IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Sicherheits-Teilfunktionen nach VDMA-Einheitsblatt 24584 – Beispiele zweikanaliger elektro-pneumatischer Steuerungen

1 Einleitung

Dieser Artikel beschreibt die Eigenschaften, Auswahl und Realisierung typischer Sicherheitsfunktionen an einer Maschine unter Verwendung von Sicherheits-Teilfunktionen aus dem VDMAEinheitsblatt 24584 „Sicherheitsfunktionen geregelter und nicht geregelter (fluid-)mechanischer Systeme“. Zwei Beispiele zeigen, wie sich mit den Sicherheits-Teilfunktionen STO (Safe Torque Off), SCA (Safe Cam) und SSC (Safe Stopping and Closing) typische Sicherheitsfunktionen einer Maschine für den pneumatischen Steuerungsteil in Kategorie 3 nach DIN EN ISO 13849 realisieren lassen. Neben der Darstellung der sicherheitsbezogenen Blockdiagramme werden mögliche Ausfälle der pneumatischen Bauteile analysiert, deren Auswirkung beschrieben und die Möglichkeiten zur Fehlererkennung/Diagnose dargestellt. Abschließend sind konstruktive Merkmale zu den Beispielen aufgezeigt und Hinweise zur Berechnung der Ausfallwahrscheinlichkeit gegeben. Dabei sind lediglich die pneumatischen und elektro-pneumatischen Komponenten berücksichtigt. Für eine Berechnung der Gesamtausfallwahrscheinlichkeit der Sicherheitsfunktionen ist auch die elektrische Steuerung zu berücksichtigen, auf die in dieser Praxishilfe nicht weiter eingegangen wird.

Mit Herstellern und Anwendern mechanischer, pneumatischer sowie hydraulischer Bauteile und unter Mitwirkung des Instituts für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) wurde im Arbeitskreis „Funktionale Sicherheit“ (AK FuSi) des Fachverbands Fluidtechnik im VDMA ein Einheitsblatt erarbeitet, das die Ideen aus der elektrischen Antriebstechnik in die pneumatische, hydraulische und mechanische Antriebstechnik transferiert.

Unter dem Titel VDMA 24584 „Sicherheitsfunktionen geregelter und nicht geregelter (fluid)mechanischer Systeme“ ist dieses Einheitsblatt seit 2016 verfügbar. Es wurde 2020 um sicherheitstechnische Anforderungen für die Hydraulik erweitert. Beschrieben werden Sicherheits-Teilfunktionen für die Technologien Mechanik, Pneumatik und Hydraulik, die bereits aus der DIN EN 61800-5-2, „Elektrische Antriebe mit einstellbarer Drehzahl, Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit“, bekannt sind.

Die Beispiele in den Kapiteln 3 und 4 dieser Praxishilfe bauen auf dem Artikel „Sicherheitsfunktionen in pneumatischer Antriebstechnik“ aus der Fachzeitschrift O+P Fluidtechnik vom März 2017 auf.

Nachdem die Überarbeitung der DIN EN 61800-5-2 Ende 2017 veröffentlicht wurde, ist eine Anpassung dieser Beispiele erfolgt. Die Norm verwendet aktuell den Begriff Sicherheits-Teilfunktion.

2 Sicherheitsfunktionen

2.1 Typische Sicherheitsfunktionen

Typische Sicherheitsfunktionen einer Maschine sind zum Beispiel:

- SF1: Schutz vor unerwartetem Anlauf eines Antriebs aus der Ruhelage bei geöffneter, trennender Schutzeinrichtung
- SF2: Anhalten einer gefahrbringenden Bewegung bei Eingriff in ein Lichtgitter

2.2 Eigenschaften von Sicherheitsfunktionen

Die im Einheitsblatt beschriebenen Sicherheits-Teilfunktionen lassen sich in aktiv und passiv einteilen. Beispielsweise wirken aktive Sicherheits-Teilfunktionen auf den Antrieb in Form von Kraft, Geschwindigkeit, Lage oder Beschleunigung durch das Zu- oder Abschalten (Bereitstellen) von Druck oder Durchfluss (Energie). Ein Ventil kann die Druckluft für einen Antrieb zuschalten, einsperren oder den Antrieb entlüften. Eine passive Sicherheits-Teilfunktion dient der Überwachung von Größen wie Druck, Durchfluss oder Position bzw. Stellung des Antriebs auf Einhaltung von Grenzwerten. Die DIN EN 61800-5-2 unterscheidet hier Stopp-Funktionen und Überwachungsfunktionen, die aktiv oder passiv ausgeführt sein können.

Typischerweise setzt sich eine Sicherheitsfunktion, wie in den Normen der funktionalen Sicherheit definiert, aus den Bestandteilen Sensorik (Erfassen auslösender Ereignisse), Logik (Auswertung der Eingangssignale mit Verknüpfung und Erzeugung von Ausgangssignalen) und Aktorik (Leistungssteuerelemente zum Schalten des Antriebs) zusammen, siehe Abbildung 1. Die Logik kann rein pneumatisch oder als elektrische Ablaufsteuerung realisiert sein. Als Aktor dienen elektrisch oder pneumatisch gesteuerte Ventile. Eine ausführliche Einführung in die „Definition von Sicherheitsfunktionen – Was ist wichtig?“ bietet auch das SISTEMA-Kochbuch 6.

