ausganges Q1. Mit dem Anzug von KM kann S2 losgelassen werden. KM erreicht die Selbsthaltung, sowohl in der Ausgangsebene der SPS als auch über die Abfrage des Schließerkontaktes KM mit dem

Eingang I3 in der SPS-Eingangsebene. Das nach dem Anzug von KM aktivierte Tachosignal erregt das zwangsgeführte Relais K1 ab einer Drehzahl $n > 0$, welches am Eingang I4 der SPS die ordnungsgemäße Drehbewegung des Motors anzeigt.

- ☐ Ein gegebener AUS/STOP-Befehl über das Betätigen der Taste S3 unterbricht direkt im Ausgangskreis Q1 der SPS die Ansteuerung des Motorschützes KM und damit dessen Selbsthaltung. Das Schließen des Öffnerkontaktes KM am Eingang I2 startet im Anwenderprogramm eine Bremszeitvorgabe, nach deren Ablauf die Magnetspule Y1 durch Rücksetzen des SPS-Ausganges Q2 stromlos geschaltet wird. Die Bremse des Motors fällt durch Federkraft ein und fixiert seine Ruhelage. Die Bremszeitvorgabe ist so bemessen, daß auch unter ungünstigen Betriebsbedingungen die Maschinenbewegung immer vor dem Einfallen der Bremse zum Stillstand gekommen ist.
- ☐ Voraussetzungen für das Öffnen der Schutztür und die dazu erforderliche Entriegelung der Zuhaltung durch die SPS sind, daß vor Betätigung des Tasters S4 (ENTRIEGELN) das Motorschütz KM abgefallen (Eingang I2 führt HIGH-Potential), die im Anwenderprogramm der SPS realisierte Bremszeitvorgabe abgelaufen und ein Stillstand der Bewegung (Eingang I4 führt LOW-Potential) signalisiert worden ist. Nur dann aktiviert das Anwenderprogramm der SPS den Ausgang Q0 und veranlaßt durch Stromfluß über die Öffnerkontakte KM und K1 das Erregen der Magnetspule Y0 und damit das Ziehen des Sperrbolzens.
- ☐ Bei einem Versagen der SPS wird das Öffnen der Schutztür verhindert, weil der zur Entriegelung der Zuhaltung notwendige Strom durch die Magnetspule Y0 wegen des dann erregten Relais K1 nicht fließen kann.
- ☐ Ein einzelnes Versagen der Zuhaltung wird — ebenso wie das Versagen des Tachogenerators bzw. des Relais K1 oder des Motorschützes KM — durch Plausibilitätsprüfungen und Zeitvorgaben im Anwenderprogramm der SPS aufgedeckt und in Folge die Schutztür verriegelt oder die gefahrbringende Bewegung stillgesetzt.

**Konstruktive Merkmale:**

- ☐ In der Schutzstellung wird die Tür formschlüssig mit dem in den Türrahmen hineinragenden Sperrbolzen der Zuhaltung verbunden und so geschlossen gehalten.
- ☐ Der Schalter S1 ist ein zwangsöffnender Positionsschalter entsprechend EN 1088. Die Zuleitungen zu dem Positionsschalter sind geschützt verlegt.
- ☐ Die Relais K1/KM haben zwangsgeführte Kontakte.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

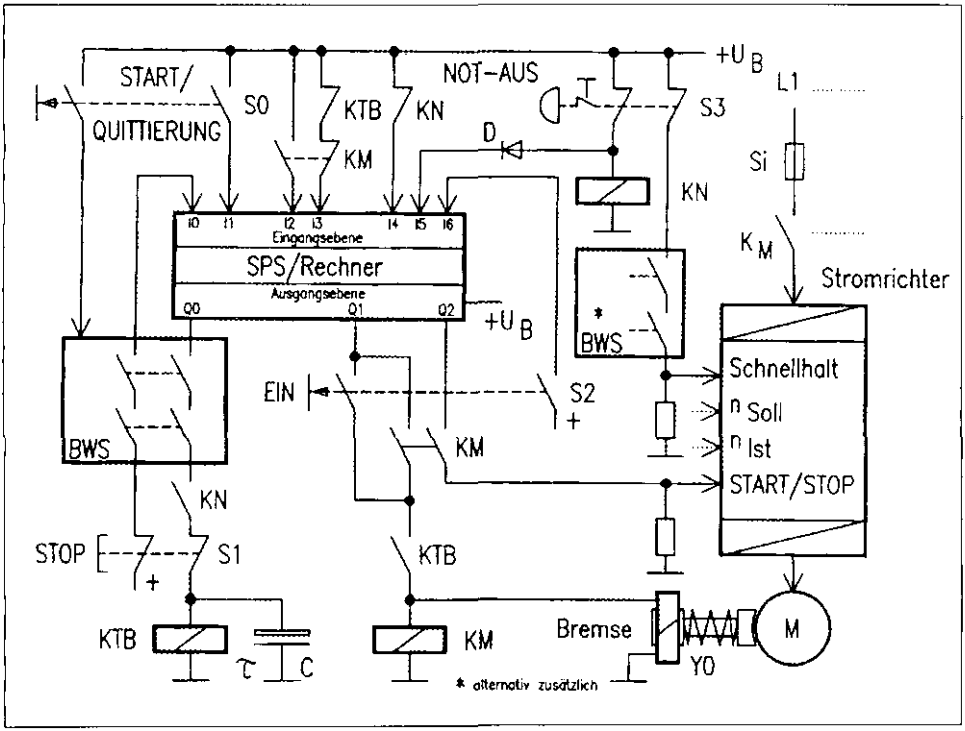
**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 39:
Rechnersteuerung nach EN 954 — Kategorie 3
Stillsetzen eines SPS-gesteuerten Stromrichterantriebes gemäß STOP-Kategorie 1 in EN 60 204:
— nach einem NOT-AUS-Befehl,
— nach einem STOP-Befehl oder
— nach dem Ansprechen einer Schutzeinrichtung (hier BWS)



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung wird redundant verhindert oder unterbrochen, wenn eine der Schutzeinrichtungen oder der NOT-AUS-Taster betätigt wurden. Das Stillsetzen des Antriebes im Notfall erfolgt nach Betätigung eines NOT-AUS-Schalters schnellstmöglich zuerst über den am Stromrichter zur Verfügung stehenden „Schnellhalt"-Eingang. Erst nach Ablauf einer in der SPS voreingestellten Zeitvorgabe (Starten der Zeitvorgabe mit LOW-Potential am Eingang I5) erfolgt, mit dem Zurücksetzen der SPS-Ausgänge Q0 bis Q2, das Entregen des Netzschützes KM und das Einfallen der Bremse Y0. Parallel hierzu wird mit dem Öffnen des Öffnerkontaktes des NOT-AUS-Schalters das Schütz KN entregt, mit dem kontaktbehaftet und unabhängig von der SPS zuerst das Zeitglied KTB/C und damit wiederum KM zum Abfallen gebracht werden.
- ☐ Das funktionsgemäße Stillsetzen des Antriebes nach einem STOP-Befehl oder nach dem Ansprechen einer Schutzeinrichtung wird eingeleitet durch Rücknahme des START/STOP-Signales am Stromrichter (LOW-Potential) mit dem SPS-Ausgang Q2 **(1. Abschaltweg!)**. Das mit dem Ansprechen einer Schutzeinrichtung oder einem STOP-Befehl verbundene Unterbrechen des Stromkreises zum Schütz KTB über C startet eine Bremszeitvorgabe, nach deren Ablauf die Ansteuerung für das Netzschütz KM unterbrochen wird **(2. Abschaltweg!)**. Die Zeitvorgabe ist so gewählt, daß unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird, noch bevor das Netzschütz KM abfällt.
- ☐ Beim Versagen der SPS, des Stromrichters oder des Zeitgliedes KTB/C wird jeweils die Stillsetzung des Antriebes sichergestellt, weil immer zwei voneinander unabhängige Abschaltwege vorhanden sind.
- ☐ Das Nichtabfallen der Schütze KM, KN oder KTB wird, wegen der vorhandenen Abfrage der zwangsgeführten Öffnerkontakte durch die SPS, spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung aufgedeckt.

**Konstruktive Merkmale:**

- ☐ Alle verwendeten Schutzeinrichtungen entsprechen mindestens der Kategorie 3.
- ☐ Die Relais/Schütze KN, KTB und KM haben zwangsgeführte Kontakte.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

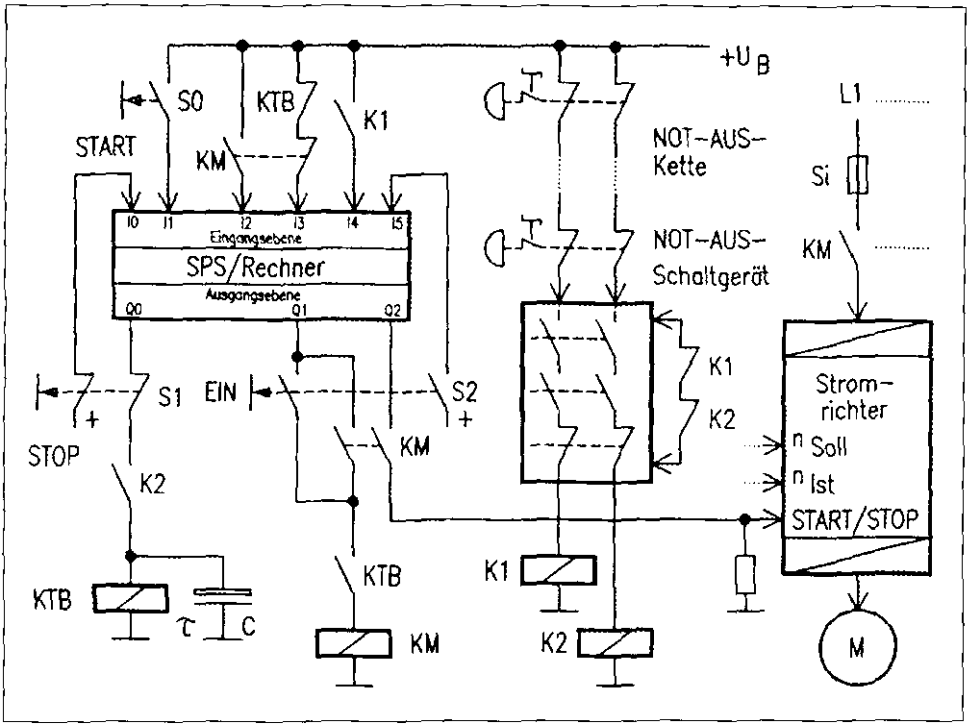
**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 40:
Rechnersteuerung nach EN 954 — Kategorie 3
Stillsetzen eines SPS-gesteuerten Stromrichterantriebes gemäß STOP-Kategorie 1 in EN 60 204 nach einem NOT-AUS-Befehl



Funktionsbeschreibung:

- ☐ Eine gefahrbringende Bewegung wird redundant verhindert oder unterbrochen, wenn eine der Schutzeinrichtungen oder der NOT-AUS-Taster betätigt wurden. Das Stillsetzen des Antriebes im Notfall erfolgt nach Betätigung eines NOT-AUS-Schalters schnellstmöglich zuerst durch Deaktivierung des NOT-AUS-Schaltgerätes einhergehend mit dem Entregen der Schütze K1 und K2. Das Öffnen des Schließerkontaktes K1 am SPS-Eingang I4 bewirkt die Rücknahme des START-Signales am Stromrichter (SPS-Ausgang Q2 führt LOW-Potential; **1. Abschaltweg!**). Mit dem Öffnen des Schließerkontaktes K2 vor dem Zeitglied KTB/C startet eine Bremszeitvorgabe, nach deren Ablauf die Ansteuerung für das Netzschütz KM unterbrochen wird **(2. Abschaltweg!)**. Die Zeitvorgabe ist so gewählt, daß unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird, noch bevor das Netzschütz KM abfällt. Das funktionsgemäße Stillsetzen des Antriebes nach einem STOP-Befehl wird eingeleitet mit dem Öffnen der Öffnerkontakte der STOP-Taste S1 und deren Abfrage durch den SPS-Eingang I0. Die Absteuerung des Stromrichters beginnt mit dem Rücksetzen des SPS-Ausganges Q2 ganz analog zu Stillsetzen im Notfall.
- ☐ Bei einem einzelnen Versagen der SPS, des Stromrichters, des Zeitgliedes KTB/C oder der Schütze K1/K2 wird jeweils das Stillsetzen des Antriebes sichergestellt, weil immer zwei voneinander unabhängige Abschaltwege vorhanden sind.
- ☐ Das Nichtabfallen der Schütze KM oder KTB wird, wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in den SPS-Eingang I3, spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung aufgedeckt. Ein Nichtabfallen der Schütze K1 und K2 wird durch Überwachung der Öffnerkontakte innerhalb des NOT-AUS-Schaltgerätes, spätestens nach dem Entriegeln des betätigten NOT-AUS-Schalters, aufgedeckt.

Konstruktive Merkmale:

- ☐ Alle verwendeten Schutzeinrichtungen entsprechen mindestens der Kategorie 3.
- ☐ Die Relais/Schütze KN, KTB und KM haben zwangsgeführte Kontakte.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

Anwendung:

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

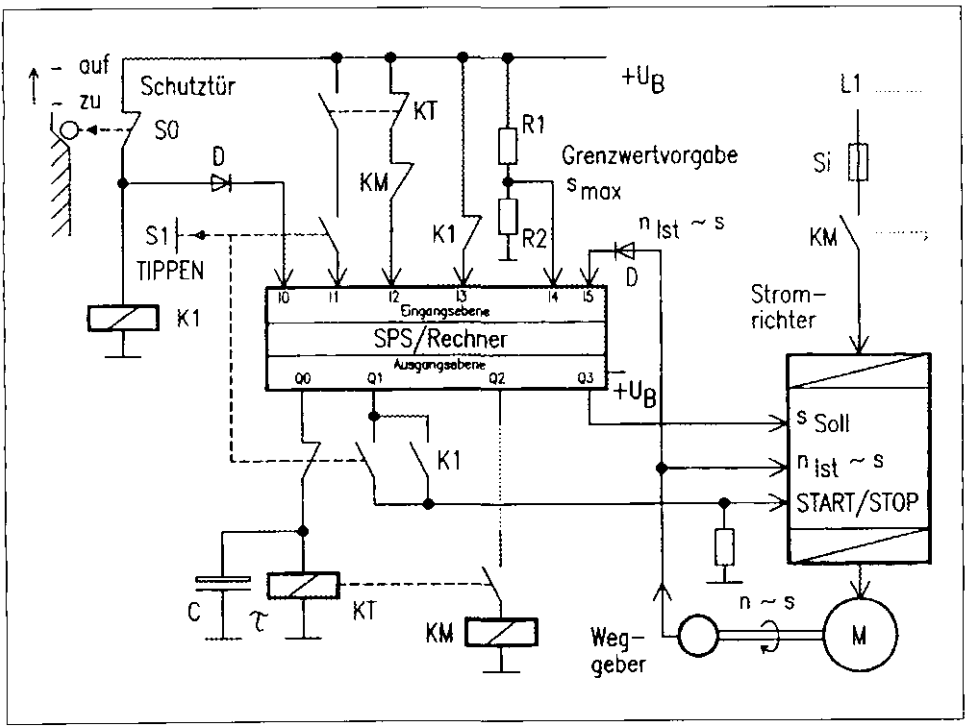
Weiterführende Literatur:

- ☐ *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 41:
Rechnersteuerung nach EN 954 — Kategorie 3
Wegbegrenztes Tippen mit SPS und separatem Zeitglied
zur Wegüberwachung im Einrichtbetrieb



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung wird bei geöffnetem Schutzgitter redundant verhindert oder unterbrochen. Bei geöffnetem Schutzgitter wird wegbegrenzter Tippbetrieb eingestellt. Der zwangsöffnende Positionsschalter S0 ist dann betätigt und das Relais/Schütz K1 entregt. Eine Aktivierung des START/STOP-Signals am Stromrichter kann durch den SPS-Ausgang Q1 nur bei betätigter TIPP-Taste S1 erfolgen. *Die Soll-Grenzwertvorgabe für den Weg* $s_{max}$ *am* SPS-Eingang I4 ist nur einmal vorhanden und wird über den SPS-Ausgang Q3 als Digitalinformation an den Stromrichter weitergegeben. Als redundante Maßnahme zur Wegermittlung wird bei jeder Betätigung des TIPP-Tasters S1 das als separate Hardware vorhandene Zeitglied KT/C angestoßen.
- ☐ Beim Versagen der SPS, des Stromrichters, des Weggebers oder bei einer falschen Soll-Grenzwertvorgabe wird die Abschaltung des Motorantriebes spätestens nach Ablauf der Zeitvorgabe durch das übergeordnet wirkende Zeitglied KT/C sichergestellt. Das Versagen des Zeitgliedes KT/C (z.B. bei Nichtabfall von KT) wird, ebenso wie das Nicht-Abfallen von KM, über das Abfragen der zwangsgeführten Öffnerkontakte durch die SPS (Eingang I2) aufgedeckt. Das Abfallen dieser Relais/Schütze nach jeder Absteuerung des Stromrichters ist Bedingungung für ein erneutes Ingangsetzen des Antriebes.

**Konstruktive Merkmale:**

- ☐ K1,K2, KT und KM sind Relais/Schütze mit zwangsgeführten Kontakten.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

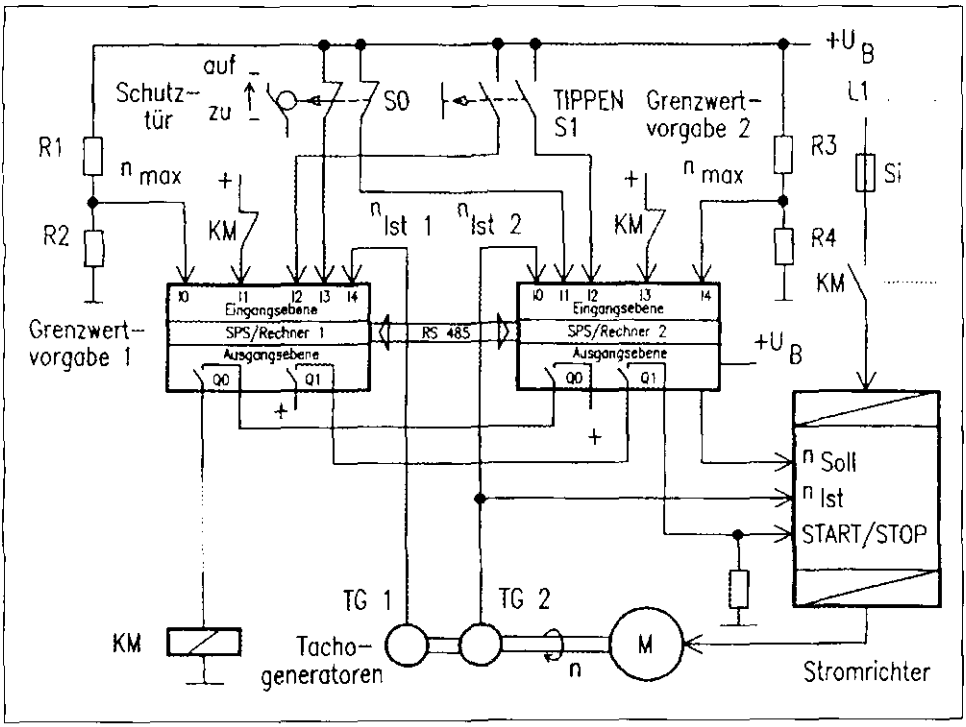
**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 42:
Rechnersteuerung nach EN 954 — Kategorie 3
SPS-Redundanz zur Erzeugung einer sicher reduzierten Geschwindigkeit mit jeweils separatem Soll-/Istvergleich in den Verarbeitungskanälen und getrennten Drehzahl-Grenzwertvorgaben



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung wird bei geöffnetem Schutzgitter redundant verhindert oder unterbrochen. Bei geöffnetem Schutzgitter wird reduzierte Geschwindigkeit eingestellt. Beide Verarbeitungskanäle erhalten an den Eingängen I0 (SPS1) und I4 (SPS2) jeweils voneinander unabhängige Soll-Grenzwertvorgaben. Auch die Abfrage der Ist-Drehzahl der reduzierten Geschwindigkeit an den Eingängen I4 (SPS1) und I0 (SPS2) erfolgt über voneinander unabhängige Tachogeneratoren. Unabhängig voneinander führt jeder Kanal den Soll-/Ist Vergleich durch.

- ☐ Über eine vorhandene serielle Schnittstelle (z.B. RS 485) wird der Austausch auch sicherheitsrelevanter Daten vorgenommen, z.B. zwecks Fehlerkennung durch Zustandsvergleich der beiden SPS bzw. Rechner.

- ☐ Beim Versagen eines Verarbeitungskanals erfolgt die Abwärtssteuerung des Stromrichters sowie des Netzschützes durch jeweils den anderen noch funktionierenden Kanal. Ein Versagen des Stromrichters, das z.B. zum unerwarteten Anlaufen, Weiterlaufen oder zu einer Erhöhung der Drehzahl führen kann, wird über die getrennte Erfassung der Drehzahlen durch die Tachogeneratoren TG 1 und TG 2 in beiden Verarbeitungskanälen erkannt. Das Nichtabfallen des Netzschützes KM wird über die in beide SPS bzw. Rechner geführten Öffnerkontakte (Eingänge I1 bzw. I3) bemerkt und führt zur Sperrung des START/STOP-Signales am Stromrichter durch beide Verarbeitungskanäle. Fehler oder Störungen der Schnittstelle werden z.B. durch Testmuster oder Tests im Übertragungsprotokoll mit mittlerer Wirksamkeit beherrscht.

**Konstruktive Merkmale:**

- ☐ KM ist ein Relais/Schütz mit zwangsgeführten Kontakten.

- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

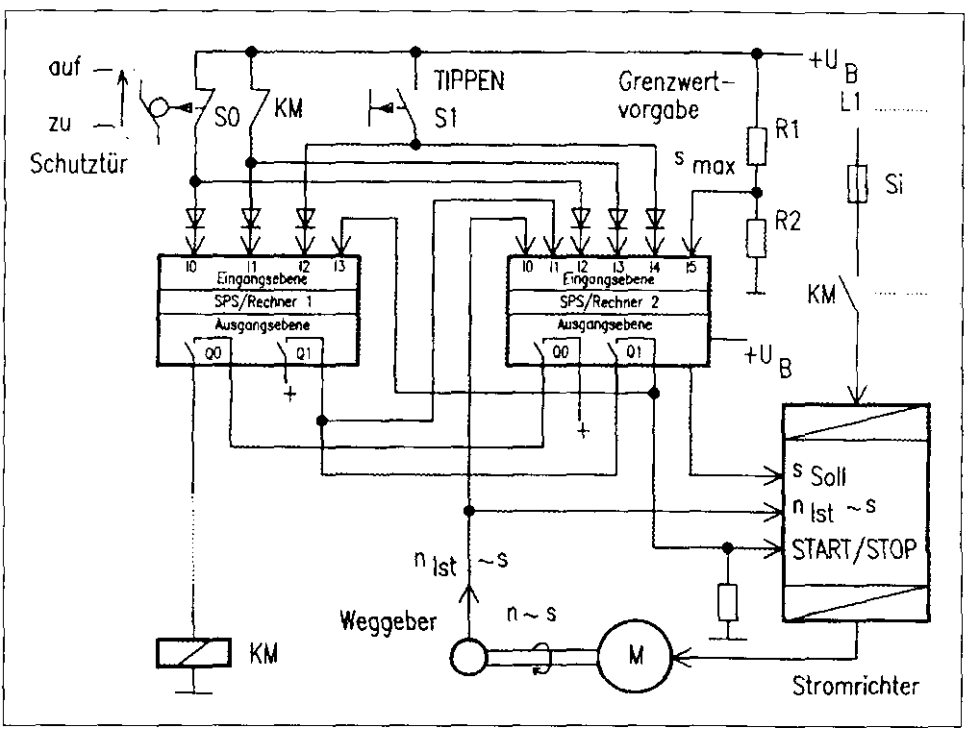
- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

***Weiterführende Literatur:***


- ☐ *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 43:
Rechnersteuerung nach EN 954 — Kategorie 3
Wegbegrenztes Tippen mit SPS-Redundanz und Ausgangsvergleich



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung wird bei geöffnetem Schutzgitter redundant verhindert oder unterbrochen. Bei geöffnetem Schutzgitter wird wegbegrenzter Tippbetrieb eingestellt. Die Soll-Grenzwertvorgabe für den Weg $s_{max}$ ist nur einmal vorhanden und wird von SPS2 als Digitalinformation am Ausgang Q2 an den Stromrichter weitergegeben. Als redundante Maßnahme zur Wegerfassung in SPS2 ist die Zeitvorgabe allein in SPS1 realisiert.
- ☐ Bei einer Wegüberschreitung erfolgt zuerst die Abwärtssteuerung des Stromrichters über den Ausgang Q1 der SPS2 durch Rücknahme des START/STOP-Signales am Stromrichter. SPS1 erwartet innerhalb seiner Zeitvorgabe diese Rücknahme des START/STOP-Signales. Bleibt die Abwärtssteuerung durch SPS2 aus, übernimmt dies SPS1 durch Rücksetzen des Ausganges Q1. Zusätzlich wird durch SPS1 das Netzschütz KM über den Ausgang Q0 entregt.
- ☐ Beim Versagen von SPS2, des Stromrichters, des Weggebers oder bei falscher Soll-Grenzwertvorgabe wird die Abschaltung des Motorantriebes spätestens nach Ablauf der Zeitvorgabe in SPS1 über die Ausgänge Q1 und Q0 sichergestellt.
- ☐ Das Versagen einer SPS bzw. eines Rechners wird, aufgrund der Rückführung der Ausgänge und durch die festgelegte Reihenfolge beim An- und Absteuern des Stromrichters, durch Plausibilitätsprüfung in beiden Verarbeitungskanälen aufgedeckt. Das Nichtabfallen des Netzschützes KM wird über den von beiden Verarbeitungskanälen abgefragten Öffnerkontakt KM (Eingänge I1 bzw. I3) bemerkt. Über das Abschalten des START/STOP-Einganges am Stromrichter (LOW-Potential!) durch beide SPS-Ausgänge Q1 wird im Fehlerfall der Stillstand der Maschinenbewegung eingeleitet und durch Speicherung des fehlerhaften Zustandes ein erneutes Ingangsetzen verhindert.

