ZVEI:
Die Elektroindustrie

Whitepaper

Fehlertoleranz in der Maschinensicherheit

Teil 1 – Grundlagen, Version 1.0

Fachverband Automation

Fehlertoleranz in der Maschinensicherheit

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Automation
Lyoner Straße 9
60528 Frankfurt

Verantwortlich:
Dr. Markus Winzenick
Telefon: +49 69 6302-426
E-Mail: winzenick@zvei.org

www.zvei.org

Juli 2019

Kurzfassung

Fehlertoleranz in der Maschinensicherheit

In der Technik bedeutet Fehlertoleranz die Eigenschaft eines technischen Systems, seine Funktionsweise auch dann aufrechtzuerhalten, wenn Ausfälle und Fehlerzustände auftreten. Fehlertoleranz erhöht die Verfügbarkeit eines Systems. In diesem Dokument wird ein Weg beschrieben, fehlertolerante Sicherheitsfunktionen zu implementieren, die einen weiteren Betrieb einer Maschine oder Anlage bei bestimmten Fehlerszenarien erlauben, ohne den Personenschutz zu vernachlässigen.

Es wird der Begriff „degradierter Betrieb" als Synonym für den Betrieb mit Sicherheitsfunktionen im degradierten Zustand eingeführt. Im degradierten Betrieb wird eine Maschine nach Erkennung eines Fehlers in einer Sicherheitsfunktion weiterbetrieben. Es werden drei verschiedene Arten des degradierten Betriebs definiert und die jeweiligen Grenzen und Einschränkungen beschrieben. Es wird ferner der Begriff „Entscheider" eingeführt, der in der Maschine bei Erkennung des Fehlers den Übergang in den Betrieb im degradierten Zustand steuert.

Schlussendlich zeigt sich, dass es Möglichkeiten gibt, die Verfügbarkeit der Maschine im Fehlerfall aufrechtzuerhalten, um zum Beispiel den laufenden Bearbeitungsschritt geordnet zu beenden, ohne die Produktion unterbrechen zu müssen.

Redaktion:

Frank Bauder	Leuze electronic
Thomas Bömer	Institut für Arbeitsschutz (IFA) der DGUV
Helmut Börjes	Wago Kontakttechnik
Dr. Tilmann Bork	Festo
Carsten Gregorius	Phoenix Contact
Joachim Greis	Beckhoff Automation
Richard Holz	Euchner
Florian Rotzinger	Pilz
Frank Schmidt	K.A. Schmersal
Thomas Schulz	BGHM – Berufsgenossenschaft Holz und Metall
Rolf Schumacher	Sick
Klaus Stark	Pilz
Manfred Strobel	ifm electronic

Inhalt

Einleitung

1.1 Motivation

Die Arbeitssicherheit im industriellen Umfeld hat seit jeher einen hohen Stellenwert. Unternehmen haben erkannt, dass der Schutz der Arbeitnehmer bei Tätigkeiten an Maschinen und Anlagen aus unterschiedlichen Gründen erforderlich ist. Motivierend wirken hier auf der einen Seite gesetzliche Regelungen und Vorschriften, deren Nichteinhaltung mit entsprechenden Sanktionen belegt ist. Andererseits wird die an Maschinen und Anlagen eingesetzte Sicherheitstechnik immer wieder als Ursache von ungewollten Maschinenstillständen gesehen, was zu Manipulationsanreizen führen kann.

Bislang beruhen Überwachungen an Schutzeinrichtungen für Maschinen und Anlagen im industriellen Umfeld auf dem Dogma des schnellstmöglichen Stillsetzens im Fehlerfall. Das heißt, für jede interne Überwachungsfunktion ist ein Erwartungswert definiert und Abweichungen von diesem Erwartungswert führen zu einer Abschaltreaktion. Steigende Produktivitätsanforderungen insbesondere unter den Aspekten von Industrie 4.0 verlangen für die Zukunft erweiterte sicherheitstechnische Konzepte.

Es ist Ziel dieses Dokuments, Alternativen zur sofortigen Abschaltung im Falle einer Fehlererkennung zu zeigen. Es wird der Rahmen definiert, in dem Maschinen nach Erkennen von Fehlern in Sicherheitsfunktionen weiterbetrieben werden können, ohne dass Personen inakzeptablen Risiken ausgesetzt werden.

1.2 Anwendungsbereich

Der Anhang I der Maschinenrichtlinie 2006/42/EG legt für den Europäischen Wirtschaftsraum die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen an Konstruktion und Bau von Maschinen verpflichtend fest. Danach muss ein Hersteller einer Maschine dafür sorgen, dass eine Risikobeurteilung vorgenommen wird, um die für diese Maschine geltenden Sicherheits- und Gesundheitsschutzanforderungen zu ermitteln. Die Maschine muss dann unter Berücksichtigung der Ergebnisse der Risikobeurteilung konstruiert und gebaut werden.

Die Norm ISO 12100 stellt Leitsätze zur Risikobeurteilung und Risikominderung auf, um Konstrukteure dabei zu unterstützen, sichere Maschinen zu konstruieren. Das vorliegende Dokument beschreibt ergänzend zu dieser Norm einen Ansatz für die Konstruktion sicherer Maschinen, der gleichzeitig, wie oben erwähnt, neuen technologischen Erfordernissen gerecht wird.

Der Anwendungsbereich des Dokuments beschränkt sich auf den Betrieb von Maschinen/Anlagen unter Fehlerbedingungen in ihren Sicherheitsfunktionen. Es richtet sich an Maschinenbauer und Systemintegratoren, die bei der Entwicklung der Maschine Sicherheitsfunktionen planen und unter Verwendung von Subsystemen umsetzen. Die Empfehlungen aus diesem Dokument sind bei der Umsetzung der Sicherheitsfunktionen gemäß den Normen ISO 13849-1 und IEC 62061 gleichermaßen anwendbar.

Im Fokus dieses Dokuments sind ausschließlich die im Maschinen- und Anlagenbau für höhere Sicherheitsanforderungen üblichen Systeme, in denen die Ausführung von Sicherheitsfunktionen auch im Fehlerfall aufgrund ihrer ursprünglich zweikanaligen Struktur weiterhin möglich ist.

Nicht betrachtet von der hier beschriebenen Anwendung sind:

- Einkanalige Sicherheitssysteme, ein sicherer Betrieb im Fehlerfall ist grundsätzlich ausgeschlossen
- Systeme mit mehr als zwei Kanälen (bekannt aus Prozessindustrie und Avionik), unabhängig von ihrer Anwendungsmöglichkeit

1.3 Normensituation

Dieses Dokument betrachtet den möglichen Betrieb von Maschinen/Anlagen im degradierten Zustand und beschreibt zusätzliche Anforderungen, die bei der Konzeption und Integration zu beachten sind. Diese Funktionalität und die Anforderungen daraus werden derzeit in keiner Norm beschrieben.

Der Betrieb im degradierten Zustand stellt eine Ergänzung zum Prinzip der Energietrennung dar. Er bezeichnet eine zusätzliche, zeitbegrenzte Funktionalität innerhalb einer Sicherheitsfunktion. Das Konzept des Betriebs im degradierten Zustand steht nicht im Widerspruch zu den in der Maschinenrichtlinie genannten Schutzzielen und den in Normen wie ISO 13849 sowie IEC 62061 und IEC 61508 genannten Anforderungen.

Dem Maschinenbauer/Integrator werden sachdienliche Hinweise zu den Überlegungen an die Hand gegeben, eine Maschine/Anlage im Fehlerfall im degradierten Betriebszustand zeitbegrenzt sicher zu betreiben. Der degradierte Betrieb muss in der technischen Dokumentation beschrieben und begründet sein. Der Betrieb einer Maschine/Anlage im degradieren Zustand darf nur in definierten Fehlerzuständen möglich sein. Dieser Betrieb ist nicht als reguläre Betriebsart gedacht, um als Ersatz für erforderliche Maßnahmen zur Risikominderung zu dienen. Dieses Dokument deckt alle Technologien ab, die in den oben angeführten Normen beschrieben werden.

2 Normativer Verweis

Die nachfolgend genannten Dokumente sind für die Anwendung dieses Dokuments hilfreich.

ISO 12100:2010 — Safety of machinery – General principles for design – Risk assessment and risk reduction

ISO 13849-1:2015 — Safety of machinery – Safety-related parts of control systems
Part 1: General principles for design

ISO 13849-2:2012 — Safety of machinery – Safety-related parts of control systems
Part 2: Validation

IEC 62061:2005 + AMD1:2012 + AMD2:2015
Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

IEC 60073:2002 — Basic and safety principles for man-machine interface, marking and identification
Coding principles for indicators and actuators

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe:

3.1.1 Sicherheit

Freiheit von unvertretbarem Risiko eines von den betrachteten sicherheitsrelvanten Systemen ausgehenden und außerhalb derselben auftretenden Schadens
[IEV 351-57-05]

3.1.2 Sicherer Zustand

Zustand einer Funktionseinheit, in dem die Sicherheit erreicht ist
[IEC 61508-4:2010, modifiziert]

3.1.3 Funktionseinheit

Einheit aus Hardware oder Software oder beidem, die zur Durchführung einer angegebenen Aufgabe geeignet ist
[ISO/IEC 2382-1, 01-01-40]

3.1.4 Fehler

Zustand einer Funktionseinheit, charakterisiert durch die Unfähigkeit, eine geforderte Funktion auszuführen, ausgenommen der Unfähigkeit während vorbeugender Wartung oder anderer geplanter Handlungen oder aufgrund des Fehlens externer Mittel
[ISO 13849-1:2015, 3.1.3, modifiziert]

3.1.5 Fehlertoleranz

Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen
[IEC 61508-4:2010, 3.6.3]

3.1.6 Ausfall

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion zu erfüllen
Anmerkung 1 zum Begriff: Nach einem Ausfall hat die Einheit einen Fehler.
Anmerkung 2 zum Begriff: Der „Ausfall" ist ein Ereignis, im Unterschied zum „Fehler", dieser ist ein Zustand.
[ISO 13849-1:2015, 3.1.4, modifiziert]

3.1.7 Gefahrbringender Ausfall

Ausfall, der das Potenzial hat, eine Funktionseinheit in einen gefährlichen Zustand oder eine Fehlfunktion zu bringen
[ISO 13849-1:2015, 3.1.5, modifiziert]

3.1.8 Sicherheitsgerichtete Ausfallreaktion

Herbeiführen eines sicheren Zustands, nachdem ein gefahrbringender Ausfall entdeckt wurde
[EN 50129:2003, 3.1.33, modifiziert]

3.2 Abkürzungen

Abkürzung	Beschreibung
CCF	**Common Cause Failure** Ausfall infolge gemeinsamer Ursache
MRL	Richtlinie 2006/42/EG des europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen
PDS/SR	**Power Drive Systems (Safety Related)** Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl, die Sicherheitsteilfunktionen zur Verfügung stellen
SF	**Safety Function** Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos führen kann
SRP/CS	**Safety-Related Part of a Control System** Sicherheitsbezogenes Teil einer Steuerung
STO	**Safe Torque Off** Sicher abgeschaltetes Drehmoment

Quelle: ZVEI

4 Fehlertoleranz in Systemen

4.1 Sicherheitsrelevante Steuerungen

4.1.1 Allgemeines

Sicherheitsrelevante Steuerungen für die Fabrikautomatisierung werden derzeit so ausgelegt, dass bei Erkennung von Fehlern in sicherheitsrelevanten Komponenten der sichere Zustand eingenommen wird. Dieser wird in nahezu allen Situationen durch Abschalten der Energie erreicht. Für eine einzelne Maschine bedeutet dies in der Regel einen Maschinenstopp. In komplexen Fertigungssystemen könnte demnach nicht nur eine einzelne Maschine gestoppt werden, sondern der gesamte Fertigungsablauf. Programmierbare sicherheitsbezogene Systeme verfügen zum Teil über Funktionen, über die je nach Fehlerart nicht das komplette System in den sicheren, das heißt energielosen, Zustand wechselt, sondern nur einzelne Baugruppen abgeschaltet oder passiviert werden (Gruppenabschaltung). Die Auswahl dieser Baugruppen ist applikationsabhängig und muss bei der Projektierung individuell festgelegt werden. Nach wie vor erfolgt jedoch eine Abschaltung bestimmter Maschinen oder Maschinenfunktionen bei Erkennen eines Fehlers bei solchen Steuerungsarchitekturen, die eine Fehlererkennung erfordern.

Bisher war dies wenig problematisch, da der Automatisierungsgrad von Maschinen/Anlagen zwar stieg, eine Vernetzung unterschiedlicher Produktionsanlagen aber nur sukzessive erfolgte. Die Dynamik der Vernetzung durch das Internet nahm in den vergangenen Jahren jedoch zu und bildet künftig die Basis für eine „Industrie 4.0“. Außerdem werden einzelne Maschinen und komplette Fertigungsstraßen nicht nur innerhalb einer Fertigungsstätte, sondern auch zwischen weit auseinanderliegenden Fertigungsstandorten miteinander verbunden. Die wachsende Anzahl dieser Verbindungen, die Komplexität weit verteilter Netzwerke und die Integration unterschiedlicher Technologien erhöhen die Flexibilität. Gleichzeitig ist aber das Stillsetzen eines komplexen Fertigungssystems aufgrund eines beliebigen Fehlers in einer Sicherheitsfunktion an einer vollkommen anderen Produktionsstelle nicht tolerierbar. Dies bedeutet, dass neue Verfahren und Methoden erforderlich sind, die es ermöglichen, einen sicheren Betrieb zu gewährleisten, obwohl ein Fehler in einer Sicherheitsfunktion erkannt wurde. Da dies nicht bei jedem Fehler akzeptiert werden kann, ist eine Einschränkung auf bestimmte tolerierbare Fehler notwendig. Diese sogenannten „fehlertoleranten Systeme“ müssen eindeutig spezifiziert werden. Hierbei stellen sich folgende Fragen:

- Können gefährliche Fehler überhaupt toleriert werden?
- Wie und/oder wie lange kann eine Maschine/Anlage betrieben werden, obwohl ein Fehler erkannt wurde?
- Kann eine Maschine/Anlage, in der ein Fehler erkannt wurde, uneingeschränkt weiter betrieben werden oder müssen Prozessabläufe geändert werden, zum Beispiel Betriebsart, Produktionsgeschwindigkeit usw.?