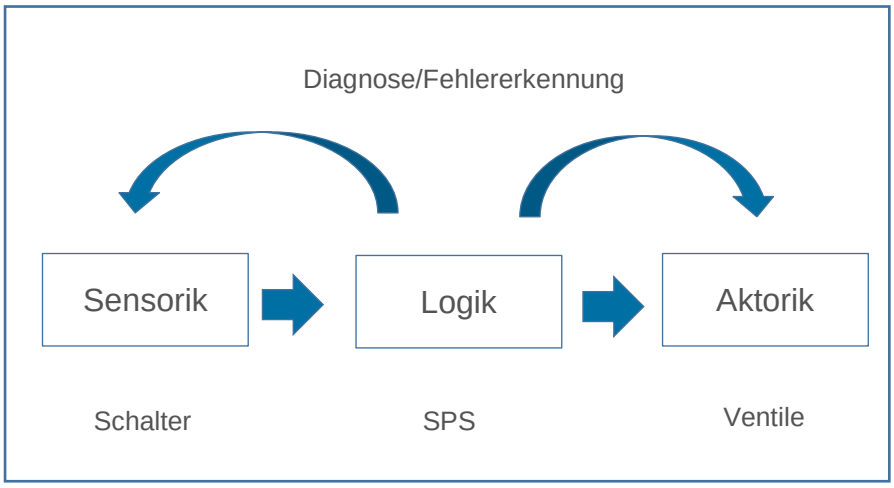

Abbildung 1: Teile einer Sicherheitsfunktion und Beispiele für eine Realisierung

Fluidtechnische Leistungselemente, die von den Leistungssteuerelementen gesteuert werden, wie Zylinder, liegen außerhalb des Anwendungsbereiches der DIN EN ISO 13849-1 und zählen daher nicht zu den an der Sicherheitsfunktion beteiligten Komponenten (SRP/CS). Treten jedoch im energielosen Zustand Gefährdungen auf, (z. B. gefahrbringende Bewegung eines Zylinders aufgrund der Einwirkung äußerer Kräfte oder interner Leckage) so müssen unter Umständen

Sicherheitsfunktionen für den energielosen Zustand ergänzt werden. Das kann z. B. durch den Einsatz von Halteeinrichtungen realisiert werden. Weitere Erläuterungen finden sich in dem Informationsblatt Fachbereich AKTUELL FB HM-050 zu fluidtechnischen Leistungselementen.

2.3 Realisierung von Sicherheitsfunktionen

Pneumatische Steuerungen zur Realisierung von Sicherheitsfunktionen sind im Gegensatz zu integrierten elektrischen Antriebssteuerungen häufig diskret aus einzelnen Ventilen aufgebaut. Abhängig von der Steuerungs-Kategorie nach DIN EN ISO 13849-1 sind fehlererkennende Maßnahmen erforderlich. Die Maßnahmen und Abläufe zur Fehlererkennung müssen häufig zusätzlich integriert, eigenständig erarbeitet und durch die Logik (Hardware inklusive Software) umgesetzt werden.

2.4 Beschreibung und Auswahl von Sicherheits-Teilfunktionen

Eine Möglichkeit zur Realisierung des Aktorteils der beiden vorgenannten typischen Sicherheitsfunktionen sind beispielsweise die Sicherheits-Teilfunktion STO oder SSC. Der STO beschreibt die Sicherheits-Teilfunktion „sicher abgeschaltetes Moment“ für den Leistungsantrieb. Bei einem elektrischen Antrieb (Motor), wird der STO über die Wegnahme der elektrischen Energie zum Motor eingeleitet. Die Ausführung des STO bei einem pneumatischen Antrieb wird durch die Entlüftung der Kolbenräume des Zylinders (Leistungsantrieb) realisiert. Für den Schutz vor unerwartetem Anlauf ist dies in der Regel einfach umzusetzen, solange keine Fremdkräfte, z. B. Schwerkraft, auf den Antrieb wirken. Soll der STO auch zum Anhalten einer Bewegung genutzt werden, muss unter anderem der Nachlaufweg bis zum Stopp der Bewegung im Rahmen der erforderlichen Risikobeurteilung berücksichtigt werden. Ist dieser Nachlaufweg zu groß, bieten sich alternative Sicherheits-Teilfunktionen wie SS1 oder SS2 an. Diese sind in der pneumatischen Steuerungstechnik weniger verbreitet. Zum schnellen Anhalten bietet sich für pneumatische Antriebe die Sicherheits-Teilfunktion SSC (Safe Stopping and Closing) an. Beispielhaft beschreiben die nächsten Kapitel die mögliche Realisierung der Sicherheitsfunktionen mit entsprechenden pneumatischen Sicherheits-Teilfunktionen aus dem VDMA-Einheitsblatt.

3 Zweikanalige elektro-pneumatische Steuerung für STO (Safe Torque Off)

Bei einem horizontal arbeitenden Zylinder wirkt durch einen ausgelösten STO kein Antriebsmoment mehr auf die Kolbenstange. Eine mögliche zweikanalige Realisierung in Kategorie 3 nach DIN EN ISO 13849 zeigt Abbildung 2. Beide Kolbenräume des Leistungsantriebs (Zylinder) werden bei Anforderung der Sicherheitsfunktion entlüftet. Ist der Zylinder nicht horizontal angeordnet und wird der STO während einer Bewegung ausgelöst, so läuft die Bewegung nach und der Antrieb hält erst schwerkraftbelastet in der unteren Endlage an. Das Erreichen der Endlage kann über die Sicherheits-Teilfunktion SCA (sichere Positionsüberwachung) abgefragt werden.

3.1 Funktionsbeschreibung der zweikanaligen elektro-pneumatischen Steuerung für STO und SCA

Der Schutz vor unerwartetem Anlauf (SF1) wird über die Sicherheits-Teilfunktion STO realisiert. Sind alle Ventile aus Abbildung 2 in Ruhestellung und werden die konstruktiven Merkmale aus Kapitel 3.5 eingehalten, gewährleistet dies eine redundante Entlüftung beider Kolbenräume.