**Konstruktive Merkmale:**

- ☐ Die notwendige Entkopplung (Rückwirkungsfreiheit) zwischen den Verarbeitungskanälen stellen die an den Eingängen gezeichneten Dioden sicher.
- ☐ Das Relais/Schütz KM hat zwangsgeführte Kontakte.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

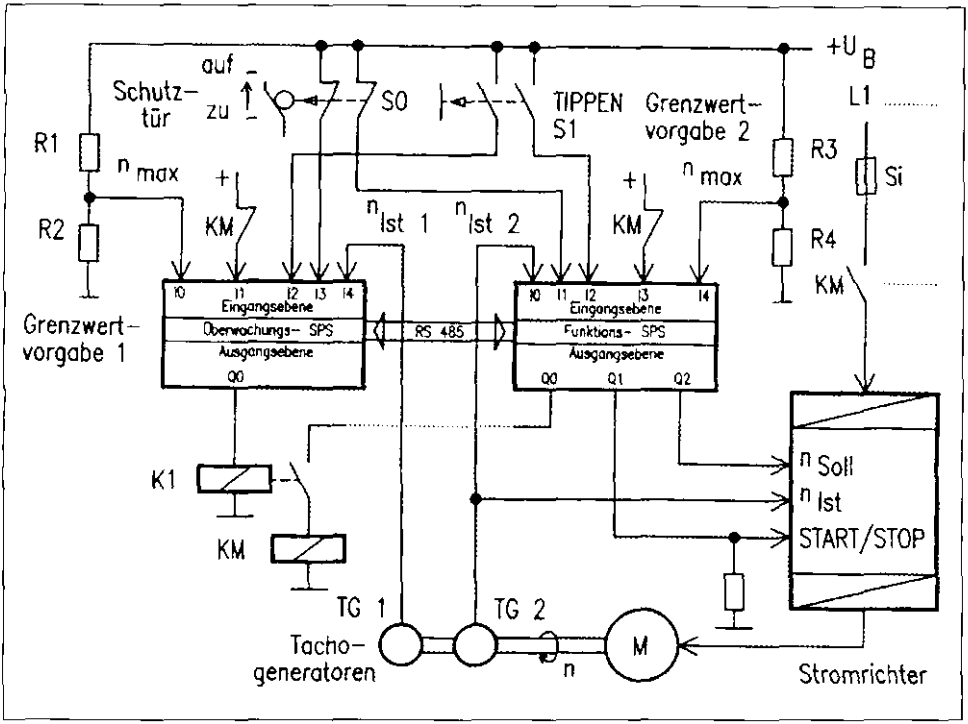
- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 3

Abbildung 44:
Rechnersteuerung nach EN 954 — Kategorie 3
„Kalte", d.h. nicht funktionsbeteiligte SPS-Redundanz



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung wird bei geöffnetem Schutzgitter redundant verhindert oder unterbrochen. Bei geöffnetem Schutzgitter wird wegbegrenzter Tippbetrieb eingestellt. Alle sicherheitsrelevanten Eingangssignale stehen redundant zur Verfügung und werden sowohl von der Funktions-SPS als auch von der Überwachungs-SPS eingelesen. In der Überwachungs-SPS werden alle sicherheitsrelevanten Signale auf Plausibilität (Zeit- und Wertrichtigkeit innerhalb von Toleranzvorgaben) geprüft.
- ☐ Über eine serielle Schnittstelle (RS 485) ist die Überwachungs-SPS in der Lage, auch Status-Informationen innerhalb der verschiedenen Betriebsmodi abzufragen und auf Richtigkeit zu überprüfen.
- ☐ Im störungsfreien Betrieb bleibt das Schütz K1 stets angezogen, also auch z.B. nach dem Entregen des Netzschützes KM. Erst beim Auftreten von Fehlern oder Störungen während des Ablaufens des Produktionsprozesses wird der Überwachungskanal aktiv in den Maschinenablauf eingreifen, K1 und damit KM entregen und so letztlich den Stillstand der Gesamtmaschine herbeiführen.
- ☐ Eine Fehlererkennung ist nur für die Funktions-SPS durch die Überwachungs-SPS möglich. Ein automatisches Testen der Abschaltfähigkeit der Überwachungs-SPS ist nicht möglich, da die Überwachungs-SPS ihre sicherheitstechnische Funktion nur dann ausführt, wenn die Funktions-SPS versagt. Die Sicherheitsfunktionen der Überwachungs-SPS müssen innerhalb der festgelegten Prüfungs- und Wartungsintervalle im Stillstand der Maschine bzw. Anlage überprüft werden.

**Konstruktive Merkmale:**

- ☐ Fehler bei der Verbindung der beiden Kanäle über die serielle Schnittstelle werden durch Testmuster (Signatur) erkannt und damit die Ausgabe fehlerhafter Daten an die Überwachungs-SPS verhindert.
- ☐ Da die Kommunikation rückwirkungsfrei erfolgt, kann ein aufgetretener Fehler in einem Kanal nicht zum Ausfall des anderen und damit zum Ausfall des Gesamtsystems führen.
- ☐ Die Relais/Schütze KM/K1 haben zwangsgeführte Kontakte.
- ☐ Die Programmierung erfolgt modular in Kontaktplandarstellung.

**Anwendung:**

- ☐ Bei mittleren bis höheren Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

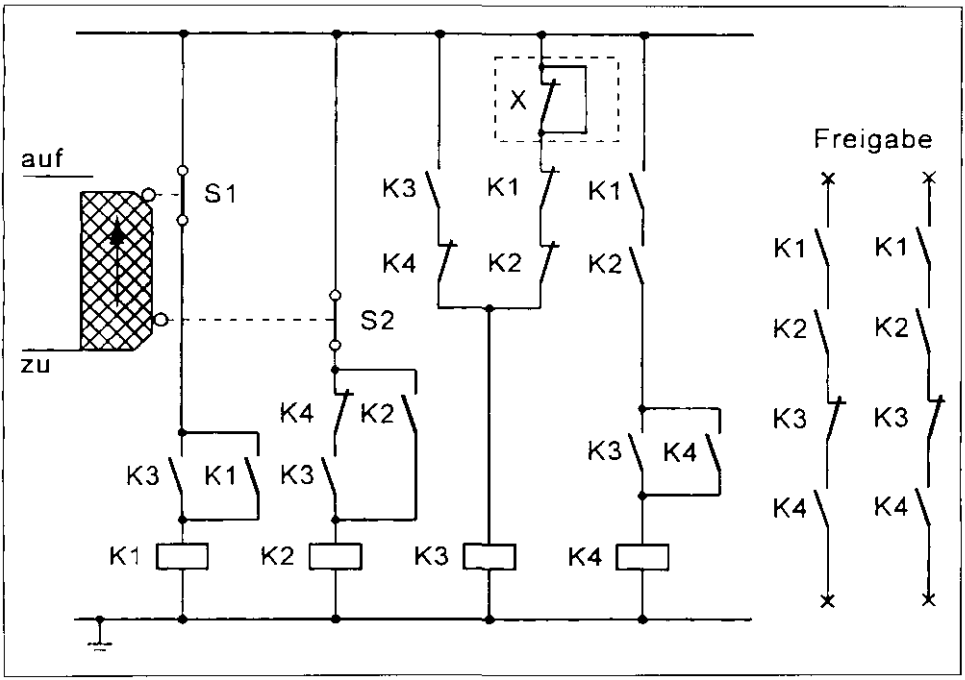
**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit speicherprogrammierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Sicherheitstechnisches Informations- und Arbeitsblatt 330 227. In: BIA-Handbuch 24. Lfg. I/95 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 45:
Elektromechanische Steuerung nach EN 954 — Kategorie 4
Stellungsüberwachung beweglicher Schutzeinrichtungen



**Funktionsbeschreibung:**

- ☐ *Gefahrbringende* Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Öffner-Schließer-Kombination unterbrochen bzw. verhindert.
- ☐ Es ist keine Anlauftestung durch Öffnen und Schließen der Schutzeinrichtung erforderlich.
- ☐ Die Sicherheitsfunktion ist auch erfüllt, wenn ein Bauteilausfall auftritt. Alle Fehler, entsprechend der Fehlerliste, werden während des Betriebes oder beim Betätigen (Öffnen und Schließen) der Schutzeinrichtung durch Unterbrechung der Freigabe erkannt.
- ☐ Eine Fehlerhäufung zwischen zwei aufeinanderfolgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.
- ☐ Die Schaltung kann an der mit einem X gekennzeichneten Stelle zur Überwachung von Leistungsschützen und Schützen zur Vervielfältigung des Freigabepfades erweitert werden.

**Konstruktive Merkmale:**

- ☐ Alle sicherheitsrelevanten Teile der Steuerung sind redundant aufgebaut.
- ☐ Der Schalter S1 ist ein zwangsöffnender Positionsschalter entsprechend EN 1088.
- ☐ Die Steuerschütze K1/K2/K3/K4 haben zwangsgeführte Kontakte.
- ☐ Die Zuleitungen zu den Positionsschaltern S1/S2 sind getrennt verlegt.
- ☐ Kategorie 4 wird nur eingehalten, wenn nicht mehrere mechanische Positionsschalter verschiedener Schutzeinrichtungen hintereinandergeschaltet werden (Kaskadierung), da sonst keine Fehlererkennung in Schaltern und Leitungen möglich ist.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

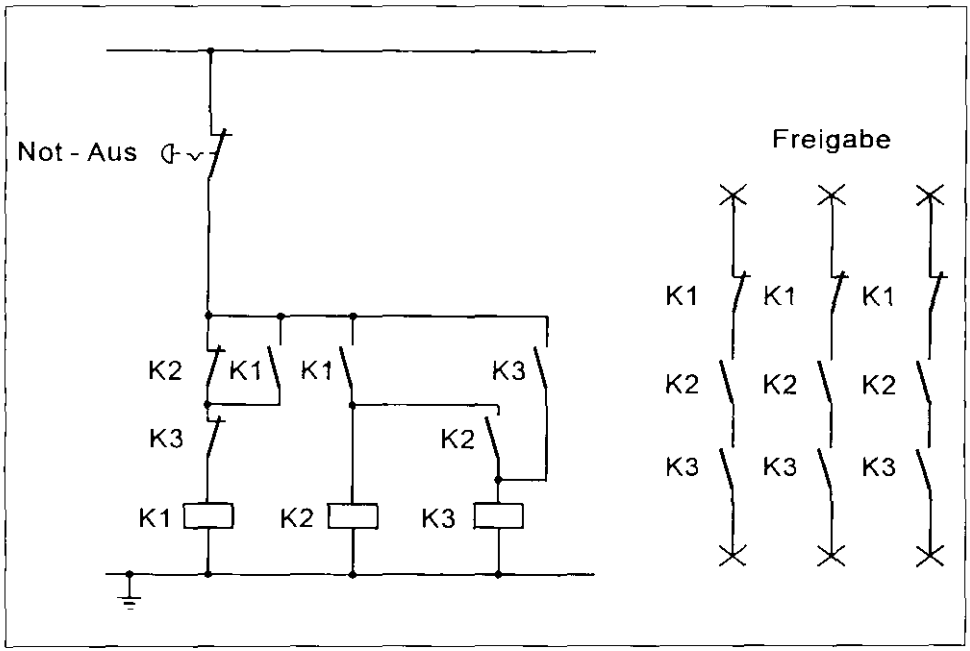
**Weiterführende Literatur:**

- ☐ *Kreutzkampf, F.; Hertel, W.:* Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X/91 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 46:
Elektromechanische Steuerung nach EN 954 — Kategorie 4
Not-Aus-Einrichtung
Fehlerausschluß bei Not-Aus-Tastern und Leitungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei Betätigung der Not-Aus-Einrichtungen durch eine selbstüberwachte Schützkombination abgeschaltet.
- ☐ Folgende Fehlerausschlüsse werden bei der Beurteilung der Kategorie gemacht:
  — Nichtunterbrechung des Not-Aus-Schaltkontaktes bei Betätigung,
  — Überbrückung der Not-Aus-Einrichtung durch Leitungsschluß.
- ☐ Die Sicherheitsfunktion der Schützkombination ist erfüllt, wenn ein Bauteilausfall auftritt. Alle Fehler, entsprechend der Fehlerliste, werden während des Betriebes oder beim Betätigen der Not-Aus-Einrichtung durch Unterbrechung der Freigabe erkannt.
- ☐ Eine Fehlerhäufung zwischen zwei aufeinanderfolgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ Befehlsgerät und Stellteil arbeiten nach dem Prinzip der Zwangsbetätigung (EN 418).
- ☐ Die Steuerschütze K1/K2/K3 haben zwangsgeführte Kontakte.
- ☐ Ein Fehlerausschluß ist nur möglich, wenn Not-Aus-Taster und Leitungen keinen besonderen Gefährdungen ausgesetzt sind.

**Anwendung:**

- ☐ Bei hohen Risiken, wenn sofortiges Abschalten der Energiezufuhr nicht zu gefährlichen Zuständen führt (Stop-Kategorie 0 nach EN 60 204-1).
- ☐ Wenn kein Fehlerausschluß (siehe oben) möglich ist, können Befehlsgeräte und Leitungen redundant (zweipolig) ausgeführt werden. Hierbei muß die Signalverarbeitung erweitert oder durch ein zweipoliges Not-Aus-Kontrollgerät ersetzt werden.

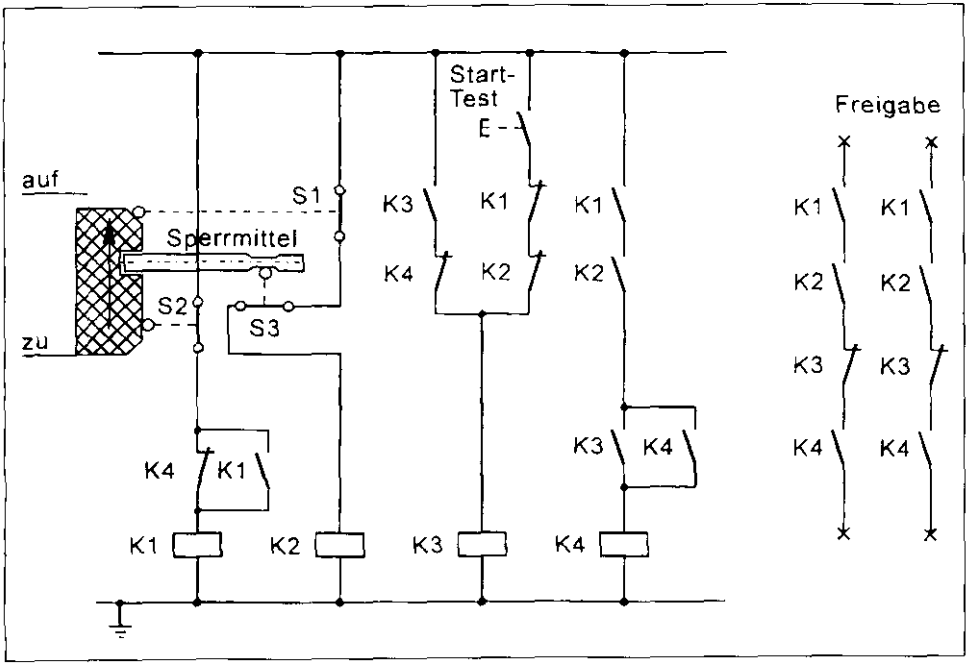
**Weiterführende Literatur:**

- ☐ *nicht bekannt*

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 47:
Elektromechanische Steuerung nach EN 954 — Kategorie 4
Stellungsüberwachung beweglicher Schutzeinrichtungen mit Zuhaltung und Anlauftestung




**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden bei geöffnetem Schutzgitter durch Öffner-Schließer-Kombination unterbrochen bzw. verhindert.
- ☐ Zusätzlich wird das Sperrmittel (Zuhaltung) durch zwangläufig wirkenden Positionsschalter überwacht.

- ☐ Es ist eine Anlauftestung vorhanden, die bei geöffneter Schutzeinrichtung durchgeführt werden muß.
- ☐ Die Sicherheitsfunktion ist auch erfüllt, wenn ein Bauteilausfall auftritt. Alle Fehler, entsprechend der Fehlerliste, werden während des Betriebes oder beim Betätigen (Öffnen und Schließen) der Schutzeinrichtung durch Unterbrechung der Freigabe erkannt.
- ☐ *Eine Fehlerhäufung zwischen zwei aufeinanderfolgenden* Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.
- ☐ Wenn durch die Stellungsüberwachung des Sperrmittels (S3) auch gleichzeitig die Stellung der Schutzeinrichtung zwangläufig erkannt wird (Fehlschließsicherung), kann S1 entfallen.

**Konstruktive Merkmale:**

- ☐ Alle sicherheitsrelevanten Teile der Steuerung zur Stellungsüberwachung der Schutzeinrichtung sind redundant aufgebaut.
- ☐ Die Schalter S1 und S3 sind zwangsöffnende Positionsschalter entsprechend EN 1088.
- ☐ Die Steuerschütze K1/K2/K3/K4 haben zwangsgeführte Kontakte.
- ☐ Die Zuleitungen zu den Positionsschaltern S1/S2/S3 sind getrennt verlegt.
- ☐ Kategorie 4 wird nur eingehalten, wenn nicht mehrere mechanische Positionsschalter verschiedener Schutzeinrichtungen hintereinandergeschaltet werden (Kaskadierung), da sonst keine Fehlererkennung in Schaltern und Leitungen möglich ist.
- ☐ Die Steuerung des Sperrmittels kann z.B. durch zeitabhängige Systeme (Gewindebolzen, Schaltuhr) oder bewegungsabhängige Systeme (Stillstandsmelder) erfolgen.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und *geringer Wahrscheinlichkeit, daß die Gefahr* durch andere Maßnahmen noch abgewendet werden kann. Die Schaltung ist anwendbar bei trennenden Schutzeinrichtungen, die so lange geschlossen und zugehalten bleiben müssen, bis ein Verletzungsrisiko durch gefährliche Maschinenfunktionen vorbei ist.

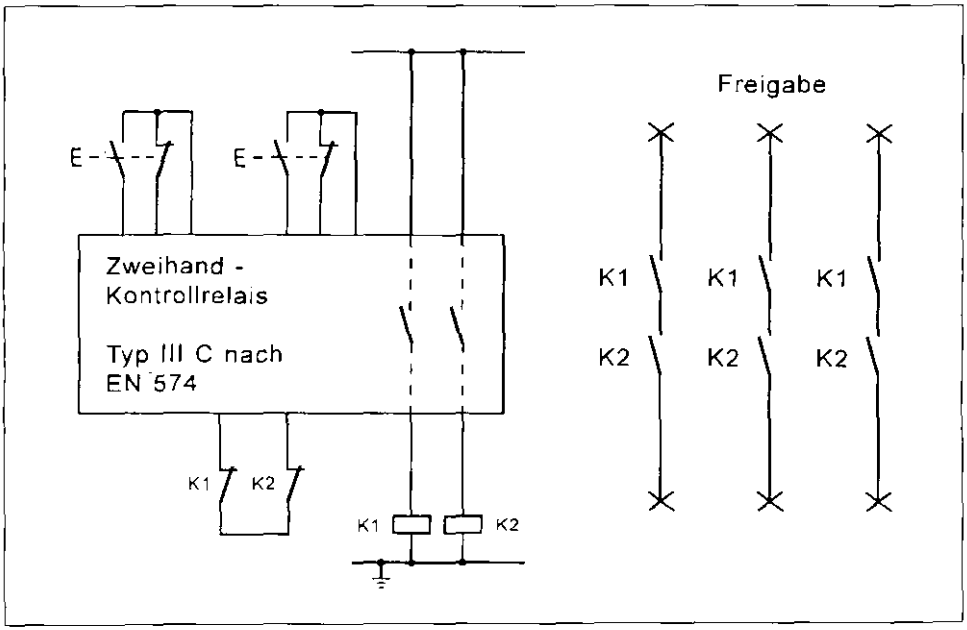
**Weiterführende Literatur:**

- ☐ *Kreutzkampf, F.; Hertel, W.*: Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 212. In: BIA-Handbuch 17. Lfg. X/91 Erich Schmidt Verlag, Bielefeld
- ☐ ZH1/153/10.95: Merkblatt für die Auswahl und Anbringung elektromechanischer Verriegelungseinrichtungen für Sicherheitsfunktionen

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 48:
Elektromechanische Steuerung nach EN 954 — Kategorie 4
Zweihandschaltung, Signalverarbeitung durch Kontrollrelais mit nachgeschalteten Steuerschützen



Funktionsbeschreibung:

☐ Gefahrbringende Bewegungen werden durch ein Zweihand-Kontrollrelais gesteuert.

☐ Durch K1 und K2 erfolgt eine Kontaktvervielfältigung.

Konstruktive Merkmale:

☐ Das Kontrollrelais entspricht Typ III C gemäß EN 574.

☐ Eine Fehlererkennung von K1 und K2 erfolgt durch Öffner im Rückführkreis.

Anwendung:

☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

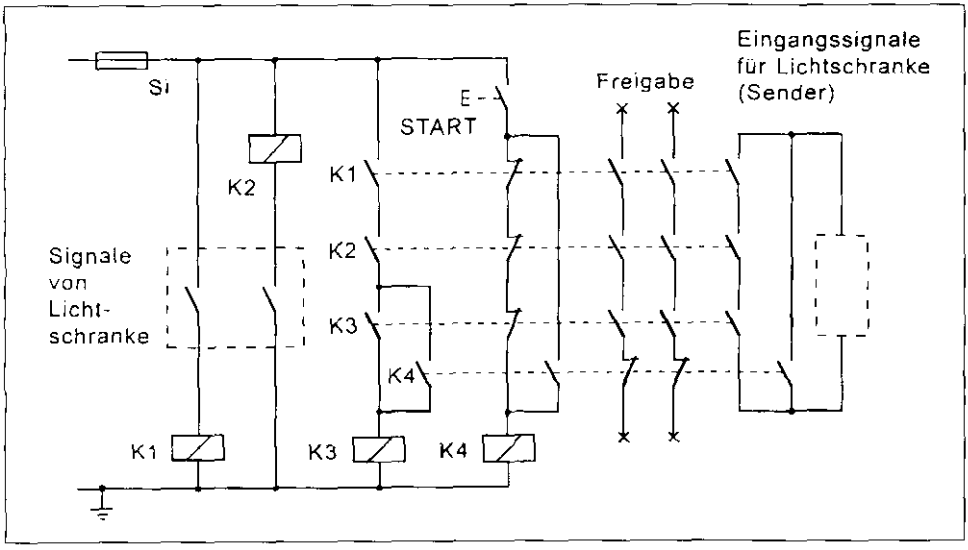
Weiterführende Literatur:

☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektromechanische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 49:
Elektromechanische Steuerung nach EN 954 — Kategorie 4
Einbindung von sicherheitsrelevanten Signalen in die Maschinensteuerung
am Beispiel einer Lichtschranke



**Funktionsbeschreibung:**

- ☐ Die sicherheitsrelevanten Signale der Lichtschranke (2 Schließer) schalten die Steuerschütze K1 und K2, die einen unterschiedlichen Spulenanschluß besitzen.
- ☐ Je ein Schließer von K1 und K2 ist im Freigabepfad und ebenfalls im Eingangskreis zum Start des Lichtschrankensenders angeordnet.
- ☐ Nach Unterbrechen der Lichtschrankensignale muß durch den Start-Taster eine willensabhängige Testung der Schütze K1, K2, K3 erfolgen und der Sender muß einen neuen Startbefehl erhalten.
- ☐ Fehler der Steuerschütze K1, K2, K3 (Verschweißen) und K4 (Abfallen) sowie eine Überbrückung des Start-Tasters werden bemerkt und führen spätestens bei Betätigung der Taste START zu einer Verhinderung der Freigabe.
- ☐ Eine Fehlerhäufung zwischen zwei aufeinanderfolgenden Startzeitpunkten kann zum Verlust der Sicherheitsfunktion führen.

**Konstruktive Merkmale:**

- ☐ Die Steuerschütze K1, K2, K3 und K4 haben zwangsgeführte Kontakte.
- ☐ Durch den unterschiedlichen Spulenanschluß von K1 und K2 führen Leitungsschlüsse zwischen unterschiedlichen Signalleitungen zum Ansprechen der Sicherung (Si). Deshalb ist keine getrennte Leitungsführung für jedes Signal notwendig.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

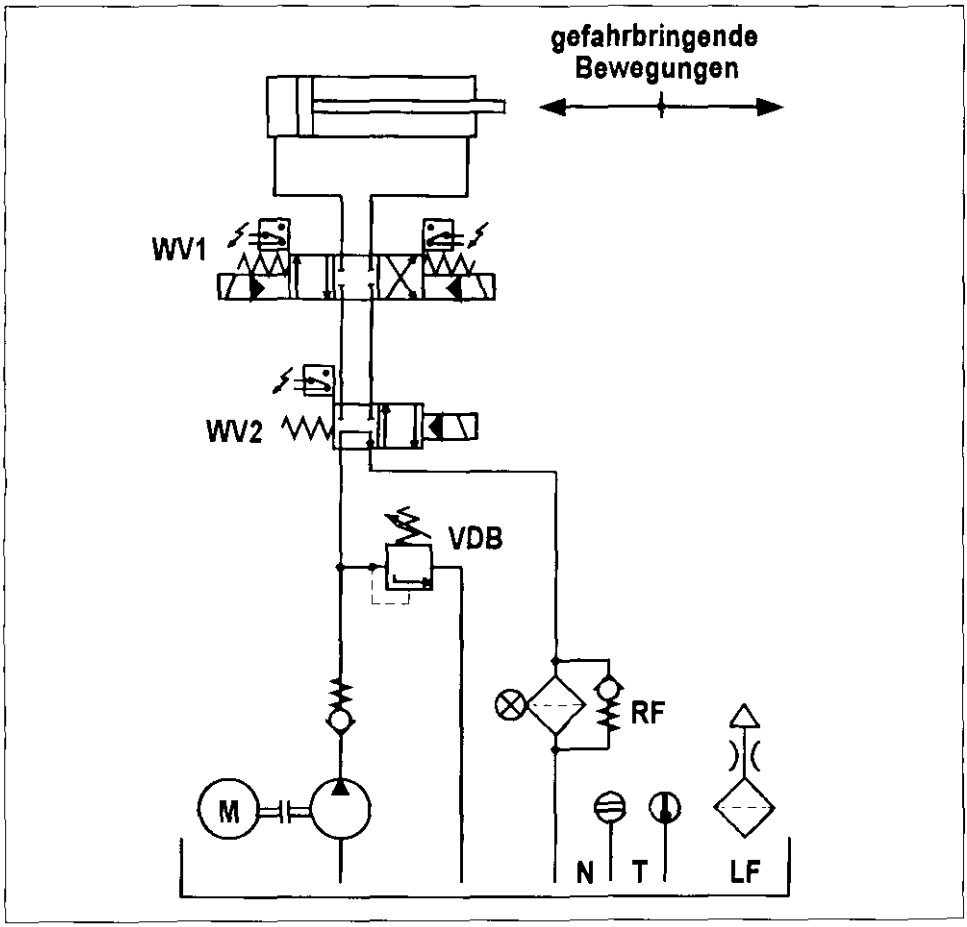
**Weiterführende Literatur:**

- ☐ nicht bekannt

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Hydraulische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 50:
Elektro-hydraulische Steuerung nach EN 954 — Kategorie 4, zur Steuerung von gefahrbringenden Bewegungen



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden durch zwei Wegeventile (WV1 und WV2) gesteuert.
- ☐ Der Ausfall eines Wegeventils führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ Beide Wegeventile werden zyklisch angesteuert.
- ☐ *An beiden Wegeventilen ist jeweils eine Maßnahme zur Fehlererkennung vorgesehen.* Der Ausfall beider Wegeventile wird erkannt; nach einem Fehler wird das Einleiten der nächsten gefahrbringenden Bewegung verhindert.

**Konstruktive Merkmale:**

- ☐ Beide Wegeventile (WV1 und WV2) haben eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung sowie mit elektrischer Stellungsüberwachung.
- ☐ Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- ☐ Die Signalverarbeitung der elektrischen Stellungsüberwachungen erfüllt entsprechende Anforderungen an den Fehlerfall.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

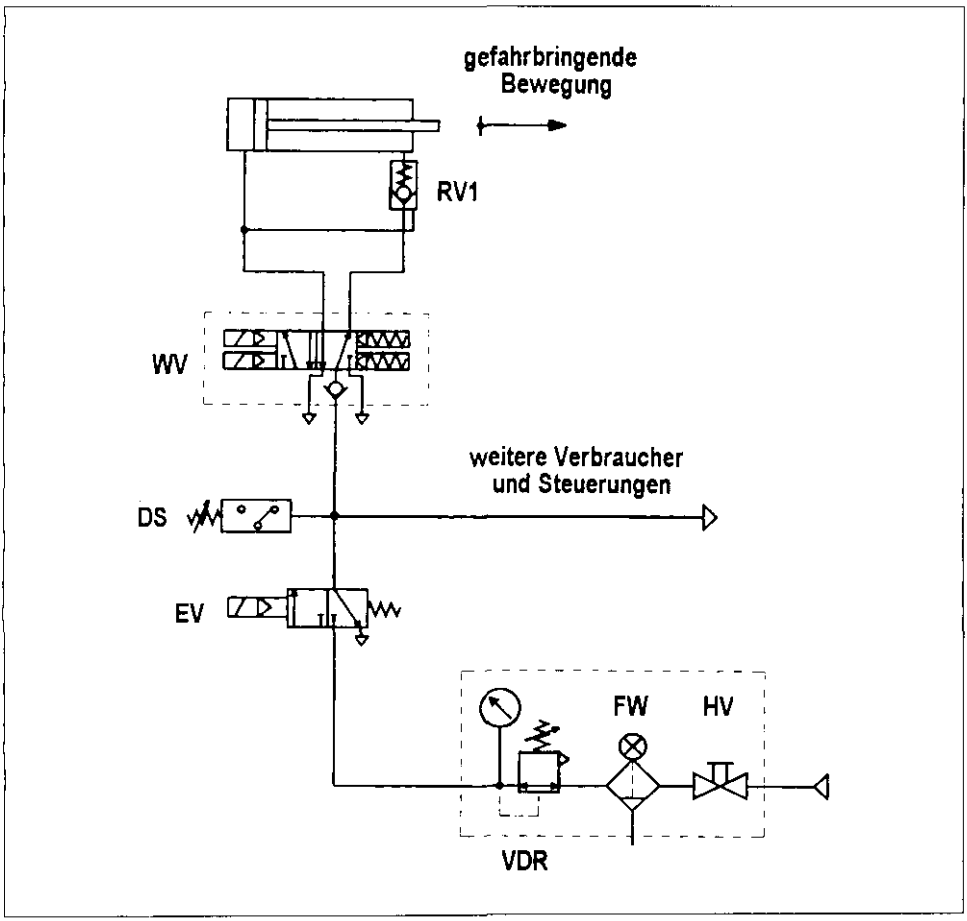
**Weiterführende Literatur:**


- ☐ *Kleinbreuer, W.*: Sicherheitstechnisch abgestufte Steuerungen in der Fluidtechnik. Die BG (1994) Nr. 3
- ☐ *Gorgs, K.-J., Kleinbreuer, W.,* und *Kühlem, W.*: Fehlerlisten für hydraulische und pneumatische Bauelemente — Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA-Handbuch, 14. Lfg. VI/90 und 15. Lfg. XI/90 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 51:
Elektro-pneumatische Steuerung nach EN 954 — Kategorie 4,
zur Steuerung von gefahrbringenden Bewegungen



Funktionsbeschreibung:

- ☐ Eine gefahrbringende Bewegung oder ein gefahrbringender Zustand wird durch eine selbstüberwachte Ventilkombination WV gesteuert, in Verbindung mit einem entsperrbaren Rückschlagventil RV1 (bei Ausfall der Druckluft und äußeren Kräften von Bedeutung).
- ☐ Ein Bauteilausfall innerhalb der Ventilkombination führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ Beide Vorsteuerventile der Ventilkombination werden getrennt angesteuert. Nach Wegnahme eines Steuersignals/beider Steuersignale erfolgt immer eine Reversierung der Bewegung.
- ☐ Der einzelne Fehler innerhalb der Ventilkombination wird erkannt; ein Einleiten der nächsten gefahrbringenden Bewegung wird verhindert.