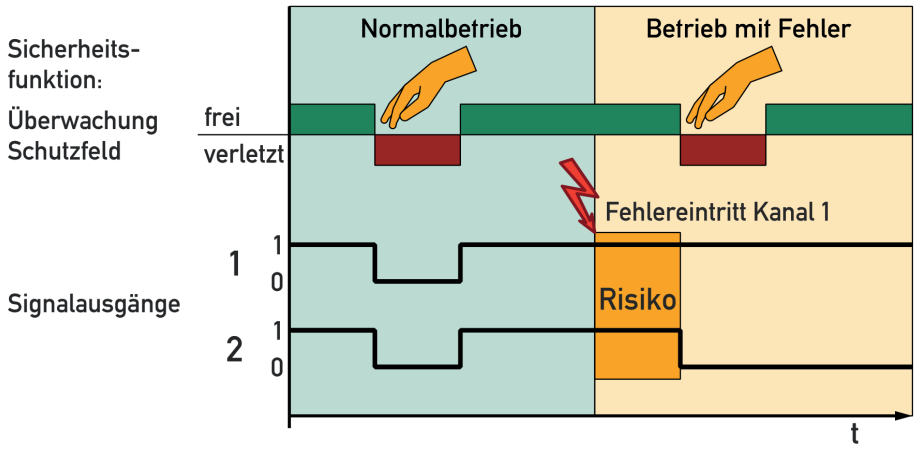
Zu diesen Fragen kann es keine generellen Antworten geben, da diese je nach Anwendungsfall unterschiedlich sein werden.

4.1.2 Fehlertoleranz

Betrachtet man die Norm ISO 13849-1, so ist bei ihrer Anwendung bereits eine nicht näher definierte „Fehlertoleranz“ enthalten. In der Kategorie 2 werden eine Fehlerdetektion und somit auch eine Fehlerreaktion erst bei Durchführung der Testfunktion verlangt. Dies bedeutet, dass in einer Sicherheitsfunktion ein Fehler zwischen zwei Testzeitpunkten existieren kann. Die Zeit zwischen zwei Tests ist demnach die Zeit, in der eine Funktionseinheit mit einem Fehler weiterbetrieben werden kann.

Bei der Anwendung der Kategorie 3 und der Kategorie 4 wird eine Fehlererkennung und die daraus folgende Fehlerreaktion spätestens bei Anfordern der Sicherheitsfunktion verlangt (s. Abb. 1). Erfolgt über einen längeren Zeitraum keine Anforderung, so kann eine Funktionseinheit unter Umständen mit einem Fehler betrieben werden – der Fehler wird für eine unbestimmte Zeit toleriert (s. Abb. 1).

Abb. 1: Betrachtung eines redundanten Systems gemäß ISO 13849-1



Quelle: ZVEI

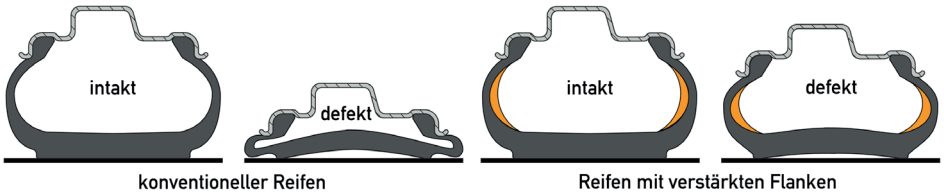
Diese Art der Tolerierung von Fehlern ist keinesfalls mit einem fehlertoleranten System gleichzusetzen. Der Unterschied ist folgender: Fehlertolerante Systeme ermöglichen einen Weiterbetrieb, obwohl bereits ein potenziell gefahrbringender Ausfall erkannt wurde. Dies ist bei den Kategorien 3 und 4 bisher nicht üblich.

In einigen Sicherheitssystemen und deren Anwendungen können über spezielle Prüf- und Testroutinen Fehler bereits erkannt werden, ohne dass eine Sicherheitsfunktion angefordert wird. Es erfolgt sehr schnell eine Fehlerreaktion, obwohl dies unter Berücksichtigung der oben genannten Kategorien nicht gefordert wird. Es ist in der jeweils betrachteten Anwendung zu entscheiden, ob eine schnelle Fehlerreaktion wirklich benötigt wird.

Bei fehlertoleranten Systemen ist neben der Fehlererkennung zusätzlich eine Fehlerbewertung erforderlich. Damit kann entschieden werden, ob der erkannte Fehler toleriert werden kann oder so schwerwiegend ist, dass ein sofortiges Stillsetzen unabdingbar ist. Eine Fehlerbewertung ist in der Fabrikautomatisierung in derzeit implementierten Sicherheitssystemen nicht üblich. Eine mögliche Anwendung und Akzeptanz in der Praxis erfordert eine eindeutige Bewertung von Fehlern und deren möglichen Auswirkungen. Hierbei muss der Aspekt der Sicherheit immer im Vordergrund stehen, um nicht durch eine leichtfertige Anwendung das Prinzip der Fehlertolerierung infrage zu stellen. Ohne eine Fehlerbewertung ist Fehlertoleranz nicht möglich.

Als ein Beispiel aus dem Alltag kennen wir heute Autoreifen mit sogenannten Notlaufeigenschaften, die es ermöglichen, unter bestimmten Betriebsbedingungen (maximale Geschwindigkeit und Strecke) den Weg bis zur nächsten Werkstatt zurückzulegen (s. Abb. 2).

Abb. 2: Beispiel Kfz-Reifen (Run-Flat-Technologie)



Quelle: ZVEI

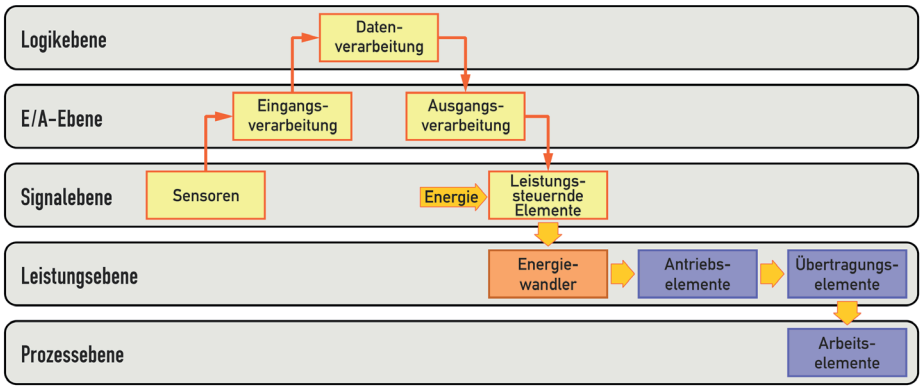
Das vorliegende Dokument beschreibt eine Adaption dieses Prinzips auf Anwendungen in der funktionalen Sicherheit an Maschinen/Anlagen.

4.2 Gefahrbringende Ausfälle

4.2.1 Prinzip der Energietrennung

Eine Maschine/Anlage besteht aus mehreren Komponenten, die zusammenwirken und die Funktion einer Maschine/Anlage sicherstellen (s. Abb. 3).

Abb. 3: Schematische Darstellung einer Maschinensteuerung



Quelle: ZVEI

Sicherheitsbezogene Systeme müssen mindestens in Übereinstimmung mit den zutreffenden Normen gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert sein sowie die grundlegenden Sicherheitsprinzipien für die bestimmte Anwendung nutzen, um Folgendem standzuhalten:

- Den zu erwartenden Betriebsbeanspruchungen
- Dem Einfluss des zu bearbeitenden Materials
- Anderen relevanten äußeren Einflüssen

Ein besonders zu beachtendes grundlegendes Sicherheitsprinzip stellt die Anwendung des Prinzips der Energietrennung dar. Der maßgebliche Vorgang zum Stillsetzen oder Verlangsamen eines Mechanismus wird demnach durch Wegnahme oder Verringerung der Energie ausgeführt. Zur Unterbrechung der Energiezufuhr kann es ausreichend sein, die für die Erzeugung eines Drehmoments oder einer Kraft erforderliche Energiezufuhr zu unterbrechen. Das kann durch Auskuppeln, Trennen, Ausschalten oder durch elektronische Hilfsmittel (z. B. ein Antriebssystem (PDS/SR)) erreicht werden, ohne dabei eine elektrische Trennung auszuführen.

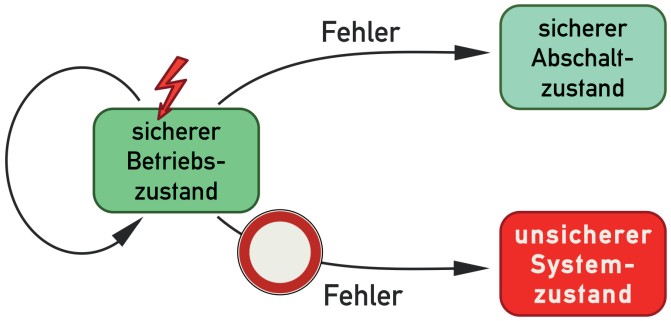
Das Prinzip der Energietrennung darf nicht angewendet werden, wenn durch einen Energieverlust eine Gefährdung entstehen würde, zum Beispiel Freigabe eines Werkzeugs durch den Verlust der Spannkraft. Wenn zu erwarten ist, dass die Wiederherstellung oder Inbetriebnahme der Energieversorgung nach einer Unterbrechung zu unerwarteten Bewegungen führt, müssen die daraus resultierenden Risiken entsprechend berücksichtigt werden. Erfolgt ein Überführen in den sicheren Abschaltzustand aufgrund eines gefahrbringenden Ausfalls, muss ein automatischer Wiederanlauf des Mechanismus solange verhindert werden, bis der Fehler behoben ist.

4.2.2 Sicherheitsgerichtete Ausfallreaktion

Die sicherheitsgerichtete Ausfallreaktion führt bei Erkennen eines Fehlers einen sicheren Zustand herbei. Dieser wird erreicht durch das Erkennen aller gefahrbringenden Fehlfunktionen und einer nachfolgenden sicherheitsgerichteten Ausfallreaktion (s. Abb. 4). Dabei gelten folgende Aussagen:

- Keine Fehlersicherheit ohne Übergang in einen anderen sicheren Betriebszustand
- Keine Fehlersicherheit ohne Existenz eines sicheren Abschaltzustands

Abb. 4: System mit sicherer Überwachungsfunktion



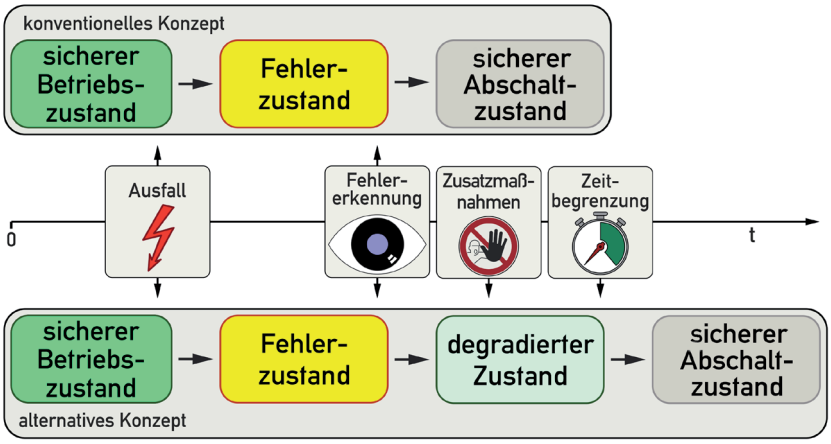
Quelle: ZVEI

Die elementarste sicherheitsgerichtete Ausfallreaktion ist das ungesteuerte Stillsetzen der gefahrbringenden Bewegung. 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 Abschaltzustand herbeigeführt werden kann. Diese Ausfallreaktion wird auch als sicher abgeschaltetes Drehmoment (STO) bezeichnet.

4.2.3 Betrieb im degradierten Zustand

Der Betrieb im degradierten Zustand stellt eine Ergänzung zum Prinzip der Energietrennung dar (s. Abb. 5). Er bezeichnet eine zusätzliche, zeitbegrenzte Funktionalität innerhalb einer Sicherheitsfunktion.

Abb. 5: Vergleich der Konzepte



Quelle: ZVEI

Ziel ist es, bei zu definierenden Fehlern (z. B. Zustand eines Kanals außerhalb der zulässigen Toleranz) die Maschinenfunktionen mit ausreichender Sicherheit in definierten Grenzen zuzulassen, damit beispielsweise ein Zyklus beendet und gleichzeitig ein sicherer Betrieb aufrechterhalten bzw. ein sicherer Abschaltzustand erreicht wird.

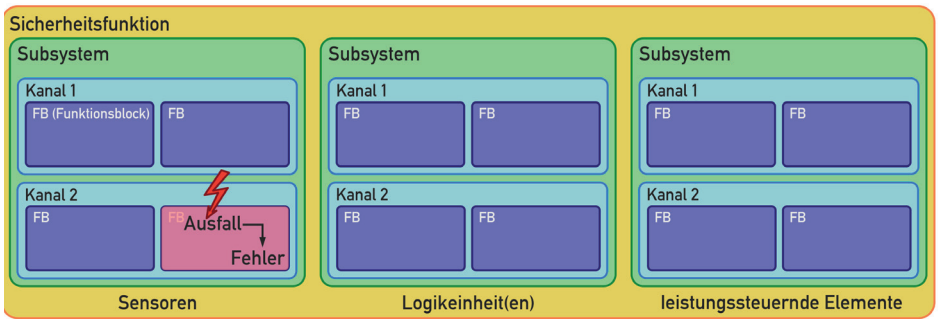
5 Risikominderung durch Sicherheitsfunktionen

5.1 Zustandsübergänge

5.1.1 Zufällige Hardwareausfälle

Ausfälle in Funktionseinheiten sind entweder zufällig (in Hardware) oder systematisch (in Hardware oder Software). Ein zufälliger Ausfall kann aus Alterungsprozessen von Werkstoffen und Materialien resultieren, der zu einer Verschlechterung der Eigenschaften eines Bauteils führt. Es gibt mehrere solcher Mechanismen, sie treten mit unterschiedlicher Häufigkeit in den verschiedenen Bauteilen auf. In ihrer Folge kommt es, aufgrund von Fertigungstoleranzen und abhängig von der jeweiligen Betriebsbelastung, nach unterschiedlichen Betriebszeiten zu Bauteilausfällen. Ausfälle von Funktionseinheiten, die viele Bauteile enthalten, treten in vorhersagbaren Wahrscheinlichkeiten, aber zu unbestimmten (d. h. zufälligen) Zeiten auf. In einigen Fällen kann ein Ausfall auch durch externe Ereignisse, wie zum Beispiel Blitz oder elektrostatische Entladung, verursacht werden. Nach einem Ausfall hat die Einheit einen Fehler (s. Abb. 6).

Abb. 6: Ausfall im Gegensatz zu Fehler



Quelle: ZVEI

Gefahrbringende Ausfälle vermindern die Wahrscheinlichkeit, dass eine Sicherheitsfunktion bei Anforderung ordnungsgemäß ausgeführt wird. Daraus entsteht möglicherweise ein gefährlicher Zustand. Ob dieses Potenzial bemerkt werden kann oder nicht, hängt von den Diagnosemöglichkeiten des Systems ab.

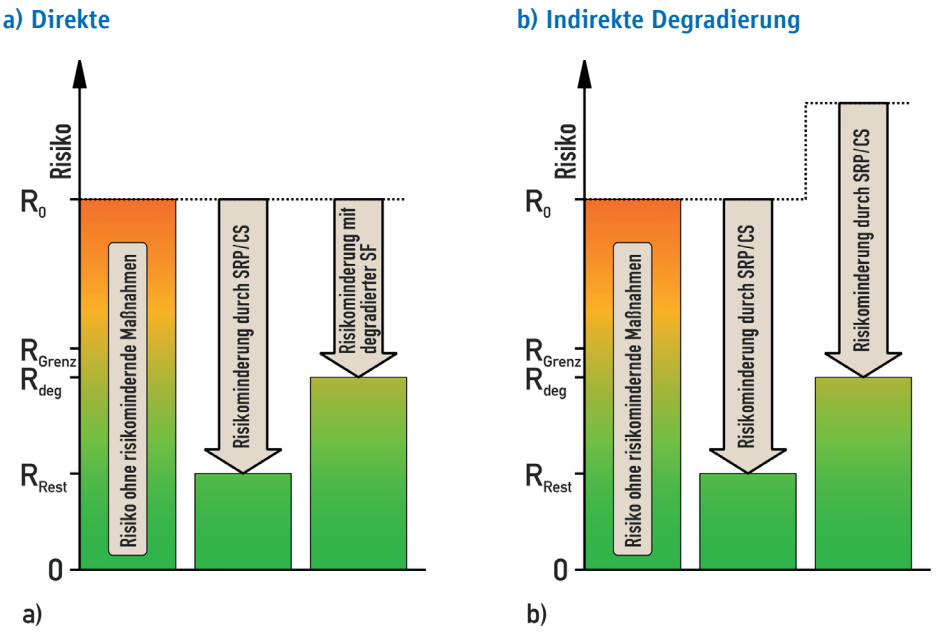
5.1.2 Degradierung von Sicherheitsfunktionen

Unter dem Begriff „Degradierung" wird in diesem Dokument das temporäre oder permanente Herabsetzen des Beitrags einer Sicherheitsfunktion zur erfolgreichen Risikominderung während des bestimmungsgemäßen Betriebs einer Maschine verstanden. Dabei kann zwischen einer direkten und einer indirekten Degradierung unterschieden werden:

- Bei der direkten Degradierung wird die Reserve der Leistungsfähigkeit der Sicherheitsfunktion genutzt (Abb. 7 a).
- Bei der indirekten Degradierung wird der Beitrag der Sicherheitsfunktion zur Risikominderung durch eine Erhöhung des Risikos (Änderung der Systemgrenzen) indirekt reduziert (Abb. 7 b). Die ursprüngliche Leistungsfähigkeit der Sicherheitsfunktion bleibt unverändert.

Bei den in Abb. 7 dargestellten Degradierungen besteht jeweils eine Erhöhung des Restrisikos, das heißt es klafft eine Lücke zwischen dem aktuell erreichten Restrisiko R_{deg} und dem ursprünglichen Restrisiko R_{Rest}. Kennzeichnend für den degradierten Zustand ist jedoch, dass das Grenzrisiko R_{Grenz} nicht überschritten wird.

Abb. 7: Darstellung der Degradierungsarten



Quelle: ZVEI

Legende

R_0	Risiko einer speziellen Gefährdungssituation, bevor Schutzmaßnahmen angewendet werden
R_{Grenz}	geforderte Risikominderung durch Schutzmaßnahmen
R_{deg}	Risikominderung durch degradierte Sicherheitsfunktion
R_{Rest}	tatsächliche, durch SRP/CS erreichte Risikominderung im Normalzustand (nicht degradiert)

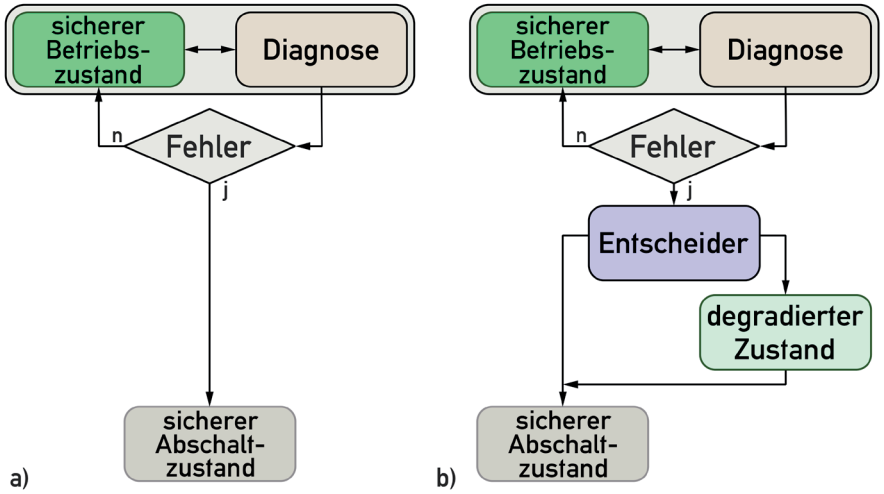
Ein typisches Beispiel für eine indirekte Degradierung kann sich im Fall eines fahrerlosen Transportfahrzeugs in einem Materialflusssystem ergeben. Bei Erkennung von Personen im geführten Fahrweg des Fahrzeugs löst eine berührungslose Schutzeinrichtung einen Stopp aus. Das dafür erforderliche Bremssystem muss so ausgelegt sein, dass das Fahrzeug anhalten kann, bevor Kontakt zwischen den festen Teilen des Fahrzeugs oder der Last und einer stehenden Person hergestellt wird. Dabei sind selbst widrige Bedingungen für die Einflussfaktoren Geschwindigkeit, Nennlast, Reibung, Boden und Gefälle vom Hersteller zu berücksichtigen (Grenzen der Maschine). Kommt es jetzt zu einem (unerwarteten) Rohrbruch in einem Bereich, in dem das Fahrzeug fährt, kann durch austretendes Wasser der Bremsweg derart vergrößert werden, dass die Betriebsreichweite der Einrichtung zur Personenerkennung nicht mehr ausreicht.

Die indirekte Degradierung wird in diesem Dokument nicht weiter betrachtet.

5.1.3 Tolerierbare Fehler

Die bisher in der Maschinenautomation übliche, konventionelle Reaktion bei Erkennen eines Fehlers in einer zweikanaligen Struktur ist der sofortige Stopp. Er stellt die einfachste Reaktion dar. Sie ist gleichzeitig aus Sicht der Verfügbarkeit unerwünscht und damit manipulationsanfällig (s. Abb. 8a).

Abbildung 8: Diagnose und Entscheider



Quelle: ZVEI

Wenn ein sicherer Weiterbetrieb der Maschine/Anlage gewährleistet werden soll, obwohl ein Fehler in einer Komponente der Sicherheitsfunktion erkannt wurde, sind neue Verfahren und Methoden erforderlich. Da ein Weiterbetrieb nicht bei jedem Fehler akzeptiert werden kann, ist eine Fehlereinschätzung und Fehlerbewertung vorzunehmen. Es gilt zu unterscheiden:

- Nicht tolerierbare Fehler, die zum Beispiel zeitnah zu einem Verlust der Funktionsreserve des (Sub-)Systems führen oder durch systematische Ausfälle bzw. Ausfälle gemeinsamer Ursache (engl: common cause failure) entstehen
- Tolerierbare Fehler, diese gefährden nicht augenblicklich die sichere Funktion des (Sub-)Systems

Je nach Bewertung des Fehlers überführt ein Entscheider das System automatisch in den sicheren Abschaltzustand oder in den Betrieb im degradierten Zustand (s. Abb. 8b).

5.1.4 Entscheider

Aufgabe dieser Entscheidung ist es, in Abhängigkeit des aktuellen Systemzustands in den degradierten Zustand oder in den sicheren Abschaltzustand zu verzweigen. Für diese Aufgabe ist eine detailliertere Diagnose (Fehler- und Zustandserkennung) als üblicherweise zur Realisierung der Anforderungen an einzelne Kategorien oder Architekturen erforderlich. Der Entscheider muss im Niveau dem der Sicherheitsfunktion mindestens gleichwertig sein.

Diagnose und Entscheidung sind besonders vor dem Hintergrund zu konzipieren, dass fehlerhafte Zustände neben zufälligen Bauteilausfällen auch durch systematische Ausfälle oder Ausfälle gemeinsamer Ursache bedingt sein können. Solche Ausfälle führen immer zu nicht tolerierbaren Fehlern. In der konkreten Umsetzung in ein technisches System erfordert die Realisierung eines Entscheiders daher ein hohes Maß an Sicherheit bei der Entscheidungsfindung, ob definitiv nur ein zufälliger Bauteilausfall für einen Fehler ursächlich ist.

5.1.5 Sicherheitsfunktion im degradierten Zustand

Die Chancen des Betriebs im degradierten Zustand wurden bisher nicht bewusst genutzt. Dabei liegen die Vorteile klar auf der Hand:

- Die Maschinenverfügbarkeit steigt, das System ist bei entsprechender Auslegung in der Lage, differenzierter auf Fehler zu reagieren.
- Der Weiterbetrieb der Maschine mit degradierter Sicherheitsfunktion vermeidet eine abrupte Produktionsunterbrechung, was Manipulationsanreize verringert.
- Die Implementierung von unterschiedlichen Szenarien unterstützt die Gestaltung flexibler Systeme (Industrie 4.0).

Um keine Missverständnisse aufkommen zu lassen, soll hier noch einmal explizit zum Ausdruck gebracht werden, dass die Funktionalität des Betriebs im degradierten Zustand durch den Maschinenhersteller/Integrator zu implementieren ist. Es ist keine Funktionalität, deren Gestaltung dem

Betreiber überlassen werden kann. Wie die Diagnose ist die beschriebene Funktionalität sicherheitsrelevant, aber keine eigenständige Sicherheitsfunktion. Für den Betrieb im degradierten Zustand sind die hierfür vorgesehenen Sicherheitsfunktionen zu erweitern um

- detaillierte Diagnose (Fehler- und Zustandserkennung),
- eine Entscheidungslogik (Fehlereinschätzung und -bewertung) und
- Grenzen des Betriebs im degradierten Zustand.

Die beiden Normen ISO 13849-1 und IEC 62061 stellen keine expliziten Anforderungen an ein Diagnose-Testintervall. In der Norm IEC 62061 geht das Diagnose-Testintervall (dort mit T2 bezeichnet) mit geringen Auswirkungen in die zu berechnende Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde (PFHD) ein. Ein zweikanaliges System ist demnach bei einem Fehler in einem Kanal durch einen zufälligen Bauteilausfall nicht unmittelbar unsicher geworden. Der verbleibende Kanal führt weiterhin die Sicherheitsfunktion aus.

5.1.6 Signalisierung des degradierten Zustands

Ist der Betrieb im degradierten Zustand eingeleitet, liegt bereits ein (tolerierbarer) Fehler in einer Funktionseinheit des sicherheitsgerichteten Steuerungssystems vor. Das Bedienpersonal muss über diesen Zustand informiert werden. Die Signalisierung kann über sicht- und/oder hörbare Anzeigen an der Maschine oder an jedem Bedienplatz erfolgen, bis hin zu Leitwarten mit einer Vielfalt von Einrichtungen zur Überwachung von Prozessen.

Die Internationale Norm IEC 60073:2002 stellt allgemeine Regeln zur Zuordnung einzelner Bedeutungen zu bestimmten sichtbaren, hörbaren und fühlbaren Anzeigen auf, um

- die Sicherheit von Personen, Eigentum und/oder Umwelt durch die sichere Überwachung und Bedienung der Einrichtungen oder Prozesse zu erhöhen,
- die genaue Beobachtung, Bedienung und Instandhaltung der Anlage zu erreichen,
- die schnelle Erkennung von Bedienungszuständen und Stellungen von Bedienteilen zu erreichen.

Farbe und die zeitliche Veränderung von Merkmalen (Blinken) sind die effektivsten Mittel, um Aufmerksamkeit zu erregen. Die Farbe, die durch eine Anzeige angezeigt werden soll, muss unter Berücksichtigung der Information, die mitgeteilt werden soll, ausgewählt werden. Der degradierte Zustand ist ein anormaler Prozesszustand. Die Farbe GELB ist für Funktionen reserviert, die eine Warnung oder einen anormalen Zustand anzeigen (s. Abb. 9). Als ein ergänzender Code zur Farbe kann die Signalisierung in der Gestalt eines gleichseitigen Dreiecks erfolgen, um Irrtümer zu vermeiden, die durch farbfehlsichtige Personen entstehen können.

Abb. 9: Allgemeine Bedeutung der Farben von Anzeigeleuchten

Farbe	Bedeutung	Erläuterung
Rot	Notfall	Gefahrbringender Zustand mit sofortiger Handlung reagieren
Gelb	Anormal	Anormaler Zustand bevorstehender kritischer Zustand
Grün	Normal	Sicherer Betriebszustand
Blau	Zwingend	Anzeige eines Zustandes, der eine zwingende Handlung des Bedieners erfordert
Weiß	Neutral	Verwenden bei Zweifel überdie Anwendung von Grün, Rot, Blau oder Gelb

Quelle: ZVEI (nach Tabelle 4, IEC 60204-1:2016)

Zur reinen Informationsvermittlung wird Dauerlicht angewendet. Um zusätzlich Aufmerksamkeit zu wecken, kann ein blinkender Anzeiger verwendet werden. Damit kann insbesondere betont werden, dass eine Änderung des Zustands bevorsteht.

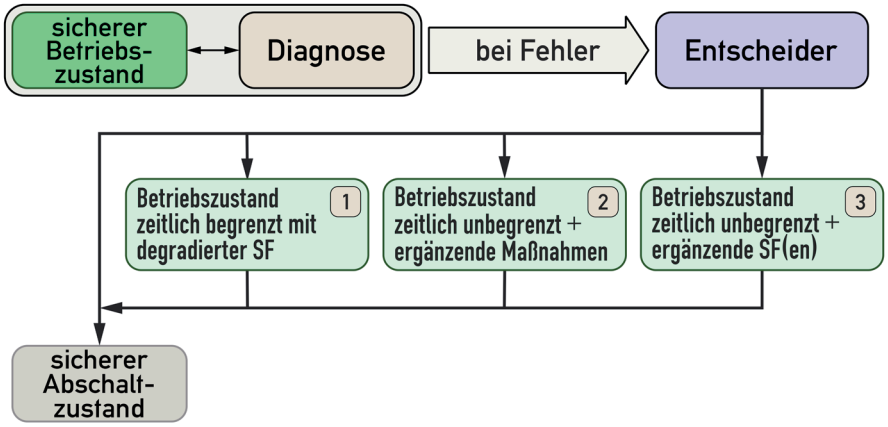
5.2 Varianten des Betriebs im degradierten Zustand

5.2.1 Allgemeines

Prinzipiell stehen bis zu drei Varianten zum Betrieb einer Sicherheitsfunktion im degradierten Zustand zur Verfügung (s. Abb. 10):