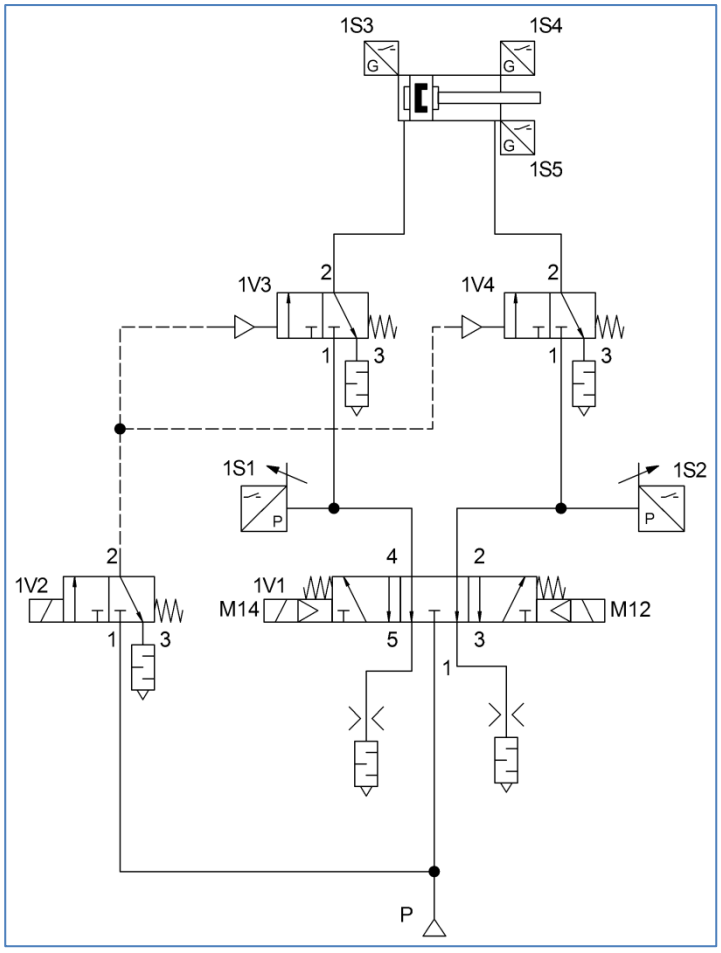

Abbildung 2: Beispiel einer zweikanaligen elektro-pneumatischen Steuerung für STO

Zum Anhalten einer gefahrbringenden Bewegung (SF2) kann ebenfalls der STO genutzt werden, wenn sich ein möglicher Nachlaufweg nicht gefahrbringend auswirkt. In der federzentrierten Mittelstellung des Wegeventils 1V1 sind die Anschlüsse 2 und 4 entlüftet. Das Wegeventil 1V2 dient der Ansteuerung der 3/2-Wege-Entlüftungsventile 1V3 und 1V4. Die Ventile 1V3 und 1V4 müssen so ausgeführt sein, dass bei Hängenbleiben des Kolbenschiebers in beliebiger Zwischenstellung

eine Entlüftung von Anschluss 2 zu den Anschlüssen 1 und/oder 3 immer gegeben ist (negative Überdeckung). In der sicherheitsgerichteten Ruhestellung von 1V3 und 1V4 muss Anschluss 1 sicher gesperrt sein (positive Überdeckung).

Wirkt an dem Zylinder eine externe Kraft, weil dieser beispielsweise nicht horizontal angeordnet ist, ist es möglich, mit der Sicherheits-Teilfunktion SCA die ausgefahrene Endlage der Kolbenstange über die beiden Initiatoren 1S4 und 1S5 redundant zu detektieren. Nachdem über SCA eine ausgefahrene Endlage detektiert worden ist, wird der STO ausgeführt. Der SCA kann als Sensorteil einer Sicherheitsfunktion dienen, die z. B. den Zugang zu einem gefahrbringenden Arbeitsbereich erst freigibt, wenn der Zylinder eine ungefährliche Endlage erreicht hat.

3.2 Sicherheitsbezogenes Blockdiagramm für den STO

Ein Fehler oder der Ausfall eines Ventils führt in der Schaltung aus Abbildung 2 nicht zum Verlust der Sicherheits-Teilfunktion STO, da das Entlüften und damit der STO redundant ausgeführt ist. Das sicherheitsbezogene Blockdiagramm in Abbildung 3 zeigt die an der Teil-Sicherheitsfunktion STO beteiligten Bauteile der pneumatischen Steuerung. 1S1 bis 1S4 sind nicht an der Ausführung der Sicherheits-Teilfunktion STO beteiligt, sondern dienen hier ausschließlich der Fehlererkennung. Der Initiator 1S5 wird für die Ausführung und für die Fehlererkennung der Sicherheits-Teilfunktion STO nicht benötigt.

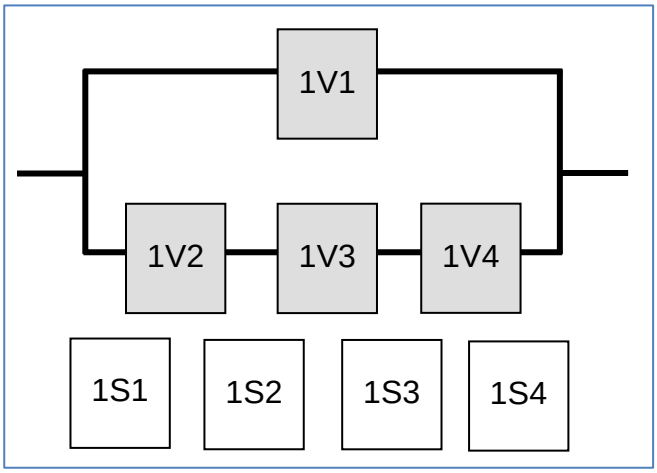

Abbildung 3: Sicherheitsbezogenes Blockdiagramm für das Beispiel STO in Kategorie 3

In der hier nicht weiter beschriebenen Sicherheits-Teilfunktion SCA bildet der Initiator 1S4 im sicherheitsbezogenen Blockdiagramm den ersten Kanal und 1S5 den zweiten Kanal.