Konstruktive Merkmale:

- ☐ WV ist eine selbstüberwachte Ventilkombination mit mechanisch getrennten Vorsteuerventilen und pneumatisch/mechanisch realisierter Fehlererkennung mit integriertem Rückschlagventil in der P-Leitung.
- ☐ Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme der Steuersignale erreicht.
- ☐ Das entsperrbare Rückschlagventil RV1 soll möglichst im Zylinder eingeschraubt sein.
- ☐ Die Fehlererkennung innerhalb der Ventilkombination erfüllt entsprechende Anforderungen an den Fehlerfall.

Anwendung:

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

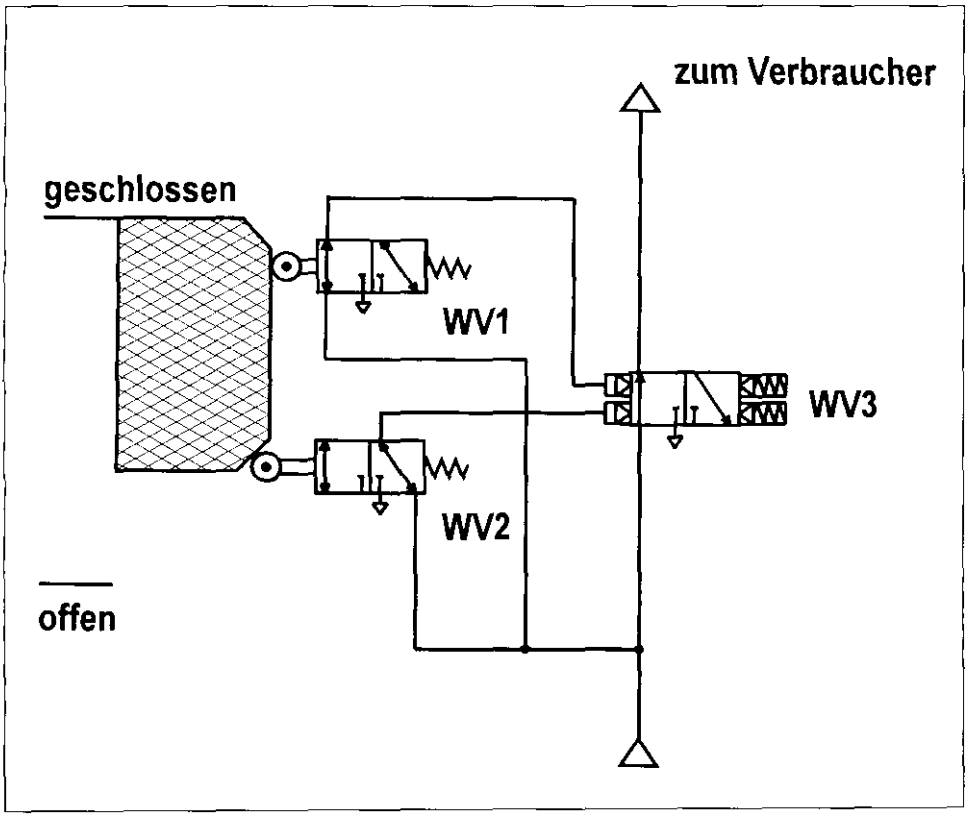
Weiterführende Literatur:


- ☐ *Kleinbreuer, W.: Sicherheitstechnisch abgestufte Steuerungen in der Fluidtechnik.* Die BG (1994) Nr. 3
- ☐ *Gorgs, K.-J., Kleinbreuer, W.* und *Kühlem, W.*: Fehlerlisten für hydraulische und pneumatische Bauelemente — Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA — Handbuch, 14. Lfg. VI/90 und 15. Lfg. XI/90 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 52:
Pneumatische Steuerung nach EN 954 – Kategorie 4,
Verriegelung beweglich trennender Schutzeinrichtung



**Funktionsbeschreibung:**

- ☐ Die Verriegelung der beweglich trennenden Schutzeinrichtung erfolgt durch zwei „pneumatische Positionsschalter" (WV1 und WV2). Diese geben jeweils einen Steuerbefehl an eine selbstüberwachte Ventilkombination WV3.
- ☐ Die Energiezufuhr (pneumatisch) erfolgt nur bei geschlossener Schutzeinrichtung.
- ☐ Ein Bauteilausfall führt nicht zum Verlust der Sicherheitsfunktion.

**Konstruktive Merkmale:**

- ☐ WV2 ist ein pneumatischer Positionsschalter mit zwangläufiger Betätigung durch die beweglich trennende Schutzeinrichtung, entsprechend EN 1088.
- ☐ Die sicherheitsgerichtete Schaltstellung der Ventilkombination WV3 wird durch Wegnahme eines Steuersignals/beider Steuersignale erreicht.
- ☐ WV1/WV2 ist eine selbstüberwachte Ventilkombination mit mechanisch getrennten Vorsteuerventilen und pneumatisch/mechanisch realisierter Fehlererkennung.
- ☐ Die Fehlererkennung innerhalb der Ventilkombination erfüllt entsprechende Anforderungen an den Fehlerfall.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

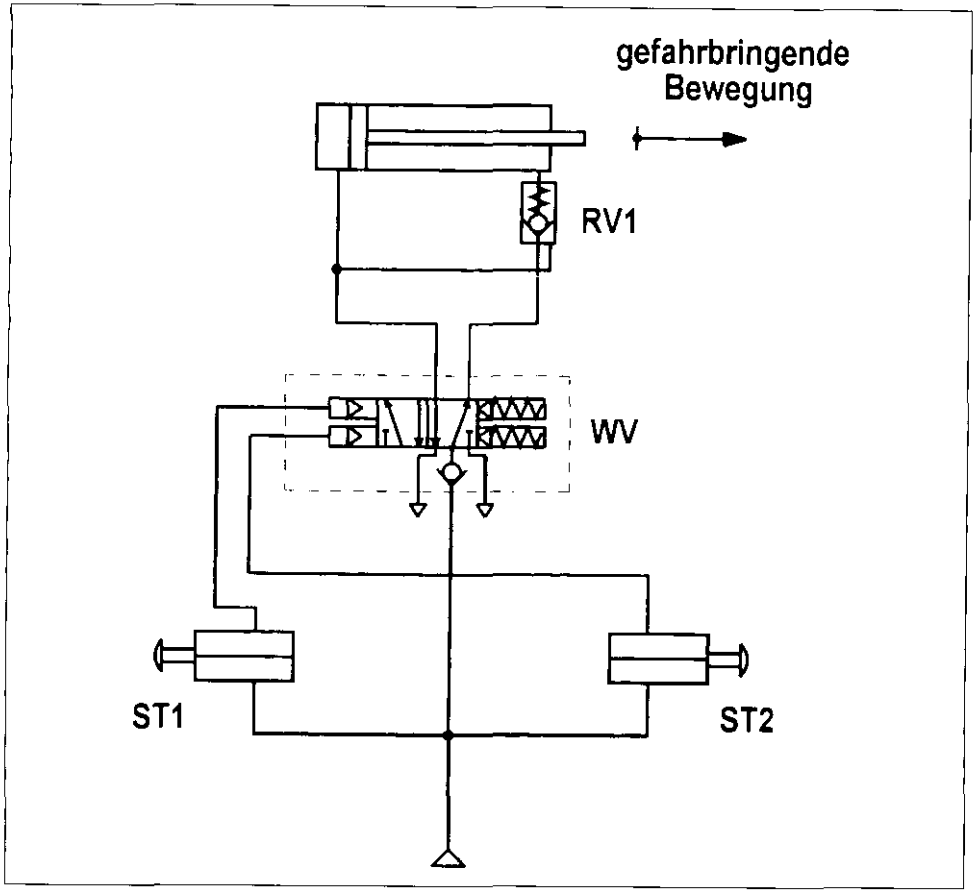
**Weiterführende Literatur:**


- ☐ *Kleinbreuer, W.:* Anforderungen an hydraulische und pneumatische Maschinensteuerungen. *Sichere Chemiearbeit (1992) Nr. 2 und Nr. 3*
- ☐ EN 1088: Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl
- ☐ *Gorgs, K.-J., Kleinbreuer, W.,* und *Kühlem, W.:* Fehlerlisten für hydraulische und pneumatische Bauelemente — Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 225. In: BIA-Handbuch, 14. Lfg. VI/90 und 15. Lfg. XI/90 Erich Schmidt Verlag, Bielefeld

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Pneumatische Steuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 53:
Pneumatische Steuerung nach EN 954 — Kategorie 4,
für Zweihandsteuerung, realisiert durch eine spezielle Ventilkombination
für direkte Ansteuerung des Zylinders



**Funktionsbeschreibung:**

- ☐ Eine gefahrbringende Bewegung oder ein gefahrbringender Zustand wird durch synchrone Betätigung der Stellteile ST1 und ST2 von einer selbstüberwachten Ventilkombination WV gesteuert, in Verbindung mit einem entsperrbaren Rückschlagventil RV1 (bei Ausfall der Druckluft und äußeren Kräften von Bedeutung).
- ☐ Ein Bauteilausfall innerhalb der Ventilkombination führt nicht zum Verlust der Sicherheitsfunktion.
- ☐ Beide Vorsteuerventile der Ventilkombination werden getrennt angesteuert. Nach Wegnahme eines Steuersignals/beider Steuersignale erfolgt immer eine Reversierung der Bewegung.
- ☐ Der einzelne Fehler innerhalb der Ventilkombination wird erkannt; ein Einleiten der nächsten gefahrbringenden Bewegung wird verhindert.

**Konstruktive Merkmale:**

- ☐ WV ist eine selbstüberwachte Ventilkombination mit mechanisch getrennten Vorsteuerventilen und pneumatisch/mechanisch realisierter Fehlererkennung mit integriertem Rückschlagventil in der P-Leitung.
- ☐ Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme der Steuersignale erreicht.
- ☐ Das entsperrbare Rückschlagventil RV1 sollte im Zylinder eingeschraubt sein.
- ☐ Die selbstüberwachte Ventilkombination erfüllt entsprechende Anforderungen an den Fehlerfall und die Anforderungen bzgl. der Beziehung zwischen Eingangssignalen und Ausgangssignal, Beendigung des Ausgangssignals, erneutes Erzeugen des Ausgangssignals und synchroner Betätigung nach EN 574. Dabei müssen die Stellteile ST1 und ST2 in Verbindung mit ihren Signalumsetzern beim Zurückziehen eines Eingangssignals, auch nach dem Auftreten eines Fehlers, das entsprechende Ansteuersignal für die Ventilkombination zurückziehen (siehe EN 574, Abschnitt 6.4.3).

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

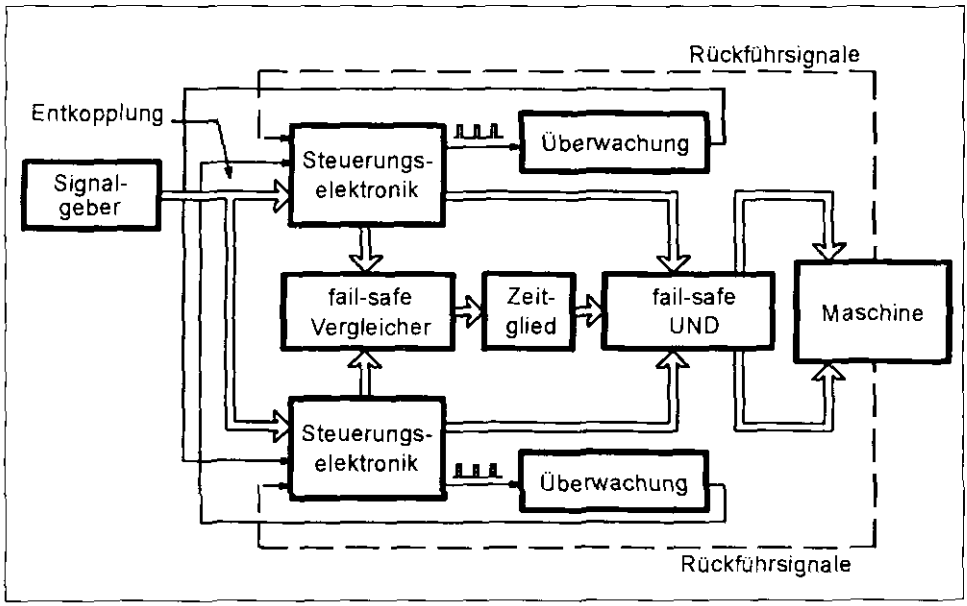
**Weiterführende Literatur:**

- ☐ *Kleinbreuer, W.*: Sicherheitstechnisch abgestufte Steuerungen in der Fluidtechnik. Die BG (1994) Nr. 3

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Elektroniksteuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 54:
Elektroniksteuerung nach EN 954 — Kategorie 4
Grobstruktur der Steuerung



**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden von zwei Kanälen unabhängig voneinander in Abhängigkeit vom Signalgeber gesteuert.
- ☐ Eine Fehlererkennung wird (spätestens innerhalb einer Stunde) durch zahlreiche Zwischenvergleiche für alle Bauelemente in der Steuerungselektronik durchgeführt.
- ☐ Eine Ungleichheit in den Ausgangssignalen oder eine Fehlererkennung an einem der Bauelemente führt zum Auslösen der Sicherheitsfunktion.

**Konstruktive Merkmale:**

- ☐ Die Maschinenreaktion läßt sich auf ihr sicherheitstechnisches Verhalten über die Rückführsignale redundant überwachen.
- ☐ Abhängig von der Maschinenreaktion werden zahlreiche Plausibilitätskontrollen zur Fehlererkennung genutzt.
- ☐ Statische Signalgeber werden redundant ausgeführt und ihre Betätigung zwangsdynamisiert.
- ☐ Bei der Verdrahtung der Signalgeber in beide Kanäle wurde darauf geachtet, daß die Eingänge so entkoppelt (z.B. durch Entkopplungsdioden) sind, daß ein Fehler in einem Kanal nicht den anderen Kanal in gleicher Weise ausfallen läßt.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

- ☐ *Jürs, H.; Reinert, D.:* Elektronik in der Sicherheitstechnik. Sicherheitstechnisches Informations- und Arbeitsblatt 330 220. In: BIA-Handbuch 20. Lfg. V/93 Erich Schmidt Verlag, Bielefeld
- ☐ *Grigulewitsch, W.; Meffert, K.:* Redundante Schaltungstechniken. Sicherheitstechnisches Informations- und Arbeitsblatt 330 226. In: BIA-Handbuch 10. Lfg. X/88 Erich Schmidt Verlag, Bielefeld

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 4

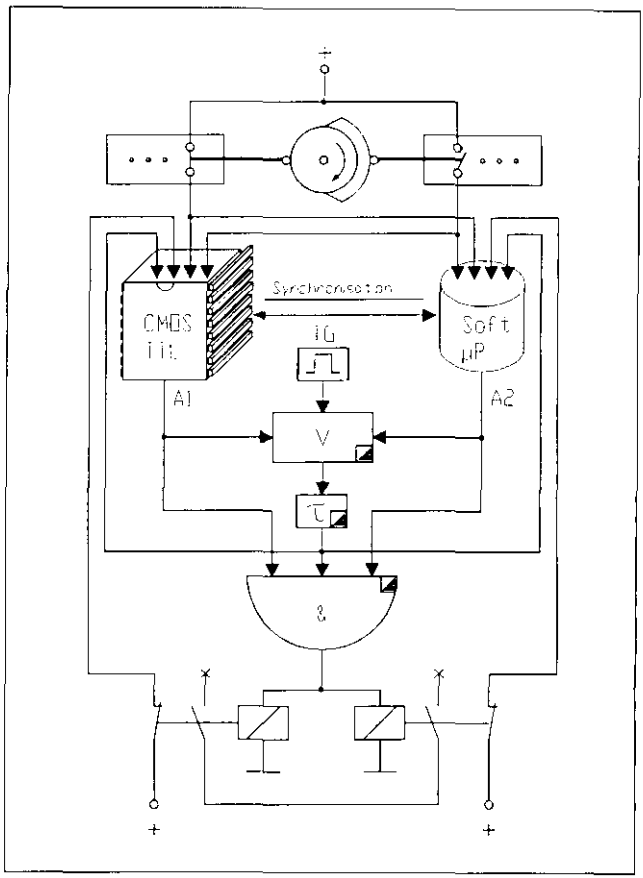



Abbildung 55:
Rechnersteuerung nach EN 954
— Kategorie 4:
Steuerung eines Prozesses
mit diversitärer Redundanz mit
Mikroprozessor-
und CMOS/TTL-logik

**Funktionsbeschreibung:**

- ☐ Gefahrbringende Bewegungen oder Zustände werden durch zwei diversitäre Kanäle (Rechnertechnik und TTL-Logik) unterbrochen bzw. verhindert. Beide Kanäle arbeiten unabhängig voneinander, werden jedoch synchronisiert.
- ☐ Die Eingangssignale des Prozesses werden durch beide Kanäle bearbeitet. Hierbei können auch nur die sicherheitsrelevanten Signale betroffen sein.
- ☐ Beim Auftreten eines Bauteilausfalles bleiben die Sicherheitsfunktionen erhalten.
- ☐ Ein einzelner Bauteilausfall in einem Kanal wird innerhalb einer Stunde aufgedeckt. Ein separater Taktgenerator erzeugt dazu Impulse, die durch einen Äquivalenzvergleicher nur dann weitergegeben werden, wenn die Signale A1 und A2 identisch sind. Das Ausgangssignal des Vergleichers und die Signale der Kanäle werden über einen Fail-safe-UND-Baustein den Ansteuerungen der gefahrbringenden Bewegungen zugeführt.

**Konstruktive Merkmale:**

- ☐ Die Diversität der beiden Verarbeitungskanäle hilft, systematische Ausfälle in der Hardware zu beherrschen und zu vermeiden.
- ☐ Die Entkopplung der Verarbeitungskanäle macht jedoch zusätzlich zur Synchronisation auch die Erlaubnis eines geringen Zeitversatzes notwendig. Das Zeitglied $\tau$ erlaubt beiden Kanälen um die entsprechende Zeit eine Antivalenz, um unterschiedliche Bearbeitungszeiten in den Kanälen auszugleichen.
- ☐ Die Stellglieder der gefahrbringenden Bewegungen werden über die Kontakte der zwangsgeführten Relais zurückgelesen, um eine bleibende Abschaltung durch den Kanal zu erreichen.

**Anwendung:**

- ☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und relativ hoher Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

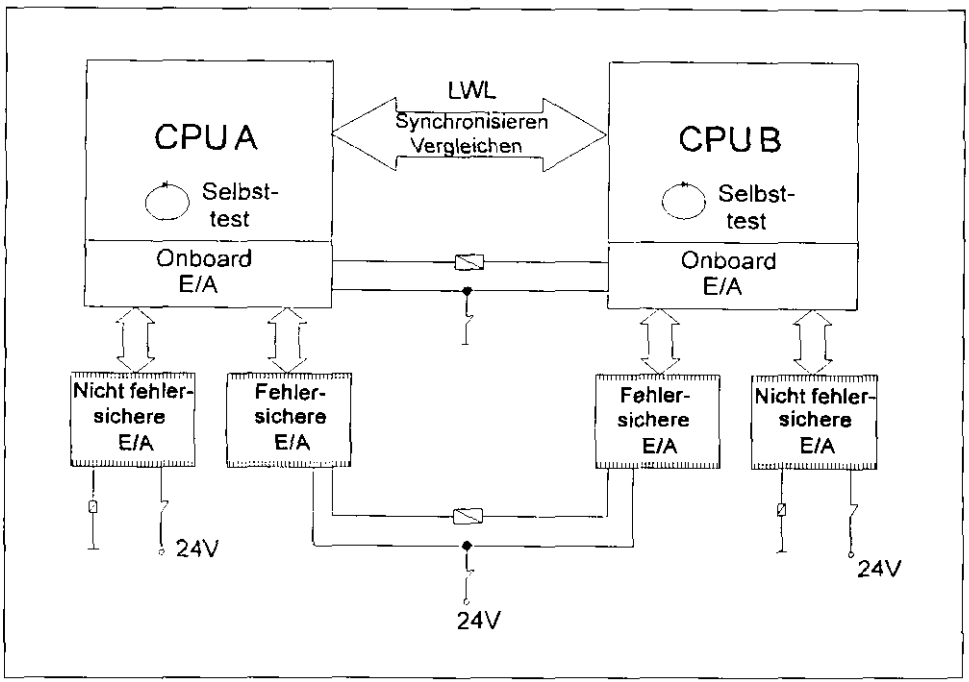
**Weiterführende Literatur:**

- ☐ *Grigulewitsch, W.; Meffert, K.; Reuß, G.*: Aufbau elektrischer Maschinensteuerungen mit diversitärer Redundanz. BIA-Report 5/86. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitssicherheit — BIA, Sankt Augustin.

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

## Rechnersteuerungen
## Beispiel für EN 954 — Kategorie 4

Abbildung 56:
Rechnersteuerung nach EN 954 — Kategorie 4
Frei programmierbare speicherprogrammierbare Steuerung



Funktionsbeschreibung:

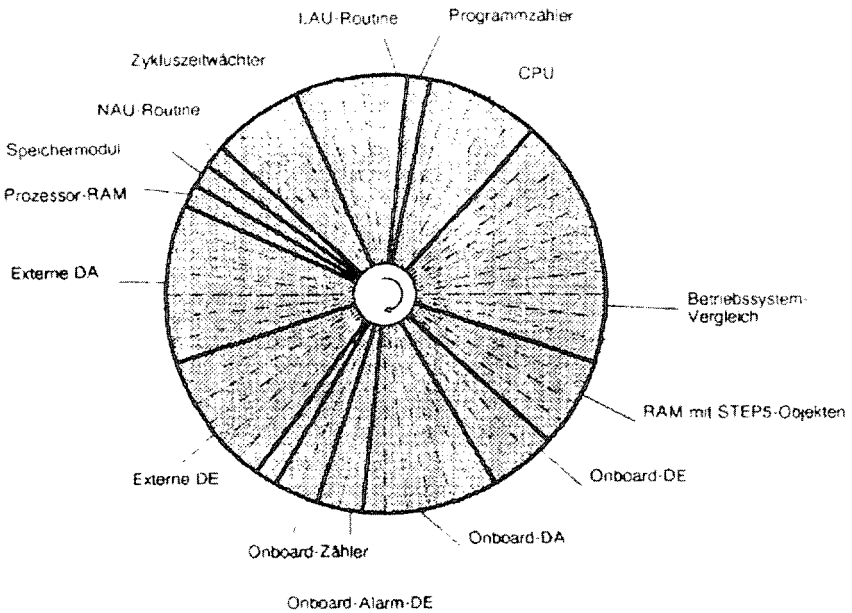
- ☐ Gefahrbringende Bewegungen oder Zustände werden durch zwei identische Zentraleinheiten unterbrochen bzw. verhindert. Die Zentraleinheiten können durch externe Peripherie-Baugruppen sowie weitere speicherprogrammierbare Steuerungen über ein BUS-System erweitert werden.
- ☐ Beim Auftreten eines Bauteilausfalles bleiben die Sicherheitsfunktionen erhalten.
- ☐ Ein einzelner Bauteilausfall in einem Kanal wird innerhalb einer Stunde aufgedeckt. Nach Fehlererkennung schalten beide Kanäle innerhalb von weniger als 10 ms alle ihre Ausgänge auf Nullpotential.
- ☐ Alle sicherheitsrelevanten Funktionen werden in der gleichen Weise in beiden Kanälen programmiert. Eine optische Übertragungsstrecke ist notwendig, um die Ergebnisse der beiden Kanäle miteinander zu synchronisieren. Zusätzlich wird die optische Übertragungsstrecke zur Fehlererkennung zu einem hochdynamischen Austausch und Vergleich benutzt. Falls ein Vergleich einen Unterschied detektiert, werden die Ausgänge beider Zentraleinheiten auf 0 gesetzt und alle Ausgangskarten kontaktbehaftet von der Versorgungsspannung abgetrennt.

Konstruktive Merkmale:

- ☐ Sogenannte Online-Tests werden für alle Baueinheiten ausgeführt, um die korrekte Funktion jeder Einheit zu überwachen. Alle Tests werden im Hintergrund in einem Zeitscheibenverfahren durchgeführt. Das Betriebssystem der speicherprogrammierbaren Steuerung garantiert, daß nach einer Stunde alle Baugruppen komplett überprüft wurden. Alle Tests werden vollständig in jedem Kanal durchlaufen. Immer dann, wenn die speicherprogrammierbare Steuerung über den Stop-Run-Schalter oder den Netzschalter oder aber über einen Fehlerzustand in den Haltzustand geschaltet wird, werden alle Tests zusammenhängend ausgeführt. Abbildung 57 zeigt die Zeiteinheiten für die verschiedenen Hintergrundtests.
- ☐ CPU: Test aller Register über eine wandernde 1 oder 0, des internen Prozessor-RAM über einen in 16 Byteeinheiten portionierten Galpattest; Test aller CPU-Befehle; Test von Programmzähler und der Adreßberechnung durch den Ansprung von Programminseln im EPROM; zeitliche Programmlaufüberwachung über die Synchronisation alle 5 ms.

# 4 Zusammenstellung der Steuerungsbeispiele für die einzelnen Kategorien

Abbildung 57:
Hintergrundtests für die Rechnerkomponenten




- ☐ EPROM: Signatur mit einer Breite eines Wortes über das Generatorpolynom X16 + X15 + X12 + X1; Vergleich des gesamten EPROM-Inhaltes beider Kanäle innerhalb einer Stunde.
- ☐ RAM mit Anwendungsprogramm: Wandernde 0 und wandernde 1 sowie Vergleich mit dem Inhalt des RAM im zweiten Kanal, wobei ein Teil invers abgespeichert wurde.