1. Zeitlich begrenzter Betrieb mit degradierter Sicherheitsfunktion (s. Kapitel 5.2.2)
2. Zeitlich unbegrenzter Betrieb mit ergänzenden Maßnahmen (s. Kapitel 5.2.3)
3. Zeitlich unbegrenzter Betrieb mit ergänzenden Sicherheitsfunktionen (s. Kapitel 5.2.4)

Abb. 10: Zustandsübergänge

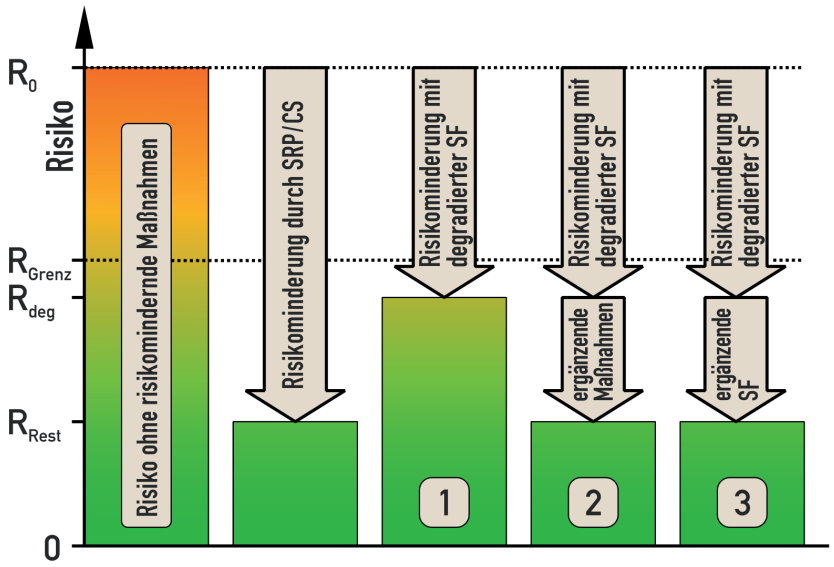


Quelle: ZVEI

In Abbildung 10 spiegelt der Übergang vom Normalzustand über den Entscheider zu den weiteren Betriebszuständen die zuvor beschriebene Sichtweise wider. Beim Eintritt eines ersten Fehlers kann durch den Entscheider in einen der vier dargestellten Zustände verzweigt werden. In einem System müssen nicht alle möglichen Betriebszustände vorgesehen sein. Optional kann auch eine Sequenz von mehreren degradierten Betriebszuständen durchlaufen werden.

Eine Übersicht über die durch die jeweiligen Zustände erreichten Beiträge zur Risikominderung ist in Abbildung 11 dargestellt.

Abb. 11: Varianten zur Risikominderung



Quelle: ZVEI

5.2.2 Zeitlich begrenzter Betrieb mit degradierter Sicherheitsfunktion

Der Grundgedanke dieses Betriebszustands ist der Sachverhalt des anfangs unveränderten Beitrags der Sicherheitsfunktion zur Risikoreduzierung. Die Ausfallwahrscheinlichkeit der Sicherheitsfunktion bleibt dabei nahezu konstant auf niedrigem Niveau. Erst mit weiterer Betriebszeit steigt die Ausfallwahrscheinlichkeit der Sicherheitsfunktion deutlich an und ihre Fähigkeit zur Risikominderung sinkt dementsprechend (s. Abb.12). Demzufolge kann bei dieser Vorgehensweise eine Maschine nur zeitlich begrenzt betrieben werden (t_{Grenz}), bis das Grenzrisiko R_{Grenz} erreicht ist.

Für ein zweikanaliges System, bei dem jeder Kanal die Sicherheitsfunktion ausführt, kann bei einem Ausfall eines Kanals folgende Betrachtung herangezogen werden: Bei der Abschätzung der Ausfallwahrscheinlichkeit für eine solche Architektur wird davon ausgegangen, dass ein erster Fehler in einem Kanal durch einen Diagnosetest erkannt und der Fehler angezeigt wird, jedoch nicht zur Abschaltung des Systems durch den Entscheider führt. Jeder weitere Fehler führt zu einer Erhöhung des Risikos. Definitionsgemäß darf dieses Risiko den Wert von R_{Grenz} nicht überschreiten.

Voraussetzungen für den zeitlich begrenzten Betrieb mit degradierter Sicherheitsfunktion sind:

a. Die Architektur des Systems

   Redundante Systeme (homogene oder diversitäre Redundanz)

b. Die ausreichend geringe Ausfallwahrscheinlichkeit

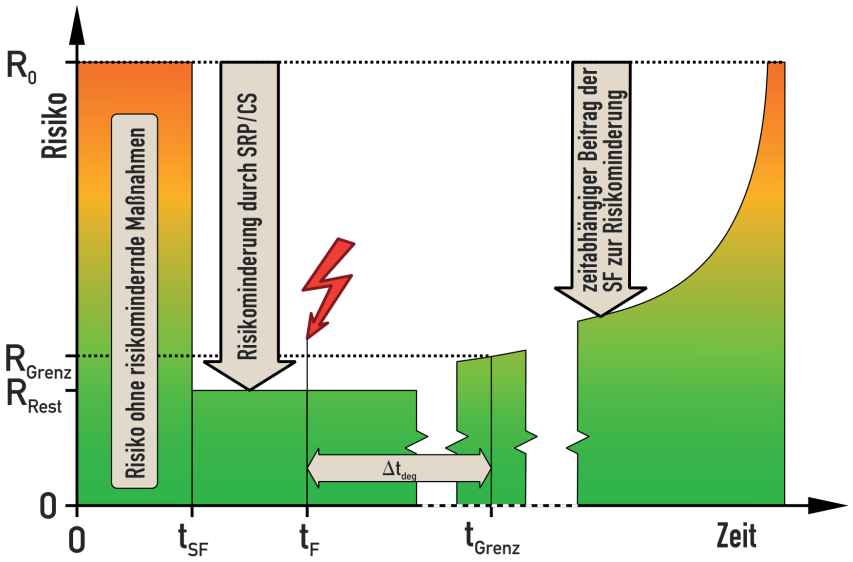
   Im System ist eine Reserve bezüglich Ausfallwahrscheinlichkeit konstruktiv vorgesehen. Die realisierte Ausfallwahrscheinlichkeit für das zu erreichende Rest-Risiko (R_{Rest}) ist geringer als die zulässige Ausfallwahrscheinlichkeit für das Grenz-Risiko (R_{Grenz}). Aktuell verfügbare Systeme erlauben einen Zeitraum Δt_{deg} von bis zu einer Woche, in dem die Riskominderung durch die nur wenig ansteigende Ausfallwahrscheinlichkeit nahezu vollständig erhalten bleibt. Abweichende Zeiträume (kürzer als eine Woche) können vom Maschinenbauer, basierend auf der Risikobeurteilung, festgelegt werden. Beim Erreichen der maximal zulässigen Zeit Δt_{deg} oder beim Zweitfehlereintritt wird vom Entscheider des Systems der als sicher definierte Zustand unmittelbar eingeleitet. Wird das System innerhalb des Zeitraums Δt_{deg}repariert, kann das System weiter betrieben werden. Eine mehrfache Nutzung von Δt_{deg} ohne zwischenzeitliche Reparatur ist nicht zulässig, da das Grenzrisiko R_{Grenz} bereits erreicht sein kann. Sollte bis zum Eintritt der maximal zulässigen Zeit Δt_{deg} kein sicherer Abschaltzustand oder eine Reparatur des Systems mit degradierter Sicherheitsfunktion eingeleitet worden sein, muss der Entscheider des Systems den als sicher definierten Zustand unmittelbar einleiten.

c. Die Widerstandsfähigkeit gegen Ausfälle aufgrund gemeinsamer Ursache (CCF)

   Die generellen CCF-Anforderungen gemäß ISO 13849-1 sind zur erfüllen. Der Nachweis (Verifizieren und Validieren), dass die Anforderungen für CCF ≥ 65 Punkte umgesetzt worden sind, muss mit größter Sorgfalt durchgeführt werden.

Sind alle diese Voraussetzungen erfüllt, ist der zeitlich begrenzte Betrieb mit degradierter Sicherheitsfunktion möglich.

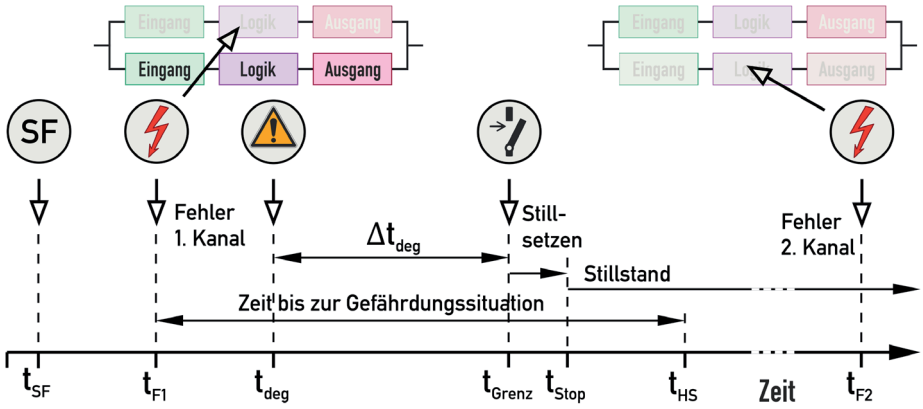
Abb. 12: Qualitativer Verlaufs des Risikos



Quelle: ZVEI

Das folgende Diagramm (s. Abb. 13) gilt für tolerierbare Erstfehler. Für nicht tolerierbare Fehler ist ein Betrieb im degradierten Zustand nicht zulässig. Bei der Festlegung der Zeitspanne Δt_{deg} müssen alle für die Anwendung relevanten Faktoren berücksichtigt werden. Dies ist beispielsweise der erforderliche Performance Level bzw. SIL der betrachteten Sicherheitsfunktion. Modellrechnungen für zweikanalige Systeme zeigen, dass eine Zeitspanne von einem oder mehreren Tagen keine nennenswerte Erhöhung der Ausfallwahrscheinlichkeit zur Folge hat. Die Zeitspanne darf wegen der Möglichkeit Common-Cause-bedingter Folgeausfälle nicht auf Werte ausgedehnt werden, die sich rein rechnerisch für zufällige Hardwareausfälle als unkritisch erweisen.

Abb. 13: Zeitbegrenzung für degradierten Zustand



Quelle: ZVEI

Legende

t_{SF}	Anfordern der Sicherheitsfunktion
t_{F1}	Eintritt Fehler erster Kanal
t_{deg}	Einleiten des Betriebs im degradierten Zustand
t_{Grenz}	Erreichen des Grenzrisikos R_{Grenz}
t_{Stop}	Erreichen des sicheren Zustands
t_{HS}	Eintritt der Gefährdungssituation
t_{F2}	Eintritt Fehler zweiter Kanal

5.2.3 Zeitlich unbegrenzter Betrieb mit ergänzenden Maßnahmen

Da nach Degradierung der Sicherheitsfunktion (bei konstant gebliebenem Ausgangsrisiko) eine Lücke in der erforderlichen Risikominderung entstehen wird, besteht die Notwendigkeit, diese zu schließen. Für die zusätzlich zu erbringenden Maßnahmen gilt:

- Sie müssen vom Maschinenhersteller konzipiert werden.
- Der Zustand muss signalisiert werden (z. B. durch Warnlampen oder akustische Signale).

Geeignete, durch den Betreiber zu erbringende Maßnahmen können sein:

- Zusätzliche trennende Schutzeinrichtungen (z. B. Absperrband)
- Manuelle Funktionsbegrenzung
- Einsatz entsprechend geschulten Personals
- An die Arbeitsbelastung angepasste Arbeits- und Pausenzeiten
- Persönliche Schutzausrüstung

Der von der Maschine gemeldete Eintritt in den degradierten Zustand muss vom Bediener zeitnah quittiert werden. Erfolgt diese Quittierung nicht innerhalb eines festgelegten Zeitraums, muss der Entscheider die Maschine in einen anderen sicheren Zustand versetzen. Dies kann zum Beispiel der sichere Stillstand sein.

5.2.4 Zeitlich unbegrenzter Betrieb mit ergänzenden Sicherheitsfunktionen

Der Grundgedanke dieses Betriebszustands besteht darin, die durch die Degradierung entstandene Lücke in der Risikominderung durch Aktivierung anderer Sicherheitsfunktionen zu schließen. Gelingt es, das Ausgangsrisiko durch diese Maßnahme derart zu senken (s. Abb. 11, Ziffer 3), dass der Beitrag der degradierten Sicherheitsfunktion zur Risikominderung ausreichend ist, unterliegt dieser Betriebszustand keiner zeitlichen Einschränkung wie bei dem zeitlich begrenzten Betrieb (s. Kapitel 5.2.2).

Dieser Betriebszustand bietet großes Potenzial zum Erhalt der Verfügbarkeit der Maschine, da er zeitlich nur von weiteren Ausfällen beschränkt wird. Wenn es gelingt, das System mit mehreren Rückfallebenen auszustatten, ist ein sehr flexibles Reagieren auf Ausfälle möglich.

Ein Beispiel für eine interne Maßnahme ist es, eine Rückfallebene dergestalt zu installieren, dass bei einem Ausfall eines Kanals eines zweikanaligen Systems ein Strukturwechsel zu einer Kategorie 2 nach ISO 13849-1 erfolgt. Wird diese Lösung umgesetzt, kann auf eine zeitliche Begrenzung verzichtet werden, wenn ebenfalls der erforderliche Performance-Level erreicht wird. Als weiteres Beispiel könnte das System bei Ausfall einer Schutzeinrichtung die gefährlichen Bewegungen nur noch im Schleichgang ausführen.

6 Fazit und Ausblick

Die Ausführungen zeigen, dass bei redundanten Sicherheitsarchitekturen – in Abhängigkeit von der Risikohöhe – ein gefährlicher Ausfall in einem Kanal für eine bestimmte Zeit toleriert werden kann, um kritische Prozesse gesteuert herunterfahren zu können. Insbesondere bei Maschinen/Anlagen, bei denen eine hohe Zuverlässigkeit gefordert wird, bedeutet diese Sichtweise einen Zugewinn an Verfügbarkeit gegenüber der bisher üblichen Realisierung, der letztlich zu einer höheren Akzeptanz beim Benutzer führt. Die Bewertung sieht sich im Einklang mit den Schutzzielen der Maschinenrichtlinie und steht nicht im Widerspruch zu den harmonisierten Normen ISO 13849 bzw. IEC 62061.

Weitergehende Fragestellungen zur applikativen Umsetzung werden in einem ergänzenden Dokument „Fehlertoleranz in der Maschinensicherheit Teil 2 – Anforderungen“ausgeführt.

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org