3.3 Fehler- und Ausfallmöglichkeiten

Um den Anforderungen der DIN EN ISO 13849-1 an die Kategorie 3 gerecht zu werden, bedarf es fehlererkennender Maßnahmen. Wenn in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden. In Tabelle 1 sind Fehler bzw. Ausfälle und ihre Auswirkung auf die Funktion des Zylinders aufgeführt. Betrachtet werden der Stillstand, in dem alle Ventile ohne Ansteuerung in Ruhestellung verbleiben sollen, und das Anhalten einer Bewegung, in der die Ventile von angesteuerter Arbeitsstellung mit Wegnahme der Ansteuerung in Ruhestellung schalten sollen.

Betriebssituation	Fehlerannahme	Auswirkung
Stillstand	Schalten von Ruhe- in Arbeitsstellung eines der Ventile	Kolbenräume bleiben druckfrei und es folgt keine gefahrbringende Bewegung
	Interne Leckage zwischen den Anschlüssen eines Ventils	
Anhalten	Nicht-Zurückschalten von 1V1	Kolbenräume über 1V3 und 1V4 entlüftet und Bewegung läuft aus
	Nicht vollständiges Zurückschalten von 1V1 bzw. Hängenbleiben in Zwischenposition	
	Nicht-Zurückschalten von 1V2	Kolbenräume über 1V1 entlüftet und Bewegung läuft aus
	Nicht vollständiges Zurückschalten von 1V2 bzw. Hängenbleiben in Zwischenposition	
	Nicht-Zurückschalten von 1V3	Kolbenräume über 1V4 und 1V1 entlüftet und Bewegung läuft aus
	Nicht vollständiges Zurückschalten von 1V3 bzw. Hängenbleiben in Zwischenposition (in negativer Überdeckung)	
	Nicht-Zurückschalten von 1V4	Kolbenräume über 1V3 und 1V1 entlüftet und Bewegung läuft aus
	Nicht vollständiges Zurückschalten von 1V4 bzw. Hängenbleiben in Zwischenposition (in negativer Überdeckung)	

Tabelle 1: Fehler- und Ausfallmöglichkeiten für das Beispiel STO

Damit die angenommenen Fehler aus der zweiten Spalte der Tabelle erkannt werden, bieten sich unterschiedliche Lösungen als fehlererkennende Maßnahmen an.

3.4 Fehlererkennende Maßnahmen bzw. Fehleraufdeckung

Zur Fehlererkennung können beispielsweise Ventile mit direkter Stellungsüberwachung eingesetzt werden. Die elektrische Steuerung führt im Arbeitszyklus eine Plausibilitätsprüfung zwischen der Ansteuerung der Ventile und dem Signal der Stellungsüberwachung der Ventile durch. Wird eine Nichtplausibilität durch die elektrische Steuerung erkannt, muss ein weiterer Betrieb der Maschine bis zur Fehlerbehebung verhindert werden.

Beim Einsatz von Ventilen ohne Stellungsüberwachung kann das Schaltverhalten von 1V1 im Arbeitszyklus über die Druckschalter 1S1 und 1S2 zur Diagnose genutzt werden. Dazu zeigen die Druckschalter bei nicht angesteuertem Ventil 1V1 die sicherheitsgerichtete (entlüftete) Mittelstellung von 1V1 an. Für die Ventile 1V2 bis 1V4 kann mithilfe der elektrischen Steuerung ein Funktionstest über einen Prüfalgorithmus realisiert werden. Damit ist es unter Einbeziehung der Zylinderschalter 1S3 und 1S4 möglich, Fehler an den Ventilen zu erkennen. Abbildung 4 beschreibt mit einem Ablaufplan beispielhaft einen Prüfalgorithmus, der aufzeigt, ob die Ventile 1V2 und 1V3 die Ruhestellung eingenommen haben. In vergleichbarer Weise kann getestet werden, ob das Ventil 1V4 die Ruhestellung eingenommen hat.

Hinweise:
Während der Prüfalgorithmus abläuft, darf es zu keiner Gefährdung des Bedienpersonals kommen. Zum Start des Funktionstests für 1V2 und 1V3 werden Druckschalter und Initiatoren auf korrekten Grundzustand abgefragt. Wird im Arbeitszyklus zusätzlich auf 1S3 = 0 abgefragt, so lässt sich auch

ein Versagen von 1S3 erkennen – diese Abfrage ist im Rahmen der Kategorieanforderungen jedoch nicht erforderlich.

Durch die fehlerkennenden Maßnahmen wird nach DIN EN ISO 13849-1 für die relevanten Bauteile ein Diagnosedeckungsgrad (DC) beschrieben. Wird das Einnehmen der Mittelstellung von 1V1 im Arbeitszyklus geprüft, so ergibt sich über diese indirekte Überwachung ein DC von 99 % für 1V1. Werden die Ventile 1V2 bis 1V4 mittels der beschriebenen Fehlererkennung beispielsweise alle acht Stunden geprüft, ergibt sich durch die indirekte Überwachung ein DC von 90 % für jedes Ventil.

Die Funktionsprüfung der Initiatoren für die Sicherheits-Teilfunktion SCA zur Erkennung der ausgefahrenen Endstellung erfolgt zyklisch über eine indirekte Überwachung durch Plausibilitätsprüfung mit Vergleich, woraus sich ein DC von 99 % für 1S4 und 1S5 ergibt.

3.5 Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien nach DIN EN ISO 13849-2 sowie die Anforderungen der Kategorie B sind für alle Bauteile eingehalten.

- Das Wegeventil 1V1 hat eine entlüftete Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. Das federrückgestellte Wegeventil 1V2 hat in Ruhestellung ausreichend positive Überdeckung.

- Die Ventile 1V3 und 1V4 haben in Ruhestellung ausreichend positive Überdeckung und sind in Zwischenstellung nicht überschneidungsfrei bzw. mit negativer Überdeckung.

- Die sicherheitsgerichtete Schaltstellung der Ventile wird jeweils durch die Wegnahme der Ansteuerung erreicht.

