

Das SISTEMA-Kochbuch 6

Definition von Sicherheitsfunktionen –
Was ist wichtig?

Version 1.1 (DE)



Verfasser: Ralf Apfeld, Michael Hauke, Stefan Otto
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstr. 111
53757 Sankt Augustin
Telefon: 02241/231-02
Telefax: 02241/231-2234
Internet: www.dguv.de/ifa

Herausgeber: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Glinkastr. 40
10117 Berlin
– Juni 2015 –

Inhaltsverzeichnis

Inhaltsverzeichnis	3
Einleitung	4
1 Risikominderung durch Sicherheitsfunktionen	5
2 Grundlegende Definition von Sicherheitsfunktionen	7
2.1 Grenzen der Sicherheitsfunktionen	7
2.2 Grundlegende Bestandteile von Sicherheitsfunktionen	8
2.3 Betriebsart	10
2.4 Der erforderliche Performance Level (PL _r)	10
2.5 Häufigkeit der Anforderung.....	10
2.6 Nachlauf	11
3 Von der Definition zur Realisierung der Sicherheitsfunktion	12
4 Besondere Aspekte	15
4.1 Ausfall der Energieversorgung und Verfügbarkeit bei schwerkraftbelasteten Achsen	15
4.2 Priorisierung von Sicherheitsfunktionen	15
4.3 Kombination von Sicherheitsfunktionen	16
5 Besondere Sicherheitsfunktionen	17
5.1 Betriebsartenwahl.....	17
5.2 Freigabefunktion.....	18
5.3 Bewegungsbegrenzung.....	18
6 Vollständige Definition von Sicherheitsfunktionen	20
7 Literatur	22

Einleitung

Unter dem Begriff der Sicherheitsfunktion versteht man nach DIN EN ISO 13849-1 [1] und DIN EN ISO 12100 [2] eine sicherheitsgerichtete Steuerungsfunktion einer Maschine, die ein von der Maschine ausgehendes Risiko auf ein akzeptables Maß reduziert. Die korrekte Definition der Sicherheitsfunktion ist daher von elementarer Bedeutung für die Maschinensicherheit. Leider kommt es auch nach fast zwei Jahrzehnten praktischer Anwendung von Sicherheitsfunktionen selbst in sicherheitsspezifischen Fachgrundnormen immer wieder zu unvollständigen, fehlerhaften oder missverständlichen Definitionen.

Dieses SISTEMA-Kochbuch benennt die wesentlichen Punkte, die bei der Definition von Sicherheitsfunktionen in der Praxis zu beachten sind und illustriert diese anhand eines fortlaufenden Beispiels (blau hervorgehoben). Zusammenfassende Leitfragen zwischen einzelnen Passagen (rot hervorgehoben) helfen bei der Detaillierung eigener Sicherheitsfunktionen. Liegt eine maschinenspezifische Produktnorm mit definierten Sicherheitsfunktionen vor, kann dieses Kochbuch als Ergänzung verwendet werden.

Damit erleichtert dieses Kochbuch die Kommunikation an der Schnittstelle zwischen Definition und Realisierung von Sicherheitsfunktionen. Es richtet sich zum einen an die Personen, die zur Risikominderung im Rahmen der Risikoanalyse einer Maschine Sicherheitsfunktionen definieren müssen. Zum anderen geht es auch auf die Sichtweise der Steuerungskonstruktion ein, indem alle relevanten Parameter erläutert werden.

1 Risikominderung durch Sicherheitsfunktionen

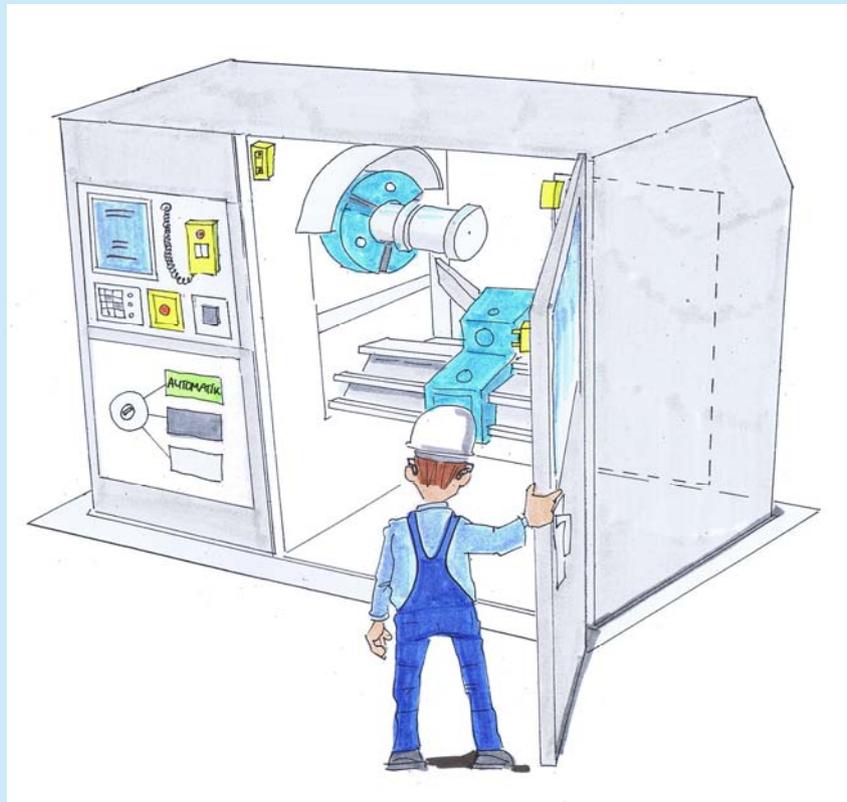
Sicherheitsfunktionen stellen einen wichtigen Bestandteil des Verfahrens zur Risikominderung dar, das in DIN EN ISO 12100 beschrieben ist. Entsprechend definiert die Norm die Sicherheitsfunktion als Funktion einer Maschine, deren Ausfall zur unmittelbaren Erhöhung des Risikos führen kann. Ob und in welchem Maß das Risiko an einer Maschine vermindert werden muss, ergibt sich aus der Risikobeurteilung. Hierbei wird das von einer Maschine in ihren verschiedenen Lebensphasen ausgehende Risiko analysiert und bewertet.

Die Risikominderung wird in der DIN EN ISO 12100 als dreistufiger Prozess beschrieben. Danach ist jedes im Prozess der Risikobeurteilung betrachtete Risiko zunächst durch eine inhärent sichere Konstruktion der Maschine zu minimieren. Nur wenn dies nicht möglich ist, sind technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen anzuwenden, zu denen trennende sowie nichttrennende Schutzeinrichtungen zählen.

Sollten trotz aller technischen Schutzmaßnahmen Restrisiken verbleiben, kann die Risikominderung im letzten, dritten Schritt nur noch durch Benutzerinformationen und organisatorische Maßnahmen erreicht werden.

Die Rolle einer Sicherheitsfunktion im Prozess der Risikominderung wird anhand des Beispiels einer Drehmaschine illustriert (siehe Abbildung 1 und Tabelle 1). In den weiteren Kapiteln wird die genannte Sicherheitsfunktion dann weiter detailliert.

Abbildung 1: Öffnen der Schutztür im Automatikbetrieb



Die Drehmaschine verfügt über eine vordere und eine hintere Schutztür mit Zugang zum Arbeitsraum. Die Rotation der Spindel mit dem Werkstück und die Achsbewegungen zum Verfahren des Werkzeugs stellen gefahrbringende Bewegungen dar. Die Türen verfügen über keine Zuhaltung, sodass ein Öffnen der Schutztüren auch im laufenden Betrieb möglich ist. Die Bearbeitung des Werkstücks ist nur im Automatikbetrieb und bei geschlossenen Türen zulässig.

Tabelle 1: Ausschnitt aus der Risikobeurteilung

Gefährdung	Inhärent sichere Konstruktion	Technische Schutzmaßnahmen	Benutzerinformation
Brand durch Entzündung des Kühlschmierstoffs	Verwendung nicht brennbarer Kühlschmierstoffe	nicht zutreffend	Die Verwendung brennbarer Kühlschmierstoffe ist nicht zulässig.
Quetschen/Scheren durch Achsbewegungen (Betriebsart „Automatik“)	nicht möglich	Sicherheitsfunktion: „Das Öffnen einer Schutztür führt zum Stillsetzen aller Maschinenbewegungen“	nicht zutreffend
Einrichten durch ungeschultes Personal (Betriebsart „Einrichtbetrieb“)	nicht möglich	nicht möglich	Zugriff auf Schlüssel des Betriebsartenwahlschalters nur für geschultes Personal

2 Grundlegende Definition von Sicherheitsfunktionen

2.1 Grenzen der Sicherheitsfunktionen

Am Anfang der Risikobeurteilung nach DIN EN ISO 12100 steht die Festlegung der Grenzen der Maschine. Analog zu diesem Vorgehen müssen auch die Grenzen der Sicherheitsfunktionen betrachtet werden:

- **Verwendungsgrenzen**

Für die Festlegung der Verwendungsgrenzen einer Sicherheitsfunktion sind unter anderem die Betriebsarten der Maschine zu betrachten. Die Tätigkeiten des Bedienpersonals unterscheiden sich in Bezug auf die Gefährdungsexposition in den verschiedenen Betriebsarten zum Teil erheblich. Während für den Automatikbetrieb der Gefährdungsbereich in vielen Fällen durch trennende Schutzeinrichtungen abgesichert ist, sind beim Einrichten einer Maschine oftmals Tätigkeiten in unmittelbarer Nähe des Gefährdungsbereichs erforderlich. So ergeben sich je nach Betriebsart unterschiedliche Anforderungen an das erforderliche Maß der Risikominderung, oder es müssen andere Risiken berücksichtigt werden. Entsprechend können in verschiedenen Betriebsarten unterschiedliche Sicherheitsfunktionen zur Anwendung kommen. Es ist sinnvoll, die Wahl der Betriebsart ebenfalls als eigene Sicherheitsfunktion zu betrachten (siehe Abschnitt 5.1).

- **Räumliche Grenzen**

Existieren an einer Maschine mehrere räumlich voneinander getrennte Gefahrstellen, so kann sich die Bedienperson zu jedem Zeitpunkt nur an einer Gefahrstelle aufhalten. In diesem Fall ist es empfehlenswert, für jede Gefahrstelle eine eigene Sicherheitsfunktion zu definieren. Müssen aus funktionalen Gründen mit Auslösung einer Sicherheitsfunktion dennoch mehrere Maschinenbewegungen stillgesetzt werden, ist es für die Definition der Sicherheitsfunktion trotzdem ausreichend, nur die Bewegungen zu berücksichtigen, von denen in der jeweiligen Situation oder am jeweiligen Standort tatsächlich eine Gefährdung ausgeht (siehe Kapitel 5.3 des BGIA-Reports 2/2008 „Funktionale Sicherheit von Maschinensteuerungen“ [3]).

Selbst bei Überlagerung mehrerer Gefahrstellen in einem Gefährdungsbereich können für die Gefährdungen durch einzelne Maschinenteile jeweils eigene Sicherheitsfunktionen definiert werden – auch wenn bei der Ausführung der Sicherheitsfunktionen teilweise identische Bauteile verwendet werden: Eine Beschreibung des hierzu notwendigen Verfahrens findet sich in dem Fachausschuss-Informationsblatt „Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen“ [4].

Anmerkung:

Die Notwendigkeit, Sicherheitsfunktionen weiter aufzuteilen, ergibt sich aus dem Einfluss der Bauteilanzahl auf deren Ausfallwahrscheinlichkeit (PFH_D) (siehe hierzu Kapitel 3).

Ähnliches wie für die gefahrbringenden Maschinenteile gilt für die betrachteten trennenden und nichttrennenden Schutzeinrichtungen, durch deren Betätigung die Sicherheitsfunktion ausgelöst werden soll: So betritt eine Person den Gefährdungsbereich nur durch eine von mehreren Schutztüren. Es ist daher in den beschriebenen Fällen völlig korrekt, je Sicherheitsfunktion nur eine Schutzeinrichtung zu betrachten. Für jede der anderen (identischen) Schutzeinrichtungen gibt es parallel wirksame eigene (identische) Sicherheitsfunktionen (siehe Abschnitt 5.3 in [3]).

Anmerkung:

Bei der Kaskadierung von Schutztüren kann es zu negativen Auswirkungen auf den Diagnosedeckungsgrad kommen. Dies ist bei der getrennten Betrachtung von Sicherheitsfunktionen für verschiedene Schutztüren zu berücksichtigen (siehe hierzu ISO/TR 24119 [5] sowie [6]).

• Zeitliche Grenzen

Bei der Beurteilung der Maschinengrenzen betrachtet DIN EN ISO 12100 zusätzlich die zeitlichen Grenzen der Maschine, die sich unter anderem auf die Gebrauchsdauer der Maschine und die Lebensdauer der Bauteile beziehen. Im Hinblick auf Sicherheitsfunktionen ist die vorgesehene Gebrauchsdauer der Maschine relevant, weil diese sich auf die spätere Berechnung der Ausfallwahrscheinlichkeit (PFH_b) der Sicherheitsfunktion auswirkt (siehe Kapitel 3). Eine begrenzte Lebensdauer der an der Sicherheitsfunktion beteiligten Bauteile wiederum kann deren vorzeitigen Austausch erforderlich machen. Im Kontext der DIN EN ISO 13849-1 wird eine Gebrauchsdauer von 20 Jahren angenommen.

2.2 Grundlegende Bestandteile von Sicherheitsfunktionen

Wie man bereits am genannten Beispiel „Das Öffnen einer Schutztür führt zum Stillsetzen aller Maschinenbewegungen“ erkennen kann, enthält die Formulierung einer Sicherheitsfunktion in der Regel drei Informationen:

1. auslösendes Ereignis
2. sicherheitsgerichtete Reaktion
3. gefahrbringendes Maschinenteil

Mit der im vorhergehenden Abschnitt vorgestellten Festlegung der Grenzen der Sicherheitsfunktion lassen sich diese drei Bestandteile nun näher spezifizieren:

• Auslösendes Ereignis

Das auslösende Ereignis ist in der Regel die Betätigung einer trennenden oder nichttrennenden Schutzeinrichtung, im Beispiel das Öffnen einer Schutztür. Dabei sollte – unter Beachtung der räumlichen Grenzen der Sicherheitsfunktion – allerdings nur die von der Bedienperson geöffnete Schutztür betrachtet werden.

Verfügt die betrachtete Maschine – wie im Beispiel – über mehrere Schutztüren, so kann bei identischem Gefährdungsbereich für jede Schutztür eine eigene Sicherheitsfunktion definiert werden. Bis auf die Schutztüren sind die Sicherheitsfunktionen identisch:

„Das Öffnen der (vorderen) Schutztür **ST1** führt zum Stillsetzen aller Maschinenbewegungen.“
„Das Öffnen der (hinteren) Schutztür **ST2** führt zum Stillsetzen aller Maschinenbewegungen.“

Im Folgenden wird nur die Sicherheitsfunktion für die vordere Schutztür weiter betrachtet.

• Sicherheitsgerichtete Reaktion

Die sicherheitsgerichtete Reaktion führt den sicheren Zustand herbei. Die elementarste sicherheitsgerichtete Reaktion ist das ungesteuerte Stillsetzen (STO – Sicher abgeschaltetes Moment) der gefahrbringenden Bewegung (siehe Abschnitt 3.1 in [7]). Dies wird in der Regel durch eine Unterbrechung der Energieversorgung erreicht. Der Vorteil des ungesteuerten Stillsetzens liegt darin, dass in den meisten Fällen durch Einhaltung des

Ruhestromprinzips auch bei Spannungsausfall automatisch der sichere Zustand herbeigeführt werden kann. Soll die gefahrbringende Bewegung nach Anforderung der Sicherheitsfunktion hingegen schnellstmöglich stillgesetzt werden und ist dies aufgrund des Nachlaufs des betrachteten Maschinenteils durch einen STO allein nicht möglich, so kann das gesteuerte Stillsetzen (SS1 – Sicherer Stopp 1) des Motors von Vorteil sein. Gesteuertes Stillsetzen mit folgendem sicheren Betriebshalt (SS2 – Sicherer Stopp 2) wird verwendet, wenn der Motor aufgrund der Anforderungen des Bearbeitungsprozesses nach Erreichen des Stillstands in Lageregelung gehalten werden muss.

In dem betrachteten Beispiel einer Drehmaschine wird davon ausgegangen, dass im Bearbeitungsprozess das Werkstück auch nach dem Stillsetzen in Lageregelung gehalten werden muss, um einen Verlust der Position zu vermeiden. Entsprechend muss – exemplarisch für das Öffnen der vorderen Schutztür – in der betrachteten Sicherheitsfunktion formuliert werden:

„Das Öffnen der Schutztür ST1 führt zum **gesteuerten Stillsetzen (SS2)** aller Maschinenbewegungen.“

Die oben beschriebenen sicherheitsgerichteten Reaktionen sind üblich für elektrische Antriebe. Sie lassen sich jedoch auch auf andere Technologien übertragen, beispielsweise auf fluidtechnische Zylinder.

Wurde durch eine sicherheitsgerichtete Reaktion ein sicherer Zustand hergestellt, so darf dieser Zustand in der Regel erst bei Rücknahme des auslösenden Ereignisses verlassen werden (Schutz vor unerwartetem Anlauf). Bei der betrachteten Sicherheitsfunktion etwa darf der stillgesetzte Antrieb bei noch geöffneter Schutztür nicht unerwartet anlaufen. In manchen Fällen kann darüber hinaus ein bewusstes Quittieren der Sicherheitsfunktion durch manuelles Rückstellen der Schutzeinrichtung notwendig sein, etwa wenn die Schutztür hintertretbar ist.

- **Gefahrbringendes Maschinenteil**

Da die Definition der Sicherheitsfunktion auf der Basis der Risikobeurteilung und der darin identifizierten Gefährdungen erfolgt, ist als gefahrbringend immer der Maschinenteil anzusehen, von dem in der jeweiligen Situation für das Bedienpersonal eine Gefährdung ausgeht, zum Beispiel durch Bewegung, Strahlung oder Hitze. Überlagern sich bei der betrachteten Maschine mehrere Gefährdungen in einem Gefährdungsbereich, kann es sinnvoll sein, diese Gefährdungen für jedes beteiligte Maschinenteil separat zu beurteilen.

In dem betrachteten Beispiel ist die folgende Aufteilung der Sicherheitsfunktionen hilfreich:

„Das Öffnen der Schutztür ST1 führt zum gesteuerten Stillsetzen (SS2) der **Achse A1**.“

„Das Öffnen der Schutztür ST1 führt zum gesteuerten Stillsetzen (SS2) der **Spindel S1**.“

Im Folgenden wird nur die Sicherheitsfunktion zum Stillsetzen der Achse A1 weiter betrachtet.

Mit der Festlegung des auslösenden Ereignisses, der sicherheitsgerichteten Reaktion und des gefahrbringenden Maschinenteils sind die drei wichtigsten Bestandteile der Sicherheitsfunktion festgehalten. Bei der Formulierung einer Sicherheitsfunktion ist es daher hilfreich, sich zunächst die folgenden drei Fragen zu stellen:

Durch welches Ereignis wird die Sicherheitsfunktion ausgelöst?

Was ist die sicherheitsgerichtete Reaktion?

Von welchem Maschinenteil geht die Gefährdung aus?

2.3 Betriebsart

Darüber hinaus müssen unter Beachtung der Verwendungsgrenzen (Abschnitt 2.1) die Betriebsarten festgehalten werden, in der die Sicherheitsfunktion verfügbar sein soll:

In welcher Betriebsart soll die Sicherheitsfunktion aktiv sein?

Das Stillsetzen einer gefahrbringenden Bewegung bei Betätigung einer Schutzeinrichtung ist eine für den Automatikbetrieb typische Sicherheitsfunktion. Im Einrichtbetrieb, in dem die Achse auch bei geöffneter Schutztür verfahren werden soll, ist diese Sicherheitsfunktion hingegen nicht sinnvoll.

„**Automatikbetrieb:** Das Öffnen der Schutztür ST1 führt zum gesteuerten Stillsetzen (SS2) der Achse A1.“

2.4 Der erforderliche Performance Level (PL_r)

Im Rahmen der Risikobeurteilung ist eine Einschätzung vorzunehmen, wie hoch das mit der jeweils betrachteten Gefährdung zusammenhängende Risiko ist. Soll das Risiko durch eine Sicherheitsfunktion gemindert werden, schlägt die DIN EN ISO 13849-1 dazu die Anwendung des Risikografen vor. Über die Einschätzung der zu erwartenden Verletzungsschwere, der Häufigkeit bzw. Dauer der Gefährdungsexposition sowie der Möglichkeit zur Gefährdungsvermeidung oder Schadensbegrenzung führt der Risikograf unmittelbar zu einer Abschätzung des erforderlichen Performance Levels PL_r der Sicherheitsfunktion.

Mit welchem Performance Level PL_r soll die Sicherheitsfunktion realisiert werden?

Für die oben genannte Sicherheitsfunktion ergibt die Risikobeurteilung laut Produktnorm den erforderlichen Performance Level PL_r = c.

2.5 Häufigkeit der Anforderung

Die Anforderung einer Sicherheitsfunktion erfolgt durch Eintritt des auslösenden Ereignisses (siehe Abschnitt 2.2) und führt bei korrekter Ausführung der Sicherheitsfunktion zur sicherheitsgerichteten Reaktion. Von der Aktivierung einer Sicherheitsfunktion spricht man hingegen, wenn die Sicherheitsfunktion – etwa durch Anwahl einer Betriebsart – generell verfügbar gemacht wird.

Sicherheitsfunktionen werden durch die sicherheitsbezogenen Teile der Steuerung (SRP/CS) ausgeführt (siehe auch Kapitel 3). Sofern hierbei verschleißbehaftete Bauteile verwendet werden – etwa Positionsschalter, Relais, Schütze, Ventile, fließt in deren Lebens-

dauer unmittelbar die Art, Dauer und Häufigkeit ihrer Verwendung ein. Über die Ausfallwahrscheinlichkeit eines Bauteils hängt auch der erreichte Performance Level der Sicherheitsfunktion direkt mit diesen Parametern zusammen. Ein weiterer Fall, für den die Anforderungsrate relevant ist, ist die Realisierung von Sicherheitsfunktionen durch Kategorie-2-Architekturen. Für die Anwendung des vereinfachten Verfahrens zur Abschätzung eines Performance Levels nach DIN EN ISO 13849-1 kann für Kategorie 2 eine gegenüber der Anforderungsrate mindestens hundertmal höhere Testrate erforderlich sein. Zur Ermittlung der notwendigen Testrate muss die Anforderungsrate daher bekannt sein. Eine zur sicheren Seite hin vorgenommene Einschätzung der Anforderungsrate ist selbst dann erforderlich, wenn diese nicht genau bekannt ist.

Der Schutz vor unerwartetem Anlauf als Bestandteil von Sicherheitsfunktionen ist nicht nur als Folge des Stillsetzens, sondern auch bei bereits erfolgtem Stillstand der gefahrbringenden Maschinenbewegungen relevant (siehe Abschnitt 2.2 „Gefahrbringendes Maschinenteil“). Eine Anforderung der Sicherheitsfunktion liegt in der Regel auch dann vor, wenn eine Schutzeinrichtung bei ruhenden Maschinenbewegungen betätigt wird, beispielsweise dann, wenn im Automatikbetrieb die Schutztür einer Maschine zum Werkstückwechsel geöffnet werden muss. Für die Anforderungsrate bedeutet dies, dass auch die Anforderung bei Stillstand der gefahrbringenden Maschinenbewegungen berücksichtigt werden muss. Die ausgelöste Steuerungskette ist in beiden Fällen identisch.

Wie häufig ist mit der Anforderung der Sicherheitsfunktion zu rechnen?

„Automatikbetrieb: Das Öffnen der Schutztür ST1 führt zum gesteuerten Stillsetzen (SS2) der Achse A1. **Im Mittel erfolgt eine Anforderung 6 Mal pro Stunde.**“

Die **Aktivierung** der Sicherheitsfunktion erfolgt durch Anwahl der Betriebsart „Automatikbetrieb“. Die **Anforderung** der Sicherheitsfunktion erfolgt, wenn die Schutztür geöffnet wird.

2.6 Nachlauf

Für jede sicherheitsgerichtete Reaktion gelten bestimmte zeitliche Vorgaben, innerhalb derer der sichere Zustand herbeigeführt sein muss, bevor eine Person die Gefahrenstelle erreichen kann. Dies gilt insbesondere dann, wenn die Absicherung durch eine berührungslos wirkende Schutzeinrichtung (z. B. ein Lichtgitter) erfolgt. Der Nachlauf des gesamten Systems, also die Reaktionszeit der Schutzeinrichtung plus die Anhaltezeit des gefahrbringenden Maschinenteils, steht dabei in wechselseitiger Abhängigkeit mit dem Sicherheitsabstand zum Gefährdungsbereich (siehe [8]).

Anmerkung:

Bei Ausfall der Energieversorgung (siehe auch Abschnitt 4.1) oder Fehler eines Bauteils kann es unter Umständen zu einem erhöhten Nachlauf kommen (siehe Abschnitt 6.4 in [7]).

In welcher Zeit nach Anforderung der Sicherheitsfunktion muss der sichere Zustand des Maschinenteils erreicht sein?

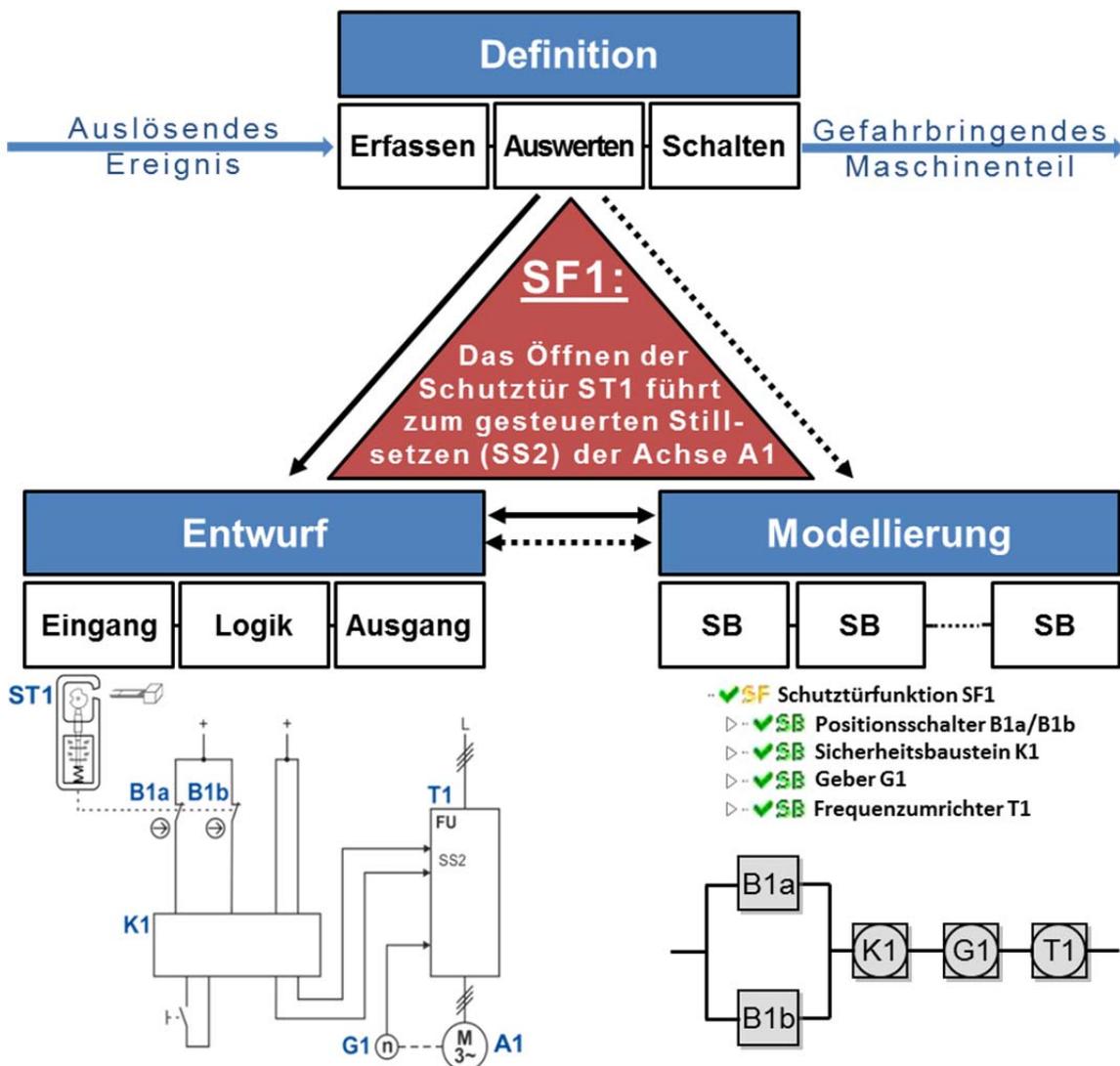
„Automatikbetrieb: Das Öffnen der Schutztür ST1 führt zum gesteuerten Stillsetzen (SS2) der Achse A1 **innerhalb von maximal 800 ms**. Im Mittel erfolgt eine Anforderung 6 Mal pro Stunde.“

3 Von der Definition zur Realisierung der Sicherheitsfunktion

Ausgeführt wird eine Sicherheitsfunktion durch die Steuerung. Den entsprechenden sicherheitsbezogenen Teilen der Steuerung (SRP/CS) ist die DIN EN ISO 13849: „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ [1] gewidmet. Mit ihrer Revision im Jahr 2006 wurde die Betrachtungsweise der Sicherheitsfunktionen um die Berechnung der Wahrscheinlichkeit ihres gefährlichen Ausfalls (PFH_D) ergänzt. Diese basiert u. a. auf den Ausfallwerten der an ihrer Ausführung beteiligten Bauteile. Die ungünstige Definition einer Sicherheitsfunktion kann – falls die Definition etwa zu viele Bauteile umfasst – nun schnell dazu führen, dass der erforderliche Performance Level als Maß für ihre Gesamtausfallwahrscheinlichkeit nicht erreicht wird. Ob die Umsetzung der Sicherheitsfunktion durch die SRP/CS dem erforderlichen Performance Level genügt, wird unter anderem durch eine Abschätzung der PFH_D – beispielsweise mithilfe von SISTEMA [9] – ermittelt.

Im Folgenden soll für Sicherheitsfunktionen der Zusammenhang von formaler Definition, steuerungstechnischem Entwurf und Modellierung in SISTEMA näher erläutert werden, siehe Abbildung 2.

Abbildung 2: Von der Definition zur Realisierung



- **Definition**

Gemäß der in Abschnitt 2.2 beschriebenen grundlegenden Bestandteile einer Sicherheitsfunktion kann diese funktional in drei Teilfunktionen gegliedert werden: das Erfassen des auslösenden Ereignisses, das Auswerten des erfassten Signals und das Schalten des gefahrbringenden Maschinenteils in den sicheren Zustand als sicherheitsgerichtete Reaktion.

- **Entwurf**

Beim Entwurf der sicherheitsbezogenen Teile der Steuerung (SRP/CS) – etwa mithilfe eines Prinzipschaltbilds – werden den drei Teilfunktionen entsprechende Bauteile zugeordnet, die durch Schnittstellen miteinander verbunden sind. Der Eingang ist für das Erfassen des auslösenden Ereignisses zuständig. Im Beispiel bildet der Positionsschalter B1 den Eingang der Sicherheitsfunktion, der das auslösende Ereignis – das Öffnen der Schutztür – detektiert. Die Auswertung der Eingangssignale erfolgt durch die Logik, an dieser Stelle realisiert durch das Sicherheitsschaltgerät K1. Die Logik verknüpft den Eingang mit dem Ausgang der Sicherheitsfunktion. Dort wird durch „Schalten“ der Ausgänge der Leistungssteuerungselemente die eigentliche sicherheitsgerichtete Reaktion ausgeführt, im Beispiel durch Auslösen der Teil-Sicherheitsfunktion SS2 im Frequenzumrichter T1. Dabei wird zusätzlich der Geber G1 zur sicheren Überwachung der Achsbewegung benötigt.

Anmerkung:

Oft wird anstelle der Gruppe Eingang – Logik – Ausgang auch von Sensor – Logik – Aktor gesprochen. Dabei kann zumindest die Verwendung des Begriffs Aktor irreführend sein, da hierunter auch der stillzusetzende Motor (oder Zylinder) der betrachteten Maschine verstanden werden kann. Der Motor selbst wird in der Regel jedoch nicht als Bestandteil der SRP/CS betrachtet, soweit ohne Antriebsenergie keine gefahrbringende Bewegung mehr möglich ist. Eine Ausnahme bilden schwerkraftbelastete Achsen, bei denen je nach realisierter Sicherheitsfunktion und Betriebsart auch der zur Achse zugehörige Motor – und gegebenenfalls vorhandene Halteeinrichtungen – in die Betrachtung einbezogen werden müssen (zum Thema schwerkraftbelastete Vertikalachsen siehe Abschnitt 4.1).

- **Modellierung**

Für die Abschätzung der PFH_D einer Sicherheitsfunktion werden die sicherheitsbezogenen Teile der Steuerung in SISTEMA auf eine Kette von Subsystemen (SB1, SB2, ...) abgebildet – logisch darstellbar in einem sicherheitsbezogenen Blockdiagramm (der gefährliche Ausfall jedes Subsystems führt zum Ausfall der Sicherheitsfunktion). Die Anzahl der Subsysteme ist nicht von vornherein festgelegt, sondern von der verwendeten Hardware und der gewählten Architektur abhängig. Dabei ist es sowohl möglich, mit einem einzelnen Subsystem die komplette Sicherheitsfunktion zu realisieren (z. B. parametrierbarer Laserscanner mit integriertem Abschaltrelais), als auch eine beliebig lange Kette von Subsystemen dafür einzusetzen. Im betrachteten Beispiel bildet der Positionsschalter B1 als Eingang der Sicherheitsfunktion mit seinen zwei zwangsöffnenden Kontakten B1a und B1b ein (zweikanaliges) Subsystem. Für die (einkanalige) Mechanik des Positionsschalters kann ein für den Anwendungsfall begründeter Fehlerausschluss formuliert werden, sodass sie im sicherheitsbezogenen Blockdiagramm unberücksichtigt bleibt. Neben dem Sicherheitsschaltgerät – der Logik der Sicherheitsfunktion – bilden sowohl der Frequenzumrichter T1 (mit integrierten Stoppfunktionen) als auch der Geber G1 – beides Bestandteile des Ausgangs der Sicherheitsfunktion – eigene gekapselte Subsysteme. Zur weiteren Vertiefung sei an dieser Stelle auf das SISTEMA-Kochbuch 1 [10] verwiesen.

- **Zeitliche Abfolge der Realisierung**

Die Modellierung einer Sicherheitsfunktion in SISTEMA erfolgt in der Praxis meist nach dem Entwurf der sicherheitsrelevanten Teile der Steuerung. In Abbildung 2 ist diese zeitliche Abfolge durch durchgezogene Pfeile dargestellt.

Oft ist es notwendig, Entwurf und Modellierung iterativ mehrmals zu durchlaufen, bis eine geeignete steuerungstechnische Realisierung gefunden ist. Dabei kann es erforderlich sein, eine Teilfunktion in mehrere Subsysteme aufzuteilen oder mehrere Subsysteme in einem Subsystem zusammenzufassen, etwa wenn ein Frequenzumrichter mit integrierten Sicherheitsfunktionen die Subsysteme Logik und Ausgang umfasst.

Anmerkung:

Alternativ können die Subsysteme auch direkt über die aus der Definition der Sicherheitsfunktion abgeleiteten Teilfunktionen ermittelt und erst im Anschluss die entsprechenden sicherheitsbezogenen Teile der Steuerung realisiert werden. In Abbildung 2 ist diese Reihenfolge durch unterbrochene Pfeile dargestellt, da dieses Vorgehen in der Praxis nur selten angewendet wird. Hierbei ist eine Aufteilung der Sicherheitsfunktion in Teilfunktionen nach Vorbild der formalen Definition sinnvoll (Erfassen – Auswerten – Schalten). Nach Abbildung jeder Teilfunktion auf ein Subsystem wird für jedes Subsystem separat nach einer geeigneten steuerungstechnischen Realisierung gesucht.

4 Besondere Aspekte

4.1 Ausfall der Energieversorgung und Verfügbarkeit bei schwerkraftbelasteten Achsen

Ein Energieausfall ist generell nicht als Fehler, sondern als vorhersehbarer Betriebszustand zu betrachten, bei dessen Eintreten die Überführung in einen sicheren Zustand gewährleistet sein muss. In den meisten Fällen stellt der energielose Zustand schon einen sicheren Zustand dar, wenn es zu keiner gefahrbringenden Bewegung kommen kann.

Schwerkraftbelastete Maschinenteile können auch im energielosen Zustand durch unbeabsichtigtes Herabsinken Gefahren auslösen. Lässt die bestimmungsgemäße Verwendung einer Maschine den Aufenthalt einer Person unter einer schwerkraftbelasteten Achse zu, ergeben sich für die Ausfallsicherheit der Maschine erhöhte Anforderungen. Zur Vertiefung sei an dieser Stelle auf das Fachbereichs-Informationsblatt „Schwerkraftbelastete Achsen – Vertikalachsen“ [11] verwiesen.

Manchmal kann es sinnvoll sein, Sicherheitsfunktionen bei vorhandener Energieversorgung (elektrisch, pneumatisch, hydraulisch, ...) von Sicherheitsfunktionen für den Ausfall der Energieversorgung zu trennen. Hier kann nach erkanntem Energieausfall ein sicherer Zustand u. U. auf anderem Wege erreicht werden (z. B. Stillsetzen einer Werkstückspindel bei Ausfall der hydraulischen Energie zur Werkstückspannung, siehe SF3 in [12]). Dabei spielt wieder die Reaktionszeit eine wichtige Rolle.

Welche sicherheitsgerichtete Reaktion ist bei Energieausfall erforderlich?

Die im Beispiel genannte Sicherheitsfunktion an der Drehmaschine ist bei vorhandener Energie aktiv. Eine eigene Sicherheitsfunktion sorgt bei Energieverlust für das Stillsetzen der gefahrbringenden Bewegungen. Die Umsetzung kann z. B. mithilfe von pneumatisch gelüfteten Bremsen erfolgen, die bei Ausfall der Energieversorgung einfallen (siehe Beispiel 14 in [7]).

4.2 Priorisierung von Sicherheitsfunktionen

Für den Fall, dass zwei konkurrierende Sicherheitsfunktionen parallel ausgelöst werden können, ist es notwendig, Prioritäten vorzusehen, um zu klären, welche der beiden Sicherheitsfunktionen auszuführen ist. Diese Fragestellung kann auch dann wichtig sein, wenn noch vor Ablauf der sicherheitsgerichteten Reaktion einer Sicherheitsfunktion eine zweite Sicherheitsfunktion ausgelöst werden sollte. Ob die Auslösung ignoriert und die in Ausführung befindliche Reaktion zu Ende gebracht oder von der zweiten Sicherheitsfunktion unterbrochen wird, muss durch eine solche Prioritätenverteilung festgelegt werden.

In den meisten Fällen wird es sinnvoll sein, Sicherheitsfunktionen in Abhängigkeit von ihren sicherheitsgerichteten Reaktionen zu priorisieren, d. h. die Sicherheitsfunktion vorrangig zu behandeln, die das Risiko einer Verletzung am stärksten vermindert. Dabei ist auch hier zu beachten, dass Sicherheitsfunktionen bei Wegfall der Energieversorgung oder Auftreten eines Fehlers ausfallen können.

Ist die Sicherheitsfunktion vor- oder nachrangig gegenüber anderen Sicherheitsfunktionen?

Bei der Drehmaschine ist die Sicherheitsfunktion zur Überwachung der Schutztür der Sicherheitsfunktion zum Stillsetzen des Antriebs bei Betätigung eines Not-Halt-Gerätes untergeordnet, siehe Tabelle 2.

Tabelle 2: Automatikbetrieb

Priorität	Sicherheitsfunktion (Kurzbezeichnung)	Sicherheitsgerichtete Reaktion
1	Not-Halt	STO
2	Schutztürüberwachung	SS2

4.3 Kombination von Sicherheitsfunktionen

Sicherheitsfunktionen können aufeinander aufbauen. So ist beispielsweise bei den meisten Maschinen eine Freigabefunktion (auch: Zustimmungsfunktion) bei offener Schutzeinrichtung nur unter der Voraussetzung einer sicher begrenzten Verfahrgeschwindigkeit der Motorachsen (SLS – Safely Limited Speed) erlaubt (siehe auch Abschnitte 5.2 und 5.3). Wenn also sichergestellt ist, dass eine Sicherheitsfunktion (hier: SLS) bei Anforderung einer zweiten (hier: Freigabefunktion) bereits aktiv ist, kann die erste als Grundlage der Risikoeinschätzung für die zweite berücksichtigt werden (siehe BGIA-Report 2/2008, Anhang A, Beispiel 4 [3]).

Anmerkung:

Dies spiegelt sich auch in der Tatsache wider, dass es sich beim Prozess der Risikominderung nach DIN EN ISO 12100 um einen iterativen Prozess handelt: Nach jeder Definition einer Sicherheitsfunktion wird erneut überprüft, ob das Risiko für die betrachtete Gefährdung ausreichend vermindert wurde, oder ob weitere Maßnahmen auf der Basis der bereits definierten notwendig sind. Der hier beschriebene Einfluss einer Sicherheitsfunktion auf die notwendige Risikominderung durch eine zweite ist daher auch nur in einer Richtung erlaubt. Eine wechselseitige Reduzierung des PL_r darf nicht erfolgen, da sonst die insgesamt erreichte Risikominderung unzureichend wäre.

Setzt der Einsatz der Sicherheitsfunktion weitere aktive Sicherheitsfunktionen voraus?

5 Besondere Sicherheitsfunktionen

In diesem Kapitel werden anhand des Beispiels der Drehmaschine drei weitere Sicherheitsfunktionen erläutert.

Abbildung 3: Arbeit bei geöffneter Schutztür im Einrichtbetrieb

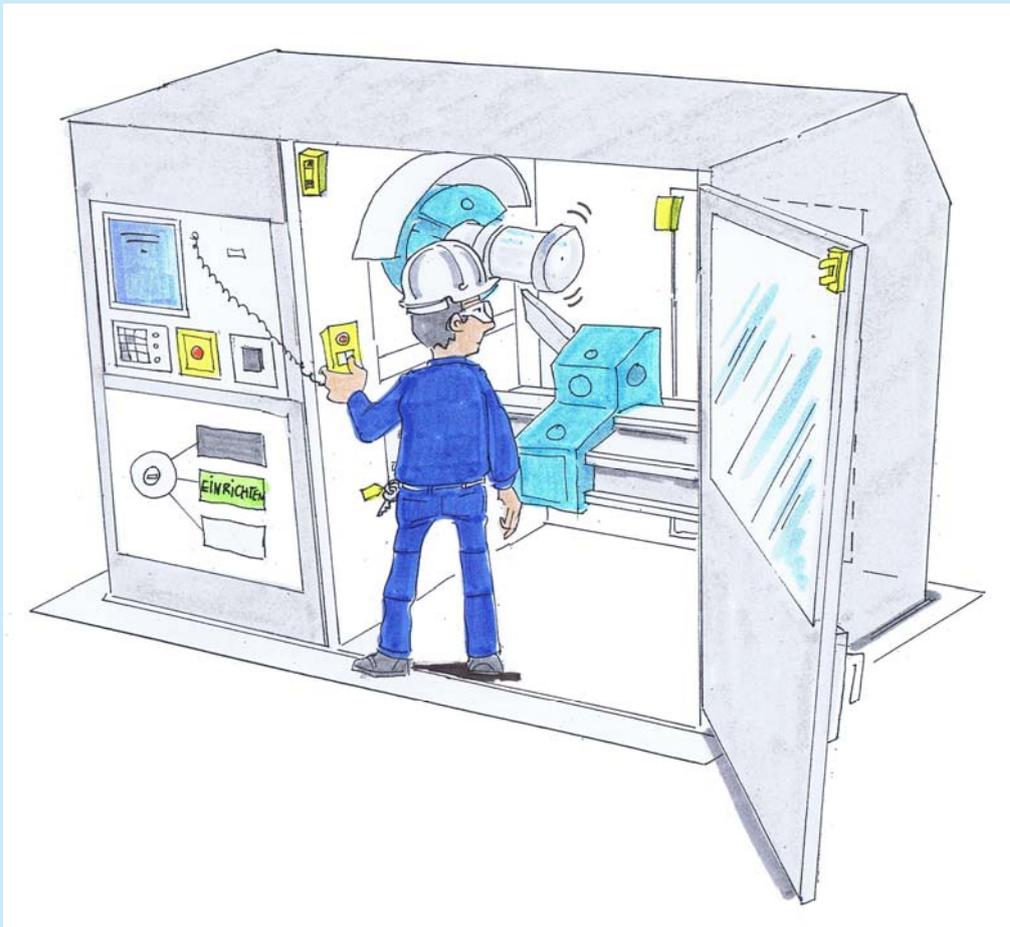


Abbildung 3 zeigt die Drehmaschine aus Abbildung 1 im Einrichtbetrieb. Eine zur Änderung der Betriebsart (über den abschließbaren Betriebsartenwahlschalter) autorisierte Fachkraft steuert bei geöffneter Schutztür mit einer Freigabeeinrichtung eine Achse der Maschine.

5.1 Betriebsartenwahl

Durch Wechsel der Betriebsart können Sicherheitsfunktionen (z. B. Schutztürüberwachung) deaktiviert und andere (z. B. Freigabefunktion) aktiviert werden. Aufgrund ihres Einflusses auf die Risikominderung durch das Bereitstellen von Sicherheitsfunktionen muss daher sichergestellt werden, dass immer nur genau eine Betriebsart angewählt ist. Ein Wechsel in eine andere Betriebsart darf nur willentlich und nicht durch Versagen der Steuerung erfolgen. Es stellt sich die Frage, ob der steuerungstechnische Anteil der Betriebsartenwahl (z. B. Betriebsartenwahlschalter) zu jeder an der Maschine realisierten Sicherheitsfunktion gehört, oder ob die Betriebsartenwahl als eigenständige Sicherheitsfunktion betrachtet werden kann.

Analog zur Vorgehensweise bei überlagerten Gefährdungen (siehe Abschnitt 2.1 und [4]), bei denen einzelne Gefährdungen separiert werden, wird die Betriebsartenwahl als eigene Sicherheitsfunktion angesehen. Damit wird auch vermieden, dass die Bauteile zur Betriebsartenwahl in jeder einzelnen Sicherheitsfunktion zusätzlich die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH_D) erhöhen. Im Regelfall lässt sich die Sicherheitsfunktion Betriebsartenwahl wie folgt definieren:

„Je nach Stellung des Betriebsartenwahlschalters werden die für die angewählte Betriebsart erforderlichen Sicherheitsfunktionen aktiviert.“

5.2 Freigabefunktion

In manchen Betriebsarten kann das Arbeiten bei geöffneter Schutzeinrichtung erforderlich sein, etwa im Störbeseitigungs- oder im Einrichtbetrieb. Hier kommen meist spezielle Steuerungsarten zur Anwendung, die gewährleisten, dass Maschinenbewegungen in jedem Moment nur auf konkrete Veranlassung der Bedienperson hin ausgeführt werden können. Dies kann etwa mithilfe eines Tippschalters und/oder einer Freigabeeinrichtung geschehen.

Der Betrieb mit Freigabeeinrichtung erfolgt mit zwei- oder dreistufigen Freigabeschaltern, wobei sowohl das Loslassen als auch das Durchdrücken (letzteres nur möglich bei dreistufigen Freigabeschaltern) ein Stillsetzen des betroffenen Maschinenteils bewirken muss. Entsprechend ist hier auch die zugehörige Sicherheitsfunktion „Freigabefunktion“ zu definieren (siehe auch Abschnitt 6, Tabelle 2):

„Einrichtbetrieb: Loslassen des zweistufigen Freigabeschalters führt zu einem gesteuerten Stillsetzen (SS2) der Vorschubachse.“

Die Sicherheitsfunktion Tippbetrieb ist analog zu definieren. Auch hier muss das Loslassen des Tippschalters zum Stillsetzen der Maschine führen.

Anmerkung:

In der Regel kann das Risiko bei geöffneter trennender Schutzeinrichtung durch Freigabefunktion oder Tippbetrieb allein nicht ausreichend gemindert werden. Erst durch die gleichzeitige Ausführung einer Sicherheitsfunktion zur Bewegungsbegrenzung kann die erforderliche Risikominderung erreicht werden (siehe Abschnitte 4.3 und 5.3).

5.3 Bewegungsbegrenzung

Für elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl werden in der Norm Teilsicherheitsfunktionen zur Bewegungsbegrenzung definiert, siehe Kapitel 3 in [7]. Dazu zählt die bereits erwähnte Sicherheitsfunktion SLS (Sicher begrenzte Geschwindigkeit), die dort folgendermaßen definiert ist: „Die SLS-Funktion verhindert, dass der Motor die festgelegte Begrenzung der Geschwindigkeit überschreitet.“ Während diese Definition der Sicherheitsfunktion aus Perspektive der Risikominderung nach DIN EN ISO 12100 bereits ausreichend erscheint, sind für die steuerungstechnische Realisierung und Bestimmung des erreichten Performance Levels nach DIN EN ISO 13849 weitere Festlegungen nötig. Hier ist im Sinne von Kapitel 2.2 die Benennung des auslösenden Ereignisses (Überschreiten der spezifizierten Maximalgeschwindigkeit) und der sicherheitsgerichteten Reaktion (Stillsetzung der überwachten Achse z. B. durch SS1) notwendig – mit Bezug auf die konkrete gefahrbringende Bewegung bzw. das gefahrbringende Maschinenteil. Weitere Begrenzungsfunktionen können sich z. B. auf Position, Beschleunigung und Drehmoment beziehen.

Ergänzend zu der in Abschnitt 5.2 genannten Sicherheitsfunktion kann folgende Sicherheitsfunktion zur Umsetzung der sicher begrenzten Geschwindigkeit (SLS) formuliert werden (siehe auch Abschnitt 6, Tabelle 2):

„Einrichtbetrieb: Das Überschreiten der Grenzgeschwindigkeit der Achse A1 führt zu einem gesteuerten Stillsetzen (SS1) der Achse A1.“

Nicht immer einfach abzuschätzen ist bei diesen Begrenzungsfunktionen die Häufigkeit der Anforderung der sicherheitsgerichteten Reaktion (siehe Kapitel 2.5). Letztlich hängt von der Zuverlässigkeit der für die Regelung der Geschwindigkeit zuständigen funktionalen (nicht sicherheitsgerichteten) Steuerung ab, wie häufig die Überwachungsfunktion auf eine Grenzwertüberschreitung reagieren muss. Bei der Abschätzung der Anforderungshäufigkeit hilft aber die Überlegung, dass eine Maschine, die ständig (z. B. mehrmals am Tag) wegen einer ausgelösten Begrenzungsfunktion stoppt und dann quittiert und wieder gestartet werden muss, in der Regel in der Anwendung nicht akzeptiert wird.

„Einrichtbetrieb: Das Überschreiten der Grenzgeschwindigkeit der Achse A1 führt zu einem gesteuerten Stillsetzen (SS1) der Achse A1. **Im Mittel erfolgt eine Anforderung 1 Mal pro Tag (Abschätzung zur sicheren Seite).**“

6 Vollständige Definition von Sicherheitsfunktionen

Auf der Basis der genannten Leitfragen wird es möglich sein, die eigene Sicherheitsfunktion nach Tabelle 3 vollständig zu beschreiben:

Tabelle 3: Tabellarische Definition einer Sicherheitsfunktion

Kurzbezeichnung	Wie lautet die Kurzbezeichnung der Sicherheitsfunktion?
Auslösendes Ereignis	Durch welches Ereignis wird die Sicherheitsfunktion ausgelöst?
Sicherheitsgerichtete Reaktion	Was ist die sicherheitsgerichtete Reaktion?
Gefahrbringendes Maschinenteil	Von welchem Maschinenteil geht die Gefährdung aus?
Betriebsart	In welcher Betriebsart soll die Sicherheitsfunktion aktiv sein?
PL_r	Mit welchem Performance Level PL _r soll die Sicherheitsfunktion realisiert werden?
Häufigkeit der Anforderung	Wie häufig ist mit einer Anforderung der Sicherheitsfunktion zu rechnen?
Nachlauf	In welcher Zeit nach Anforderung der Sicherheitsfunktion soll der sichere Zustand erreicht sein?
Verhalten bei Energieausfall	Welche sicherheitsgerichtete Reaktion ist bei Energieausfall erforderlich?
Priorität	Ist die Sicherheitsfunktion vor- oder nachrangig gegenüber anderen Sicherheitsfunktionen?
Ergänzende Sicherheitsfunktion	Setzt der Einsatz der Sicherheitsfunktion weitere aktive Sicherheitsfunktionen voraus?
Zusätzliche Parameter	Welche zusätzlichen Parameter müssen berücksichtigt werden?

In Tabelle 4 sind die in diesem SISTEMA-Kochbuch genannten Beispiele vollständig aufgelistet und – wo nötig – beispielhaft ergänzt.

Tabelle 4: Beispiele für die vollständige Definition von Sicherheitsfunktionen

	SF1	SF2	SF3
Kurzbezeichnung	Schutztürfunktion	Freigabefunktion	Sicher begrenzte Geschwindigkeit (SLS)
Auslösendes Ereignis	Öffnen der vorderen Schutztür	Loslassen des zweistufigen Freigabetasters	Überschreiten der Grenzgeschwindigkeit
Sicherheitsgerichtete Reaktion	Gesteuertes Stillsetzen (SS2)	Gesteuertes Stillsetzen (SS2)	Gesteuertes Stillsetzen (SS1)
Gefahrbringendes Maschinenteil	Vorschubachse	Vorschubachse	Vorschubachse
Betriebsart	Automatikbetrieb	Einrichtbetrieb	Einrichtbetrieb
PL _r	c	d	c
Häufigkeit der Anforderung	6 x pro Stunde	10 x pro Tag	1 x pro Tag
Reaktionszeit	800 ms	200 ms	200 ms
Verhalten bei Energieausfall	Ungesteuertes Stillsetzen (STO) der Vorschubachse	Ungesteuertes Stillsetzen (STO) der Vorschubachse	Ungesteuertes Stillsetzen (STO) der Vorschubachse
Priorität	2 (der „Not-Halt-Funktion“ untergeordnet)	3 (der „Sicher begrenzten Geschwindigkeit (SLS)“ untergeordnet)	2 (der „Freigabefunktion“ übergeordnet)
Ergänzende SF	-	Sicher begrenzte Geschwindigkeit (SLS)	-
Zusätzliche Parameter	-	-	-
Bemerkung	-	-	-

7 Literatur

- [1] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (12.08). Beuth, Berlin 2008
- [2] DIN EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (03.11). Beuth, Berlin 2011
- [3] Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Borowski, T.; Büllsbach, K.-H.; Dorra, M.; Foermer-Schaefer, H.-G.; Grigulewitsch, W.; Heimann, K.D.; Köhler, B.; Krauß, M.; Kühlem, W.; Lohmaier, O.; Meffert, K.; Pilger, J.; Reuß, G.; Schuster, U.; Zilligen, H.: Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849. BGIA-Report 2/2008. Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2008. www.dguv.de/webcode/d18588
- [4] Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachausschuss-Informationsblatt Nr. 047. Ausgabe 05/2010. Hrsg.: Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau, Mainz 2010. www.bghm.de, Webcode 626
- [5] ISO/TR 24119: Safety of machinery — Evaluation of fault masking in serial connections of guard interlocking devices with potential-free contacts (voraussichtlich 2015)
- [6] Apfeld, R.: Überwachung von Schutztüren an Maschinen – Hilfestellung durch die neue DIN EN ISO 14119. Technische Sicherheit 4 (2014) Nr. 4, S. 45-49
www.dguv.de/webcode/m621988
- [7] Apfeld, R.; Zilligen, H.; Köhler, B.: Sichere Antriebssteuerungen mit Frequenzumrichtern. IFA Report 7/2013. Hrsg.: Deutsche Gesetzliche Unfallversicherung, Berlin 2013.
www.dguv.de/webcode/d639540
- [8] DIN EN ISO 13855: Sicherheit von Maschinen — Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (10.10). Beuth, Berlin 2010
- [9] SISTEMA: Software-Assistent zur Bewertung von sicherheitsbezogenen Maschinensteuerungen nach DIN EN ISO 13849. www.dguv.de/webcode/d11223
- [10] Apfeld, R.; Hauke, M.; Schaefer, M.; Rempel, P.; Ostermann, B.: Das SISTEMA-Kochbuch 1 – Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2010. www.dguv.de/webcode/d109240
- [11] Schwerkraftbelastete Achsen – Vertikalachsen. Fachbereich-Informationsblatt Nr. 005. Ausgabe 09/2012. Hrsg.: Fachbereich Holz und Metall der DGUV, Mainz 2012. www.bghm.de, Webcode 626
- [12] Drehmaschinen – „Werkstückspannen“ – Beispielrechnung einer Sicherheitsfunktion nach DIN EN ISO 13849. DGUV Information FB-HM-039. Ausgabe 10/2014. Hrsg.: Fachbereich Holz und Metall der DGUV, Mainz 2014. www.bghm.de, Webcode 626