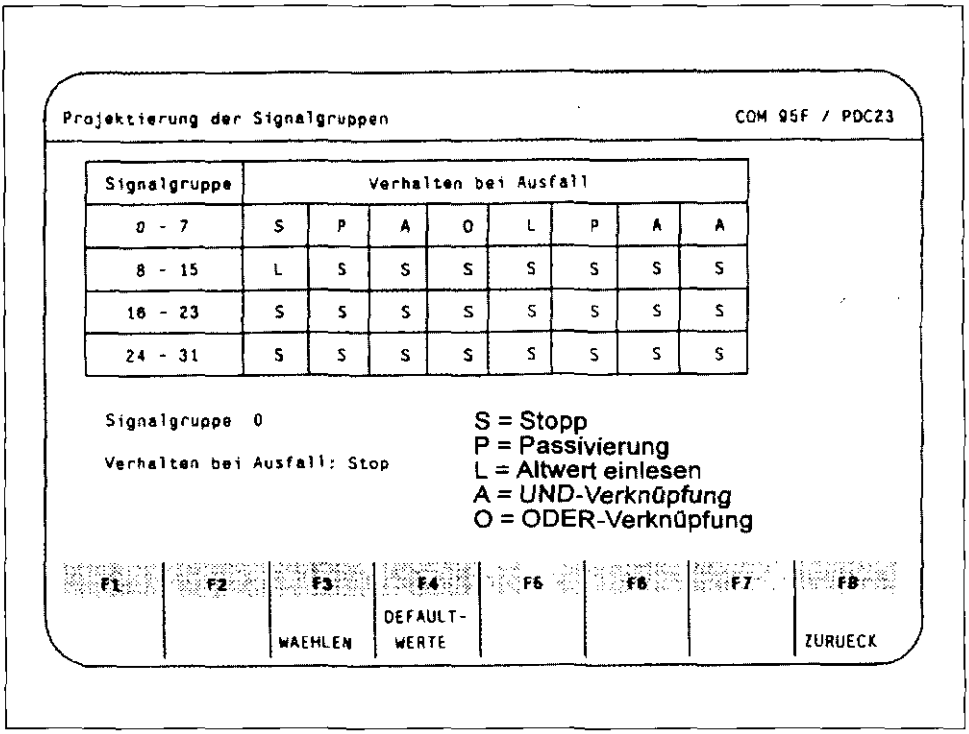
- ☐ Ein-/Ausgabeeinheiten: Test aller digitalen Eingänge über eine wandernde 1 und wandernde 0 über spezielle digitale Ausgänge; die Ein- und Ausgangsdaten werden über die Lichtwellenleiterkopplung verglichen; alle Ausgänge werden zweikanalig und invers ausgegeben. Alle Ausgänge werden überwacht.
- ☐ Datenleitungen (interne Kommunikation): Spezielle Übertragungsprotokolle; Informationsredundanz (teilweise invers) mit Vergleich in jedem Kanal.
- ☐ Stromversorgung: Alle Versorgungsspannungen werden überwacht; Power-down-Routine mit Speicherung aller sicherheitsrelevanten Daten; die Pufferbatterie für das RAM wird kontinuierlich überwacht.
- ☐ Takt und Programmablauf: Getesteter Watchdog mit getrennter Zeitbasis ohne Zeitfenster; gegenseitige zeitliche und logische Programmlaufüberwachung der einzelnen Kanäle innerhalb von 5 ms und über den Austausch einer programmabhängigen Variablen.
- ☐ Externe Kommunikation: Jeder Datenaustausch über das Bussystem zwischen verschiedenen SPSen wird über eine Signatur mit doppelter Wortbreite (CRC) und Vergleich in beiden Kanälen überwacht; die Kommunikation mit dem Programmiergerät wird durch einen Änderungsvergleicher und einen Verfälschungsvergleicher überwacht; gegenüber externen elektromagnetischen Störeinstrahlungen wurden Filter installiert und sämtliche Kommunikation wird über ein Übertragungsprotokoll gesichert (dynamisches Prinzip).
- ☐ Alle sicherheitsrelevanten Ein- und Ausgänge müssen projektiert werden, bevor die Anwendungssoftware ausgeführt werden kann. Für jeden Ein- und Ausgang auf jeder Baugruppe muß spezifiziert werden, ob es sich um einen redundanten Ein-/Ausgang handelt, mit welcher Flanke der entsprechende Eingang schalten soll, wie groß die Diskrepanzzeit (das ist die Zeit, die redundante Ein- und Ausgänge unterschiedliche Potentiale haben dürfen) der redundanten Ein- und Ausgänge sein darf und ob ein Testausgang für die Überwachung eines relativ statischen Eingangs benutzt wird. Alle Ein-/Ausgänge werden auf diese Weise über ein menügesteuertes Programm projektiert, mit dem die Projektierung auch entsprechend dokumentiert werden kann. Wenn z.B. ein Ausgang, der als redundant projektiert wurde, nicht redundant verbunden wird, verhindert das Betriebssystem der SPS den Start des gesamten Anwenderprogramms. Dasselbe passiert, wenn der gleiche Eingang der beiden Kanäle nicht den gleichen Zustand innerhalb der Diskrepanzzeit einnimmt.

- Zusätzlich muß für jede Signalgruppe (das ist eine Gruppe von Signalen, die logisch zusammengehört) die Reaktion im Falle eines detektierten Fehlers spezifiziert werden (siehe Abbildung 58). Fünf unterschiedliche Reaktionen sind möglich: Das Abschalten der Signalgruppe über ein internes Relais (S); das Ignorieren aller Signale dieser Gruppe (alle Ein- und Ausgänge werden auf 0 gesetzt) (P); das Fortfahren mit dem alten Wert (L); das Einlesen des fehlerhaften Signals mit 0 (A) oder 1 (O).

- Für Sensoren wird das Ruhestromprinzip verwendet. Zusätzlich werden Fehler dadurch aufgedeckt, daß ein Eingangsvergleich zusammen mit einem Testmuster für statische Eingänge (Übersprechen von benachbarten Signalleitungen werden aufgedeckt) durchgeführt wird. Bei den Stellgliedern werden Fehler durch das Ruhestromprinzip aufgedeckt, und die gegenseitige Überwachung von redundanten Stellgliedern (Übersprechen von benachbarten Signalleitungen) wird aufgedeckt.

- Um die sicherheitsrelevante Anwenderprogrammierung zu vereinfachen, wurden Standardsoftwaremodule zusammen mit einer spezifischen Ein-/Ausgangskonfiguration integriert. Als ein Beispiel soll die Ausführung eines Not-Aus über den Funktionsbaustein „Not-Aus" beschrieben werden: Die beiden Kontakte des Not-Aus-Tasters werden mit den redundanten Eingangsleitungen der SPS verbunden. Zusätzlich sind sie mit einer Ausgangsleitung verbunden, damit Kurzschlüsse in den Signalleitungen des Not-Aus-Tasters aufgedeckt werden können. Die redundanten Schütze für die Abschaltung werden über redundante Ausgangskanäle der SPS angesteuert (ein Schütz mit positivem und das andere mit negativem Ausgang). Zwei Öffnerkontakte werden dazu benutzt, die korrekte Funktionsweise der Schütze zu überwachen. Der Funktionsbaustein garantiert eine Reaktionszeit von 14 ms für die On-Bord-Peripherie und 135 ms für die externen Ein-/Ausgabebaugruppen. Eine detaillierte Benutzeranweisung beschreibt für diesen Funktionsbaustein im Detail, wie die Sensoren und die Stellglieder zu verbinden sind, wie die verschiedenen Ein-/Ausgänge projektiert werden müssen und wie der Funktionsbaustein im Programm aufgerufen werden muß. Andere Funktionsbausteine sind verfügbar. Alle diese Module können nicht durch den Benutzer verändert werden. Die Fehler bei der Anwendung dieser Funktionsbausteine werden minimiert, und es ist sehr einfach, diese Standardbausteine in die sicherheitsrelevante Anwendung zu integrieren.

Abbildung 58:
Projektierung der Ein-/Ausgänge der SPS




| Signalgruppe | Verhalten bei Ausfall | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 - 7 | S | P | A | O | L | P | A | A |
| 8 - 15 | L | S | S | S | S | S | S | S |
| 16 - 23 | S | S | S | S | S | S | S | S |
| 24 - 31 | S | S | S | S | S | S | S | S |

☐ Häufig sind Änderungen in der Software die Quelle von gefährlichen Fehlern. Aus diesem Grund wurde ein sogenannter Änderungsvergleicher implementiert, der die sicherheitsrelevante Software überprüfen kann. Diese Firmware vergleicht die geänderte Software mit der vorherigen Version und markiert alle geänderten Stellen, so daß ein Überblick über die Änderungen dokumentiert werden kann.

**Anwendung:**

☐ Bei hohen Risiken, z.B. bei regelmäßigem Eingriff in den Gefahrbereich und geringer Wahrscheinlichkeit, daß die Gefahr durch andere Maßnahmen noch abgewendet werden kann.

**Weiterführende Literatur:**

☐ *Reinert, D.; Reuß, G.*: Sicherheitstechnische Beurteilung und Prüfung mikroprozessorgesteuerter Sicherheitseinrichtungen. Sicherheitstechnisches Informations- und Arbeitsblatt 310 222. In: BIA-Handbuch 17. Lfg. X/91 Erich Schmidt Verlag, Bielefeld

☐ *Reinert, D.; Reuß, G.; Jürs, H.; Faller, R.; Hammerschall, J.*: Validation of functional safety of programmable electronic systems according to IEC 1508. In: Preprints of fifth international working conference on dependable computing for critical applications. Urbana-Champaign 1995

☐ *Barradonge, W.; Cluang A.; Sohl, W.*: Techniques for testing the microprocessor family. In: Proceedings of the IEEE 64 (1976), Nr. 6, S. 943-950

☐ *Maehle, E.*: Entwurf von Selbsttestprogrammen für Mikrocomputer. In: Microcomputing. Berichte der Tagung III/79 des German Chapter of the ACM/ Remmele, W., Schecher, H. (Hrsg.), Stuttgart, Teubner 1979, S. 204-216

☐ *Vasa, S.*: Calculating an error checking character in software. In: Computer Design (1976), Nr. 5

# 5 Schlußbetrachtung

Mit dem vorliegenden Report wird der Fachwelt deutlich, daß mit Veröffentlichung der EN 954 Teil 1 die Sicherheitstechnik von Schutzeinrichtungen und Steuerungen in Deutschland nicht völlig verändert wird. Auch in der Vergangenheit hat es schon bewährte Bauteile und Prinzipien gegeben, wurden Schaltungsstrukturen mit einer „Anlauftestung" versehen, gab es in den Unfallverhütungsvorschriften das Prinzip der „Einfehlersicherheit" und wurden „selbstüberwachte" Steuerungen und Schutzeinrichtungen gebaut und beurteilt, die der Kategorie 4 entsprechen. So sind denn die Beispiele dieses Reports aus der langjährigen Erfahrung des BIA entstanden. Die Norm hat viele grundlegende Maßnahmen, die in Deutschland schon seit Jahren angewendet werden, systematisch klassifiziert und z.T. neu bezeichnet. So stellen die grundlegenden Sicherheitsprinzipien das dar, was zu einer solide aufgebauten Sicherheitssteuerung dazu gehört. Die bewährten Sicherheitsprinzipien finden sich verstreut in den unterschiedlichen nationalen Normen der Vergangenheit. Der risikobezogene Ansatz ist in Deutschland schon seit über zehn Jahren in der Diskussion und hat die Technik der Schutz- und Steuereinrichtungen, auch durch Veröffentlichung der DIN V 19 250 [6], seit längerem gestaltet. Mit der neuen EN 954 [5] werden also wesentliche Aspekte der in Deutschland angewandten Sicherheitstechnik bei Maschinen auf die europäische Ebene übertragen.

Zur Zeit laufen die Arbeiten für einen Teil 2 der EN 954, in dem die Validierung der einzelnen Kategorien für die unterschiedlichen Technologien festgelegt werden soll. Es ist vorgesehen, daß in diesem zukünftigen Teil 2 konkrete Fehlerlisten aufgenommen und weitere Einzelheiten zur Umsetzung der Kategorien gegeben werden. Damit stünde eine offizielle Interpretation der Norm zur Verfügung. Bis der Teil 2 Weißdruck wird, können allerdings noch mehrere Jahre vergehen. Bis dahin kann dieser Report die weitere Normungarbeit befruchten und in der Übergangszeit Hilfen für eine Interpretation der Norm geben.

Weiterhin ist geplant, die Europanorm auf die internationale Ebene der ISO-Standardisierung zu bringen. Gelingt dieses Vorhaben, so werden die Kategorien auch über Europa hinaus Standard werden. Deutsche Hersteller tun deshalb gut daran, sich schon heute dieses Gedankengut zu eigen zu machen und es in Produkte umzusetzen.

# Literaturverzeichnis


[1] Richtlinie des Rates vom 14. Juni 1989 zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten für Maschinen (89/392/EWG). In: Amtsblatt der Europäischen Gemeinschaften 1989. L 183, S. 9-32

[2] *Massimi P.; Van Gheluwe, J.-P.:* Die Rechtsvorschriften der Gemeinschaft für *Maschinen. Erläuterungen zu den Richt*linien 89/392/EWG und 91/368/EWG. Bundesanzeiger Verlag. Luxemburg 1993

[3] EN 292: Sicherheit von Maschinen — Grundbegriffe, allgemeine Gestaltungsleitsätze. *Teil 1: Grundsätzliche Ter*minologie, Methodik. Beuth-Verlag, Berlin 1991

[4] EN 1050: Sicherheit von Maschinen — Leitsätze zur Risikobeurteilung. Beuth-Verlag, Berlin 1996

[5] EN 954-1: Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen. Teil 1: Allgemeine Gestaltungsleitsätze. Beuth-Verlag, Berlin 1996

[6] DIN V 19 250: Leittechnik. Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. Beuth-Verlag, Berlin 1994

[7] prEN 1760-1: Sicherheit von Maschi*nen* — Druckempfindliche Schutzeinrichtungen. Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltmatten und Schaltplatten. Beuth-Verlag, Berlin 1995

[8] prEN 50 100: Sicherheit von Maschinen — Berührungslos wirkende Schutzeinrichtungen. Teil 1: Allgemeine Anforderungen und Prüfungen. Brüssel 1994

[9] EN 574: Sicherheit von Maschinen — Zweihandschaltungen. Funktionelle Aspekte — Gestaltungsleitsätze. Beuth-Verlag, Berlin 1995

[10] EN 1088: Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl. *Beuth-Verlag, Berlin 1996*

[11] DIN 25 424-1: Fehlerbaumanalyse: *Methode und Bildzeichen. Beuth-Verlag,* Berlin 1981

[12] *Bömer, T.; Reinert, D.: Empfehlungen* für die Prüfung scannender opto-elektronischer Taster. Sicherheitstechnisches Informations- und Arbeitsblatt 310 242. In: BIA-Handbuch 27. Lfg. Erich Schmidt Verlag, Bielefeld 1996

[13] DIN 25 419: Ereignisablaufanalyse: Verfahren, graphische Symbole und Auswirkung. Beuth-Verlag, Berlin 1985

[14] DIN 25 448: Ausfalleffektanalyse. Beuth-Verlag, Berlin 1990

[15] *Meffert, K.*: Klassifikation von Risiken und technischen Maßnahmen. In: Die BG (1993) Nr. 7, S. 406-412

[16] DIN VDE 0801 (IEC 1508): Entwurf: Funktionale Sicherheit. Sicherheitssysteme, Teile 1-7. Beuth-Verlag, Berlin 1996

[17] DIN V VDE 0801: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, mit Anhang A1. Beuth-Verlag, Berlin 1990 und 1994

[18] DIN EN 60 204: Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen. Beuth-Verlag, Berlin 1993

[19] EN 60 947-5-1: Niederspannungs-Schaltgeräte — Teil 5-1: Elektromechanische Steuergeräte. Beuth-Verlag, Berlin 1995

[20] DIN EN 982: Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Hydraulik. Beuth-Verlag, Berlin 1996

[21] DIN EN 983: Sicherheit von Maschinen — Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile — Pneumatik. Beuth-Verlag, Berlin 1996

[22] DIN EN 1037: Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf. Beuth-Verlag, Berlin 1996

[23] ISO 1219-1: Fluid power systems and components — Graphic symbols and circuit diagrams — Part 1: Graphic symbols. ISO-Verlag, Genf 1991

[24] DIN ISO 1219-2: Fluidtechnik — Graphische Symbole und Schaltpläne. Teil 2: Schaltpläne. Beuth-Verlag, Berlin 1994

[25] DIN ISO 8573-1: Druckluft für allgemeine Anwendungen. Teil 1: Verunreinigungen und Qualitätsklassen. Beuth-Verlag, Berlin 1995

[26] *Felgendreher, K.; Meffert, K.*: Klassifikation von Risiken — Beispiel zur Anwendung von DIN V 19 250 Kraftbetätigte Fenster, Türen und Tore. Sicherheitstechnisches Informations- und Arbeitsblatt 320 190 In: BIA-Handbuch 11. Lfg. Erich Schmidt Verlag, Bielefeld 1989

[27] *Bock, H.; Bömer, T.*: Klassifikation von Risiken — Beispiel zur Anwendung von DIN V 19 250 Auffahrschutz an fahrerlosen Flurförderzeugen. Sicherheitstechnisches Informations- und Arbeitsblatt 320 121. In: BIA-Handbuch 19. Lfg. Erich Schmidt Verlag, Bielefeld 1992

[28] *Meffert, K.; Schwind H.*: Klassifikation von Risiken — Beispiel zur Anwendung von DIN V 19 250 Planschneidemaschine. Sicherheitstechnisches *Informations- und Arbeitsblatt* 320 180. In: BIA-Handbuch 11. Lfg. Erich Schmidt Verlag. Bielefeld 1989

[29] *Grigulewitsch, W.; K. Meffert und G. Reuß*: Fehlerliste für elektrische Bauelemente. Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 220 In: BIA-Handbuch 13. Lfg. Erich Schmidt Verlag, Bielefeld 1989

[30] *Gorgs, K.-J.; W. Kleinbreuer* und *W. Kühlem*: Fehlerlisten für hydraulische und pneumatische Bauelemente. Bei der Prüfung unterstellte Fehlerarten. *Sicherheitstechnisches Informations-* und Arbeitsblatt 340 225 In: BIA-Handbuch 14. Lfg. Erich Schmidt Verlag, Bielefeld 1990

# Anhang

# Anhang A: Beispiele zur Risikoabschätzung an Maschinen

Es sind zahlreiche Verfahren bekannt, eine Risikoeinschätzung und -bewertung bei technischen Systemen durchzuführen [5, 6, 16][1]. Alle Verfahren greifen an den beiden Risikoelementen „Ausmaß des möglichen Schadens" und „Wahrscheinlichkeit des Eintritts dieses Schadens" an. Sie bestimmen in der Risikobewertung die erforderliche Risikoreduzierung, um ein tolerables Restrisiko für eine technische Anwendung zu erreichen.

In diesem Report soll das auf [6] aufbauende Verfahren, das sich im informativen Anhang B der EN 954-1 wiederfindet, beispielhaft beschrieben werden. Dazu wird dieses Verfahren auf konkrete Beispiele aus dem Bereich des Maschinenschutzes angewendet und die erforderliche Kategorie bestimmt.

[1] Im Teil 5 von [16] werden quantitative und qualitative Verfahren zur Risikoeinschätzung und -bewertung vorgestellt. Der Anhang C dieses Teiles beschreibt die quantitative Vorgehensweise, die eine quantitative Vorgabe des akzeptablen Restrisikos erfordert. Anhang D skizziert das in Deutschland genormte Verfahren zur Risikoabschätzung über den Risikographen nach [6]. Anhang E stellt eine qualitative Methode aus dem Bereich der Prozeßindustrie in den USA dar.

## A.1 Der Risikograph

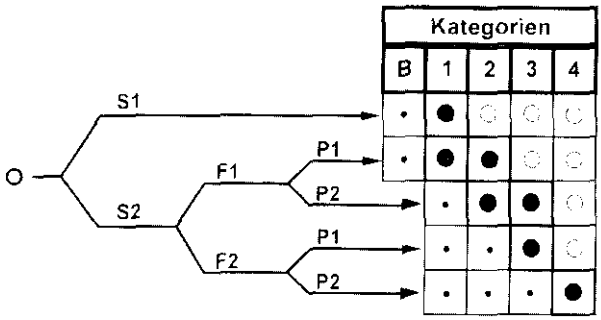
Der durch den informativen Anhang B der EN 954-1 eingeführte Risikograph liefert ein Verfahren, das dem Prozeß innewohnende Risiko durch die Risikoelemente der EN 1050 auf die Kategorien als Risikoreduzierungsmaßnahmen abzubilden (Abbildung A1, siehe Seite 166). Die Eintrittswahrscheinlichkeit eines Gefährdungsereignisses hat dabei einen Einfluß darauf, ob die bevorzugte Kategorie niedriger oder höher gewählt werden muß.

Man erkennt sofort, daß es sich nicht um eine multiplikative Verknüpfung von „Schwere der Verletzung" S und „Häufigkeit" H handelt, sondern je nach „Schwere der Verletzung" S die Elemente „Häufigkeit und/oder Dauer der Gefährdungsexposition" F, „Möglichkeit zur Vermeidung der Gefährdung" P oder nur S in die Beurteilung des Risikos eingehen. Dies liegt daran, daß z.B. für das Risikoelement S1 eine Charakterisierung der Häufigkeit durch die Parameter F und P zu keinen sinnvollen weiteren Abstufungen des Risikos führen.

Der Risikograph führt zu unterschiedlichen Kategorien, wobei mit der Ordnungszahl der Kategorie auch das von dem sicherheitsrelevanten Teil einer Steuerung zu beherrschende Teilrisiko wächst. Analog zu diesem Teilrisiko

wachsen mit steigender Kategorie, wie der Report gezeigt hat, auch die zu ergreifenden Maßnahmen, um das Teilrisiko auf ein tolerierbares Maß zu reduzieren.

Die einzelnen Risiken werden allerdings nur dann direkt Steuerungskategorien zugeordnet, wenn die erforderliche Risikoreduzierung ausschließlich durch steuerungstechnische Maßnahmen erreicht wurde. Eine Reduzierung der Kategorie ist möglich, wenn zusätzliche nicht technische Maßnahmen, z.B. Betrieb nur nach Betätigung eines Schlüsselschalters durch besonders unter-




S - Schwere der Verletzung
- S1 - Leichte (üblicherweise reversible) Verletzung
- S2 - Schwere (üblicherweise irreversible) Verletzung, einschließlich Tod

F - Häufigkeit und Aufenthaltsdauer
- F1 - Selten bis öfter und/oder kurze Dauer der Exposition
- F2 - Häufig bis dauernd und/oder lange Dauer der Exposition

P - Möglichkeit zur Vermeidung von Gefährdungen
- P1 - Möglich unter bestimmten Bedingungen
- P2 - Kaum möglich

● - Bevorzugte Kategorie

• - Zusätzliche Maßnahmen erforderlich

. - Überdimensionierte Kategorie

Abbildung A1:
Hinweise zur Auswahl der Kategorien

wiesene Personen, ergriffen werden. Inwieweit die Gesamtrisikoreduzierung auf technische und nicht technische Maßnahmen aufgeteilt werden kann, ist aus den Erfahrungen mit äquivalenten Anwendungen im Einzelfall zu entscheiden. Die Tabelle gibt einen Überblick über das Gesamtverfahren der Risikoreduzierung nach dem oben vorgestellten Prinzip.

Tabelle:
Gesamtverfahren zur Risikoreduzierung

| **Vorgaben durch** | **Aktion** | **Hilfsmittel** |
|---|---|---|
| Konzept der Gesamtmaschine/ Vergleich mit bestehenden Lösungen, EN 1050 | Beschreibung der jeweiligen Gefährdung durch die Maschine | Fehlerbaumanalyse (FTA), Ausfallarten und Ausfallauswirkungsanalyse (FMECA), Studien zu Gefährdung und Betrieb (HAZOP) |
| EN 1050, EN 954 Anhang B | Bestimmung der Risikoelemente ohne irgendwelche *Schutzmaßnahmen* | Risikograph |
| Verbindliche Systemspezifikation | Auflistung der nicht steuerungstechnischen Maßnahmen | Ereignisablaufanalyse (ETA) |
| bestehende lösungen, iteratives Vorgehen | Welche nicht steuerungstechnischen Maßnahmen wirken auf welche Risikoelemente? | — |
| EN 954 Anhang B | Bestimmung der Kategorie für die jeweiligen STS | Risikograph |
| anwendungsspezifische Normen | Beschreibung der nichttechnischen Schutzmaßnahmen | Ereignisablaufanalyse (ETA) |
| EN 954, IEC 1508 | Beschreibung der verbleibenden Maßnahmen für die STS | IEC 1508, dieser Report, DIN V 19 251, DIN V VDE 0801 |

## A.2 Beispiele der Anwendung des Risikographen

In Abbildung A2 ist die Risikoeinschätzung für die Schließkantensicherung[2] an kraftbetätigten Fenstern, Türen oder Toren [26] dargestellt. Mit der Bewegung kraftbetätigter Fenster-, Tür- und Torflügel (siehe Abbildung A2) ist in der Regel die Bildung von Quetsch- und Scherstellen verbunden. Diese Gefahrstellen werden im allgemeinen nur dann gebildet, wenn sich der Flügel seinen Endstellungen nähert. Verletzungen an derartigen Gefahrstellen lassen sich z.B. durch Schließkantensicherungen vermeiden. Die Schließkantensicherungen, z.B. Schaltleisten, werden auf die Schließkanten der Flügel gesetzt.

Die Quetsch- und Scherstellen können an kraftbetätigten Fenster-, Tür- und Torflügeln Ursache für schwere, u.U. tödliche Verletzungen sein, so daß als Schadensausmaß S2 angenommen werden muß. Personen halten sich im Bereich der zeitlich begrenzt auftretenden Quetsch- und Scherstellen nur selten und auch nur für kurze Zeit auf (F1). Normalerweise haben gefährdete Personen die Möglichkeit, sich aus dem vom bewegten Flügel gebildeten Gefahrenbereich zu entfernen (P1). Bei Schnellauftoren ist diese Möglichkeit eingeschränkt (P2). Nach Abbildung A2 sollte die Schließkantensicherung selbst bei Schnellauftoren damit der Steuerungskategorie 2 entsprechen.

Da ein fahrerloses Transportfahrzeug sich mit u.U. tonnenschwerer Last bewegt, ist eine schwere irreversible Verletzung bei einer Kollision mit dem Fahrzeug, wenn sie bei voller Geschwindigkeit stattfindet, wahrscheinlich (S2). Die Fahrwege des Fahrzeuges sind für Personen frei zugänglich, und es muß deshalb mit einer relativ häufigen Aufenthaltsdauer von Personen im Gefahrenbereich gerechnet werden (F2). Da das Fahrzeug mit recht niedrigen Geschwindigkeiten fährt (in der Regel 3—5 km/Stunde), hat ein Fußgänger bei Herannahen eines solchen Fahrzeuges in der Regel die Möglichkeit, dem Fahrzeug auszuweichen (P1). Der Auffahrschutz an fahrerlosen Flurförderzeugen sollte damit der Steuerungskategorie 3 entsprechen [27] (Abbildung A3, siehe Seite 170).

Mit der in Abbildung A4 (siehe Seite 171) dargestellten Planschneidemaschine [28] werden dicke Stapel von

[2] Schließkantensicherungen fallen z.Z. noch unter die Bauproduktenrichtlinie. Es ist aber beabsichtigt, daß die Schließkantensicherungen bei der nächsten Überarbeitung mit in die Maschinenrichtlinie aufgenommen werden. Die Schließkantensicherung an einem kraftbetätigten Tor ist ein klassisches Beispiel für die Anwendung der Kategorie 2 und wurde deshalb in diesen Anhang aufgenommen.

Papier nach der Schnittauslösung über eine Zweihandschaltung zuerst gepreßt und dann geschnitten. Der Benutzer muß vor jedem Schneidvorgang in die Gefahrstelle eingreifen. Das Lichtgitter verhindert zusammen mit der Zweihandschaltung sowie einer sicher ausgeführten Steuerung der Gesamtmaschine, daß es bei der Beschickung zu Verletzungen kommen kann.

Der Benutzer der Planschneidemaschine ist dem Risiko einer schweren Handverletzung (S2) sehr häufig (nämlich bei

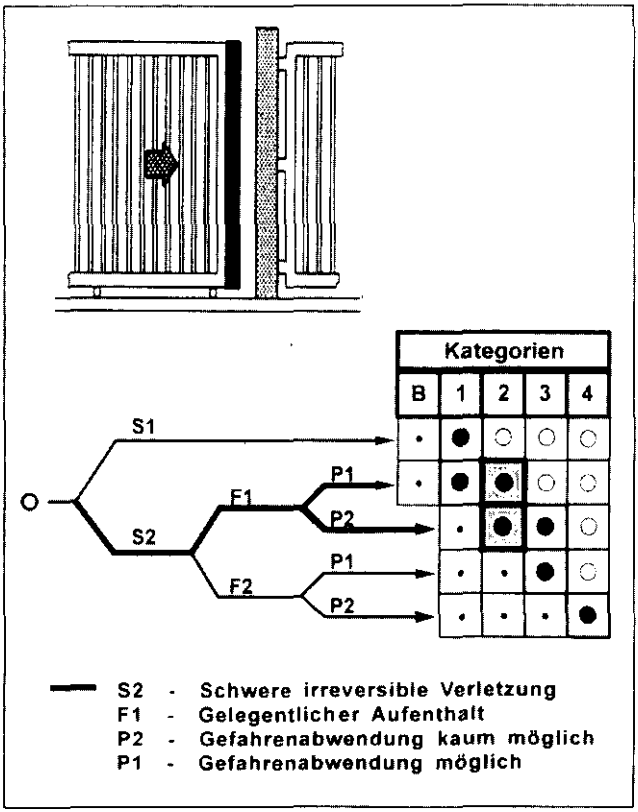



Abbildung A2:
Risikoeinschätzung für die Schließkantensicherungen an kraftbetätigten Fenster, Türen und Toren

jeder Beschickung (F2)) ausgeliefert und hat bei einer Fehlsteuerung der Maschine kaum eine Möglichkeit, der Gefahr zu entrinnen (P2). Die Schutzeinrichtung und die gesamte Sicherheitssteuerung eines derartigen Systems sollte damit der Steuerungskategorie 4 entsprechen (Abbildung A4).

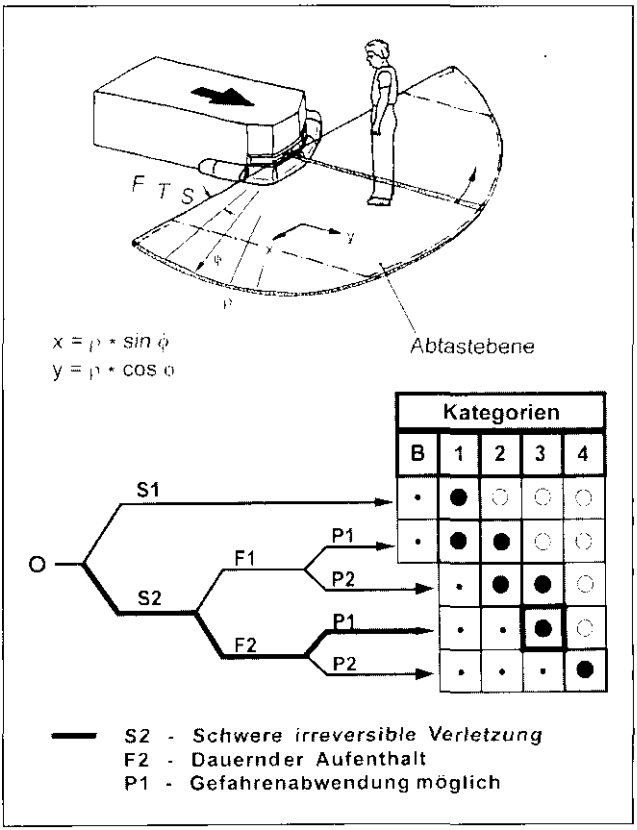



Abbildung A3:
Risikoeinschätzung für den Auffahrschutz an einem fahrerlosen Flurförderzeug

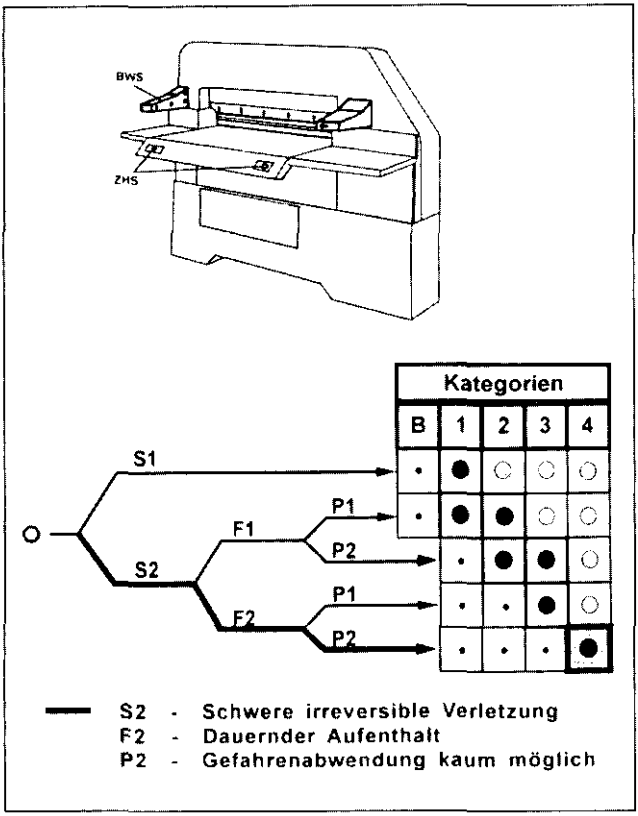



Abbildung A4:
Risikoeinschätzung für die Steuerung einer Planschneidemaschine

Diese Beispiele zeigen, daß bei gleichem Schadensausmaß sehr unterschiedliche Risiken vorliegen können, die dann zu unterschiedlichen Steuerungskategorien führen.

Alle diese Beispiele sind dem BIA-Handbuch entnommen, in dem sich zahlreiche weitere Anwendungen aus dem Maschinenschutz finden. Die Ergebnisse, die noch den Risikographen der DIN V 19 250 zugrunde legen, können durch Tabelle 8 aus Kapitel 4 auf die Kategorien der EN 954-1 übertragen werden.

# Anhang B: Fehlerlisten
## *(im Original übernommen)*

Die Kategorien stellen eine Einteilung der sicherheitsbezogenen Teile einer Steuerung (STS) in bezug auf ihre Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall dar, die aufgrund der Zuverlässigkeit und/oder der strukturellen Anordnung der Teile erreicht wird (siehe Tabelle 3). Diese im Kapitel 3 dieses Reportes gemachte Feststellung zeigt die Bedeutung einer für alle Beteiligten verbindlichen Fehlerliste, in der, speziell ausgerichtet für den industriellen Maschinen- und Anlagenbau, die zugrundegelegten Fehlerarten für die unterschiedlichen elektrischen und fluidtechnischen Bauteile aufgeführt werden.

Im BIA-Handbuch [29, 30] haben die Autoren derartige Fehlerlisten, die im Laufe der Zeit mehrfach überarbeitet und um Hinweise aus der einschlägigen Literatur und den technischen Regeln ergänzt worden sind, veröffentlicht. Wesentliche Gedanken der BIA-Fehlerlisten haben inzwischen Eingang in europäische Arbeitspapiere oder auch erste Normentwürfe [8] gefunden. Das Grundprinzip für jedes Bauteil, leicht reproduzierbare Fehlerannahmen, Fehlerausschlüsse und Anmerkungen zu letzteren aufzulisten, wurde beibehalten. Einige Fehler und Fehlerausschlüsse wurden modifiziert. Trotzdem glauben die Autoren, daß die BIA-Fehlerlisten vor der endgültigen Veröffentlichung der Arbeitspapiere und Normentwürfe eine gute Basis bei der Konstruktion und der Bewertung von sicherheitsrelevanten Teilen von Steuerungen und Schutzeinrichtungen darstellen. Aus diesem Grund und wegen der hohen Nachfrage nach diesen Listen im Zusammenhang mit der Anwendung der EN 954-1 werden die BIA-Fehlerlisten in diesem Anhang abgedruckt.

Berufsgenossenschaftliches Institut für Arbeitssicherheit

Sicherheitstechnisches Informations- und Arbeitsblatt

# Fehlerliste für elektrische Bauelemente – Bei der Prüfung unterstellte Fehlerarten –

## 1 Einleitung

An technischen Einrichtungen, bei denen beim Versagen der Steuerung Personen zu Schaden kommen können, werden bestimmte Sicherheitsanforderungen bezüglich des Verhaltens im Fehlerfall gestellt. Beispiele hierfür finden sich im Bereich

- der Maschinen- und Anlagentechnik, z.B. [1 bis 8],
- der technischen Schutzeinrichtungen und *sicherheitsrelevanten Bauteile*, z.B. [9 bis 13],
- der Verkehrs- und Transporttechnik, z.B. [14 bis 21],
- der Medizintechnik, z.B. [22],
- der Energietechnik, z.B. [23; 24].

Welche Auswirkungen auftretende Fehler in sicherheitsrelevanten Steuerungen haben können, wird im sicherheitstechnischen Informations- und Arbeitsblatt 330 250 dieses Handbuches gezeigt.

Die in den technischen Regeln und Unfallverhütungsvorschriften gestellten Sicherheitsanforderungen sind sehr stark von der jeweiligen Anwendung abhängig und reichen im einfachsten Fall von organisatorischen Maßnahmen, wie regelmäßige, willensabhängige Funktionsprüfungen, über automatische Testschaltungen bis hin zu sogenannten selbstüberwachten Steuerungen, bei denen sich aufgetretene Fehler selbsttätig bemerkbar machen. Die Gesamtheit der Überlegungen, die notwendig sind, das sicherheitstechnische Verhalten einer Einrichtung im Fehlerfall zu beschreiben und auch praktisch zu überprüfen, nennt man Fehlerbetrachtung. Eine der wichtigsten Fragen im Rahmen der Fehlerbetrachtung ist, welche Fehler an *elektrischen Bauelementen* unterstellt werden. Eine solche Fehlervereinbarung [25] ist als Basis notwendig, um dem Entwickler verbindliche Kriterien für den Entwurf seines steuerungstechnischen Sicherheitskonzepts zu liefern. Andererseits soll mit dieser Fehlervereinbarung gewährleistet werden, daß verschiedene Prüfstellen und Prüfer beim gleichen Prüfobjekt nicht zu unterschiedlichen Ergebnissen gelangen.

Welche Fehler sind nun in eine solche Fehlerliste *aufzunehmen*? *Würde man* alle theoretisch denkbaren Fehler eines Bauelementes bei der Fehlerbetrachtung unterstellen, so gäbe dies nicht nur einen extrem hohen Prüfaufwand, teilweise wäre die Prüfung überhaupt nicht mehr durchführbar. In vielen Fällen wäre es sogar unmöglich, eine sichere Steuerung aufzubauen, da das Prinzip fehlersicherer Schaltungen voraussetzt, Bauelemente zur Verfügung zu haben, bei denen bestimmte Fehler ausgeschlossen werden können (Fehlerausschluß).

Für den Anwendungsbereich Eisenbahnsignaltechnik sind in der Vergangenheit Fehlerkataloge für elektrische Bauelemente erstellt worden [26; 27]. Auch aus der Literatur, z.B. [28], und aus Technischen Regeln und Richtlinien, z.B. [3; 14; 15; 23; 29], lassen sich Hinweise auf unterstellte Fehler und Fehlerausschlüsse entnehmen. Diese Fehlerlisten sind jedoch nur bedingt auf allgemeine industrielle Anwendungen übertragbar und widersprechen sich sogar teilweise in Detailfestlegungen. In den meisten Normen und Sicherheitsregeln sind jedoch keine Aussagen enthalten, welche Fehler bei der *Fehlerbetrachtung* konkret zu unterstellen sind.

## 2 Anforderungen an eine Fehlerliste

Um für steuerungstechnische Sicherheitsprüfungen immer gleiche Voraussetzungen zu schaffen, wurden im *Berufsgenossenschaftlichen Institut für Arbeitssicherheit – BIA* die bei *Prüfungen zugrundegelegten Fehlerarten* elektrischer Bauelemente zusammengestellt. Diese Zusammenstellung – speziell ausgerichtet für den industriellen Maschinen- und *Anlagenbau – wurde im Laufe der Zeit* mehrfach überarbeitet und ergänzt um Hinweise aus der einschlägigen Literatur und den Technischen Regeln. Die Liste – seit mehreren Jahren in der Prüfpraxis erprobt – stellt einen Kompromiß verschiedener, sich teilweise widersprechender Anforderungen dar, die nachstehend erläutert werden:

**Hoher Fehlerabdeckungsgrad**

Die bei der Fehlerfallprüfung unterstellten Fehler sollten möglichst viele der insgesamt möglichen Fehler abdecken. Je höher der Fehlerabdeckungsgrad, desto geringer ist das Risiko, unter Umständen gefährliche Fehlerarten zu übersehen.

**Durchführbarkeit**

Je komplexer ein Bauelement ist, desto größer ist die Vielfalt der möglichen Fehler. So sind beispielsweise in [27] für den Transistor alleine 51 Fehlerarten aufgeführt; schon bei LSI-Bausteinen ergeben sich astronomisch hohe, unterschiedliche Fehlermöglichkeiten. Zur Durchführung der Fehlerfallprüfung müssen deshalb die theoretisch möglichen Fehlerarten eingeschränkt werden. Diese Einschränkung muß so erfolgen, daß trotzdem – was die Fehlerauswirkung betrifft – ein hoher Fehlerabdeckungsgrad erreicht wird. Eine gute Möglichkeit, einerseits die Fehlerfallprüfung einfach durchführen zu können, andererseits aber auch einen hohen Fehlerabdeckungsgrad zu haben, ist die Annahme eines „worst-case"-Fehlers bei einem komplexen integrierten Bauteil oder auch bei einer ganzen Baugruppe. „Worst-case"-Fehler bedeutet hier, daß an den Ausgängen des Bauelementes oder der Baugruppe der sicherheitstechnisch ungünstigste – meist logische oder sequentielle – Fehler unterstellt wird.

**Möglichkeit des Fehlereinbaus**

Nach Möglichkeit sollten Fehler unterstellt werden, die in die zu prüfende Originalschaltung auch eingebaut werden können. Dies ist nicht immer möglich, wenn man beispielsweise an bestimmte interne Driftvorgänge in Halbleiter-Bauelementen denkt. Je nach Schaltungsprinzip bleibt hier u.U. nichts anderes übrig, als die Auswirkung solcher Fehler mit Hilfe theoretischer Berechnungsverfahren zu ermitteln.

**Reproduzierbarkeit**

Die eingebauten Fehler sollten, soweit möglich, so ausgewählt sein, daß sich ein reproduzierbares Prüfergebnis ergibt. Dies ist nicht immer selbstverständlich, wenn man beispielsweise bei CMOS-Bausteinen die Unterbrechung eines Eingangs-Anschlußpins unterstellt. Hier müssen u.U. besondere Prüfverfahren greifen, wie beispielsweise „Potential ziehen" (stuck-at-Fehler).

**Wirtschaftlichkeit**

Die unterstellten Fehler sollen einen rationellen Fehlereinbau erlauben. Der Einbau der Fehler in die Originalschaltung nimmt bei experimentellen Methoden den größten Zeitumfang ein.

**Herstellerunabhängigkeit**

Die Art der eingebauten Fehler sollte weitgehend unabhängig vom Hersteller der Bauelemente sein. Eine Ausnahme bildet hier die Inanspruchnahme eines Fehlerausschlusses.

**Realistische Fehlerausschlüsse**

Es wurde bereits erwähnt, daß ohne die Annahme konkreter Fehlerausschlüsse sichere Steuerungen nicht realisierbar sind. Nun stellen diese Fehlerausschlüsse – sieht man von bestimmten, physikalisch begründeten Einzelfällen ab – wiederum einen Kompromiß zwischen den sicherheitstechnischen Erfordernissen und den technisch/wirtschaftlichen Möglichkeiten dar. So können Fehlerausschlüsse beispielsweise begründet werden

- durch die physikalische Unmöglichkeit einer bestimmten Fehlerart (Beispiel: starke Zunahme der Kondensatorkapazität),
- durch allgemein anerkannte – anwendungsunabhängige – technische Regeln (Beispiel: Kontaktzwangsführung bei Relais),
- durch technisch/wirtschaftliche Aspekte die anwendungsabhängig und damit abhängig vom konkreten Risiko der Anwendung sind (Beispiel: Leitungsschluß bei externen Kabeln).

Die beiden erstgenannten Gründe für einen Fehlerausschluß stellen den Regelfall dar. Dennoch können in bestimmten Anwendungen weitergehende Fehlerausschlüsse gemacht werden. Diese zusätzlichen Fehlerausschlüsse – meist in technischen Regeln konkretisiert – sind abhängig vom Risiko der jeweiligen Anwendung und richten sich insbesondere nach der Wahrscheinlichkeit des Auftretens dieser Fehler. Die Auftrittswahrscheinlichkeit kann durch konkrete Ausfallraten belegt oder durch Erfahrungen aufgrund von Betriebsbewährung abgeschätzt werden.

## 3 Behandelte Bauteile und Komponenten

In den nachstehenden Listen sind die bei den Prüfungen zugrundegelegten Fehlerarten so-

wie die konstruktiven Randbedingungen für mögliche Fehlerausschlüsse zusammengestellt. Dabei werden folgende elektrische Bauteile behandelt:

1 Leitungen und Verbindungen
1.1 Leitungen/Kabel
1.2 Leiterplatte
1.3 Klemmstellen
1.4 Mehrpolige Steckverbindung

2 Hilfsstromschalter
2.1 Mechanische Positionsschalter
2.2 Handbetätigte Schalter und Taster
2.3 Berührungslos wirkende Positionsschalter
2.4 Relais/Schütz

3 Diskrete elektrische Bauelemente
3.1 Transformator, Übertrager
3.2 Drahtwiderstand
3.3 Schichtwiderstand
3.4 Widerstandsnetzwerk
3.5 Potentiometer
3.6 Kondensator, Trimmer

4 Elektronische Bauelemente
4.1 Diskrete Halbleiter (z.B. Diode, Transistor)
4.2 Optokoppler
4.3 Integrierter Schaltkreis (SSI, MSI)
4.4 Integrierter Schaltkreis (LSI, z.B. Speicher, $\mu$P)

## Schrifttum


[1] DIN VDE 0113 Teil 1: Elektrische Ausrüstung von Industriemaschinen – Allgemeine Festlegungen.

[2] DIN VDE 0160: Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln.

[3] Sicherheitsregeln für Steuerungen an kraftbetriebenen Pressen der Metallverarbeitung (ZH 1/457).

[4] Richtlinien für kraftbetriebene Fenster, Türen und Tore (ZH 1/494).

[5] Richtlinien für Lagereinrichtungen und -geräte (ZH 1/428).

[6] Sicherheitsregeln für Schwenkarmstanzen mit Schwenkhilfe (ZH 1/505).

[7] Sicherheitsregeln für Stapelautomaten, Setzmaschinen und automatische Abtragegeräte in der Baustoffindustrie (ZH 1/520).

[8] Unfallverhütungsvorschrift Druck und Papierverarbeitung (VBG 7 i).

[9] Sicherheitsregeln für berührungslos wirkende Schutzeinrichtungen an kraftbetriebenen Arbeitsmitteln (ZH 1/597).

[10] Sicherheitsregeln für berührungslos wirkende Schutzeinrichtungen an kraftbetriebenen Pressen der Metallverarbeitung (ZH 1/281).

[11] Sicherheitsregeln für Zweihandschaltungen an kraftbetriebenen Pressen der Metallverarbeitung (ZH 1/456).

[12] DIN 24980: Zweihandschaltungen.

[13] DIN VDE 0660 Teil 209: Niederspannungsschaltgeräte – Zusatzbestimmungen für berührungslos wirkende Positionsschalter für Sicherheitsfunktionen.

[14] DIN VDE 0831: Elektrische Bahnsignalanlagen.

[15] DIN VDE 0832: Straßenverkehrssignalanlagen (SVA).

[16] Sicherheitsregeln für Verschiebewagen in Stetigförderanlagen (ZH 1/158).

[17] Richtlinien für fahrerlose Flurförderzeuge (ZH 1/473).

[18] TRA 200: Personenaufzüge, Lastenaufzüge, Güteraufzüge.

[19] EN 115: Fahrtreppen.

[20] Richtlinien für Fahrtreppen und Fahrsteige (ZH 1/484).

[21] Richtlinien für Funkfernsteuerung von Kranen (ZH 1/547).

[22] DIN IEC 601 VDE 0750: Sicherheit elektromedizinischer Geräte. Allgemeine Festlegungen. (sowie Teile 2 . . .).

[23] DIN VDE 0116: Elektrische Ausrüstung von Feuerungsanlagen.

[24] DIN 25434: Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems.

[25] VDI/VDE 3541 Blatt 2: Steuerungseinrichtungen mit vereinbarter gesicherter Funktion.

[26] Orе: Frage A 118: Verwendung von elektronischen Bauelementen in der Signaltechnik, Bericht Nr. 2. Forschungs- und Versuchsamt des internationalen Eisenbahnverbandes.

[27] Allgemeine Richtlinien für signaltechnisch sichere Schaltungen und Einrichtungen der Elektronik. Ausfall-Liste 43120 Entwurf. Bundesbahn-Zentralamt München.

[28] Bajenescu, T.I.: Zuverlässigkeit elektronischer Komponenten. VDE-Verlag.

[29] TRA 101: Richtlinie für die Prüfung von Bauteilen.



**Bearbeiter:**

Dipl.-Ing. W. Grigulewitsch, Dr.-Ing. K. Meffert und Dipl.-Ing. G. Reuß
*Fachbereich Elektrotechnik – Steuerungstechnik*

## 1 Leitungen und Verbindungen

### 1.1 Leitungen/Kabel

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Kurzschluß zwischen zwei beliebigen Leitern | – Kurzschluß zwischen Leitern im elektrischen Einbauraum, sofern Leitungen und Einbauraum den einschlägigen DIN VDE-Bestimmungen genügen<br>– Kurzschluß zwischen Leitern, die zu verschiedenen Mantelleitungen gehören<br>– Kurzschluß zwischen Leitern, die durch besondere Maßnahmen vor äußerer Beschädigung geschützt sind (Kabelkanal, Panzerrohr) [1, 2] | [1] Bei festverlegten Leitungen<br>[2] Dieser Fehlerausschluß ist nur zulässig bei Einrichtungen mit relativ geringem Risiko, vergleiche VBG 5 § 15 |
| Unterbrechung jedes Leiters | n e i n | |
| Erd- und Masseschluß eines Leiters | n e i n | |

### 1.2 Leiterplatte

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Kurzschluß zwischen benachbarten Leiterbahnen | – Kurzschluß zwischen benachbarten Leiterbahnen, wenn die Leiterplatte nach einschlägigen Regeln der Technik [1] gebaut und die Leiterplatte durch geeignete Maßnahmen vor leitfähigen Fremdkörpern (auch Leiterbahnabbrüchen) geschützt wird [2] | [1] Wenn Basismaterial nach IEC 249-1 verwendet ist und die Luft- und Kriechstrecken mindestens nach Verschmutzungsgrad 2/ Einsatzklasse III nach IEC 664 (1980) und IEC 664 A (1981) bemessen sind. Dies gilt auch für die Luft- und Kriechstrecken zwischen Leiterbahnen und bestückten Bauteilen, insbesondere bei einer Leiterbahnführung unterhalb von Bauteilen, z. B. bei Anwendung von SMD-Technik |
| Unterbrechung jeder Leiterbahn | n e i n | [2] Geeignete Maßnahmen können z. B. sein, Einbau der LP in Gehäuse mit IP ≥ 54 und Abdeckung mit einer alterungsbeständigen Lack- oder Schutzschicht |

### 1.3 Klemmstellen (z. B. Reihenklemmen)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung einzelner Klemmen | n e i n | [1]) Wenn Ausführung nach einschlägigen DIN VDE-Bestimmungen und geeignete Anschlußtechniken verwendet werden |
| Kurzschluß zwischen benachbarten Klemmen | – Kurzschluß zwischen benachbarten Klemmen [1]) | |

### 1.4 Mehrpolige Steckverbindungen

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung einzelner Steckerstifte | n e i n | [1]) Sichergestellt durch konstruktive Maßnahmen, z. B. Formgebung, Schrumpfschlauch über Verbindungsstelle . . . Kriech- und Luftstrecken, Abstände nach einer Isolationsbeanspruchung entsprechend der Einteilung in IEC 664 (1980) und IEC 664 A (1981) mit Verschmutzungsgrad 3/Einsatzklasse III |
| Kurzschluß zwischen benachbarten Steckerstiften | – Kurzschluß zwischen benachbarten Steckerstiften [1]) | |

## 2 Hilfsstromschalter

### 2.1 Mechanische Positionsschalter

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Nichtschließen eines Kontaktes | n e i n | [1]) Bei Hilfsstromschaltern nach DIN VDE 0660 Teil 206 |
| Nichtöffnen eines Kontaktes | – Nichtöffnen eines zwangsläufig öffnenden Kontaktes [1]) | [2]) Mechanisch ausreichende Fixierung, Anfahren des Schalters nach Herstellerangabe. Dieser Fehlerausschluß ist nur zulässig bei Einrichtungen mit relativ geringem Risiko, vergleiche VBG 5 § 15 |
| Nichtbetätigen des Schalters aufgrund mechanischen Versagens (z. B. Stößelbruch, Abnutzung der Betätigungsrolle, Dejustage) | – Nichtbetätigen . . . [2]) | [3]) Ausreichende Kriech- und Luftstrecken zwischen den Kontakten. Sich lösende leitfähige Teile dürfen die Isolation zwischen den Kontakten nicht überbrücken, vergleiche DIN VDE 0660 Teil 206 |
| Betätigt bleiben des Schalters aufgrund mechanischen Versagens | n e i n | |
| Kurzschluß von Kontakten, die voneinander isoliert sind | – Kurzschluß . . . [3]) | |
| Gleichzeitiger Kurzschluß zwischen den drei Polen eines Wechselkontaktes | – Gleichzeitiger Kurzschluß . . . [1, 3]) | |

### 2.2 Handbetätigte Schalter und Taster

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Nichtschließen eines Kontaktes | n e i n | [1] Sich lösende leitfähige Teile dürfen den Kontakt nicht überbrücken. Formschlüssige Verbindung zwischen Stellteil und elektrischem Kontakt |
| Nichtöffnen eines Kontaktes | – Nichtöffnen eines zwangsläufig öffnenden Kontaktes [1] | [2] Bei mechanisch formschlüssiger Kraftübertragung vom Stellteil zum elektrischen Kontakt |
| Nichtbetätigen des Schalters aufgrund mechanischen Versagens | – Nichtbetätigen . . . [2] | [3] Ausreichende Kriech- und Luftstrecken zwischen den Kontakten. Sich lösende leitfähige Teile dürfen die Isolation zwischen den Kontakten nicht überbrücken |
| Kurzschluß von Kontakten, die voneinander isoliert sind | – Kurzschluß . . . [3] | [4] in vielen Fällen – insbesondere bei relativ geringem Risiko (Beispiel: Tippbetrieb) – wird dieser Fehler akzeptiert |
| Betätigt bleiben des Schalters [4] aufgrund mechanischen Versagens | – Betätigt bleiben . . . [2] | |
| Gleichzeitiger Kurzschluß zwischen den drei Polen eines Wechselkontaktes | – Gleichzeitig Kurzschluß . . . [1, 3] | |

### 2.3 Berührungslos wirkender Positionsschalter

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausgang dauernd niederohmig [2] (durchgeschaltet) | – Fehlerhafter Übergang des Ausgangs in den unsicheren Schaltzustand [1, 2] | [1] Schalter muß Prüfgrundsatz GS-ET-14 bzw. DIN VDE 0660 Teil 209 entsprechen |
| Ausgang dauernd hochohmig [2] (kein Durchschalten) | – Fehlerhafter Übergang des Ausgangs in den unsicheren Schaltzustand [1, 2] | [2] Je nach Auslegung kann der nieder- oder hochohmige Ausgangszustand den sicheren Schaltzustand signalisieren |
| Spannungsversorgung unterbrochen | n e i n | [3] Mechanisch ausreichende Fixierung von Schalter und Gegenstück. Dieser Fehlerausschluß ist nur zulässig bei Einrichtungen mit relativ geringem Risiko, vergleiche VBG 5 § 15 |
| Nichtbetätigen des Schalters aufgrund mechanischen Versagens (z.B. Verlust des Gegenstückes, Dejustage) | – Nichtbetätigen . . . [3] | |
| Kurzschluß zwischen den drei Anschlüssen eines Wechselkontaktes (bei Reedschaltern) | n e i n | |

### 2.4 Relais/Schütz

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Nicht-Abfall | n e i n | [1]) Werden Relais/Schütze mit Zwangsführung verwendet, kann wegen der strengen Antivalenz von Öffner- und Schließerkontakten das Nichtöffnen eines Kontakes abgefragt werden (Anzugs-/Abfallüberwachung!). Geprüft wird dies durch Nicht-Anzug/Nicht-Abfall, da grundsätzlich Vollzwangsführung unterstellt wird, d. h., öffnet ein Schließerkontakt nicht, so bleiben alle anderen Schließer geschlossen. Für das Nichtöffnen von Öffnern gilt gleiches sinngemäß. |
| Nicht-Anzug | n e i n | |
| Unterbrechung der Spule oder des Kontaktweges | n e i n | |
| Nichtöffnen von einzelnen Kontakten [1]) | n e i n | |
| Gleichzeitiger Kurzschluß zwischen den drei Polen eines Wechselkontaktes | – Gleichzeitig Kurzschluß . . . [1]) | |
| Äquivalenter Schaltzustand von Öffner und Schließer (*gleichzeitiges geschlossen sein*) | – Äquivalenter Schaltzustand von Öffner und *Schließer (gleichzeitig* geschlossen sein) [1]) | |
| Kurzschluß zwischen Kontakten untereinander und Kontakten und Wicklung | – Kurzschluß . . . [2]) | [2]) Wenn Kriech- und Luftstrecken, Abstände nach einer Isolationsbeanspruchung entsprechend der Einteilung in IEC 664 (1980) und IEC 664 A (1981) mit Verschmutzungsgrad 3/Einsatzklasse III gewählt und geeignete Anschlußtechniken verwendet werden |

## 3 Diskrete elektrische Bauelemente

### 3.1 Transformator, Übertrager

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung einer Wicklung | n e i n | [1]) Es müssen die Anforderungen nach IEC 742 (1983) erfüllt sein. Im letzten Fall ist auch für Nennspannungen kleiner als 500 V die Isolation für mindestens 2500 V Prüfwechselspannung zu bemessen. Bei sekundärem Kurzschluß darf keine zu hohe Erwärmung auftreten. Windungs- und Wicklungsschlüsse müssen durch geeignete Maßnahmen verhindert werden, z. B. durch<br>– Tränkung der Wicklungen, so daß alle Hohlräume zwischen Wikkelkörper und Wicklung ausgefüllt sind<br>– Verwendung von Wikkeldrähten für erhöhte Anforderungen an die Isolation und Wärmebeständigkeit |
| Kurzschluß zwischen Wicklungen | – Kurzschluß zwischen Wicklungen [1]) | |

### 3.2 Drahtwiderstand

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung | n e i n | [1]) Wicklung einlagig und glasiert oder vergossen |
| Kurzschluß | – Kurzschluß [1]) | [2]) Wird geprüft, wenn zu erwarten ist, daß die Schaltung empfindlich gegenüber Driftausfällen ist. Bei digitaler Signalverarbeitung ist in der Regel damit nicht zu rechnen |
| Drift [2])<br>a) Widerstandsverringerung $0\ \Omega \leq R \leq R_N$ | a) Widerstandsverringerung [1]) $0{,}8 \cdot R_N \leq R \leq R_N$ | |
| b) Widerstandserhöhung $R_N \leq R \leq 10 \cdot R_N$ | n e i n | |

### 3.3 Schichtwiderstand

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung | n e i n | [1] Widerstandsschicht gewendelt, mit axialen Drahtanschlüssen und Lackumhüllung. Die zulässigen Grenzwerte, wie Dauerspannung und Leistung, dürfen auch unter ungünstigen Bedingungen (worst case) nicht überschritten werden |
| Kurzschluß | – Kurzschluß [1] | |
| Drift [3] | | |
| a) Widerstandsverringerung $0{,}5 \cdot R_N \leq R \leq R_N$ | a) Widerstandsverringerung [2] $0{,}8 \cdot R_N \leq R \leq R_N$ | [2] Ausführung wie unter [1] jedoch mit einer Widerstandstoleranz $\leq \pm 5\,\%$, Betriebsspannung $\leq 0{,}5$ x höchstzulässige Dauerspannung. Bei höheren Widerstandstoleranzen wird der Driftbereich erweitert |
| b) Widerstandserhöhung $R_N \leq R \leq 10 \cdot R_N$ | n e i n | [3] Wird geprüft, wenn zu erwarten ist, daß die Schaltung empfindlich gegenüber Driftausfällen ist. Bei digitaler Signalverarbeitung ist in der Regel damit nicht zu rechnen |

### 3.4 Widerstandsnetzwerk

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung einzelner Anschlüsse | n e i n | [1] *Wird nur unterstellt, wenn* zu erwarten ist, daß die Schaltung empfindlich gegenüber Driftausfällen ist. |
| Kurzschluß zwischen beliebigen Anschlüssen | n e i n | |
| Drift von Einzelwiderständen [1] $0\,\Omega \leq R_N \leq 10 \cdot R_N$ | n e i n | |

### 3.5 Potentiometer

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung einzelner Anschlüsse | n e i n | [1]) Beim Drahtpotentiometer wird nur Kurzschluß zwischen Anzapfung und einem der Außenanschlüsse angenommen |
| Kurzschluß gleichzeitig zwischen allen Anschlüssen | – Kurzschluß gleichzeitig zwischen allen Anschlüssen[1]) | |
| Drift | | |
| a) Widerstandsverringerung $0\,\Omega \leq R \leq R_N$ | n e i n | |
| b) Widerstandserhöhung $R_N \leq R \leq 10 \cdot R_N$ | n e i n | |

### 3.6 Kondensator, Trimmer

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung | n e i n | [1]) Fehlerausschluß auch nicht bei selbstheilenden MP-Kondensatoren |
| Kurzschluß[1]) | n e i n | [2]) Wird nur unterstellt, wenn zu erwarten ist, daß die Schaltung empfindlich gegenüber Driftausfällen ist |
| Drift[2]) $0\,F \leq C \leq 2 \cdot C_N$[3]) $\tan\delta$[2]) | n e i n | [3]) Zeigt sich bei der Prüfung, daß die Kapazitätserhöhung sicherheitskritisch ist, so wird nur die maximale Kapazität gemäß Herstellerangabe unterstellt |

## 4 Elektronische Bauelemente

### 4.1 Diskrete Halbleiter (z. B. Diode, Transistor)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Kurzschluß zwischen je zwei beliebigen Anschlüssen | n e i n | [1]) Wird nur unterstellt, wenn zu erwarten ist, daß die Schaltung gegenüber Driftausfällen empfindlich ist |
| Unterbrechung jedes einzelnen Anschlusses | n e i n | |
| Drift von Ausgangspotentialen und Kennwerten[1]) | n e i n | |

### 4.2 Optokoppler

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung einzelner Anschlüsse | nein | [1] Anforderungen nach DIN VDE 0884 müssen erfüllt sein |
| Kurzschluß zwischen beliebigen Anschlüssen | | [2] Durch geeignete Beschaltung des Optokopplers kann sichergestellt werden, daß die Mindestenergie für die am Ausgang zu treibende Last von der Eingangsseite nicht zur Verfügung steht |
| a) eingangsseitig (Sender) | nein | |
| b) ausgangsseitig (Empfänger) | nein | |
| c) zwischen Ein- und Ausgang[2] | c) Kurzschluß zwischen beliebigen Anschlüssen der Eingangs- und Ausgangsseite[1] | |

### 4.3 Integrierter Schaltkreis (SSI, MSI)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Unterbrechung jedes einzelnen Anschlusses | nein | [1] Wegen der unterstellten Kurzschlüsse bzw. dem gleichzeitigen Versagen aller Teilfunktionen in einem IC, müssen sicherheitstechnische Signale voneinander getrennt in verschiedenen IC's verarbeitet werden |
| Kurzschluß zwischen je zwei beliebigen Anschlüssen[1] | nein | |
| Stuck-at-Fehler Statisches „0"- und „1"-Signal an allen Ein- und Ausgängen einzeln oder gleichzeitig[1, 2] | nein | [2] Wird nur unterstellt, wenn zu erwarten ist, daß die Schaltung empfindlich gegenüber dieser Fehlerannahme ist |
| Drift von Ausgangspotentialen[2, 4] | nein | |
| Oszillation von Ausgängen[2, 3, 4] | nein | [3] Frequenz und Tastverhältnis ist abhängig von der Schaltungstechnik und der äußeren Beschaltung. Bei der Prüfung werden die in Frage kommenden treibenden Stufen abgeklemmt |
| | | [4] Wird nur unterstellt bei Einrichtungen mit erhöhtem Risiko, vgl. VBG 5, § 15 (2) |

### 4.4 Integrierter Schaltkreis (LSI, z. B. Speicher, $\mu$P)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausfall der Gesamt- oder Teilfunktion [1])<br>Der Ausfall kann<br>– statisch sein<br>– die Logik verändern<br>– abhängig von Bit-Sequenzen sein | n e i n | [1]) Einem $\mu$P werden falsche Bit- und Wortkombinationen sowie falsche Programmabarbeitung unterstellt. Im „worst-case"-Fall bedeutet dies, daß z. B. eingebaute Selbsttests zwar richtig durchgeführt werden, die Ergebnisse jedoch falsch ermittelt werden |
| Unerkannte Fehler in der Hardware,<br>die wegen der Komplexität des IC nicht entdeckt werden [1]) | n e i n | |
| Unerkannte Fehler im gespeicherten Programm [1]) | n e i n | |

BIA
Berufsgenossenschaftliches Institut für Arbeitssicherheit
BG

Sicherheitstechnisches Informations- und Arbeitsblatt

# Fehlerlisten für hydraulische und pneumatische Bauelemente – Bei der Prüfung unterstellte Fehlerarten –

## 1 Einleitung

In Unfallverhütungsvorschriften, Richtlinien und Sicherheitsregeln sowie in verschiedenen Regeln der privaten Normensetzer sind u. a. sicherheitstechnische Anforderungen an Steuerungen, Schutzeinrichtungen und Systeme enthalten, z. B. in [1 bis 11]. Diese Anforderungen sind z. T. technologieunabhängig formuliert, gelten dann auch für hydraulische und pneumatische, also für fluidtechnische Steuerungen sowie Schutzeinrichtungen und Systeme.

In einigen Vorschriften und Regeln umfassen die sicherheitstechnischen Anforderungen auch direkte oder indirekte Aussagen über das Verhalten im Fehlerfall. So wird z. B. in [5] in Abhängigkeit von definierten Bedingungen u. a. eine „einfehlersichere" hydraulische bzw. pneumatische Steuerung gefordert. Um Anforderungen dieser Art erfüllen zu können, ist zunächst eine sog. „Fehlerbetrachtung" notwendig. Darunter versteht man nach [12] die Gesamtheit der Überlegungen, um das sicherheitstechnische Verhalten einer Einrichtung im Fehlerfall beschreiben und praktisch überprüfen zu können. Ein entscheidender Faktor bei dieser Fehlerbetrachtung ist die Festlegung, d. h. die Vereinbarung der anzunehmenden Fehler. Eine solche Fehlervereinbarung ist für den Entwickler eine wichtige Voraussetzung, um die geforderte steuerungstechnische Sicherheit (mit vorhandenen Bauelementen) konzipieren und realisieren zu können. Außerdem soll eine Fehlervereinbarung gewährleisten, daß verschiedene Prüfstellen und Prüfer beim gleichen Prüfobjekt nicht zu unterschiedlichen Ergebnissen gelangen.

Nur in wenigen Vorschriften und Regeln (z. B. [5; 6; 11]) sind bisher Hinweise darüber enthalten, welche Fehler an hydraulischen und pneumatischen Bauelementen anzunehmen sind und welche ausgeschlossen werden können. In der fluidtechnischen Fachliteratur befinden sich ebenfalls nur wenige Angaben über das mögliche technische Versagen der betrachteten Bauelemente, z. B. [13; 14]. Eine umfassende, detaillierte Fehlerliste ist bisher für fluidtechnische Bauelemente nicht bekannt geworden. Für elektrische Bauelemente ist im sicherheitstechnischen Informations- und Arbeitsblatt 340 220 dieses Handbuches [12] eine solche Fehlerliste bereits vorhanden.

## 2 Anforderungen an eine Fehlerliste

Im Berufsgenossenschaftlichen Institut für Arbeitssicherheit – BIA wurden die bei sicherheitstechnischen Prüfungen von hydraulischen und pneumatischen Steuerungen, Schutzeinrichtungen und Systemen zugrundegelegten Fehlerannahmen und Fehlerausschlüsse für die entsprechenden Bauelemente zusammengestellt. Diese Fehlerliste, speziell für den industriellen Maschinen- und Anlagenbau konzipiert, beruht insbesondere auf den Erfahrungen, die in einer etwa zehnjährigen Prüfpraxis gesammelt wurden. Relevante Angaben in Vorschriften, Regeln sowie in der Fachliteratur wurden berücksichtigt. Wie die Fehlerliste für elektrische Bauelemente, so stellt auch die vorliegende Liste einen Kompromiß verschiedener, sich teilweise widersprechender Anforderungen dar, die nachstehend erläutert werden.

### Hoher Fehlerabdeckungsgrad

Die bei der Fehlerfallprüfung unterstellten Fehler sollten möglichst viele der insgesamt möglichen abdecken. Je höher der Fehlerabdeckungsgrad, desto geringer das Risiko, unter Umständen gefährliche Fehlerarten zu übersehen.

### Durchführbarkeit

Hydraulische und pneumatische Bauelemente sind zum Teil weniger komplex aufgebaut als elektrische, insbesondere als integrierte Halbleiter-Schaltkreise. Trotzdem können bei der Fehlerfallprüfung meist nicht alle theoretisch möglichen Fehler berücksichtigt werden. Eine gute Möglichkeit, um die Fehlerfallprüfung relativ einfach bei ausreichend hohem Fehlerabdeckungsgrad durchführen zu können, besteht häufig in der Annahme des

sicherheitstechnisch ungünstigsten Zustandes des Ausgangs-Bauelements. So ist es z. B. meistens ausreichend, bei pneumatischen Schaltkreisen, die u. a. aus Gliedern der Informationsverarbeitung (z. B. Und-, Oder-, Nicht-Glieder) aufgebaut sind, dem Ausgangsventil entsprechende Fehler zu unterstellen.

#### Möglichkeiten des Fehlereinbaues

Nach Möglichkeit sollten Fehler unterstellt werden, die in das zu prüfende Bauelement bzw. in die zu prüfende Originalschaltung auch eingebaut werden können. Häufig ist die Fehlerursache, z. B. Feststoffverschmutzung des Druckmediums, nicht mit vertretbarem Aufwand realistisch zu simulieren. Die Auswirkungen der Fehlerursache, z. B. Hängenbleiben des bewegten Bauteils, können aber in der Regel als Fehler eingebaut werden. Deshalb wurden bevorzugt Fehler (Fehlerauswirkungen) in der vorliegenden Liste aufgenommen, die sich auch bei der Prüfung einbauen lassen.

#### Reproduzierbarkeit

Die eingebauten Fehler sollten möglichst so ausgewählt sein, daß sich ein reproduzierbares Prüfergebnis ergibt.

#### Wirtschaftlichkeit

Die unterstellten Fehler sollen einen rationellen Fehlereinbau erlauben. Der Einbau der Fehler in das betrachtete Bauelement bzw. in die Originalschaltung erfordert aber auch dann noch einen deutlich größeren Zeitaufwand als die theoretische Fehlerbetrachtung. Deshalb sollte man sich bei einfach zu übersehenden Bauelementen und Schaltungen mit einer theoretischen Fehlerbetrachtung begnügen.

#### Herstellerunabhängigkeit

Die unterstellten Fehler sollten weitgehend unabhängig vom Hersteller der Bauelemente sein. Fehlerausschüsse können aber meistens nur konstruktionsspezifisch formuliert werden und sind damit manchmal indirekt herstellerabhängig.

#### Realistische Fehlerausschlüsse

Ohne die Annahme konkreter Fehlerausschlüsse sind keine sicheren Steuerungen zu realisieren. Diese Fehlerausschlüsse sind, abgesehen von wenigen, physikalisch begründeten Einzelfällen, jeweils ein Kompromiß zwischen den sicherheitstechnischen Erfordernissen und den technisch/wirtschaftlichen Möglichkeiten. Fehlerausschlüsse sind insbesondere begründet durch

- die physikalische Unmöglichkeit einer definierten Fehlerart (Beispiel: Vergrößerung des Volumenstroms einer Konstantpumpe ohne Änderung der Betriebs- und Antriebsparameter),
- weitgehend anerkannte, anwendungsunabhängige, technische Erfahrungen (Beispiel: plötzlicher Bruch eines Ventil-Schieberkolbens in viele Einzelstücke),
- technisch/wirtschaftliche Aspekte, die anwendungsbestimmt und damit abhängig vom konkreten Risiko der Anwendung sind (Beispiel: selbständiges Schalten eines Ventils ohne Ansteuerung bei Anwendungen mit relativ niedrigem Risiko).

Die beiden erstgenannten Gründe für einen Fehlerausschluß stellen den Regelfall dar. Bei definierten Anwendungen können jedoch weitergehende Fehlerausschlüsse vorgenommen werden. Diese zusätzlichen Fehlerausschlüsse sind abhängig vom Risiko der jeweiligen Anwendung und richten sich insbesondere nach der Wahrscheinlichkeit des Auftretens dieser Fehler. Die Auftrittswahrscheinlichkeit kann durch konkrete Ausfallraten belegt oder durch Erfahrungen aufgrund von Betriebsbewährung abgeschätzt werden. Konkrete Ausfallraten von fluidtechnischen Bauelementen bei industriellen Bedingungen sind praktisch nicht bekannt geworden, so daß hier auf entsprechende, betriebliche Erfahrungen zurückgegriffen werden muß.

## 3 Behandelte Bauelemente

Nachstehend sind die Fehlerlisten für hydraulische Bauelemente und für pneumatische Bauelemente aufgeführt. Obwohl diese Listen jeweils viele Gemeinsamkeiten aufweisen, wäre eine zusammengefaßte Liste mit Angabe der jeweiligen hydraulischen/pneumatischen Besonderheiten zu unübersichtlich für den Anwender.

Für jedes Bauelement sind in den Listen die Fehlerannahmen, die Fehlerausschlüsse und entsprechende Bemerkungen aufgeführt. Diese Bemerkungen enthalten Begründungen, Erläuterungen und allgemeine Hinweise. Folgende hydraulische und pneumatische Bauelemente werden behandelt:

1 Ventile
1.1 Wegeventile
1.2 Sperrventile
1.3 Stromventile
1.4 Druckventile

2 Leitungen
2.1 Rohrleitungen
2.2 Schlauchleitungen
2.3 Verbindungselemente

3 Zylinder

4 Druckübersetzer/Druckmittelwandler

Außerdem folgende hydraulische Bauelemente:

5 Filter

6 Energiespeicher (Druckbehälter)

7 Pumpen/Motoren

8 Sensoren.

Außerdem folgende pneumatische Bauelemente:

5 Druckluft-Aufbereitung
5.1 Filter
5.2 Öler
5.3 Schalldämpfer

6 Energiespeicher (Druckbehälter)

7 Motoren

8 Sensoren

9 Informationsverarbeitung
9.1 Verknüpfungsglieder
9.2 Verzögerungsglieder
9.3 Umformer.

**Schrifttum**

[1] Unfallverhütungsvorschrift „Kraftbetriebenes Arbeitsmittel" (VBG 5). Carl Heymanns Verlag, Köln (10/1985 und 4/1987).

[2] Unfallverhütungsvorschrift „Hydraulische Pressen" (VBG 7n 5.2). Carl Heymanns Verlag, Köln (4/1987).

[3] Unfallverhütungsvorschrift „Gießereien" (VBG 32). Carl Heymanns Verlag, Köln (4/1979 u. 4/1986)

[4] Richtlinien für kraftbetätigte Fenster, Türen und Tore (ZH 1/494). Carl Heymanns Verlag, Köln (4/1989).

[5] Sicherheitsregeln für die Steuerungen von Druck- und Papierverarbeitungsmaschinen (ZH 1/170). Carl Heymanns Verlag, Köln (10/1988).

[6] Sicherheitsregeln für Steuerungen an kraftbetriebenen Pressen der Metallbearbeitung (ZH 1/457). Carl Heymanns Verlag, Köln (2/1978).

[7] Sicherheitsregeln an Zweihandschaltungen an kraftbetriebenen Pressen der Metallbearbeitung (ZH 1/456). Carl Heymanns Verlag, Köln (2/1978).

[8] DIN 24980: Zweihandschaltung, Sicherheitstechnische Anforderungen, Prüfung. Beuth Verlag, Berlin (8/1987).

[9] DIN 24346: Hydraulische Anlagen, Ausführungsgrundlagen. Beuth Verlag, Berlin (12/1984).

[10] VDI 3229: Technische Ausführungsrichtlinien für Werkzeugmaschinen und andere Fertigungsmittel, P-Pneumatische Ausrüstung. Beuth Verlag, Berlin (5/1967).

[11] VDI 2854, Entwurf: Sicherheitstechnische Anforderungen an automatische Fertigungssysteme. Beuth Verlag, Berlin (10/1989).

[12] *Grigulewitsch, W., K. Meffert* und *G. Reuß*: Fehlerliste für elektrische Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Sicherheitstechnisches Informations- und Arbeitsblatt 340 220 in: BIA-Handbuch, 7. Lfg. VI/87 und 13. Lfg. XI/89. Erich Schmidt Verlag, Bielefeld.

[13] *Böinghoff, O.*: Ursachen und Folgen der Verschmutzung von Hydraulikflüssigkeiten. Grundlagen der Landtechnik 24 (1974) Nr. 2, S. 46–50.

[14] *Weule, H.*: Sicherung der Verfügbarkeit hydraulischer Anlagen in Planung und Betrieb. 8. Aachener Fluidtechnisches Kolloquium, März 1988, Fachgebiet Hydraulik, Band 1, S. 5–47. Hrsg.: Verein zur Förderung der Forschung und Anwendung der Hydraulik und Pneumatik e.V., Aachen.

**Bearbeiter:**

Dipl.-Ing. K.-J. Gorgs, Dr.-Ing. W. Kleinbreuer
und Dipl.-Ing. W. Kühlem
Fachbereich Elektrotechnik – Steuerungstechnik

**Fehlerliste für hydraulische Bauelemente**

**1 Ventile (hydraulische Bauelemente ≙ Hy)**

**1.1 Wegeventile (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung (Verlängerung) der Schaltzeiten | nein [1])<br>ja, bei zwangläufiger Betätigung des bewegten Bauteils[2]), sofern die Betätigungskraft ausreichend groß ist und wenn Dimensionierung und Ausführung des Betätigungsmechanismus nach den allgemeinen anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | [1]) Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinflüsse, Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich.<br>[2]) Eine zwangläufige Betätigung des bewegten Bauteils ist bei mechanischer, formschlüssiger Betätigung gegeben und kann z. B. durch Kufen einer beweglichen Schutzeinrichtung erfolgen. Bei manueller Betätigung (Hand, Fuß) ist die Betätigungskraft für Ventile nach [3]) im allgemeinen nicht ausreichend groß. |
| Nichtschalten (Hängenbleiben des bewegten Bauteils in einer Endlage bzw. Nullage) oder<br>nicht vollständiges Schalten (Hängenbleiben des bewegten Bauteils in beliebiger Zwischenstellung) | nein [3])<br>ja, bei zwangläufiger Betätigung . . . | [3]) Das gilt generell bei Schieberventilen und bei Sitzventilen mit ähnlichen Führungsverhältnissen am bewegten Bauteil (Cartridge- oder Patronenbauform), aber in der Regel auch bei Kugelsitzventilen, weil hierbei zusätzlich die Führungsverhältnisse des Betätigungsmechanismus (z. B. Betätigungsstößel) berücksichtigt werden müssen. In diesen Fällen ist wegen [1]) kein Fehlerausschluß möglich. |
| Selbsttätiges Verändern der Ausgangs-Schaltstellung des bewegten Bauteils (ohne Ansteuerung) | nein, bei den Anforderungsstufen „Einfehlersicherheit" und „Selbstüberwachung". Wenn jedoch die Federkraft beim Federbruch weitgehend erhalten bleibt[4]) und normale Einbau- und Betriebsbedingungen vorliegen[5]), ist ein Fehlerausschluß möglich<br>ja, bei einer geringeren Anforderungsstufe, wenn normale Einbau- und Betriebsbedingungen vorliegen[5]) | [4]) Die Federkraft bleibt weitgehend erhalten, wenn der Drahtdurchmesser > Windungsabstand ist (Ineinanderdrehen nach Drahtbruch verhindert) und die Feder ausreichend geführt ist (Ausknicken nach Drahtbruch verhindert).<br>[5]) Normale Einbau- und Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten |

*1.1 Wegeventile (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | ja, bei zwangläufiger Betätigung des bewegten Bauteils[2]), wenn Dimensionierung und Ausführung des Betätigungsmechanismus nach den allgemein anerkannten Regeln der Technik erfolgt sind | sind, wenn sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt (z. B. waagerechter Einbau), wenn keine besondere Massenkraft auf das bewegte Bauteil einwirkt (z. B. Bewegungrichtung bei der Anordnung auf bewegten Maschinenteilen beachtet) und keine extremen Schwingungs- und Schockbeanspruchungen gegeben sind. |
| Leckage | nein, bei Schieberventilen[6])<br>ja, bei Sitzventilen, wenn normale Einsatzbedingungen vorliegen und eine ausreichende Filtrierung vorhanden ist<br>nein, bei Sitzventilen, wenn keine normalen Einsatzbedingungen vorliegen[7]) | [6]) Bei Schieberventilen (metallische Abdichtung) ist eine Leckage wegen der Spalte konstruktionsbedingt vorhanden.<br>[7]) Nicht normale Einsatzbedingungen liegen z. B. bei erheblicher Feststoffbelastung des Druckmediums (innere und äußere Ursachen) und/oder hohem Feuchtigkeitsgehalt der Umgebungsluft bei ungenügender Filtrierung vor; ferner, wenn die Gefahr von Kavitationserosion am Ventilsitz besteht (ungünstige Strömungsverhältnisse). |
| Veränderung des Leckagevolumenstroms | nein [8]) | [8]) Über einen längeren Betrachtungszeitraum werden Veränderungen des Passungsspiels bzw. des Ventilsitzes (z. B. Verschleiß) angenommen. Zusätzlich werden partielle Deformationen an Ventilsitzen bei nicht normalen Einsatzbedingungen unterstellt (s. [7])). Nicht angenommen werden Materialausbrüche an Steuerkanten, Ventilstegen und Ventilsitzen. |

*1.1 Wegeventile (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Unkontrolliertes Steuer- und Regelverhalten von Servo- und Proportionalventilen durch hydraulische Fehler, insbesondere ohne Ansteuerung. (Diese Fehlerannahme erfolgt bei den genannten Ventilen zusätzlich zu den bereits aufgeführten Fehlerannahmen. Wenn neben der sicheren Schaltstellung (Mittel- oder Endstellung) beliebige Zwischenstellungen sicherheitsrelevant sind, muß die elektronische Ansteuerung zusätzlich sicherheitstechnisch betrachtet werden, siehe „Fehlerliste für elektrische Bauelemente".) | nein, bei Servoventilen und Proportional-Wegeventilen mit Servovorstufe<br>ja, bei Proportional-Wegeventilen, wenn diese aufgrund der konstruktiven Ausführung sicherheitstechnisch wie konventionelle Wegeventile beurteilt werden können[9]) | [9]) Wichtige Beurteilungskriterien in diesem Zusammenhang sind z. B.<br>– Einnahme der sicheren Schaltstellung bei Ausfall der Steuerenergie durch ausreichend große mechanische Rückführkräfte (Federn)<br>– sichere elektrische Trennung der Steuerenergie als Voraussetzung für die Einnahme der sicheren Schaltstellung<br>– ausreichende positive Überdeckung in der sicheren Schaltstellung<br>– die Ausführung des Vorsteuerventils bei mehrstufigen Proportional-Wegeventilen (das Vorsteuerventil muß konstruktiv ähnlich wie ein konventionelles Ventil ausgeführt sein oder, wenn das Vorsteuerventil als Servoventil ausgeführt ist, muß eine Trennung in der sicheren Schaltstellung durch ein konventionelles Wegeventil zwischen Vor- und Hauptstufe erfolgen). |
| Anmerkung:<br>Werden Ventilfunktionen (Schaltsymbole) durch die Funktionen von mehreren Bauteilen (Einzelventilen) gebildet (z. B. 4/3-Wege-Funktion durch vier einzelne 2/2-Wege-Einbauventile realisiert), so muß die Fehlerbetrachtung für jedes einzelne dieser bewegten Bauteile durchgeführt werden. Bei vorgesteuerten Ventilen ist entsprechend zu verfahren. | | |

### 1.2 Sperrventile (Sitzventile) (Hy)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung (Verlängerung) der Schaltzeiten | nein [1] | [1] Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinwirkung, Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich. |
| Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen sowie nicht vollständiges Schließen (Hängenbleiben des bewegten Bauteils in einer Endlage oder in beliebiger Zwischenstellung) | nein, wenn die Führungsverhältnisse des bewegten Bauteils ähnlich wie bei Schieberkolben ausgeführt sind [2]<br>ja, wenn die Führungsverhältnisse des bewegten Bauteils wie bei einem Kugelsitzventil ausgeführt sind [3] und eine Anforderungsstufe unterhalb der „Selbstüberwachung" vorliegt. | [2] Das gilt z. B. bei Rückschlagventilen in Cartridge- oder Patronenbauform, aber in der Regel *auch bei gesteuerten* Kugelsitzventilen (z. B. entsperrbares Rückschlagventil), weil hierbei zusätzlich die Führungsverhältnisse der Betätigungseinrichtung (z. B. Betätigungskolben) berücksichtigt werden müssen. In diesen Fällen ist wegen [1] kein Fehlerausschluß möglich.<br>[3] Bei nicht gesteuerten Kugelsitzventilen sind die Führungsverhältnisse im allgemeinen so ausgebildet, daß ein Hängenbleiben des bewegten Bauteils wegen [1] hinreichend unwahrscheinlich ist. |
| Selbsttätiges Verändern der Ausgangs-Schaltstellung (ohne Ansteuerung) | ja, bei normalen Einbau- und Betriebsbedingungen [4] und wenn eine ausreichende Schließkraft aufgrund der vorliegenden Druck- und Flächenverhältnisse gegeben ist | [4] Normale Einbau- und Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten sind, keine besondere Massenkraft auf das bewegte Bauteil einwirkt und keine *extremen Schwingungs-* und Schockbeanspruchungen gegeben sind. |
| *Gleichzeitiger Verschluß* beider Eingangsanschlüsse bei Wechselventilen | ja, *wenn aufgrund von* Konstruktion und Ausführung des bewegten Bauteils der gleichzeitige Verschluß hinreichend *unwahrscheinlich* ist. | |
| Leckage | ja, wenn normale Einsatz*bedingungen* vorliegen und eine ausreichende Filtrierung vorhanden ist. | |

*1.2 Sperrventile (Sitzventile) (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | nein, wenn keine normalen Einsatzbedingungen vorliegen [5] | [5] Nicht normale Einsatzbedingungen liegen z. B. bei erheblicher Feststoffbelastung des Druckmediums (innere oder äußere Ursachen) und/oder hohem Feuchtigkeitsgehalt der Umgebungsluft bei ungenügender Filtrierung vor; ferner, wenn die Gefahr von Kavitationserosion am Ventilsitz besteht (ungünstige Strömungsverhältnisse). |
| Veränderung des Leckagevolumenstroms | nein [6] | [6] Über einen längeren Betrachtungszeitraum werden Veränderungen des Ventilsitzes (z. B. durch Verschleiß) angenommen. Zusätzlich werden partielle Deformationen an Ventilsitzen bei nicht normalen Einsatzbedingungen unterstellt (siehe [5]). Nicht angenommen werden Materialausbrüche an Ventilsitzen. |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**1.3 Stromventile (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung | ja, bei Stromventilen ohne bewegte Bauteile [1] (Festwiderstände, Drosselventile) wenn normale Einsatzbedingungen vorliegen und eine ausreichende Filtrierung vorhanden ist [2] [4]<br>nein, bei Stromventilen mit bewegten Bauteilen, z. B. bei Stromregelventilen [3] [4] | [1] Die Verstelleinrichtung wird hier nicht als bewegtes Bauteil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz und der Viskosität sind bei diesem Ventiltyp physikalisch bedingt und nicht Gegenstand dieser Fehlerannahme<br>[2] Normale Einsatzbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten und kein ungewöhnlich hoher Abrieb und keine größeren Fest- |

*1.3 Stromventile (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | | stoffpartikel (in Relation zum Querschnitt des *hydraulischen Widerstandes*) im System zu erwarten sind. |
| Veränderung des Volumenstromes bei nicht einstellbaren, kreisförmigen Blenden und Düsen | ja, wenn der Durchmesser ≥ 0,8 mm beträgt, normale Einsatzbedingungen vorliegen [2]) und eine ausreichende Filtriertung vorhanden ist | [3]) Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinflüsse, Verstopfen von Blenden und Düsen muß ein unkontrolliertes Verhalten des bewegten Bauteils (Druckwaage) unterstellt werden.<br>[4]) Wenn ein Rückschlagventil in das Stromventil integriert ist, sind dafür zusätzlich die Fehlerannahmen für Sperrventile zu beachten. |
| Veränderung des Volumenstromes durch ungewollte Veränderung des Einstellwertes bei Proportional-Stromventilen. (Diese Fehlerannahme erfolgt bei den genannten Ventilen zusätzlich zu den anderen Fehlerannahmen) | *nein* [5]) | [5]) *Da der zur Einstellung erforderliche Sollwert aus der Elektronik vorgegeben wird und bewegte Bauteile vorhanden sind*[3]), ist in der Regel kein Fehlerausschluß möglich. |
| *Selbsttätige Veränderung der* Verstelleinrichtung | *ja, bei wirksamer und dem* Einsatzfall angepaßter Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen (z. B. Plombieren) | |
| Unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung | ja, wenn eine wirksame formschlüssige Sicherung gegen Herausdrehen vorhanden ist | |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

### 1.4 Druckventile (Hy)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Nichtöffnen oder nicht ausreichendes Öffnen (weg- und zeitmäßig) beim Überschreiten des Einstelldruckes<br>oder<br>Nichtschließen oder nicht vollständiges Schließen (weg- und zeitmäßig) beim Unterschreiten des Einstelldruckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils) [1]) | nein, wenn die Führungsverhältnisse des bewegten Bauteils ähnlich wie bei Schieberkolben ausgeführt sind [2] [3])<br><br>ja, wenn die Führungsverhältnisse des bewegten Bauteils wie bei einem Kugelsitzventil ausgeführt sind [4]) und eine Anforderungsstufe unterhalb der „Selbstüberwachung" vorliegt | [1]) Diese Fehlerannahme gilt nur, wenn die Funktion von Druckventilen insbesondere für Kraftwirkungen (z. B. Schnittandeuter, Niederhalter) und das Steuern von gefahrbringenden Bewegungen (z. B. Hochhalten von Lasten, Druckaufbau in Werkzeugschließrichtung) bestimmend ist. Sie gilt nicht für ihre normale Funktion in Hydrauliksystemen (z. B. Druckbegrenzung, Druckminderung). Sie gilt ebenfalls nicht für den vorgesehenen Anwendungsbereich von typgeprüften Druckbegrenzungsventilen. Bei der letzt genannten Anwendung erfolgt nur ein gelegentliches Ansprechen des Ventils, wodurch Einflüsse nach [2]) weniger wahrscheinlich sind.<br>[2]) Durch z. B. Verschleiß, Fremdeinflüsse, Verstopfen von Blenden und Düsen ist ein Hängenbleiben des bewegten Bauteils nicht auszuschließen.<br>[3]) Das gilt z. B. bei Druckventilen in Schieber- oder Cartridgebauform, aber in der Regel auch bei direkt gesteuerten Kugelsitzventilen mit Dämpfungseinrichtung, weil hierbei zusätzlich die Führungsverhältnisse der Dämpfungseinrichtung berücksichtigt werden müssen. In diesen Fällen ist wegen [2]) kein Fehlerausschluß möglich.<br>[4]) Bei Kugelsitzventilen ohne Dämpfungseinrichtung sind die Führungsverhältnisse im allgemeinen so |

*1.4 Druckventile (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | | ausgebildet, daß ein Hängenbleiben des bewegten Bauteils wegen [2]) hinreichend unwahrscheinlich ist. |
| Veränderung des Druck-Regelverhaltens ohne Veränderung der Verstelleinrichtung [1]) | nein [5])<br>ja, bei direkt betätigten Druckbegrenzungsventilen, *wenn die Federkraft bei* Federbruch weitgehend erhalten bleibt [6]) | [5]) Durch z. B. Materialermüdung (Regelfeder), Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich.<br>[6]) Die Federkraft bleibt weitgehend erhalten, wenn der Drahtdurchmesser > Windungsabstand ist (Ineinanderdrehen nach Drahtbruch verhindert) und die Feder ausreichend geführt ist (Ausknicken nach Drahtbruch verhindert). |
| Veränderung des Druck-Regelverhaltens durch ungewollte Veränderung des Einstellwertes bei Proportional-*Druckventilen* [1]). (Diese Fehlerannahme erfolgt bei den genannten Ventilen zusätzlich zu den anderen Fehlerannahmen) | *nein* [7]) | [7]) Da der zur Einstellung erforderliche Sollwert aus der Elektronik vorgegeben wird und bewegte Bauteile vorhanden sind [2]), ist in der Regel kein Fehlerausschluß möglich. |
| Selbsttätige Veränderung der Verstelleinrichtung | ja, bei wirksamer und dem Einsatzfall angepaßter Sicherung der Verstelleinrichtung *unter Beachtung* sicherheitstechnischer Festlegungen (z. B. Plombieren) | |
| Unbeabsichtigtes Herausdrehen des Verstellteils der Verstelleinrichtung | ja, wenn eine wirksame formschlüssige Sicherung gegen Herausdrehen vorhanden ist | |
| Leckage | nein, bei Schieberventilen [8])<br>*ja, bei Sitzventilen, wenn* normale Einsatzbedingungen vorliegen und eine ausreichende Filtrierung vorhanden ist<br>nein, bei Sitzventilen, wenn keine normalen Einsatzbedingungen vorliegen [9]) | [8]) Bei Schieberventilen (metallische Abdichtung) ist eine Leckage wegen der Spalte konstruktionsbedingt vorhanden.<br>[9]) Nicht normale Einsatzbedingungen liegen z. B. bei erheblicher Feststoffbelastung des Druckmediums (innere und äußere Ursachen) und/oder hohem Feuchtigkeitsgehalt der Umge- |

*1.4 Druckventile (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | | bungsluft bei ungenügender Filtrierung vor; ferner, wenn die Gefahr von Kavitationserosion am Ventilsitz besteht (ungünstige Strömungsverhältnisse). |
| Veränderung des Leckagevolumenstromes | nein [10] | [10] Über einen längeren Betrachtungszeitraum werden Veränderungen des Passungsspiels bzw. des Ventilsitzes (z. B. durch Verschleiß) angenommen. Zusätzlich werden partielle Deformationen an Ventilsitzen bei nicht normalen Einsatzbedingungen unterstellt (siehe [9]). Nicht angenommen werden Materialausbrüche an Steuerkanten, Ventilstegen und Ventilsitzen. |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile (außer Regelfeder) sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind. | |

## 2 Leitungen (Hy)

### 2.1 Rohrleitungen (Hy)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten und Leckage | ja, wenn insbesondere Dimensionierung, Materialauswahl, Herstellung, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Abreißen am Verbindungselement | ja, bei Verwendung von gebräuchlichen Verbindungselementen, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden [1] und wenn Dimensionierung, Materialauswahl, Herstellung, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | [1] Keine besonderen sicherheitstechnischen Anforderungen liegen vor, wenn z. B. durch das Versagen der Rohrleitung keine gefahrbringende Maschinenbewegung zu erwarten ist und wenn die Aufenthaltsdauer von Personen im möglichen Gefahrenbereich der Rohrleitung gering ist. |

*2.1 Rohrleitungen (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | nein, bei Verwendung von Schneidringverschraubungen u. ä., wenn besondere sicherheitstechnische Anforderungen gestellt werden[2])<br>ja, bei Verwendung von Anschweißverschraubungen, Anschweißflanschen und Bördelverschraubungen, wenn Dimensionierung . . . | [2]) Besondere sicherheitstechnische Anforderungen liegen z. B. vor, wenn Massen hydraulisch hochgehalten oder abgebremst werden (bei großer kinetischer Energie) und Personen im Gefahrenbereich zu erwarten sind oder eine unmittelbare Gefährdung von Personen durch austretendes Druckmedium besteht. |
| Zusetzen (Verstopfen) | ja, bei Leitungen im Kraftkreis<br>ja, bei Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen an das Steuer- oder Meßsignal gestellt werden<br>nein, bei Steuer- und Meßleitungen, wenn besondere sicherheitstechnische Anforderungen an das Steuer- und Meßsignal gestellt werden[3]) und die Nennweite < 3 mm beträgt | [3]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines fehlerhaften Steuer- oder Meßsignals eine Gefährdung entstehen kann z. B. bei Ventilüberwachung mittels Druckschalter. |

**2.2 Schlauchleitungen (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten, Ausreißen aus Einbindung und Leckage | ja, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden[1]) und wenn insbesondere Dimensionierung, Materialauswahl, Herstellung und Anordnung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind<br>nein, wenn besondere sicherheitstechnische Anforderungen gestellt werden[2]) (auch wenn Dimensionierung . . .) | [1]) Keine besonderen sicherheitstechnischen Anforderungen liegen vor, wenn z. B. durch das Versagen der Schlauchleitung keine gefahrbringende Maschinenbewegung zu erwarten ist und wenn die Aufenthaltsdauer von Personen im möglichen Gefahrenbereich der Schlauchleitung gering ist.<br>[2]) Besondere sicherheitstechnische Anforderungen liegen z. B. vor, wenn Massen hydraulisch hochgehalten oder abgebremst werden (bei großer kinetischer Energie) und Personen im Gefahren- |

*2.2 Schlauchleitungen (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | | bereich zu erwarten sind oder eine unmittelbare Gefährdung von Personen durch das Versagen der Schlauchleitung (austretendes Druckmedium, Aufpeitschen) besteht. Hierbei sind vor allem Fertigungsmängel bei der Schlauch- und Schlauchleitungsherstellung sowie leistungsmindernde Einflüsse durch Alterung anzunehmen. |
| Zusetzen (Verstopfen) | ja, bei Leitungen im Kraftkreis<br>ja, bei Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen an das Steuer- oder Meßsignal gestellt werden<br>nein, bei Steuer- und Meßleitungen, wenn besondere sicherheitstechnische Anforderungen an das Steuer- oder Meßsignal gestellt werden[3]) und die Nennweite < 3 mm beträgt | [3]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines fehlerhaften Steuer- oder Meßsignals eine Gefährdung entstehen kann z. B. bei Ventilüberwachung mittels Druckschalter. |

**2.3 Verbindungselemente (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten, Versagen von Befestigungsschrauben oder Ausreißen von Gewinden | ja, wenn Dimensionierung, Materialauswahl, Herstellung, Anordnung und Verbindung zur Leitung bzw. zum fluidtechnischen Bauteil nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Leckage (Versagen der Dichtwirkung) | nein [1]) | [1]) Durch Verschleiß, Alterung, Nachlassen der Elastizität etc. ist kein Fehlerausschluß für eine längere Zeitspanne möglich. Nicht angenommen wird ein plötzliches weitgehendes Versagen der Dichtwirkung. |

*2.3 Verbindungselemente (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Zusetzen (Verstopfen) | ja, bei Anwendungen im Kraftkreis<br>ja, bei Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen an das Steuer- oder Meßsignal gestellt werden<br>nein, bei Anwendungen in Steuer- und Meßleitungen, wenn besondere sicherheitstechnische Anforderungen an das Steuer- oder Meßsignal gestellt werden [2]) und die Nennweite < 3 mm beträgt | [2]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines fehlerhaften Steuer- oder Meßsignals eine Gefährdung entstehen kann z. B. bei Ventilüberwachung mittels Druckschalter. |

## 3 Zylinder (Hy)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Undichtwerden der Druckräume bzw. Veränderung der Dichtwirkung | nein [1]) | [1]) Durch Verschleiß von Dichtungen, Abstreifern und Führungen ist kein Fehlerausschluß für eine längere Zeitspanne möglich. Nicht angenommen wird ein plötzliches weitgehendes Versagen von Dichtungen. |
| Versagen der Endlagendämpfung | ja, wenn dem in der Endlagendämpfung vorhandenen Sperrventil kein Versagen unterstellt wird [2])<br>nein, wenn dem in der Endlagendämpfung vorhandenen Sperrventil Versagen unterstellt wird [2]) | [2]) siehe 1.2 Sperrventile (Hy) („Nichtschließen") |
| Lösen der Verbindung Kolben/Kolbenstange sowie Kolbenstange/Mechanik | ja, wenn Konstruktion und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind sowie ggf. spezifischen Sicherheitsanforderungen entsprechen | |

*3 Zylinder (Hy) (Fortsetzung)*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten der Druckräume sowie Bruch von Befestigungs- und Deckelschrauben | ja, wenn Dimensionierung, Materialauswahl, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Ausknicken von Kolbenstangen | ja, wenn Dimensionierung, Materialauswahl, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**4 Druckübersetzer/Druckmittelwandler (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Undichtwerden der Druckräume bzw. Veränderung der Dichtwirkung | nein [1]) | [1]) Durch Verschleiß von Dichtungen und Führungen ist kein Fehlerausschluß für eine längere Zeitspanne möglich. Nicht angenommen wird ein plötzliches weitgehendes Versagen von Dichtungen. |
| Bersten der Druckräume sowie Bruch von Befestigungs- und Deckelschrauben | ja, wenn Dimensionierung, Materialauswahl, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**5 Filter (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Zusetzen des Filterelementes | nein [1]) | [1]) Insbesondere nach Erst- und Wiederinbetriebnahmen, nach Reparatur- und Wartungsarbeiten ist durch „Urverschmutzung" ein Zusetzen des Filterelementes zu erwarten, auch bei richtiger Dimensionierung |

*5 Filter (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bruch des Filterelementes | ja, wenn eine ausreichende Druckfestigkeit des Filterelementes und ein wirksames Bypassventil bzw. eine wirksame Verschmutzungsüberwachung vorhanden ist | |
| Versagen des Bypassventils | ja, wenn die Führungsverhältnisse des Bypassventils ähnlich wie bei einem Kugelsitzventil ausgeführt sind[2]) | [2]) Siehe 1.2 Sperrventile (Hy) („Nichtöffnen") |
| | ja, wenn keine besonderen sicherheitstechnischen Anforderungen im Zusammenhang mit der Anordnung des Filters erfüllt werden müssen | [3]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn z. B. durch eine Erhöhung des Druckes vor dem Filter gefahrbringende Bewegungen entstehen können (Lösen von Bremsen, Vergrößerung von Nachlaufwegen, Schalten von Ventilen u. ä.). |
| | nein, wenn besondere sicherheitstechnische Anforderungen im Zusammenhang mit der Anordnung des Filters erfüllt werden müssen[3]) und dem Bypassventil Versagen unterstellt werden muß[2]) | |
| Versagen der Verschmutzungsanzeige bzw. der Verschmutzungsüberwachung | nein, bei üblicher Ausführung | |
| Bersten des Filtergehäuses und Bruch der Deckelschrauben bzw. des Verbindungsgewindes | ja, wenn Dimensionierung, Materialauswahl, Anordnung im System und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind[4]) | [4]) In Ausnahmefällen (hoher Druck, großes Volumen) kann es erforderlich sein, darüber hinaus die Anforderungen der Druckbehälterverordnung einschließlich der dort genannten Regeln zu beachten. |

**6 Energiespeicher (Druckbehälter) (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten des Druckbehälters und Bruch von Verbindungs- und Deckelschrauben sowie Ausreißen von Anschlußgewinden | ja, wenn Bau, Ausrüstung und Anordnung im System den Anforderungen entsprechen[1]) sowie nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | [1]) Anforderungen an Bau und Ausrüstung sind insbesondere in der Druckbehälterverordnung und in den dort genannten Regeln festgelegt. |

*6 Energiespeicher (Druckbehälter) (Fortsetzung)*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Undichtwerden des Trennngliedes zwischen Gas und Druckflüssigkeit | nein [2]) | [2]) Durch Verschleiß von Dichtungen und Führungen (Kolbenspeicher) sowie durch Alterung von Membranen oder Speicherblasen (Membran- und Blasenspeicher) ist kein Fehlerausschluß über eine längere Zeitspanne möglich. |
| Versagen des Trennngliedes zwischen Gas und Druckflüssigkeit | nein, bei Membran- und Blasenspeichern<br>ja, bei Kolbenspeichern [3]) | [3]) Ein plötzliches weitgehendes Versagen von Dichtungen wird nicht angenommen. |
| Versagen des Füllventils auf der Gasseite | ja, wenn das Füllventil nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik ausgeführt ist und ein ausreichender Schutz vor äußeren Einflüssen gegeben ist | |

**7 Pumpen/Motoren (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung des Volumen-/Schluckstromes bei Konstantpumpen/-motoren | ja, bei kürzeren Betrachtungszeiträumen [1]) | [1]) Bei längeren Betrachtungszeiträumen muß eine Veränderung durch Verschleiß der bewegten Teile und Dichtungen angenommen werden. |
| Selbsttätige Veränderung der Volumen-/Schluckstromeinstellung ohne Betätigung der Verstelleinrichtung bei Verstellpumpen/-motoren | ja, bei mechanisch verstellten Pumpen/-Motoren<br>ja, bei druck- und volumenstromgeregelten Pumpen/-Motoren, wenn keine besonderen Anforderungen an die Konstanthaltung der Einstellparameter gestellt werden<br>nein, bei druck- und volumenstromgeregelten Pumpen/-Motoren, wenn besondere Anforderungen an die Konstanthaltung der Einstellparameter gestellt werden [2]) | [2]) Besondere Anforderungen liegen vor, wenn z. B. Geschwindigkeiten oder Drehzahlen mit den Anforderungsstufen „Einfehlersicherheit" oder „Selbstüberwachung" eingehalten werden müssen. Veränderung der Schaltzeiten und Hängenbleiben der bewegten Bauteile, Verstopfen von Blenden und Düsen sowie Veränderung von Federkräften in der Regel- oder Stelleinrichtung müssen angenommen werden, s. 1.1 Wegeventile (Hy), Abs. [1]), [4]). |

*7 Pumpen/Motoren (Hy) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bruch oder Lösen der an-/abtriebsseitigen Verbindungselemente (Kupplungen) sowie Bersten des Gehäuses und Bruch von Deckel- und Befestigungsschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**8 Sensoren (Hy)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausfall des Sensors [1]) | nein [2]) | [1]) Unter diese Begriffsbestimmung fällt hier die Signalerfassung, -verarbeitung und -ausgabe insbesondere von Druck, Volumenstrom, Temperatur und Weg. |
| Veränderung der Erfassungs- und Ausgabecharakteristik | nein [2]) | [2]) Durch z. B. Verschleiß, Materialermüdung, (u. a. Federn), Fremdeinflüsse, Verstopfen von Blenden und Düsen sowie Ausfall und/oder Veränderung im Verhalten der elektrisch/elektronischen Bauteile ist kein Fehlerausschluß möglich. |

**Fehlerliste für pneumatische Bauelemente**

**1 Ventile (pneumatische Bauelemente ≙ Pn)**

**1.1 Wegeventile (Pn)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung (Verlängerung) der Schaltzeiten | nein [1])<br>ja, bei zwangläufiger Betätigung des bewegten Bauteils [2]), sofern die Betätigungskraft ausreichend groß ist und wenn Dimensionierung und Ausführung des Betätigungsmechanismus nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | [1]) Durch z. B. Verschleiß, Materialermüdung (u. a. *Federn*), *Fremdeinflüsse*, chem. Einflüsse von Schmierstoffen auf Dichtungen, Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich.<br>[2]) Eine zwangläufige Betätigung des bewegten Bauteils ist bei mechanischer, formschlüssiger Betätigung gegeben und kann z. B. durch Kufen einer beweglichen Schutzeinrichtung oder durch manuelle Betätigung (Hand, Fuß) erfolgen. |
| Nichtschalten (Hängenbleiben des bewegten Bauteils in einer Endlage bzw. Nullage) oder<br>nicht vollständiges Schalten (Hängenbleiben des bewegten Bauteils in beliebiger Zwischenstellung) | nein [1])<br>ja, bei zwangläufiger . . . [2]) | |
| Selbsttätiges Verändern der Ausgangs-Schaltstellung des bewegten Bauteils (ohne Ansteuerung, durch Schwingungs- oder/und Schockbeanspruchung) | ja, bei Schieberventilen mit elastischer Abdichtung<br>nein, bei Schieberventilen mit metallischer Abdichtung und bei Sitzventilen, wenn die Anforderungsstufe „Einfehlersicherheit" oder „Selbstüberwachung" gefordert ist. Wenn jedoch die Federkraft beim Federbruch weitgehend erhalten bleibt [3]) und normale Einbau- und Betriebsbedingungen vorliegen [4]), ist ein Fehlerausschluß möglich<br>ja, bei Schieberventilen mit metallischer Abdichtung und bei Sitzventilen, wenn eine geringere Anforderungsstufe gefordert ist und normale *Einbau- und Betriebsbedingungen* vorliegen | [3]) Die Federkraft bleibt weitgehend erhalten, wenn der Drahtdurchmesser > Windungsabstand ist (Ineinanderdrehen nach Drahtbruch verhindert) und die Feder ausreichend geführt ist (Ausknicken nach Drahtbruch verhindert).<br>[4]) Normale Einbau- und Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Betriebsbedingungen eingehalten sind und wenn sich die Gewichtskraft des bewegten Bauteils sicherheitstechnisch nicht ungünstig auswirkt sowie keine besondere Massenkraft auf das bewegte Bauteil einwirkt (z. B. |

*1.1 Wegeventile (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | ja, bei zwangläufiger Betätigung des bewegten Bauteils[2]), wenn Dimensionierung und Ausführung des Betätigungsmechanismus nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | Bewegungsrichtung bei der Anordnung auf bewegten Maschinenteilen beachtet) und keine extremen Schwingungs- und Schockbeanspruchungen gegeben sind. |
| Selbsttätiges Verändern der Ausgangs-Schaltstellung des bewegten Bauteils (ohne Ansteuerung, durch Leckage) | ja, bei Ventilen, die bedingt durch ihre Bauart nur durch Belüftungssignale (positive Signale, Druckaufbau) geschaltet werden<br>nein, bei Ventilen, die bedingt durch ihre Bauart durch Entlüftungssignale (negative Signale, Druckabbau) geschaltet werden | |
| Leckage | ja, bei Schieberventilen mit elastischer Abdichtung, sofern eine ausreichende positive Überdeckung vorhanden ist[5]) und bei Sitzventilen, wenn normale Einsatzbedingungen vorliegen und eine ausreichende Aufbereitung der Druckluft erfolgt<br>nein, bei Schieberventilen mit metallischer Abdichtung[6])<br>nein, bei Schieberventilen mit elastischer Abdichtung und bei Sitzventilen, wenn keine normalen Einsatzbedingungen vorliegen[7]) | [5]) Bei Schieberventilen mit elastischer Abdichtung kann eine Leckage, die sich sicherheitstechnisch ungünstig auswirken kann, in der Regel ausgeschlossen werden. Eine geringe Leckage über einen größeren Zeitraum ist jedoch vorhanden.<br>[6]) Bei Schieberventilen mit metallischer Abdichtung ist eine Leckage wegen der Spalte konstruktionsbedingt vorhanden.<br>[7]) Nicht normale Einsatzbedingungen liegen z. B. vor bei erheblicher Feststoffbelastung und/oder hohem Feuchtigkeitsgehalt und/oder hohem Schmierstoffanteil in der Druckluft. |
| Veränderung des Leckagevolumenstroms | nein [8]) | [8]) Angenommen werden, über einen längeren Betrachtungszeitraum, Veränderungen des Passungsspiel durch Verschleiß (metallische Abdichtung) oder durch chemische Veränderungen des Dichtungswerkstoffes |

*1.1 Wegeventile (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | | (z. B. Volumenabnahme) sowie Verschleiß bei elastischer Abdichtung. Zusätzlich werden partielle Deformationen an Dichtungen und/oder Ventilsitzen bei nicht normalen Einsatzbedingungen unterstellt (siehe [7]). |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Unkontrolliertes Steuer- und Regelverhalten von Servo- und Proportionalventilen durch pneumatische Fehler, insbesondere ohne Ansteuerung. (Diese Fehlerannahme erfolgt bei den genannten Ventilen zusätzlich zu den bereits aufgeführten Fehlerannahmen. Wenn neben der sicheren Schaltstellung (Mittel- oder Endstellung) beliebige Zwischenstellungen sicherheitsrelevant sind, muß die elektronische Ansteuerung zusätzlich sicherheitstechnisch betrachtet werden, siehe „Fehlerliste für elektrische Bauelemente") | nein, bei Servoventilen<br>ja, bei Proportional-Wegeventilen, wenn diese aufgrund der konstruktiven Ausführung sicherheitstechnisch wie konventionelle Wegeventile beurteilt werden können[9]) | [9]) Wichtige Beurteilungskriterien in diesem Zusammenhang sind z. B.<br>– sichere elektrische Trennung der Steuerenergie als Voraussetzung für die Einnahme der sicheren Schaltstellung<br>– Einnahme der sicheren Schaltstellung bei Ausfall der Steuerenergie durch ausreichend große mechanische Rückführkräfte (Federn)<br>– ausreichende positive Überdeckung in der sicheren Schaltstellung. |
| Anmerkung:<br>Werden Wegeventile durch mehrere Einzelventile aufgebaut (z. B. 5/4 Wege-Funktion aus 4 einzelnen 2/2-Wege-Ventilen), so muß die Fehlerbetrachtung für jedes dieser Einzelventile durchgeführt werden. Bei vorgesteuerten Ventilen ist entsprechend zu verfahren. | | |

### 1.2 Sperrventile (Rückschlag-, Schnellentlüftungs- und Wechselventile) (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung (Verlängerung) der Schaltzeiten | nein [1]) | [1]) Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinflüsse, chemische Einflüsse von Schmierstoffen auf Dichtungen sowie Verstopfen von Blenden und Düsen ist *kein Fehlerausschluß* möglich. |
| Nichtöffnen, nicht vollständiges Öffnen, Nichtschließen sowie nicht vollständiges Schließen (Hängenbleiben des bewegten Bauteils in einer Endlage oder in beliebiger Zwischenstellung) | nein, wenn die Führungsverhältnisse des bewegten Bauteils ähnlich wie bei Schieberkolben ausgeführt sind [2])<br>ja, wenn die Führungsverhältnisse des bewegten Bauteils ähnlich wie bei einem Kugelsitzventil ausgeführt *sind* [3]) *und eine Anforderungsstufe* unterhalb der „Selbstüberwachung" vorliegt. | [2]) Das gilt z. B. bei Rückschlagventilen in Patronenbauform, aber in der Regel auch bei gesteuerten Sperrventilen in Kugel-, Kegel- oder Tellerbauart (z. B. entsperrbares Rückschlagventil), weil hierbei zusätzlich die Führungsverhältnisse der Betätigungseinrichtung (z. B. Betätigungskolben) berücksichtigt werden müssen. In diesen Fällen ist wegen [1]) kein Fehlerausschluß möglich.<br>[3]) Das kann z. B. bei Kugel-, Kegel- oder Tellerbauart des bewegten Bauteils *gelten, wenn ein Hängenbleiben* wegen [1]) aufgrund der Führungsverhältnisse hinreichend unwahrscheinlich ist. |
| Selbsttätiges Verändern der Ausgangs-Schaltstellung (ohne Ansteuerung) | ja, bei normalen Einbau- und Betriebsbedingungen [4]) und wenn eine ausreichende Schließkraft aufgrund der vorliegenden Druck- und Flächenverhältnisse gegeben ist | [4]) Normale Einbau- und Betriebsbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten sind und wenn keine extremen Schwingungs- und Schockbeanspruchungen gegeben sind. |
| Gleichzeitiger Verschluß beider Eingangsanschlüsse bei Wechselventilen | ja, wenn aufgrund von Konstruktion und Ausführung des bewegten Bauteils der gleichzeitige Verschluß hinreichend unwahrscheinlich ist. | |
| Leckage | ja, wenn normale Einsatzbedingungen vorliegen und eine ausreichende Aufbereitung der Druckluft vorhanden ist | [5]) Nicht normale Einsatzbedingungen liegen z. B. vor bei erheblicher Feststoffbelastung und/oder hohem |

*1.2 Sperrventile (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | nein, wenn keine normalen Einsatzbedingungen vorliegen[5]) | Feuchtigkeitsgehalt und/ oder hohem Schmierstoffanteil in der Druckluft. |
| Veränderung des Leckagevolumenstroms | nein[6]) | [6]) Über einen längeren Betrachtungszeitraum werden Veränderungen des Ventilsitzes (z. B. durch Verschleiß, chemische Veränderungen des Dichtungswerkstoffes) angenommen. Zusätzlich werden partielle Deformationen an Dichtungen und/ oder Ventilsitzen bei nicht normalen Einsatzbedingungen unterstellt (siehe [5])). |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**1.3 Stromventile (Pn)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung | ja, bei Stromventilen ohne bewegte Bauteile[1]) (Festwiderstände, Drosselventile) wenn normale Einsatzbedingungen vorliegen und eine ausreichende Aufbereitung der Druckluft erfolgt[2])<br>nein, bei Stromventilen mit bewegten Bauteilen[3]) | [1]) Die Verstelleinrichtung wird hier nicht als bewegtes Bauteil betrachtet. Veränderungen des Volumenstroms durch Änderung der Druckdifferenz sind bei diesem Ventiltyp physikalisch bedingt und nicht Gegenstand dieser Fehlerannahme.<br>[2]) Normale Einsatzbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten und keine größeren Feststoffpartikeln (in Relation z. B. zum Querschnitt der Drossel) im System zu erwarten sind. |

*1.3 Stromventile (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Selbsttätige Veränderung der Verstelleinrichtung | ja, bei wirksamer und dem Einsatzfall angepaßter Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen (z. B. Plombieren) | [3]) Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinflüsse muß ein unkontrolliertes Verhalten des bewegten Bauteils unterstellt werden (z. B. bei Drosselrückschlagventilen). |
| Unbeabsichtigtes Herausdrehen des Stellteils der Verstelleinrichtung | ja, wenn eine wirksame formschlüssige Sicherung gegen Herausdrehen vorhanden ist | |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**1.4 Druckventile (Pn)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Nichtöffnen oder nicht ausreichendes Öffnen (weg- und zeitmäßig) beim Überschreiten des Einstelldruckes oder<br>Nichtschließen oder nicht vollständiges Schließen (weg- und zeitmäßig) bei *Unterschreiten des Einstell*druckes (Hängenbleiben oder Schwergängigkeit des bewegten Bauteils [1])) | nein, wenn die Führungsverhältnisse des bewegten Bauteils ähnlich wie bei Schieberkolben ausgeführt sind [2])[3]) | [1]) Diese Fehlerannahme gilt nur, wenn die Funktion von Druckventilen insbesondere für Kraftwirkungen (z. B. Niederhalter) bestimmend ist. Sie gilt nicht für ihre normale Funktion im Pneu*matiksystem (z. B. Druck*minderung, Druckbegrenzung). Sie gilt ebenfalls nicht für den vorgesehenen Anwendungsbereich von typgeprüften Druckbegrenzungsventilen. Bei der letzt genannten Anwendung erfolgt nur ein gelegentliches Ansprechen *des Ventils wodurch* Einflüsse nach [3]) weniger wahrscheinlich sind. |
| | ja, wenn die Führungsverhältnisse des bewegten Bauteils ähnlich wie bei einem *Kugel-, Kegel- oder Mem*branventil (z. B. bei Druckminderventil mit Sekundärentlüftung) ausgeführt sind [4]) und eine Anforderungsstufe unterhalb der „Selbstüberwachung" vorliegt | [2]) Dies gilt z. B. bei Druckregelventilen in Kolbenbauart. Hier ist wegen [3]) kein Fehlerausschluß möglich.<br>[3]) Durch z. B. Verschleiß, Fremdeinflüsse, Verstopfen von Düsen, *chemische Einflüsse von* Schmierstoffen auf Dichtungen ist ein Hängenbleiben des bewegten Bauteils nicht auszuschließen. |

*1.4 Druckventile (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | | [4]) Bei Kugel-, Kegel- oder Membranventilen sind die Führungsverhältnisse im allgemeinen so ausgebildet, daß ein Hängenbleiben des bewegten Bauteils wegen [3]) hinreichend unwahrscheinlich ist. |
| Veränderung des Druck-Regelverhaltens ohne Veränderung der Verstelleinrichtung[1]) | nein[5])<br>ja, bei direkt betätigten Druckbegrenzungsventilen sowie Druckschaltventilen, wenn die Federkraft bei Federbruch weitgehend erhalten bleibt[6]) | [5]) Durch z. B. Materialermüdung (Regelfeder, Membrane), Verstopfen von Düsen ist kein Fehlerausschluß möglich.<br>[6]) Die Federkraft bleibt weitgehend erhalten, wenn der Drahtdurchmesser > Windungsabstand ist (Ineinanderdrehen nach Drahtbruch verhindert) und die Feder ausreichend geführt ist (Ausknicken nach Drahtbruch verhindert). |
| Veränderung des Druck-Regelverhaltens durch ungewollte Veränderung des Einstellwertes bei Proportional-Druckventilen[1]). (Diese Fehlerannahme erfolgt bei den genannten Ventilen zusätzlich zu den anderen Fehlerannahmen) | nein[7]) | [7]) Da der zur Einstellung erforderliche Sollwert aus der Elektronik vorgegeben wird und bewegte Bauteile vorhanden sind[3]), ist in der Regel kein Fehlerausschluß möglich. |
| Selbsttätige Veränderung der Verstelleinrichtung | ja, bei wirksamer und dem Einsatzfall angepasster Sicherung der Verstelleinrichtung unter Beachtung sicherheitstechnischer Festlegungen (z. B. Plombieren) | |
| Unbeabsichtigtes Herausdrehen des Verstellteils der Verstelleinrichtung | ja, wenn eine wirksame formschlüssige Sicherung gegen Herausdrehen vorhanden ist | |
| Leckage | ja, bei Sitzventilen, Membranventilen und Ventilen in Kolbenbauart mit elastischen Dichtungen, wenn normale Einsatzbedingungen vorliegen und eine ausreichende Aufbereitung der Druckluft vorhanden ist<br>nein, bei Sitzventilen, wenn keine normalen Einsatzbedingungen vorliegen[8]) | [8]) Nicht normale Einsatzbedingungen liegen z. B. vor bei erheblicher Feststoffbelastung der Druckluft (innere und äußere Ursachen) und/oder hohem Schmierstoffanteil in der Druckluft. |

*1.4 Druckventile (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung des Leckagevolumenstroms | nein[9]) | [9]) Über einen längeren Betrachtungszeitraum werden Veränderungen des Ventilsitzes (z. B. durch Verschleiß, chemische Veränderungen des Dichtungswerkstoffes) angenommen. Zusätzlich werden partielle Deformationen an Dichtungen oder/ und Ventilsitzen bei nicht normalen Einsatzbedingungen unterstellt (siehe [8])). |
| Bersten des Ventilgehäuses und Bruch der bewegten Bauteile (außer Regelfeder und Membrane) sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind. | |

## 2 Leitungen (Pn)

### 2.1 Rohrleitungen (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten und Leckage | ja, wenn insbesondere Dimensionierung, Materialauswahl, Herstellung, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind[1]) | [1]) Bei der Verwendung von Kunststoffrohren sind die Herstellerangaben zu beachten, insbesondere bzgl. betrieblicher Umgebungseinflüsse (z. B. thermische Einflüsse, chemische Einflüsse, Einflüsse durch Strahlung). Bei der Verwendung von nicht mit korrosionshemmenden Mitteln behandelten Stahlrohren ist insbesondere eine ausreichende Trocknung der Druckluft erforderlich. |
| Abreißen am Verbindungselement | ja, bei Verwendung von gebräuchlichen Verbindungselementen, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden[2]) und wenn Dimensionierung, Materialauswahl, Herstellung, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind. | [2]) Keine besonderen sicherheitstechnischen Anforderungen liegen vor, wenn z. B. durch das Versagen der Rohrleitung keine gefahrbringende Maschinenbewegung zu erwarten ist. |

*2.1 Rohrleitungen (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | nein, bei Verwendung von Verbindungselementen für Kunststoffrohr (Steck-, Quetschsystem u. ä.), wenn besondere sicherheitstechnische Anforderungen gestellt werden[3]<br>ja, bei Verwendung von Schneidringverschraubungen oder Gewinderohren (also Stahlrohren), wenn Dimensionierung . . . | [3]) Besondere sicherheitstechnische Anforderungen liegen z. B. vor, wenn Massen pneumatisch hochgehalten oder abgebremst werden (bei großer kinetischer Energie) und Personen im Gefahrenbereich zu erwarten sind. |
| Zusetzen (Verstopfen) | ja, bei Rohrleitungen im Leistungskreis sowie bei Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden.<br>ja, wenn die Nennweite der Leitung $\geq$ 2 mm beträgt<br>nein, wenn besondere sicherheitstechnische Anforderungen gestellt werden[4] und die Nennweite der Leitung $<$ 2 mm beträgt | [4]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines fehlerhaften Signals eine Gefährdung entstehen kann, z. B. bei Ventilüberwachung mittels Druckschalter. |
| Abknicken der Kunststoffrohrleitungen mit geringer Nennweite | ja, bei Leitungen im Leistungskreis sowie bei Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen[4] gestellt werden<br>ja, wenn eine entsprechend geschützte Verlegung bei Berücksichtigung der entsprechenden Herstellerangaben (z. B. minimaler Biegeradius) der Leitungen erfolgt ist<br>nein, wenn besondere sicherheitstechnische Anforderungen[4] vorliegen und keine entsprechend geschützte Verlegung bei Berücksichtigung der entsprechenden Herstellerangaben (z. B. minimaler Biegeradius) der Leitungen erfolgt ist | |

## 2.2 Schlauchleitungen (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten, Ausreißen aus Einbindung und Leckage | ja, wenn keine besonderen sicherheitstechnischen Anforderungen [1]) gestellt werden und wenn insbesondere Dimensionierung, Materialauswahl, Herstellung und Anordnung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind<br>nein, wenn besondere sicherheitstechnische Anforderungen [2]) gestellt werden (auch wenn Dimensionierung ...<br>ja, bei besonderen sicherheitstechnischen Anforderungen, wenn Schlauchleitungen nach DIN 20066, bestehend aus entsprechenden Schläuchen (mindestens Schläuche mit Textileinlage, Typ 2 TE nach DIN 20021, Teil 2 mit den entsprechenden Schlaucharmaturen, verwendet und angeordnet werden [3]) | [1]) Keine besonderen sicherheitstechnischen Anforderungen liegen vor, wenn z. B. durch das Versagen der Schlauchleitung keine gefahrbringende Maschinenbewegung zu erwarten ist und wenn die Aufenthaltsdauer von Personen im möglichen Gefahrenbereich der Schlauchleitung gering ist.<br>[2]) Besondere sicherheitstechnische Anforderungen liegen z. B. vor, wenn Massen pneumatisch hochgehalten oder abgebremst werden (bei großer kinetischer Energie) und Personen im Gefahrenbereich zu erwarten sind oder eine unmittelbare Gefährdung von Personen durch das Versagen der Schlauchleitung (Aufpeitschen) besteht. Hierbei sind vor allem Fertigungsmängel bei der Schlauch- und Schlauchleitungsherstellung sowie leistungsmindernde Einflüsse durch Alterung und betriebliche Umgebungseinflüsse anzunehmen.<br>[3]) Ein Versagen der Schlauchleitung kann als hinreichend unwahrscheinlich angenommen werden, wenn die Schlauchleitung nach DIN 20006 ausgeführt und angeordnet ist. |
| Zusetzen (Verstopfen) | ja, bei Schlauchleitungen im Leistungskreis sowie bei Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden<br>ja, wenn die Nennweite der Leitung $\geq$ 2 mm beträgt<br>nein, wenn besondere sicherheitstechnische Anforderungen [4]) gestellt werden und die Nennweite der Leitung $<$ 2 mm beträgt | [4]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines fehlerhaften Signals eine Gefährdung entstehen kann, z. B. bei Ventilüberwachung mittels Druckschalter. |

### 2.3 *Verbindungselemente* (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten, Versagen von Befestigungsschrauben oder Ausreißen von Gewinden | ja, wenn Dimensionierung, Materialauswahl, Herstellung, Anordnung und Verbindung zur Leitung bzw. zum fluidtechnischen Bauteil nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Leckage (Versagen der Dichtwirkung) | nein [1] | [1] Durch Verschleiß, Alterung, Nachlassen der Elastizität etc. ist kein Fehlerausschluß für eine längere Zeitspanne möglich. Nicht angenommen wird ein plötzliches weitgehendes Versagen der Dichtwirkung. |
| Zusetzen (Verstopfen) | ja, bei Anwendungen im Leistungskreis sowie in Steuer- und Meßleitungen, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden<br>ja, wenn die Nennweite $\geq$ 2 mm beträgt<br>nein, wenn besondere sicherheitstechnische Anforderungen gestellt werden [2] und die Nennweite $<$ 2 mm beträgt | [2] Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines fehlerhaften Signals eine Gefährdung entstehen kann z. B. bei Ventilüberwachung mittels Druckschalter. |

### 3 Zylinder (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Undichtwerden der Druckräume bzw. Veränderung der Dichtwirkung | nein [1] | [1] Durch Verschleiß von Dichtungen und Führungen ist kein Fehlerausschluß für eine längere Zeitspanne möglich. Nicht angenommen wird ein plötzliches weitgehendes Versagen von Dichtungen. |
| Versagen der Endlagendämpfung | ja, wenn dem in der Endlagendämpfung vorhandenen Stromventil (Drosselrückschlagventil) kein Versagen unterstellt wird [2] | [2] siehe 1.3 Stromventile (Pn) (Veränderung des Volumenstroms ohne Veränderung der Verstelleinrichtung) |

*3 Zylinder (Pn) Fortsetzung*

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| | nein, wenn dem in der Endlagendämpfung vorhandenen Stromventil (Drosselrückschlagventil) Versagen unterstellt wird [2]) | |
| Lösen der Verbindung Kolben/Kolbenstange sowie Kolbenstange/Mechanik | ja, wenn Konstruktion und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind sowie ggf. spezifischen Sicherheitsanforderungen entsprechen | |
| Bersten der Druckräume sowie Bruch von Befestigungs- und Deckelschrauben | ja, wenn Dimensionierung, Materialauswahl, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |
| Ausknicken von Kolbenstangen | ja, wenn Dimensionierung, Materialauswahl, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

**4 Druckübersetzer/Druckmittelwandler (Pn)**

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Undichtwerden der Druckräume bzw. Veränderung der Dichtwirkung | nein [1]) | [1]) Durch Verschleiß von Dichtungen und Führungen ist kein Fehlerausschluß für eine längere Zeitspanne möglich. Nicht angenommen wird ein plötzliches weitgehendes Versagen von Dichtungen. |
| Bersten der Druckräume sowie Bruch von Befestigungs- und Deckelschrauben | ja, wenn Dimensionierung, Materialauswahl, Anordnung und Befestigung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

## 5 Druckluftaufbereitung (Pn)

### 5.1 Filter (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Zusetzen des Filterelementes | nein [1] | [1] Insbesondere nach Arbeiten an der Drucklufterzeugungsanlage und den Leitungen des Druckluftnetzes sowie bei nicht oder nur mangelhaft aufbereiteter Druckluft ist ein Zusetzen des Filterelementes zu erwarten, auch bei richtiger Dimensionierung |
| Bruch des Filterelementes | ja, wenn eine ausreichende Druckfestigkeit des Filterelementes vorhanden ist | |
| Versagen der Verschmutzungsanzeige | nein | |
| Bersten des Filtergehäuses und Bruch der Deckelschrauben bzw. der Verbindungsschrauben | ja, wenn Dimensionierung, Materialauswahl, Anordnung im System und Befestigung nach den allgemein anerkannten Regeln der Technik [2] und dem Stand der Technik erfolgt sind | [2] In Ausnahmefällen (großes Volumen) kann es erforderlich sein, darüber hinaus die Anforderungen der Druckbehälterverordnung einschließlich der dort genannten Regeln zu beachten. |

### 5.2 Öler (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung des eingestellten Wertes (Ölvolumen pro Zeiteinheit) ohne Veränderung der Verstelleinrichtung | nein [1] | [1] Durch Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich. |
| Selbsttätige Veränderung der Verstelleinrichtung | ja, wenn keine extremen Schwingungsbelastungen gegeben sind | |
| Unbeabsichtigtes Herausdrehen des Verstellteils der Verstelleinrichtung | ja, wenn eine wirksame formschlüssige Sicherung gegen Herausdrehen vorhanden ist | |
| Bersten des Gehäuses sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

### 5.3 Schalldämpfer (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Zusetzen des Schalldämpferelementes | ja, wenn keine besonderen sicherheitstechnischen Anforderungen gestellt werden<br>nein, wenn besondere sicherheitstechnische Anforderungen [1]) gestellt werden<br>ja, wenn aufgrund von Konstruktion und Ausführung ein Zusetzen des Schalldämpferelementes ausgeschlossen werden kann [2]) | [1]) Besondere sicherheitstechnische Anforderungen liegen vor, wenn aufgrund eines erhöhten Staudruckes in der Abluft eine Gefährdung entstehen kann z. B. durch Nichtschalten oder ungewolltes Schalten oder verzögertes Schalten eines Ventils<br>[2]) Das Zusetzen des Schalldämpferelementes bzw. die Erhöhung des Staudruckes in der Abluft über einen kritischen Wert ist hinreichend unwahrscheinlich bei einer entsprechenden Querschnittsgröße und/oder entsprechenden Konstruktion des Schalldämpferelementes. |
| Unbeabsichtigtes Herausdrehen des Schalldämpfer/ Schalldämpferelementes | ja, wenn eine wirksame Sicherung gegen Herausdrehen vorhanden ist | |
| Bruch/Bersten des Schalldämpfergehäuses sowie Bruch des Befestigungsgewindes | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

### 6 Energiespeicher (Druckbehälter) (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Bersten des Druckbehälters und Bruch von Verbindungs- und Deckelschrauben sowie Ausreißen von Anschlußgewinden | ja, wenn Bau, Ausrüstung und Anordnung im System den Anforderungen [1]) entsprechen sowie nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | [1]) Anforderungen an Bau und Ausrüstung sind insbesondere in der Druckbehälterverordnung und in den dort genannten Regeln festgelegt. |

## 7 Motoren (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Veränderung des Schluckstromes bei Druckluftmotoren | ja, bei kürzeren Betrachtungszeiträumen [1] | [1] Bei längeren Betrachtungszeiträumen muß eine Veränderung durch Verschleiß der bewegten Teile und Dichtungen angenommen werden. |
| Selbsttätige Veränderung der Schluckstromeinstellung ohne Betätigung der Verstelleinrichtung bei Druckluftmotoren | ja, bei Druckluftmotoren mit Druck- oder/und Volumenstromregelung, wenn keine besonderen Anforderungen an die Konstanthaltung der Einstellparameter gestellt werden<br>nein, bei Druckluftmotoren mit Druck- oder/und Volumenstromregelung, wenn besondere Anforderungen [2] an die Konstanthaltung der Einstellparameter gestellt werden | [2] Besondere Anforderungen liegen vor, wenn z. B. Geschwindigkeiten/Drehzahlen oder Drehmoment mit den Anforderungsstufen „Einfehlersicherheit" oder „Selbstüberwachung" eingehalten werden müssen (entsprechende Fehlerannahmen siehe 1.3 Stromventile (Pn) und/oder 1.4 Druckventile (Pn). |
| Bruch oder Lösen der abtriebsseitigen Verbindungselemente (Kupplungen) sowie Bersten des Gehäuses und Bruch von Deckel- und Befestigungsschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

## 8 Sensoren (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausfall des Sensors [1]<br>Veränderung der Erfassungs- und Ausgabecharakteristik | nein [2]<br>nein [2] | [1] Unter diese Begriffsbestimmung fällt hier die Signalerfassung, -verarbeitung und -ausgabe insbesondere von Druck, Volumenstrom, Temperatur und Weg.<br>[2] Durch z. B. Verschleiß, Materialermüdung, (u. a. Federn), Fremdeinflüsse, Verstopfen von Blenden und Düsen sowie Ausfall und/oder Veränderung im Verhalten der elektrisch/elektronischen Bauteile ist kein Fehlerausschluß möglich. |

## 9 Informationsverarbeitung (Pn)

### 9.1 Verknüpfungsglieder (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausfall des Verknüpfungsgliedes [1]) durch z. B. Veränderung der Schaltzeiten, Nichtschalten oder nicht vollständiges Schalten | nein [2])<br>ja [2]) | [1]) Unter diese Begriffsbestimmung fallen pneumatische Verknüpfungsglieder wie z. B. UND-Glied, ODER-Glied, Speicher-Glied.<br>[2]) Entsprechende Fehlerannahmen sowie Fehlerausschlüsse siehe<br>1.1 Wegeventile (Pn)<br>1.2 Sperrventile (Pn) und<br>1.3 Stromventile (Pn) |

### 9.2 Verzögerungsglieder (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausfall des Verzögerungsgliedes [1]) oder Veränderung der Erfassungs- und Ausgabecharakteristik | nein [2])<br>ja, bei Verzögerungsgliedern ohne bewegte Bauteile (z. B. Festwiderstände), wenn normale Einsatzbedingungen vorliegen und eine ausreichende Aufbereitung der Druckluft erfolgt [3]) | [1]) Unter diese Begriffsbestimmung fallen pneumatische sowie pneumatisch/mechanische Zeit- und Zählglieder.<br>[2]) Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinflüsse, chemische Einflüsse von Schmierstoffen auf Dichtungen, Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich.<br>[3]) Normale Einsatzbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten und keine größeren Feststoffpartikeln (in Relation z. B. zum Querschnitt des Festwiderstandes) im System zu erwarten sind. |
| Bersten des Gehäuses sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |

### 9.3 Umformer (Pn)

| Fehlerannahme | Fehlerausschluß | Bemerkungen |
|---|---|---|
| Ausfall des Umformers[1] oder Veränderung der Erfassungs- und Ausgabecharakteristik | nein[2]<br>ja, bei Umformern ohne bewegte Bauteile (z. B. Reflexdüse), wenn normale Einsatzbedingungen vorliegen und eine ausreichende Aufbereitung der Druckluft erfolgt[3] | [1] Unter diese Begriffsbestimmung fallen Bauelemente für z. B. die Umformung eines pneumatischen in ein elektrisches Signal, die Erfassung von Positionen (Zylinderschalter, Reflexdüse), die Verstärkung von pneumatischen Signalen<br>[2] Durch z. B. Verschleiß, Materialermüdung (u. a. Federn), Fremdeinflüsse, chemische Einflüsse von Schmierstoffen auf Dichtungen, Verstopfen von Blenden und Düsen ist kein Fehlerausschluß möglich.<br>[3] Normale Einsatzbedingungen liegen vor, wenn die vom Hersteller vorgesehenen Bedingungen eingehalten und keine größeren Feststoffpartikeln (in Relation z. B. zum Querschnitt der Düse) im System zu erwarten sind. |
| Bersten des Gehäuses sowie Bruch der Befestigungs- und Deckelschrauben | ja, wenn Konstruktion, Dimensionierung und Ausführung nach den allgemein anerkannten Regeln der Technik und dem Stand der Technik erfolgt sind | |