- Ein stabiler Aufbau zur Betätigung der Initiatoren, die als Zylinder-, Positions- oder Näherungsschalter ausgeführt sein können, ist sichergestellt. Der Schaltpunkt und die Hysterese sind so gewählt, dass ein Verlassen der Endlage des Zylinders erkannt wird.

- Der pneumatische Schaltpunkt der Druckschalter, der zum Umschalten des elektrischen Ausgangssignals führt, ist so gewählt, dass die sicherheitsgerichtete Schaltstellung (Anschlüsse 2 und 4 entlüftet) von 1V1 erkannt wird.

- Die Verarbeitung der Signale von Druckschaltern und Initiatoren erfolgt z. B. in einer elektrischen Logik/Speicherprogrammierbaren Steuerung (SPS) bzw. für die Sicherheits-Teilfunktion SCA in einer Sicherheits-SPS.

3.6 Berechnung der Ausfallwahrscheinlichkeit

Mit üblichen $MTTF_D$- bzw. B_{10D}-Werten, den Diagnosedeckungsgraden aus Abschnitt 3.4 und der Einhaltung der grundlegenden und bewährten Sicherheitsprinzipien sowie ausreichenden Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache CCF (Common Cause Failures), entspricht die Schaltung einer Kategorie 3. Die nach DIN EN ISO 13849-1 erforderliche Bestimmung der Wahrscheinlichkeit gefahrbringender Ausfälle (PFH_D) kann mit der Software SISTEMA des IFA erfolgen. Dazu ist als weitere Angabe die Schalthäufigkeit pro Jahr (n_{op}) der Komponenten erforderlich.

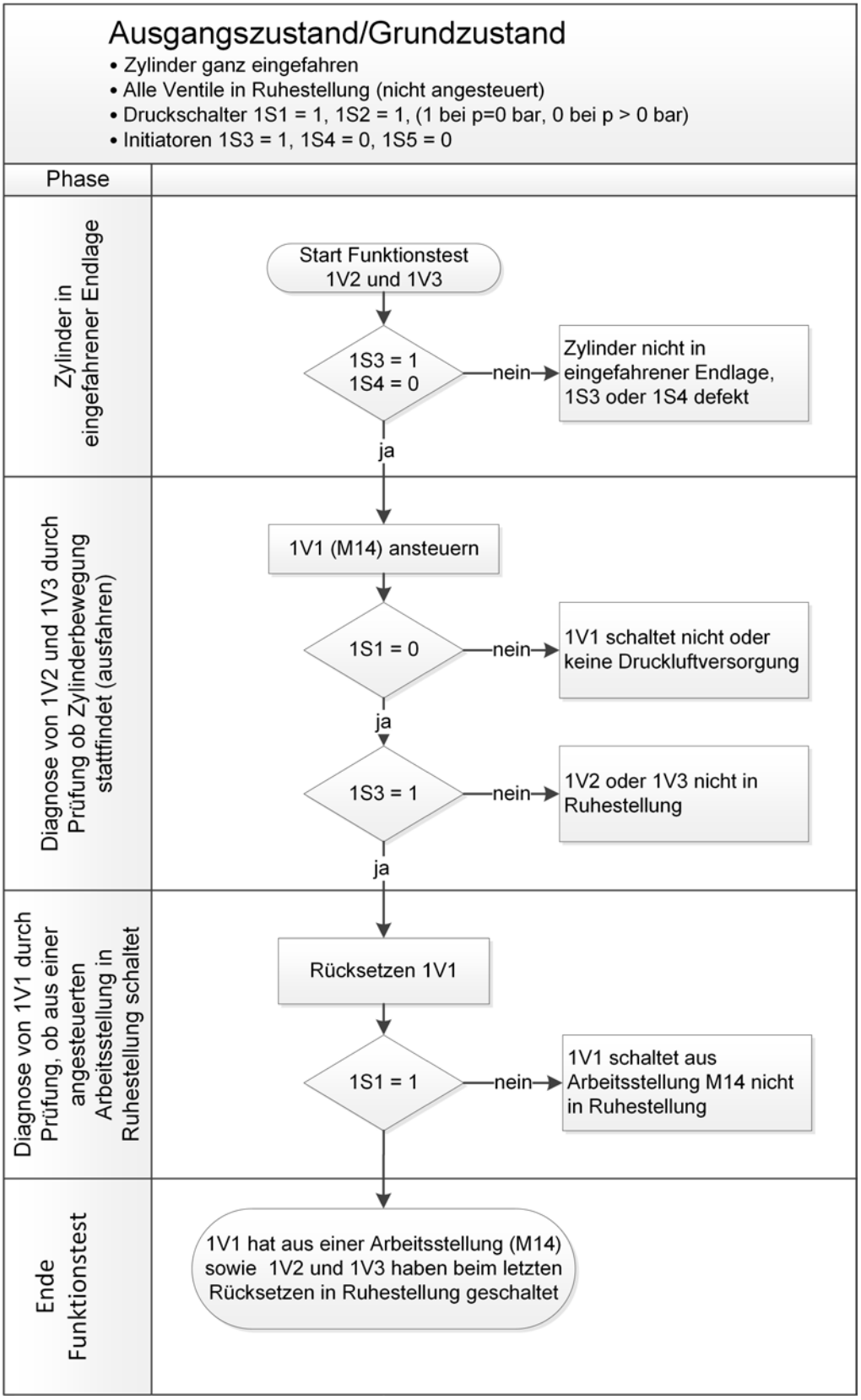

Abbildung 4: Ablaufplan zur Fehlererkennung an Ventilen für das Beispiel STO

4 Zweikanalige elektro-pneumatische Steuerung für SSC (Safe Stopping and Closing)

Mit der Sicherheits-Teilfunktion SSC werden die Kolbenräume des Zylinders im Gegensatz zum STO nicht entlüftet, sondern die Luft wird in den Kolbenräumen eingesperrt. Das bewirkt in der Regel ein schnelleres Anhalten einer Bewegung im Vergleich zu einem STO. Außerdem kann der Zylinder in einer Zwischenstellung stoppen. Der SSC bietet ebenfalls Schutz vor unerwartetem Anlauf. Die Abbildung 5 zeigt eine zweikanalige Realisierung.

4.1 Funktionsbeschreibung der zweikanaligen elektro-pneumatischen Steuerung für SSC

In diesem Beispiel wird eine schwerkraftbelastete Achse betrachtet. Der Schutz vor unerwartetem Anlauf (SF1) ist, solange die auf den Zylinder wirkenden Kräfte F konstant bleiben, aus jeder Kolbenstellung möglich und wird über die Sicherheits-Teilfunktion SSC realisiert. Auch das Anhalten wird – unabhängig von Bewegungsrichtung und Kolbenstellung (SF2) – durch SSC realisiert. Ein möglicher Nachlaufweg ist dabei zu berücksichtigen.

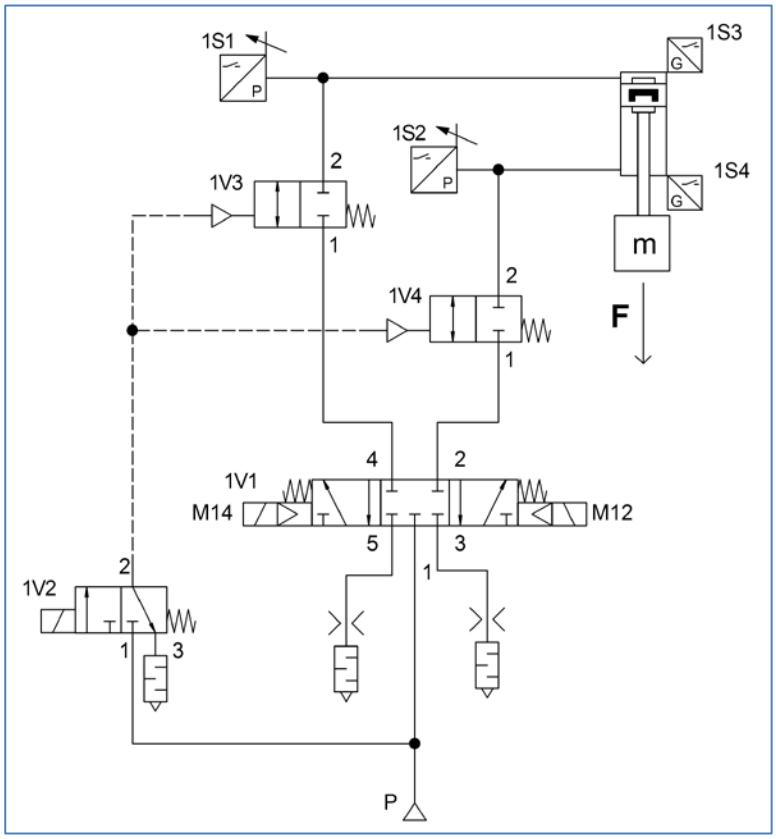

Abbildung 5: Beispiel einer zweikanaligen elektro-pneumatischen Steuerung für SSC

In der federzentrierten Mittelstellung des Wegeventils 1V1 sind die Anschlüsse 2 und 4 abgesperrt. Das Wegeventil 1V2 dient der Ansteuerung der 2/2-Wege-Sperrventile 1V3 und 1V4. Die Sperrventile sind in den Zylinder eingeschraubt. Die beiden Endlagen der Kolbenstange werden über die Initiatoren 1S3 und 1S4 detektiert. Die Druckschalter 1S1 und 1S2 zeigen den belüfteten Zustand an und dienen der Fehlererkennung an den Ventilen.

4.2 Sicherheitsbezogenes Blockdiagramm für SSC

Ein Fehler oder der Ausfall eines Ventils führt in der Schaltung aus Abbildung 5 nicht zum Verlust der Sicherheits-Teilfunktion SSC. Das Einsperren der Druckluft und damit SSC werden redundant ausgeführt. Das sicherheitsbezogene Blockdiagramm in Abbildung 6 zeigt die an der Sicherheits-Teilfunktion SSC beteiligten Bauteile der pneumatischen Steuerung. 1S1 bis 1S4 sind nicht zur Ausführung der Sicherheits-Teilfunktion erforderlich, sondern dienen ausschließlich der Fehlererkennung.

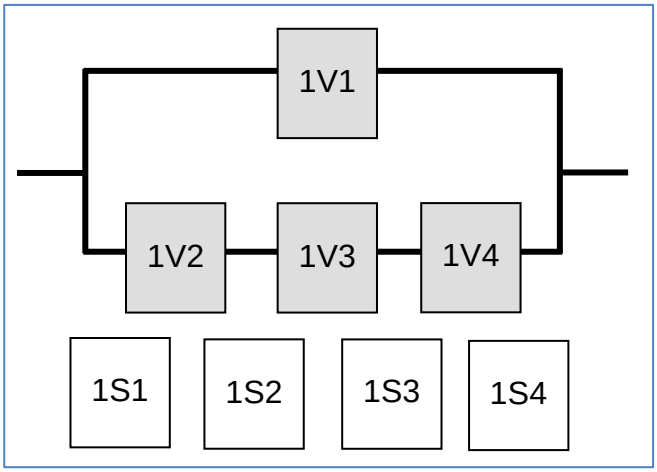

Abbildung 6: Sicherheitsbezogenes Blockdiagramm für das Beispiel SSC in Kategorie 3

4.3 Fehler- und Ausfallmöglichkeiten

Um den Anforderungen der DIN EN ISO 13849-1 an die Kategorie 3 gerecht zu werden, bedarf es fehlererkennender Maßnahmen. Wenn in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden. In Tabelle 2 sind Fehler bzw. Ausfälle und ihre Auswirkung auf die Funktion des Zylinders aufgeführt. Betrachtet werden der Stillstand, in dem alle Ventile ohne Ansteuerung in Ruhestellung verbleiben sollen, und das Anhalten einer Bewegung, in der die Ventile von angesteuerter Arbeitsstellung mit Wegnahme der Ansteuerung in Ruhestellung schalten sollen.

Betriebssituation	Fehlerannahme	Auswirkung
Stillstand	Schalten von Ruhe- in Arbeitsstellung oder interne Leckage zwischen den Anschlüssen von 1V1	Druckluft bleibt in beiden Kolbenräumen eingesperrt und es folgt keine gefahrbringende Bewegung
	Schalten von Ruhe- in Arbeitsstellung von 1V2, 1V3 oder 1V4 oder interne Leckage zwischen den Anschlüssen von 1V4	Kann zu einer kurzen Bewegung des Zylinders führen, die sich nicht gefahrbringend auswirken darf
	Leckage von Anschluss 2 zur Atmosphäre oder Steueranschluss der Ventile 1V3 und 1V4	Kann zu einer langsamen Bewegung des Zylinders führen, die sich nicht gefahrbringend auswirken darf
Anhalten	Nicht-Zurückschalten von 1V1	Druckluft wird über 1V2 und 1V3 in den Kolbenräumen eingesperrt und Bewegung stoppt
	Nicht vollständiges Zurückschalten von 1V1 bzw. Hängenbleiben in gesperrter Zwischenposition oder Leckage der Anschlüsse 2 oder 4 zur Atmosphäre	
	Nicht-Zurückschalten von 1V4	Druckluft wird über 1V1 und 1V3 in den Kolbenräumen eingesperrt und Bewegung stoppt, u. U. verlängerter Anhalteweg
	Nicht vollständiges Zurückschalten von 1V4 bzw. Hängenbleiben in gesperrter Zwischenposition	
	Nicht-Zurückschalten von 1V2	Druckluft wird über 1V1 in den Kolbenräumen eingesperrt und Bewegung stoppt, u. U. verlängerter Anhalteweg
	Nicht vollständiges Zurückschalten von 1V2 bzw. Hängenbleiben in Zwischenposition	
	Nicht-Zurückschalten von 1V3	Druckluft wird über 1V1 und 1V4 in den Kolbenräumen eingesperrt und Bewegung stoppt, u. U. verlängerter Anhalteweg
	Nicht vollständiges Zurückschalten von 1V3 bzw. Hängenbleiben in Zwischenposition	

Tabelle 2: Fehler-/Ausfallmöglichkeiten für das Beispiel SSC

Damit die angenommenen Fehler aus der zweiten Spalte der Tabelle erkannt werden, bieten sich unterschiedliche Lösungen als fehlererkennende Maßnahmen an.

4.4 Fehlererkennende Maßnahmen bzw. Fehleraufdeckung

Zur Fehlererkennung können beispielsweise Ventile mit direkter Stellungsüberwachung eingesetzt werden. Die elektrische Steuerung führt im Arbeitszyklus eine Plausibilitätsprüfung zwischen Ansteuerung der Ventile und dem Signal der Stellungsüberwachung der Ventile durch. Wird eine Nichtplausibilität durch die elektrische Steuerung erkannt, muss ein weiterer Betrieb der Maschine bis zur Fehlerbehebung verhindert werden.

Werden Ventile ohne Stellungsüberwachung verwendet, ist nachfolgend beschrieben, wie eine entsprechende Diagnose erfolgen kann. Für alle an der Sicherheitsfunktion beteiligten Ventile kann mittels der elektrischen Steuerung ein Prüfalgorithmus realisiert werden, um unter Einbeziehung der Druckschalter 1S1 und 1S2 sowie der Initiatoren 1S3 und 1S4 Fehler an den Ventilen zu erkennen.

Abbildung 7 beschreibt mit einem Ablaufplan beispielhaft einen Prüfalgorithmus, der abfragt, ob die Ventile 1V1, 1V2, 1V3 und 1V4 die Ruhestellung eingenommen haben. Wird die Abfrage der Druckschalter über einen längeren Zeitraum durchgeführt, lassen sich auch sicherheitsrelevante Leckagen der Ventile erkennen.

Hinweis:
Während der Prüfalgorithmus abläuft, darf es zu keiner Gefährdung des Bedienpersonals kommen. Zum Start des Funktionstests werden Druckschalter und Initiatoren auf korrekten Grundzustand abgefragt. Werden im Arbeitszyklus auch die Zustände abgefragt, die vom Prüfalgorithmus nicht erfasst werden, lässt sich zudem ein Versagen der Druckschalter bzw. Initiatoren erkennen, was im Rahmen der Kategorieanforderungen allerdings nicht erforderlich ist.

Durch die fehlerkennenden Maßnahmen wird nach DIN EN ISO 13849-1 für die relevanten Bauteile ein Diagnosedeckungsgrad (DC) beschrieben. Werden das Einnehmen der Ruhestellung und die Leckageprüfung zum Beispiel alle acht Stunden durchgeführt, so ergibt sich durch die indirekte Überwachung ein DC von 90 % für jedes Ventil.

4.5 Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien nach DIN EN ISO 13849-2 sowie die Anforderungen der Kategorie B sind für alle Bauteile eingehalten.

- Das Wegeventil 1V1 hat eine gesperrte Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.

- Die federrückgestellten Wegeventile 1V2, 1V3 und 1V4 haben in Ruhestellung ausreichend positive Überdeckung.

- Die sicherheitsgerichtete Schaltstellung der Ventile wird jeweils durch die Wegnahme der Ansteuerung erreicht.

- Ein stabiler Aufbau zur Betätigung der Initiatoren, die als Zylinder-, Positions- oder Näherungsschalter ausgeführt sein können, ist sichergestellt. Der Schaltpunkt und die Hysterese sind so gewählt, dass ein Verlassen der Endstellung des Zylinders erkannt wird.

- Der pneumatische Schaltpunkt der Druckschalter, der zum Umschalten des elektrischen Ausgangssignals führt, ist so gewählt, dass ein Druckabfall unterhalb des für die Anwendung vorgesehenen Betriebsdruckbereiches zum Signalwechsel führt. Über dieses Verhalten wird die sicherheitsgerichtete Schaltstellung der Ventile sowie eine Leckage erkannt.

- Die Verarbeitung der Signale von Druckschaltern und Initiatoren erfolgt z. B. in einer elektrischen Logik/SPS.

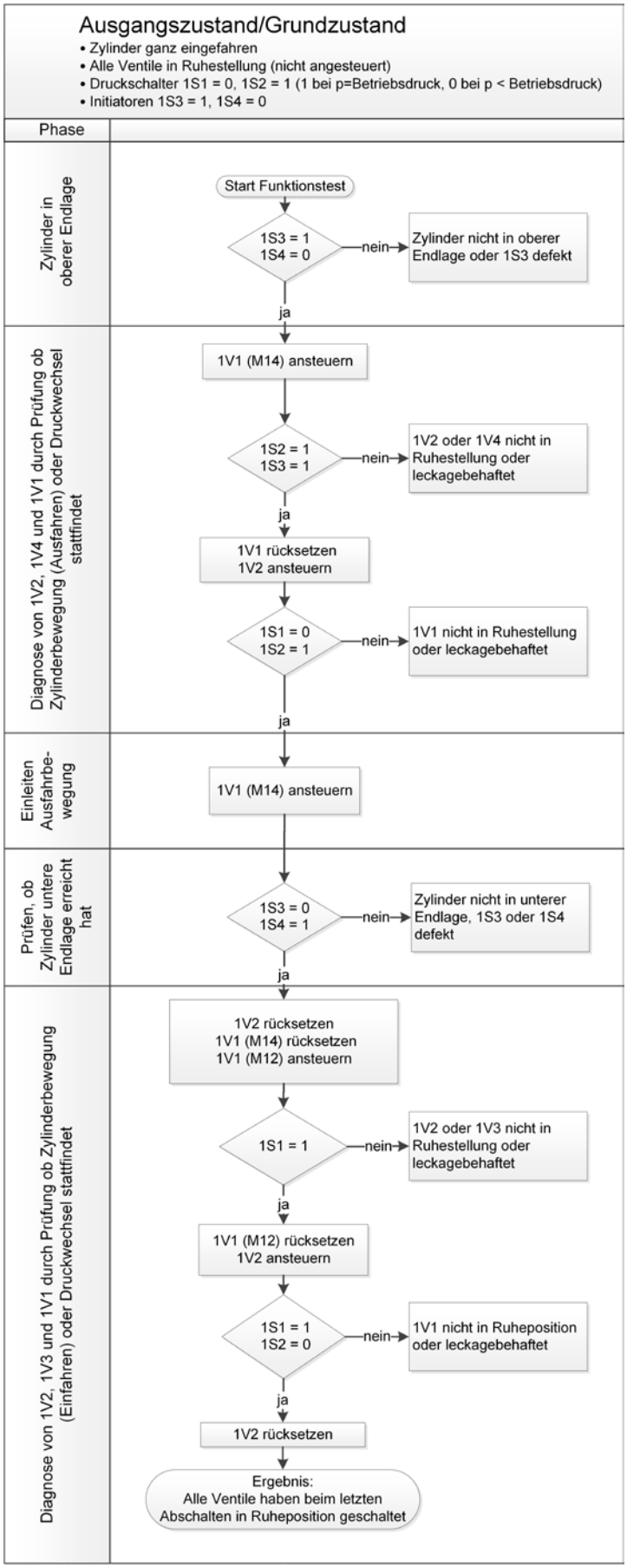

Abbildung 7: Ablaufplan zur Fehlererkennung an Ventilen für Beispiel SSC

Hinweis:
Bei hochgehaltenen Lasten sind unter Umständen besondere Anforderungen an das Leitungssystem zu beachten. Treten außerdem Gefährdungen (gefahrbringende Bewegungen), z. B. durch interne Leckage im Zylinder auf, so muss diese Gefährdung zusätzlich sicherheitstechnisch berücksichtigt werden. Das kann z. B. durch den Einsatz von Bremsen oder Halteeinrichtungen geschehen, siehe auch Fachbereich AKTUELL FBHM-050 zu fluidtechnischen Leistungselementen. Maschinenspezifische C-Normen enthalten teilweise konkrete Vorgaben.

4.6 Berechnung der Ausfallwahrscheinlichkeit

Mit üblichen $MTTF_D$- bzw. B_{10D}-Werten, den Diagnosedeckungsgraden aus Abschnitt 4.4 und der Einhaltung der grundlegenden und bewährten Sicherheitsprinzipien sowie ausreichenden Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF), entspricht die Schaltung einer Kategorie 3. Die nach DIN EN ISO 13849-1 erforderliche Bestimmung der Wahrscheinlichkeit gefahrbringender Ausfälle (PFH_D) kann mit der Software SISTEMA aus dem IFA erfolgen. Dazu sind weitere Angaben zur Schalthäufigkeit pro Jahr (n_{op}) der Ventile erforderlich.

Weiterführende Informationen

- VDMA-Einheitsblatt 24584: Sicherheitsfunktionen geregelter und nicht geregelter (fluid)mechanischer Systeme (2020-10). Beuth, Berlin 2020

- Sicherheitsfunktionen in pneumatischer Antriebstechnik. O+P Fluidtechnik (März 2017) Nr. 3, S. 24-27

- Fachbereich AKTUELL FB HM-050 „Fluidtechnische Leistungselemente – Fluidtechnische Leistungselemente - Hydraulische und pneumatische Motoren und Zylinder“, Ausgabe 10/2018, Fachbereich Holz und Metall FBHM, Mainz

- Apfeld R., Hauke M., Otto S.: Das SISTEMA Kochbuch 6 – Definition von Sicherheitsfunktionen – Was ist wichtig?, Version 1.1, Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2015

Autor: Dipl.-Ing. Jürgen Uppenkamp, Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin