ZVEI:
Die Elektroindustrie

Whitepaper

Fehlertoleranz in der Maschinensicherheit

Teil 2 – Anforderungen, Version 1.0

Fachverband Automation

Fehlertoleranz in der Maschinensicherheit Teil 2

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

Mai 2021

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.

Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Herausgebers unzulässig.

Das gilt insbesondere für Vervielfältigungen, Übersetzung, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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 die Anforderungen an den Personenschutz zu vernachlässigen.

Der Teil I des Whitepapers beschreibt die theoretischen Grundlagen für einen Betrieb im degradierten Zustand. Der Teil II (dieses Dokument) beschreibt die erforderlichen Voraussetzungen für den Betrieb im degradierten Zustand. Voraussetzung für die Anwendung des Teils II ist die Berücksichtigung von Teil I.

Es werden Anforderungen für die Teilsysteme definiert, die für einen degradierten Betrieb geeignet sind. Es wird ein Verfahren beschrieben, wie der Integrator einer Sicherheitsfunktion den degradierten Betrieb auslegen und in der Maschine unter Verwendung dafür geeigneter Teilsysteme implementieren kann. Zusätzlich gibt es dem Hersteller von Sicherheitskomponenten hierzu eine Orientierungshilfe.

Der Teil III des Whitepapers beschreibt weitere Anforderungen an ein Gesamtsystem, das für einen Betrieb im degradierten Zustand geeignet ist, wie zum Beispiel die Beherrschung von systematischen Ausfällen unter Beachtung von Ausfällen infolge gemeinsamer Ursache, etc.

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
Jens Mehnert	K.A. Schmersal
Michael Niehaus	Lenze
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

1 Einleitung

1.1 Motivation

Die Arbeitssicherheit im industriellen Umfeld hat seit jeher einen hohen Stellenwert. Unternehmen haben erkannt, dass der Schutz der Beschäftigten 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 und Steuerungen 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 sicherheitsgerichteten Ausfallreaktion.

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 der Fehlererkennung aufzuzeigen. Es werden Konzepte definiert, unter denen Maschinen bei Erkennung von Fehlern in Sicherheitsfunktionen weiter betrieben werden können, ohne dass Personen inakzeptablen Risiken ausgesetzt werden.

1.2 Anwendungsbereich

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

Die Notwendigkeit der Implementierung von Sicherheitsfunktionen ist immer eines der Ergebnisse der sich aus der Risikobeurteilung ergebenden Maßnahmen zur Risikominderung an einer Maschine oder Anlage. Basis für die Risikobeurteilung bildet die ISO 12100, die alle Anforderungen an den iterativen Prozess beschreibt. Verfahren zur Einschätzung des für eine Sicherheitsfunktion erforderlichen Sicherheitsniveaus sind in den Normen ISO 13849-1 und IEC 62061 beschrieben. Es kann so mit den Ergebnissen der Risikobeurteilung – vor Durchführung von risikomindernden Maßnahmen – in einem weiteren Schritt detailliert nachgewiesen werden, dass das Restrisiko im fehlertoleranten Betrieb zu keinem Zeitpunkt und in keinem Betriebszustand der Maschine oder Anlage über dem vorher definierten Grenzrisiko liegt.

Fokus dieses Dokuments sind ausschließlich die im Maschinen- und Anlagenbau für höhere Sicherheitsanforderungen üblichen Systeme, in denen die Ausführung der Sicherheitsfunktion auch im Fehlerfall durch ihre ursprünglich zweikanalige Struktur weiterhin möglich ist.

Nicht betrachtet von der hier beschriebenen Anwendung sind insbsondere:

- Einkanalige Sicherheitssysteme, in welchen ein sicherer Betrieb im Fehlerfall ausgeschlossen ist,
- Systeme mit mehr als zwei Kanälen (bekannt z.B. aus der Prozessindustrie und der Avionik),
- Systeme mit Votern, in denen ein fehlerhafter Kanal zum Beispiel durch eine Mehrheitsentscheidung erkannt und abgeschaltet werden kann.
- Hot-Standby Systeme, in denen im Fehlerfall ein mitlaufendes Reservesystem die Aufgaben des ausgefallenen Systems übernimmt.
- Cold-Standby Systeme, in denen im Fehlerfall ein Reservessystem ausreichend schnell hochgefahren wird, um die Aufgaben des ausgefallenen Systems zu übernehmen.

2 Begriffe

2.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe:

2.1.1 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]

2.1.2 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]

2.1.3 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]

2.1.4 Tolerierbarer Fehler

Ein tolerierbarer Fehler in einem zweikanaligen System ist ein Fehler, der eindeutig in einem Kanal des Systems lokalisiert werden kann, so dass eine Auswirkung auf den zweiten Kanal ausgeschlossen werden kann.
Anmerkung 1: Die eindeutige Lokalisierung des Fehlers in einem Kanal erfordert Diagnosemaßnahmen im System, die eventuell über die Diagnose zur allgemeinen Erkennung eines Fehlers im System hinausgehen.
Anmerkung 2: Führt die Erkennung eines Fehlers nicht zur unmittelbaren Abschaltung der Sicherheitsfunktion, so muss in der Entwicklung besondere Sorgfalt auf die Vermeidung und Beherrschung möglicher Folgefehler gelegt werden, um ein späteres Übergreifen des Fehlers auf den zweiten Kanal zu verhindern (z.B. als Folge von fehlerhafter Kommunikation oder Erwärmung).

2.1.5 Fehlertoleranz

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

2.1.6 Funktionseinheit

Einheit aus Hardware oder Software oder beidem, die zur Durchführung einer angegebenen Aufgabe geeignet ist
[ISO/IEC 2382-1, 01-01-40]
Anmerkung: Funktionseinheiten können nicht nur Logikeinheiten, sondern auch Sensoren und Leistungsantriebe sein.

2.1.7 Interface-Typ

Der Interface-Typ beschreibt eine standardisierte Schnittstelle zwischen Sendern von Signalen (Quellen) und Empfängern von Signalen (Senken) mit Festlegungen über die Erzeugung und Auswertung von Testimpulsen.

- Typ A für potentialfreie Kontakte als Informationsquelle;
- Typ B für diskrete Halbleiterausgänge mit externer Taktung;
- Typ C für diskrete Halbleiterausgänge mit integrierter Diagnose;
- Typ D für plus-minus-schaltende Halbleiterausgänge mit integrierter Diagnose.

[Quelle: ZVEI-Empfehlung 2021.01-Positionspapier CB24I]

2.1.8 Link-Typ

Der Link-Typ beschreibt eine standardisierte Schnittstelle zur Übertragung von sicherheitsbezogenen Informationen, sowie Diagnoseinformationen zwischen Logikeinheiten und Feldgeräten.

2.1.9 Logik-Typ

Der Logik-Typ beschreibt eine standardisierte Struktur der Logik von sicherheitsbezogenen Funktionseinheiten zur Verknüpfung von Ein- und Ausgängen:

- Typ E eine SSF realisiert aus diskreten Komponenten;
- Typ 1 eine feste SSF im Gerät;
- Typ 2 eine von n SSF auswählbar;
- Typ 3 eine parametrierbare SSF;
- Typ 4 mehrere SSF mit Kommunikation.

[Quelle: ZVEI Whitepaper „Sicherheitsaspekte für Software in industriellen Anwendungen"]

2.1.10 Sicherer Zustand

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

2.1.11 Sicherheit

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

2.1.12 Sicherheits-Teilfunktion (SSF)

Teil einer Sicherheitsfunktion, dessen Ausfall zu einem Ausfall der Sicherheitsfunktion führen kann.
[ISO/DIS 13849-1:2020, 3.1.51]

2.1.13 Sicherheitsgerichtete Ausfallreaktion

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

3 Abkürzungen

Abkürzung	Beschreibung
ASW	**Application Software** Programm für eine bestimmte Benutzeranwendung
CCF	**Common Cause Failure** Ausfall infolge gemeinsamer Ursache
EUC	**Euqipment Under Control** Einrichtung, die zur Fertigung, zum Transport oder anderen Tätigkeiten verwendet wird
FSCP	**Functional Safety Communication Profile** funktional sicheres Kommunikationsprofil
FS-DI	**Functional Safety Digital Input** funktional sicherer digitaler Eingang
FS-DO	**Functional Safety Digital Output** funktional sicherer digitaler Ausgang
IGBT	**Insulated-gate bipolar transistor** Bipolartransistor mit isolierter Gate-Elektrode
MooN (D)	**M out of N** Architektur mit M-aus-N Kanälen (mit Diagnose)
MSF	**Mechanic Subfunction** Mechanik-Teilfunktion
OSSD	**Output Signal Switching Device** Ausgangsschaltelement
PDS (SR)	**Power Drive Systems (Safety Related)** Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl, die Sicherheits-Teilfunktionen zur Verfügung stellen
SDCI	**Single Drop Communication Interface** digitale Punkt-zu-Punkt-Kommunikationsschnittstelle
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
SSF	**Safety Subfunction** Sicherheits-Teilfunktion
STO	**Safe Torque Off** Sicher abgeschaltetes Drehmoment

Quelle: ZVEI

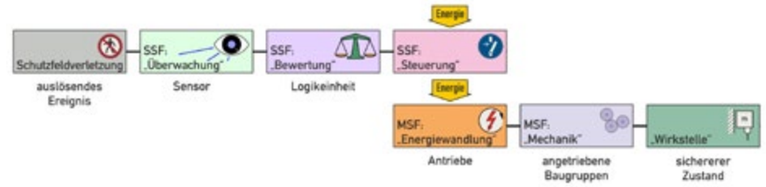
4 Betrieb im degradierten Zustand

4.1 Diagnose und Entscheider

4.1.1 Sicherheits-Teilfunktionen

Ein Teil des Prozesses zur Risikominderung[1] ist es, die erforderlichen Sicherheitsfunktionen für die Maschine zu definieren, beispielsweise „Sicherer Halt einer gefahrbringenden Bewegung“. Eine Sicherheitsfunktion wird im Allgemeinen durch mehrere Teilsysteme realisiert (siehe Abbildung 4.1). Diese Teilsysteme führen dann entsprechende Sicherheits-Teilfunktionen aus [z.B. ein Leistungsantrieb die SSF „Sicherer Stopp 1“ (en: safe stop 1, SS1)]. Mehrere Sicherheitsfunktionen können einzelne Teilsysteme gemeinsam nutzen, häufig ist das mindestens die Logikeinheit. Umgekehrt können ebenfalls mehrere Sicherheits-Teilfunktionen durch ein einzelnes Teilssystem (z.B. Sensor: SSF „Überwachung“ & SSF „Bewertung“) ausgeführt werden. Die Funktion eines mechanischen Übertragungssystems lässt sich ebenfalls in Mechanik-Teilfunktionen aufteilen.

Abb. 4.1: Teilsysteme und ihre Funktionalitäten



4.1.2 Fehlertoleranz in der Maschinensicherheit

Die bisher in der Maschinenautomation übliche 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.

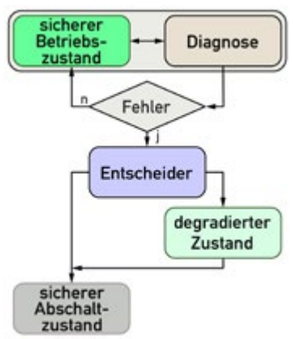
Wenn ein sicherer Weiterbetrieb der Maschine/Anlage gewährleistet werden soll, obwohl ein Fehler in einer Komponente der Sicherheitsfunktion erkannt wurde, sind neue Verfahren und Methoden erforderlich. Da ein Weiterbetrieb nicht bei jedem Fehler akzeptiert werden kann, ist eine Fehlereinschätzung und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

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

Je nach Bewertung eines Fehlers überführt ein Entscheider (siehe Abbildung 4.2) das System automatisch in den sicheren Abschaltzustand oder in den Betrieb im degradierten Zustand.

Anmerkung: Funktionseinheiten können nicht nur Logikeinheiten, sondern auch Sensoren und Leistungsantriebe sein.

Abb. 4.2: Diagnose und Entscheider



[1] In diesem Dokument werden nur mechanische Gefährdungen durch bewegte Teile betrachtet.

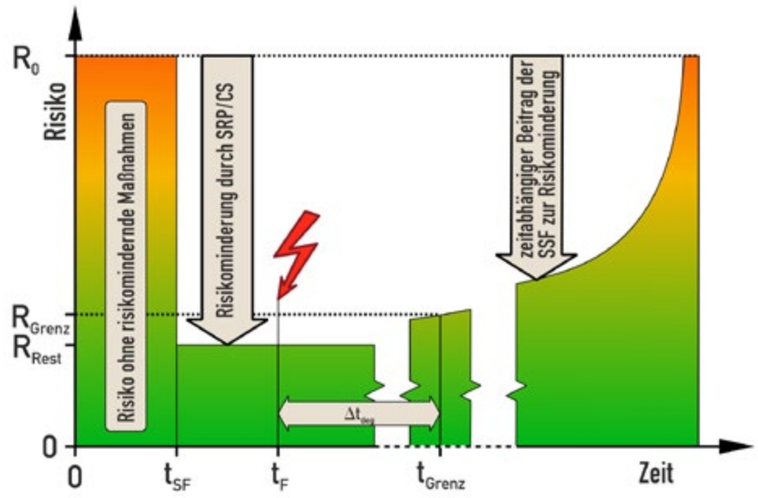
Aufgabe dieser Entscheidung ist es, in Abhängigkeit des aktuellen Systemzustands in den degradierten Zustand oder in den sicheren Abschaltzustand zu verzweigen. Für diese Aufgabe ist eine detailliertere Diagnose (Fehler- und Zustandserkennung) als üblicherweise zur Realisierung der Anforderungen an einzelne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

Diagnose und Entscheidung sind besonders vor dem Hintergrund zu konzipieren, dass fehlerhafte Zustände neben zufälligen Bauteilausfällen auch durch systematische Ausfälle bzw. Ausfälle infolge 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 Qualität bei der Entscheidungsfindung, ob definitiv nur ein zufälliger Bauteilausfall für einen Fehler ursächlich ist.

4.1.3 Zeitlich begrenzter Betrieb mit degradierter Sicherheits-Teilfunktion

Der Grundgedanke dieses Betriebszustands ist der Sachverhalt des anfangs unveränderten Beitrags der Sicherheits-Teilfunktion zur Risikoreduzierung. Die Ausfallwahrscheinlichkeit der Sicherheits-Teilfunktion bleibt dabei nahezu konstant auf niedrigem Niveau (siehe Abbildung 4.3). Erst mit weiterer Betriebszeit steigt die Ausfallwahrscheinlichkeit der Sicherheits-Teilfunktion deutlich an und ihre Fähigkeit zur Risikominderung sinkt dementsprechend. Demzufolge kann dann bei dieser Vorgehensweise eine Maschine nur zeitlich begrenzt betrieben werden (t_{Grenz}), bis das Grenzrisiko RGrenz erreicht ist.

Abb. 4.3: Qualitativer Verlaufs des Risikos



Voraussetzungen für den zeitlich begrenzten Betrieb mit degradierter Sicherheits-Teilfunktion sind:

a. Die Architektur des Systems

Das Teilsysteme ist redundant ausgelegt (homogene oder diversitäre Redundanz).

b. Eine ausreichend geringe Ausfallwahrscheinlichkeit

Im Teilsystem 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 Teilsysteme erlauben einen Zeitraum Δt_{deg} von bis zu einer Woche, in dem die Risikominderung 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 Teilsystems der als sicher definierte Zustand unmittelbar eingeleitet. Wird das Teilsystem innerhalb des Zeitraums Δt_{deg} repariert, kann das Teilsystem 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 keine Reparatur des Teilsystems mit degradierter Sicherheits-Teilfunktion eingeleitet worden sein, muss der Entscheider des Teilsystems den als sicher definierten Zustand unmittelbar herbeiführen.

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

Die generellen CCF-Anforderungen gemäß ISO 13849-1 sind zu 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 Sicherheits-Teilfunktion möglich.

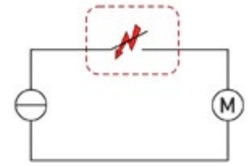
4.2 Qualifizierte Diagnose

4.2.1 Ausfallverhalten von Systemen

Als Beispiel zur Veranschaulichung des Ausfallverhaltens von Systemen soll ein einfacher Stromkreis dienen (siehe Abbildung 4.4). Ein einzelner Fehler in dem Schalter führt zu folgendem Verhalten:

- ein Nichtöffnen des Schalters verhindert das Abschalten der Last
- ein Nichtschließen des Schalters verhindert das Einschalten der Last.

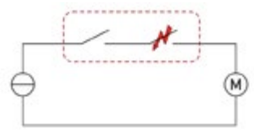
Abb. 4.4: Einkanaliger Stromkreis (1oo1)



Soll im Fehlerfall ein Abschalten der Last sichergestellt werden, kann ein zweikanaliges System zur Anwendung kommen (siehe Abbildung 4.5). Ein Fehler in einem der beiden Schalter führt zu folgendem Verhalten:

- ein Nichtöffnen eines Schalters verhindert NICHT das Abschalten der Last
- ein Nichtschließen eines Schalters verhindert das Einschalten der Last.

Abb. 4.5: Zweikanalige Abschaltung (1oo2)



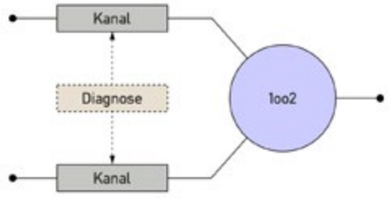
Allgemein beschreibt man diese Systeme als MooN (‚M out of N'). Dabei bezeichnet N die Anzahl der vorhandenen Kanäle. M ist die Anzahl der Kanäle, die funktionsfähig sein müssen, damit die Architektur ihre (Teil-) Sicherheitsfunktion korrekt ausführt.

[2] Beispiele zur Bestimmung folgen im Teil III

4.2.2 1oo2-Architektur

Diese Architektur besteht aus zwei parallelen Kanälen, so dass jeder der Kanäle die Sicherheits-Teilfunktion ausführen kann (siehe Abbildung 4.6). Daher muss ein gefahrbringender Ausfall in beiden Kanälen vorliegen, bevor die Sicherheits-Teilfunktion bei Anforderung ausfallen würde. Es wird angenommen, dass jeder durch Diagnose erkannte Fehler nur meldet und keine Ausgangszustände oder den Ausgangsvergleich ändert [siehe Anhang B.3.2.2.2., IEC 61508-6:2010].

Abb. 4.6: Blockschaltbild für 1oo2

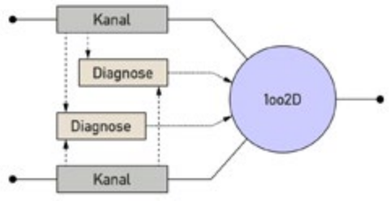


Im Maschinenbereich ist es nicht üblich, nur eine Fehlermeldung ohne Änderung des Ausgangszustands auszugeben. Vielmehr wird bei einem erkannten Fehler der oder die Ausgänge in den sicheren Zustand versetzt. Dies ist die bisher übliche Architektur für die Ausgänge von sicherheitsbezogenen Geräten mit zweikanaliger Struktur. Im Fall eines einzelnen Fehlers ist ein Abschalten der Last sichergestellt.

4.2.3 1oo2D-Architektur

Diese Architektur besteht aus zwei parallelen Kanälen. Jeder der Kanäle kann die Sicherheits-Teilfunktion ausführen. Sollte die Diagnose in einem Kanal einen Fehler erkennen, wird der Ausgangsvergleich angepasst, so dass der Gesamtausgangszustand dem anderen Kanal folgt (siehe Abbildung 4.7). Falls die Diagnose in beiden Kanälen Fehler erkennt oder eine Abweichung, die keinem der beiden Kanäle zugeordnet werden kann, wird der Ausgang in den sicheren Zustand versetzt. Um eine Abweichung zwischen den beiden Kanälen zu erkennen, kann jeder Kanal den Zustand des anderen durch von ihm unabhängige Mittel bestimmen [siehe Anhang B.3.2.2.4., IEC 61508-6:2010].

Abb. 4.7: Blockschaltbild für 1oo2D



Diese Architektur ermöglicht einen fehlertoleranten Weiterbetrieb bei einem Einzelfehler in einem Kanal, unabhängig von der Art des Fehlers.

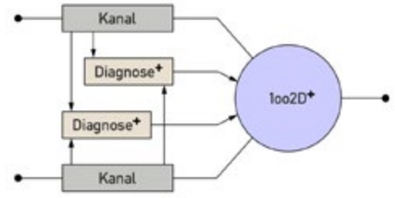
[1] In diesem Dokument werden nur mechanische Gefährdungen durch bewegte Teile betrachtet.

4.2.4 1oo2D+-Architektur

Diese Architektur entspricht 1002D, beinhaltet aber zusätzlich eine erweiterte Diagnose. Diese sogenannte „Qualifizierte Diagnose" bewertet:

- Welcher Fehler liegt vor?
- Wo liegt dieser Fehler? (z.B. welcher Kanal)
- Kann die Sicherheits-Teilfunktion weiter ausgeführt werden?

Abb. 4.8: Blockschaltbild für 1oo2D+



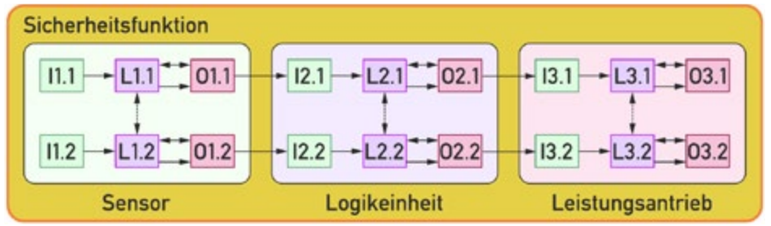
Das Ergebnis der qualifizierten Diagnose kann als Diagnosestatus (in Anlehnung an Namur NE 131) zusätzlich über Statussignale zur Verfügung gestellt werden:

- Ausfall:
  Aufgrund einer Funktionsstörung im Sicherheitsgerät oder an seiner Peripherie ist das Ausgangssignal ungültig.
- Funktionskontrolle:
  Am Sicherheitsgerät wird gearbeitet, das Ausgangssignal ist daher vorübergehend ungültig (z.B. eingefroren)
- Außerhalb der Spezifikation:
  Vom Gerät durch Selbstüberwachung ermittelte Abweichungen von den zulässigen Umgebungs- oder Prozessbedingungen oder Störungen im Gerät selbst weisen darauf hin, dass die Messunsicherheit bei Sensoren oder die Sollwertabweichung bei Aktoren wahrscheinlich größer ist, als unter Betriebsbedingungen zu erwarten.
- Wartungsbedarf:
  Das Ausgangssignal ist zwar noch gültig, aber die Funktionsreserve wird demnächst erschöpft oder aufgrund von Einsatzbedingungen eine Funktion in Kürze eingeschränkt sein (z.B. Betrieb im degradierten Zustand).
- Sind keine Statussignale gesetzt, ist von einer bestimmungsgemäßen Funktion des Sicherheitsgeräts auszugehen.

4.3 Sicherheitsbezogenes System

Die folgenden Abschnitte betrachten ein typisches System aus Sensoren, einer Logikeinheit und Leistungsantrieben, die gemeinsam Sicherheitsfunktionen ausführen (siehe Abbildung 4.9).

Abb. 4.9: Sicherheitsbezogenes Blockdiagramm



Dieses Dokument beschränkt sich auf elektrische Leistungsantriebssysteme [PDS(SR)]. Prinzipiell lässt sich die Vorgehensweise auch auf fluidtechnische Antriebssteuerungen übertragen.

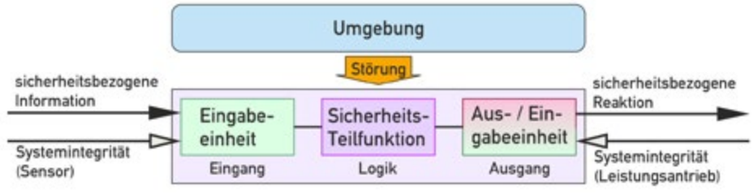
5 Sicherheitsbezogene Logikeinheiten

5.1 Aufbau

Eine sicherheitsbezogene Logikeinheit (siehe Abbildung 5.1) besteht mindestens aus:

- einer Eingabeeinheit,
  Statusinformationen (Systemintegrität) und sicherheitsbezogene Informationen von der Maschine bzw. dem Prozess werden zum Ein-/Ausgabe-System der Logikeinheit durch binäre, digitale, inkrementelle oder analoge Signale übertragen;
- einer Verarbeitungseinheit (Sicherheits-Teilfunktion),
  entsprechend des Anwendungsprogramms verarbeitet die Verarbeitungseinheit Signale, die von den Sensoren und dem internen Datenspeicher geliefert werden, und sie erzeugt Signale, die sowohl an die Aktoren als auch an den internen Speicher geleitet werden;
- einer Ausgabeeinheit
  die von der Sicherheits-Teilfunktion ermittelten Entscheidungen und Ergebnisse werden durch die Verwendung von geeigneten binären, digitalen, inkrementellen oder analogen Signalen zur Maschine bzw. zum Prozess übermittelt.

Abb. 5.1: Sicherheitsbezogene Logikeinheit



Logikeinheiten haben als „letzter Entscheider“ die folgenden Aufgaben zu erfüllen:

- Erkennung und Beurteilung von Fehlern der Sensoren oder der Leistungssteuerung an Ein- und Ausgängen.
- Auswertung der Diagnoseinformationen der Feldgeräte.
- Aufrechterhaltung eines Betriebs im degradierten Zustand mit Hilfe der Diagnoseinformationen.
- Abschaltung des Betriebs im degradierten Zustand nach einer definierten Maximalzeit.
- Abschaltung des Betriebs im degradierten Zustand nach Wegfall der Bedingungen für den degradierten Betrieb.

Eine geeignete Logikeinheit muss über die folgenden Eigenschaften verfügen:

- Möglichkeit zur Klassifizierung von Fehlerbildern mit zugeordneten Verhaltensweisen (degradierter Betrieb, Stillsetzen).
- Möglichkeit zur Aufrechterhaltung des degradierten Betriebs bei Fehlererkennung.
- Möglichkeit zur Einstellung von Rahmenbedingungen für den degradierten Betrieb (z.B. maximale degradierte Betriebszeit).
- Es muss sich um ein qualifiziertes SRP/CS mit mindestens einer Architektur 1oo2D handeln.

5.2 Realisierungsformen von Logikeinheiten

5.2.1 Allgemein

Kennzeichnende Merkmale der hier beschriebenen Funktionalitäten von Verarbeitungseinheiten in Logikeinheiten sind Logik-Typen (siehe ZVEI Whitepaper „Sicherheitsaspekte für Software in industriellen Anwendungen“).

Eine Logikeinheit muss einen Betrieb der Sicherheitsfunktion im degradierten Zustand mit Hilfe der Diagnoseinformationen jederzeit aufrechterhalten können. In diesem Dokument wird zunächst davon ausgegangen, dass eine Logikeinheit keinen Betrieb im degradierten Zustand zulässt. Jeder erkannte Fehler sollte sofort den sichernen Zustand herbeiführen. Generell ist ein Betrieb im degradierten Zustand ebenfalls für Logikeinheiten möglich.

Im Folgenden werden drei Grundformen von Logikeinheiten dargestellt. Mischformen daraus sind möglich.

5.2.2 Sicherheitsschaltgeräte

Ein Sicherheitsschaltgerät besteht aus:

- einer Verarbeitungseinheit,
  Logik-Typ 1 oder Typ 2 (eine aktive SSF im Gerät);
- einer Ein-/Ausgabeeinheit,
  integriert, nicht erweiterbar;
- optional:
  manuelle Rücksetzfunktion,
  Überwachung externer Steuerungsteile (EDM).

5.2.3 Modulare Sicherheitssteuerungen

Eine modulare Sicherheitssteuerung besteht aus:

- einer Verarbeitungseinheit,
  Logik-Typ 4 (mehrere aktive SSF, mit Kommunikation);
- einer oder mehreren Ein-/Ausgabeeinheit(en),
  lokal (Kommunikation über Rückwandbus), und/oder
  extern (Kommunikation über Feldbus).

5.2.4 Eingebettete Systeme

Ein eingebettetes System besteht aus:

- einer Verarbeitungseinheit,
  Logik-Typ 4 (mehrere aktive SSF, mit Kommunikation);
- keiner Ein-Ausgabeeinheit, dafür mit
  einer Kommunikationsschnittstelle für eine direkte Kommunikation zwischen der Verabeitungseinheit, anderen Logikeinheiten und den Feldgeräten (Feldbus).

5.3 Ein-/Ausgabeeinheiten von Logikeinheiten

5.3.1 Eigenschaften von Ein-/Ausgabeeinheiten

Ein-/Ausgabeeinheiten zeigen im Allgemeinen eine modulare Ausprägung, die eine Konfiguration der Logikeinheit gemäß den Anforderungen von Maschine oder Fertigungsprozess und auch eine spätere Erweiterung (bis zur maximalen Konfiguration) gestatten.

Eine Ein-/Ausgabeeinheit kann lokal in unmittelbarer Nähe zur Verarbeitungseinheit untergebracht sein oder sie kann in der Nähe der Sensoren oder Aktoren von Maschine oder Fertigungsprozess, d. h. entfernt (extern) von der Verarbeitungseinheit, installiert sein.

5.3.2 Lokale Ein-/Ausgabeeinheiten

Die Schnittstellenfunktion zu Sensoren und Aktoren wandelt Folgendes um:

- die Eingangssignale und/oder Daten, die von der Maschine oder dem Fertigungsprozess geliefert werden, in geeignete Signalpegel zur Weiterverarbeitung;

- die Ausgangssignale und/oder Daten, die von der Signalverarbeitungsfunktion geliefert werden, in geeignete Signalpegel, um Aktoren und/oder Anzeigen zu steuern.

Die Kommunikation zwischen der Verarbeitungseinheit und den lokalen Ein-/Ausgabesystemen erfolgt im Allgemeinen über eine Kommunikationsschnittstelle mit proprietärem Protokoll (Rückwandbus).

5.3.3 Externe Ein-/Ausgabeeinheiten

Die Schnittstellenfunktion zu Sensoren und Aktoren ist identisch zu den lokalen Systemen. Die Kommunikation zur Verarbeitungseinheit erfolgt über eine Kommunikationsschnittstelle mit offenem Protokoll (Feldbus).

5.4 Anforderungen an Schnittstellenfunktion

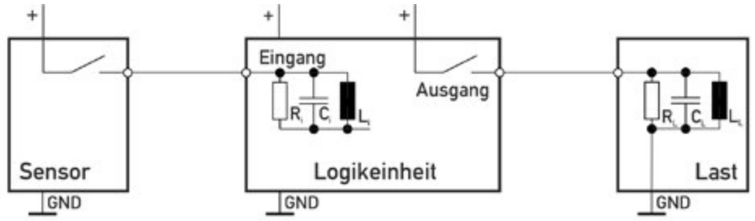
Die im Folgenden beschriebenen Funktionen der Ein- und Ausgänge gelten gleichbedeutend für Ein-/Ausgabeeinheiten von Sensoren und Leistungsantrieben

5.4.1 Nicht-sicherheitsbezogene digitale Ein-/Ausgänge

Positive Logik (stromziehende Eingänge/stromliefernde Ausgänge, siehe Abbildung 5.2):

- Digitale Eingänge entsprechen den Anforderungen nach IEC 61131-2:2017, Kapitel 6.4.4.2.
- Digitale Ausgänge entsprechen den Anforderungen nach IEC 61131-2:2017, Kapitel 6.4.6.1.

Abb. 5.2: Positive Logik



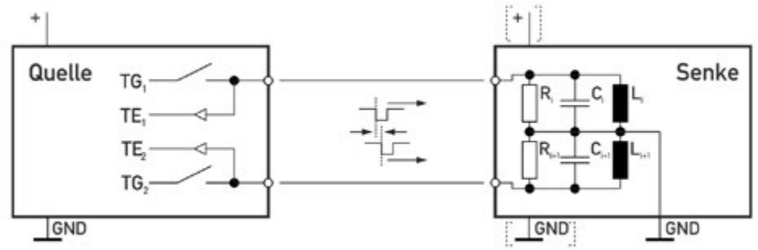
5.4.2 Sicherheitsbezogene digitale Ein-/Ausgänge

Binäre 24-V-Schnittstellen mit dynamischer Testung im Bereich der Funktionalen Sicherheit. Kennzeichnende Merkmale dieser Schnittstellen sind Interface-Typen (siehe ZVEI-Empfehlung 2021.01-Positionspapier CB24I):

- Interface-Typ C (zweikanaliger Ausgang mit Eigenüberwachung, siehe Abbildung 5.3)

Eine Quelle schaltet im eingeschalteten Zustand die Versorgungsspannung auf den Ausgang. Im ausgeschalteten Zustand wird der Ausgang von der Versorgungsspannung getrennt. Im eingeschalteten Zustand sendet die Quelle Testimpulse auf den Ausgang. Die korrekte Funktion des Ausgangs wird in der Quelle selbst überwacht.

Abb. 5.3: Interface-Typ C (zweikanalig)

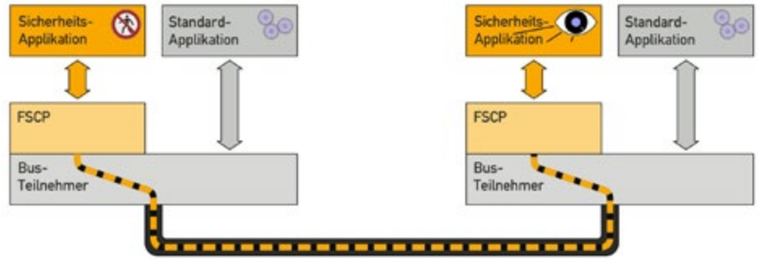


Interface-Typ C wird häufig für „OSSD"-Ausgänge (Output Signal Switching Device) verwendet - z.B. bei Sicherheitsausgängen von Lichtvorhängen.

5.3.4 Funktional sichere Kommunikationsschnittstelle

Die meisten sicherheitsbezogenen Kommunikationsfunktionen folgen dem „Black Channel"- Prinzip. Ein existierender Feldbus wird als Übertragungskanal für einen speziellen Typ von Nachrichten aus Sicherheitsdaten und zusätzlichen Sicherungsmassnahmen genutzt (siehe Abbildung 5.4). Zweck dieser Massnahmen ist die Begrenzung der Restfehlerwahrscheinlichkeit für die Datenübertragung im Betrieb auf das von relevanten Sicherheitsnormen geforderte Maß oder besser.

Abb. 5.4: Black Channel



Die Kommunikationsfunktion erfolgt im Allgemeinen durch serielle Datenübertragung über einen Feldbus (FSCP) oder über eine Punkt-zu-Punkt-Verbindung (SDCI). Für die funktional sichere Kommunikation über Feldbusse wurden mehrere Profile in der IEC 61784-3-x-Serie standardisiert.

6 Schnittstellen zu Sensoren

6.1 Selbsterstellte Teilsysteme

Als Sensoren und Leistungsantriebe werden häufig qualifizierte Teilsysteme verwendet, beispielsweise:

- Sicherheits-Lichtvorhänge
- Sicherheits-Laserscanner
- Servoantriebe mit integrierten Sicherheits-Teilfunktionen [PDS(SR)]

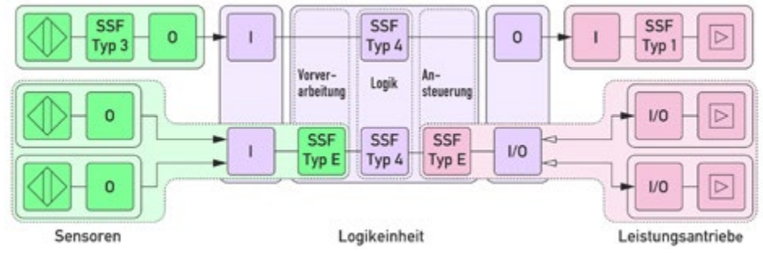
Qualifizierte Teilsysteme führen ihre Diagnosen innerhalb des jeweiligen Teilsystems aus. Andererseits können Teilsysteme als Kombinationen aus diskreten (nicht sicherheitsbezogenen) Komponenten wie Positionsschaltern, Schützen oder Ventilen aufgebaut werden (siehe Abbildung 6.1). Im Fall von solchen selbsterstellten Teilsystemen wird die Diagnose nicht innerhalb des Teilsystems selbst ausgeführt, vielmehr muss sie in der Logikeinheit von der Anwendungssoftware (ASW) realisiert werden.

Idealerweise folgt die sicherheitsbezogene Anwendungssoftware dem allgemeinen Architekturmodell für Software (siehe Bild 7, ISO 13849-1:2015):

- Vorverarbeitung
  Auswerten der Signale von sicherheitsbezogenen Sensoren,
- Logik
  Realisieren der spezifizierten Sicherheits-Teilfunktionen (Logik-Typ 4),
- Ansteuerung
  Steuern und überwachen der Antriebselemente entsprechend den Ergebnissen der Logik.

Für Sensoren kann eine Diagnose nur Informationen aus dem Vergleich oder der zeitlichen Abfolge der Eingangssignale nutzen (Vorverarbeitung). Ausgangsseitig werden für eine Diagnose zusätzliche Signale, wie beispielsweise Stellungsüberwachungen benötigt (Ansteuerung).

Abb. 6.1: Interne/externe Diagnose von Teilsystemen



Bei den Sicherheits-Teilfunktionen von selbsterstellten Teilsystemen handelt es sich um den Logik-Typ E. Der Integrator realisiert das Teilsystem durch Verschaltung von nicht-sicherheitsbezogenen Komponenten. Die Bestimmung des erreichbaren Sicherheitsniveaus liegt in der Verantwortung des Integrators.

Selbsterstellte Teilsysteme aus diskreten Bauteilen besitzen typischerweise keine eigene Logik. Daher lassen sich eine Diagnose und ein Entscheider nicht in solche Teilsysteme selbst integrieren. Diese Funktionalitäten können nur in der Logikeinheit realisiert werden. Die Bestimmung der maximal zulässigen Zeit Δt_{deg} für einen Betrieb im degradierten Zustand muss in diesen Fällen durch den Integrator erfolgen.

Eine qualifizierte Diagnose und einen Entscheider für ein selbsterstelltes Teilsystem in der Logikeinheit zu realisieren, ist in Einzelfällen möglich. In diesem Dokument werden nur Sensoren und Leistungsantriebe als qualifizierte Teilsysteme weiter behandelt.

6.2 Sicherheitsbezogene Sensoren

6.2.1 Übersicht

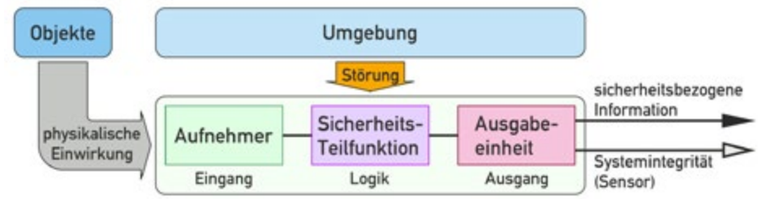
Ein sicherheitsbezogener Sensor (siehe Abbildung 6.2) besteht mindestens aus:

- einer Sensoreinheit (Aufnehmer)
  sie sammelt Informationen über die physikalischen Eigenschaften der Objekte und/oder Umwelteinflüsse und liefert sie als Eingabe für die Verarbeitungseinheit;
- einer Verarbeitungseinheit (Sicherheits-Teilfunktion)
  sie verarbeitet die von der Sensoreinheit erzeugten Informationen, um sicherheitsbezogene Informationen zu erzeugen;
- einer Ausgabeeinheit
  sie stellt sicherheitsbezogene Informationen bereit.

Die Ausgabeeinheit kann ein oder mehrere der folgenden Arten eines elektrischen Signals bereitstellen (siehe 5.4):

- sicherheitsbezogene digitale Ausgänge
- nicht sicherheitsbezogene digitale Ausgänge
- funktional sichere Kommunikationsschnittstelle

Abb. 6.2: Sicherheitsbezogener Sensor



6.2.2 Eigenschaften des Aufnehmers

Die Sensoreinheit gehört nicht zum Anwendungsbereich dieses Dokuments

6.2.3 Funktionalitäten der Sicherheits-Teilfunktion

Kennzeichnende Merkmale der hier beschriebenen Funktionalitäten sind Logik-Typen (siehe ZVEI Whitepaper „Sicherheitsaspekte für Software in industriellen Anwendungen“).

Logik-Typ 1 (eine feste SSF im Gerät):

- Sicherheitsbezogener Sensor (z.B. Näherungsschalter, Lichtvorhang),
- interner Aufbau fix, ohne Möglichkeiten zur Veränderung der SSF.

Logik-Typ 2 (eine von n SSF auswählbar):

- Sicherheitsbezogener Sensor mit mehreren SSF, von denen eine durch Schalter vor der Inbetriebnahme ausgewählt werden muss oder die Auswahl mittels Codierung durch Verdrahtung erfolgt (z.B. für das Auflösungsvermögen des Sensors).

Logik-Typ 3 (parametrierbare SSF):

Variante 1: Auswahl der Sicherheits-Teilfunktion:

- Sicherheitsbezogener Sensor mit mehreren SSF, von denen eine mittels (externem) „Programmiergerät“ vor der Inbetriebnahme ausgewählt und zum Sensor übertragen werden muss.

Variante 2: Auswahl der Parameter:

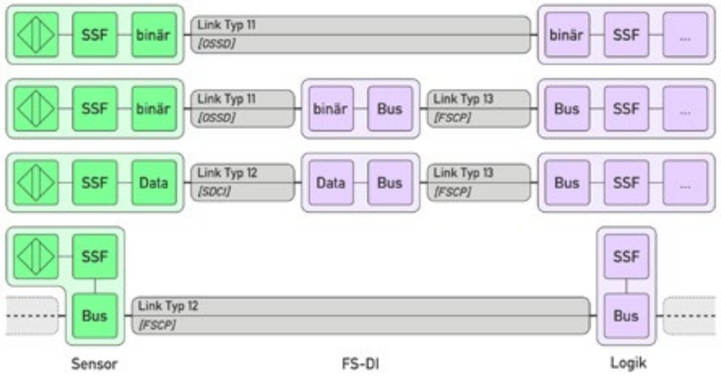
- Sicherheitsbezogener Sensor mit einer oder mehreren SSF (jeweils immer nur eine SSF aktiv), die mittels (externem) „Programmiergerät“ vor der Inbetriebnahme parametriert und die Parameter zum Sensor übertragen werden müssen (z.B. Schutzfeld beim Sicherheits-Laserscanner).

6.3 Klassifizierung von Schnittstellen zu Sensoren

6.3.1 Übersicht

Das Teilsystem „Sensor“ beinhaltet eine qualifizierte Diagnose und einen Entscheider. Anforderungen an die Schnittstelle hängen nicht von dem Logik-Typ des Sensors ab. Kennzeichnende Merkmale der erforderlichen Funktionalitäten sind die nachfolgend definierten Link-Typen.
Folgende Schnittstellen werden betrachtet (siehe Abbildung 6.3):

Abb. 6.3: Link-Typen für Sensorschnittstellen



6.3.2 Link-Typ 11

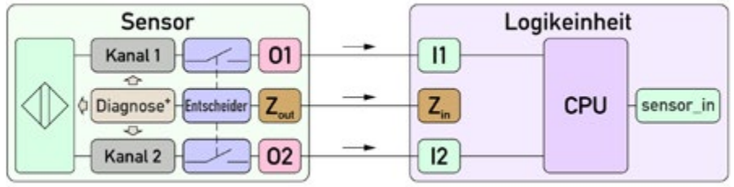
Verwendung

- Verbindung sicherheitsbezogener Sensor mit Steuerung:

Aufbau (siehe Abbildung 6.4):

- Zweikanaliger Ausgang des Sensors (Interface-Typ C),
- Digitaler Ausgang (nicht sicherheitsbezogen) vom Sensor zur Steuerung,
- Sensor enthält qualifizierte Diagnose und Entscheider.

Abb. 6.4: Link-Typ 11



Verhalten:

- Sensor erkennt Fehler (und Zustände, die zu Fehlern führen könnten)
- Wenn der Entscheider im Sensor den Fehler klar zuordnen kann und als tolerierbar beurteilt, werden die Ausgänge nicht abgeschaltet.
- Das Statussignal „Betrieb im degradierten Zustand“ wird über den Meldeausgang zur Verfügung gestellt.
- Nach Ablauf der sensorspezifischen maximal zulässigen Zeit Δt_{deg} werden die Ausgänge abgeschaltet

6.3.3 Link-Typ 12

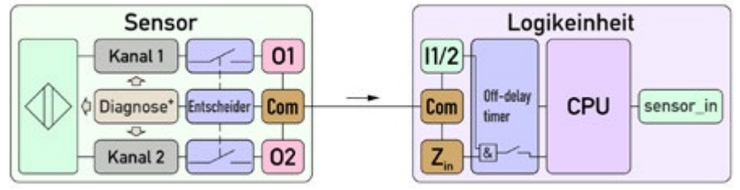
Verwendung:

- Verbindung sicherheitsbezogener Sensor mit Steuerung
- Verbindung sicherheitsbezogener Sensor mit FS-DI

Aufbau (siehe Abbildung 6.5):

- Kommunikation des Sensors mit der Steuerung über
  - eine sicherheitsbezogene serielle Punkt-zu-Punkt Verbindung (SDCI), oder
  - ein sicherheitsbezogenes Feldbusprotokoll (FSCP)
- Sicherheitsbezogene Ausgangsinformation über mindestens ein Datenbit
- Sicherheitsbezogenes Statussignal „Betrieb im degradierten Zustand“ über ein weiteres Datenbit (Qualifier Bit)
  - Qualifier Bit HIGH: Betrieb im degradierten Zustand (Toleranzzeit läuft)
- Zusätzlich können in einem funktionalen Teil des Protokolls Fehlernummern, Langtexte, etc. übertragen werden.
- Sensor enthält qualifizierte Diagnose und Entscheider

Abb. 6.5: Link-Typ 12



Verhalten:

- Sensor erkennt Fehler (und Zustände, die zu Fehlern führen könnten).
- Wenn der Entscheider im Sensor den Fehler klar zuordnen kann und als tolerierbar beurteilt, wird die Ausgangsinformation nicht zurückgesetzt.
- Das Statussignal „Betrieb im degradierten Zustand“ wird an die Steuerung / den FS-DI gemeldet.
- Nach Ablauf der sensorspezifischen maximal zulässigen Zeit Δt_{deg} wird die Ausgangsinformation zurückgesetzt.
- Die Logikeinheit kann mit einem parametriebaren Funktionsbaustein (Off-delay-timer, siehe Anhang A) eine kürzere Begrenzung für den Betrieb im degradierten Zustand applikationsspezifisch vorsehen.

6.3.4 Link-Typ 13

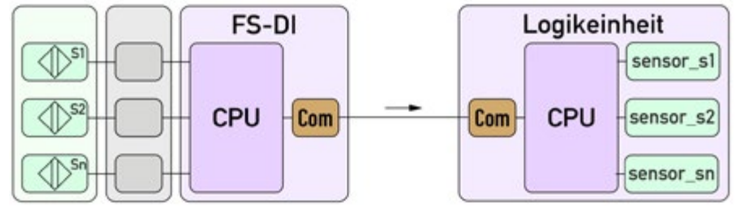
Verwendung:

- Verbindung FS-DI mit Steuerung

Aufbau (siehe Abbildung 6.6):

- Kommunikation des FS-DI mit der Steuerung über
  - einen sicherheitsbezogenen Rückwandbus, oder
  - ein sicherheitsbezogenes Feldbusprotokoll
- „Konzentrator“ für Ausgangs- und Diagnoseinformation aller angeschlossenen Sensoren (Link-Typ 11, 12)
- FS-DI kann für sich selbst optional qualifizierte Diagnose und Entscheider enthalten.

Abb. 6.6: Link-Typ 13



7 Schnittstellen zu Leistungsantrieben

7.1 Sicherheitsbezogene Leistungsantriebe [PDS(SR)]

7.1.1 Übersicht

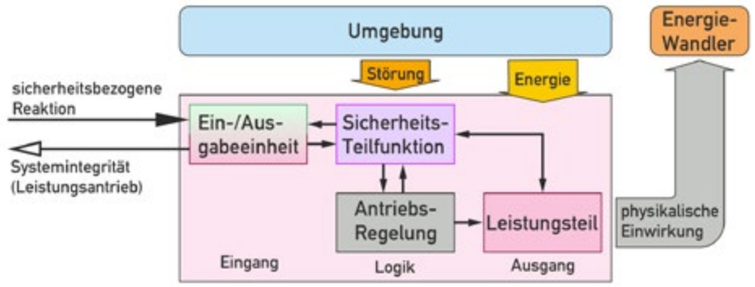
Ein sicherheitsbezogener Leistungsantrieb (siehe Abbildung 7.1) besteht mindestens aus:

- einer Ein-/ Ausgabeeinheit
  sie stellt sicherheitsbezogene Informationen bereit.
- einer Verarbeitungseinheit (Sicherheits-Teilfunktion)
  sie verarbeitet die von der Steuerung empfangenen Informationen, um die Leistungssteuerung zu ermöglichen;
- einem Leistungsteil (Antriebsgrundmodul)
  es regelt die Leistung von der Versorgung zum Energiewandler;

Die Ein-/Ausgabeeinheit kann drei Arten eines elektrischen Signals verarbeiten:

- analoge elektrische Signale (z. B. Strom, Spannung),
- hybride analoge und digitale elektrische Signale (z. B. digitale Schalter und I/O-Link)
- rein digitale Signale (z. B. über ein Feldbusprotokoll).

Abb. 7.1: Sicherheitsbezogene Leistungsantrieb



7.1.2 Eigenschaften des Leistungsteils

Der Leistungsteil gehört nicht zum Anwendungsbereich dieses Dokuments. Bestimmte Leistungsantriebe, wie beispielsweise Robotersteuerungen, benötigen mehrere Leistungsteile, um die unterschiedlichen Achsen parallel zu steuern. Nach außen verhält sich eine solche Steuerung identisch wie ein Leistungsantrieb mit einem einzigen Leistungsteil.

7.1.3 Funktionalitäten der Sicherheits-Teilfunktion

Kennzeichnende Merkmale der hier beschriebenen Funktionalitäten sind Logik-Typen (siehe ZVEI Whitepaper „Sicherheitsaspekte für Software in industriellen Anwendungen“).

Logik-Typ 1 (eine feste SSF im Gerät):

- Sicherheitsbezogener Leistungsantrieb (z.B. Safe Torque Off (STO))
- interner Aufbau fix, ohne Möglichkeiten zur Veränderung der SSF.

Logik-Typ 2 (eine aus n SSF auswählbar):

- Sicherheitsbezogener Leistungsantrieb mit mehreren SSF, von denen eine durch Schalter vor der Inbetriebnahme ausgewählt werden muss oder die Auswahl mittels Codierung durch Verdrahtung erfolgt (z.B. für die Stoppkategorie).

Logik-Typ 3 (parametrierbare SSF):

Variante 1: Auswahl der Sicherheits-Teilfunktion:

- Sicherheitsbezogener Leistungsantrieb mit mehreren SSF, von denen eine mittels (externem) „Programmiergerät“ vor der Inbetriebnahme ausgewählt und zum Sensor übertragen werden muss.

Variante 2: Auswahl der Parameter:

- Sicherheitsbezogener Leistungsantrieb mit einer oder mehreren SSF (jeweils immer nur eine SSF aktiv), die mittels (externem) „Programmiergerät“ vor der Inbetriebnahme parametriert und die Parameter zum Sensor übertragen werden müssen (z.B. Bremsrampe).

Logik-Typ 4 (mehrere SSF mit Kommunikation):

- Sicherheitsbezogener Leistungsantrieb mit mehreren (aktiven) SSF, die mittels (externem) „Programmiergerät“ vor der Inbetriebnahme ausgewählt, gegebenenfalls Ein-/ Ausgabe-konfiguriert (Software-Verdrahtung) und parametriert werden müssen und die Konfiguration zum Schaltgerät übertragen werden muss.

7.1.4 Sicherheits-Teilfunktionen von Leistungsantrieben

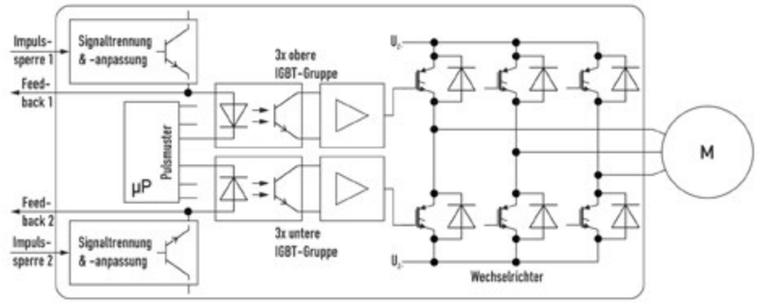
Üblicherweise führen sicherheitsbezogene Sensoren (siehe Kapitel 5.2) jeweils nur eine einzelne Sicherheits-Teilfunktionen aus. Im Gegensatz hierzu können Leistungsantriebe unterschiedliche SSF gleichzeitig ausführen (für weitere Details siehe IEC 61800-5-2). Diese lassen sich in zwei Gruppen einteilen:

- Stopp-Funktionen,
  Funktion zum Stillsetzen von Antrieben:
  - Sicher abgeschaltetes Drehmoment (en: safe torque off, STO),
  - Sicherer Stopp 1 (en: safe stop 1, SS1),
  - Sicherer Stopp 2 (en: safe stop 2, SS2).

- Überwachungsfunktionen,
  Funktion zum Überwachen von Antriebsparametern:
  - Verhindern des Über-/Unterschreitens eines einzelnen Grenzwerts.
  - Einhalten eines Bereichs innerhalb festgelegter Grenzwerte.
  - Das Ansprechen einer Überwachungsfunktion löst in der Regel eine Stopp-Funktion aus.

Die SSF „STO“ nimmt in einem Leistungsantrieb eine Sonderrolle ein. Diese SSF wird im Allgemeinen als Impulssperre ausgeführt (siehe Abbildung 7.2). Sie ist die gemeinsame sicherheitsgerichtete Ausfallreaktion für alle weiteren in den Antrieb integrierten Teilfunktionen. Üblicherweise wird STO mit zwei Kanälen realisiert (weitere Details Kapitel 4.2.2, IFA Report 4/2018). Dabei sperrt jeder Kanal die Hälfte der Impulssignale zu den Leistungstransistoren (IGBT).

Abb. 7.2: Impulssperre (Quelle: IFA Report 4/2018)



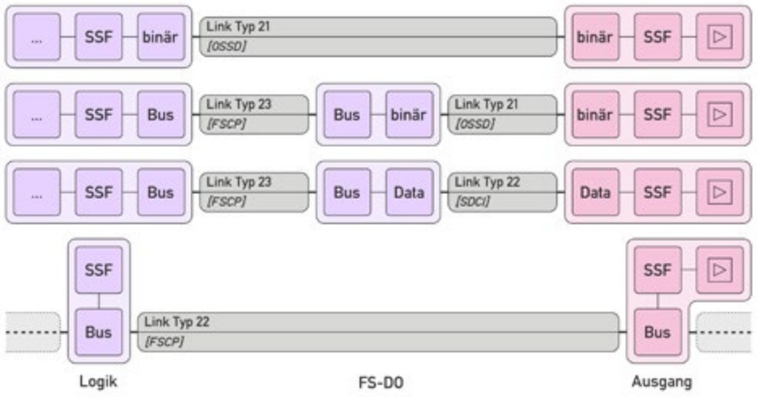
Es ist möglich, für die SSF „STO“ ebenfalls einen Betrieb im degradierten Zustand zu integrieren. Tatsächlich sollte aber hier jeder Fehler sofort zur Abschaltung führen.

7.2 Klassifizierung von Schnittstellen zu Leistungsantrieben

7.2.1 Übersicht

Das Teilsystem „Leistungsantrieb“ beinhaltet eine qualifizierte Diagnose und einen Entscheider. Anforderungen an die Schnittstelle hängen nicht vom Logik-Typ des Leistungsantriebs ab. Kennzeichnende Merkmale der erforderlichen Funktionalitäten sind die nachfolgend definierten Link-Typen. Folgende Schnittstellen werden betrachtet (siehe Abbildung 7.3):

Abb. 7.3: Link-Typen für Leistungsantriebe



7.2.2 Link-Typ 21

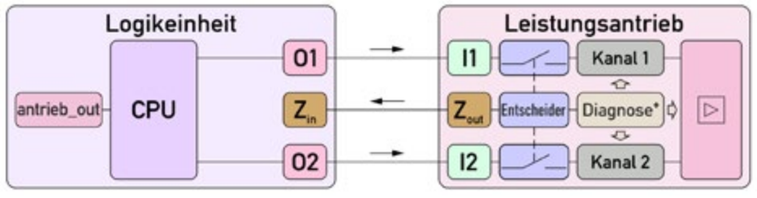
Verwendung:

- Verbindung Steuerung mit Leistungsantrieb:

Aufbau (siehe Abbildung 7.4):

- Zweikanaliger Ausgang der Steuerung (Interface-Typ C).
- Digitaler Ausgang (nicht sicherheitsbezogen) vom Leistungsantrieb zur Steuerung.
- Leistungsantrieb enthält qualifizierte Diagnose und Entscheider.

Abb. 7.4: Link-Typ 21



Verhalten:

- Leistungsantrieb erkennt Fehler (und Zustände, die zu Fehlern führen könnten).
- Wenn der Entscheider im Leistungsantrieb den Fehler klar zuordnen kann und als tolerierbar beurteilt, wird der Leistungsteil nicht abgeschaltet.
- Das Statussignal „Betrieb im degradierten Zustand“ wird über den Meldeausgang zur Verfügung gestellt.
- Nach Ablauf der gerätespezifischen maximal zulässigen Zeit Δt_{deg} wird der Leistungsteil abgeschaltet

7.2.3 Link-Typ 22

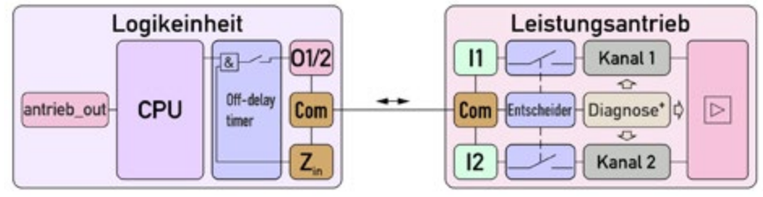
Verwendung:

- Verbindung Steuerung mit Leistungsantrieb
- Verbindung FS-DO mit Leistungsantrieb

Aufbau (siehe Abbildung 7.5):

- Kommunikation Steuerung mit Leistungsantrieb über:
  - eine sicherheitsbezogene serielle Punkt-zu-Punkt Verbindung (SDCI),
  - ein sicherheitsbezogenes Feldbusprotokoll (FSCP).
  - Sicherheitsbezogene Ausgangsinformation über mindestens ein Datenbit.
  - Sicherheitsbezogenes Statussignal „Betrieb im degradierten Zustand“ über ein weiteres Datenbit (Qualifier Bit)
  - Qualifier Bit HIGH: Betrieb im degradierten Zustand (Toleranzzeit läuft).
  - Zusätzlich können in einem funktionalen Teil des Protokolls Fehlernummern, Langtexte, etc. übertragen werden.
  - Leistungsantrieb enthält qualifizierte Diagnose und Entscheider.

Abb. 7.5: Link-Typ 22



Verhalten:

- Leistungsantrieb erkennt Fehler (und Zustände, die zu Fehlern führen könnten).
- Wenn der Entscheider im Leistungsantrieb den Fehler klar zuordnen kann und als tolerierbar beurteilt, wird der Leistungsteil nicht abgeschaltet.
- Das Statussignal „Betrieb im degradierten Zustand“ wird an die Steuerung / den FS-DO gemeldet.
- Nach Ablauf der gerätespezifischen maximal zulässigen Zeit Δtdeg wird der Leistungsteil abgeschaltet.
- Die Logikeinheit kann mit einem parametriebaren Funktionsbaustein (Off-delay-timer, siehe Anhang A) eine kürzere Begrenzung für den Betrieb im degradierten Zustand applikationsspezifisch vorsehen.

7.2.4 Link-Typ 23

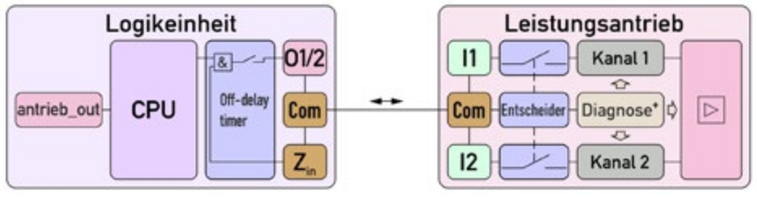
Verwendung:

- Verbindung Steuerung mit FS-DO

Aufbau (siehe Abbildung 7.6):

- Kommunikation der Steuerung mit dem FS-DO über:
  - einen sicherheitsbezogenen Rückwandbus,
  - ein sicherheitsbezogenes Feldbusprotokoll.
- „Konzentrator“ für Ausgangs- und Diagnoseinformation aller angeschlossenen Leistungsantriebe (Link-Typ 21, 22)
- FS-DO kann für sich selbst optional qualifizierte Diagnose und Entscheider enthalten.

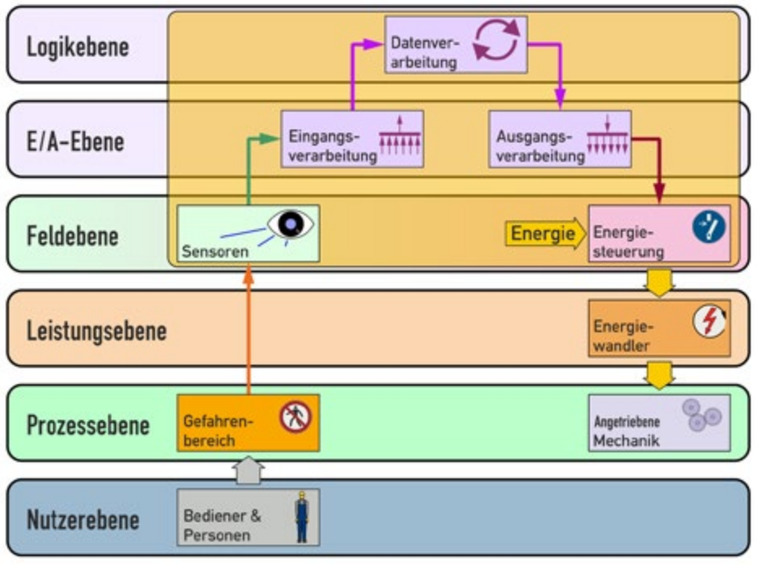
Abb. 7.6: Link-Typ 23



8 Fazit und Ausblick

Eine Maschine ist ein komplexes technisches Arbeitsmittel (EUC) mit einer Hauptfunktion, beispielsweise Aufbereiten, Behandeln oder Verarbeiten von Arbeitsgegenständen durch Wirkbewegungen. Sie ist gekennzeichnet durch eine funktionelle Verkettung von Mechanismen zum Umwandeln von Energiearten (siehe Abbildung 8.1).
Das Arbeitsmittel wird gesteuert und überwacht durch ein EUC-Steuerungssystem, das auf Eingangssignale des Prozesses und/oder eines Bedieners reagiert und Ausgangssignale erzeugt, welche die Betriebsmittel in der gewünschten Art arbeiten lassen.

Abb. 8.1: EUC-Steuerungssystem



Die Verarbeitungseinheit einer sicherheitsbezogenen Logikeinheit kann ebenfalls eine qualifizierte Diagnose und einen Entscheider für sich selbst beinhalten. Dabei muss sichergestellt sein, dass sie jederzeit einen zeitlich begrenzten Betrieb der gesamten Sicherheitsfunktion im degradierten Zustand gewährleisten kann.

Im Fall von selbsterstellten Teilsystemen aus nicht sicherheitsbezogenen Komponenten können sicherheitsbezogene Logikeinheiten eine qualifizierte Diagnose ausführen und den Entscheider beinhalten, wenn sie selbst die Vorverarbeitung von Sensorsignalen oder die Ansteuerung von Leistungsantrieben durchführen.

Das Statussignal „Betrieb im degradierten Zustand“ wird entsprechend der verwendeten Schnittstelle (Link-Typ) als Meldesignal oder als sicherheitsbezogenes Signal übertragen.

Weitergehende Fragestellungen zur Integration in Produkte werden in einem ergänzenden Dokument „Fehlertoleranz in der Maschinensicherheit Teil 3 – Integration“ ausgeführt.

Die Ausführungen zeigen, dass die Umsetzung eines zeitlich begrenzten Betriebs mit degradierter Sicherheits-Teilfunktion in sicherheitsbezogenen Sensoren und Leistungsantrieben im Einklang mit den Schutzzielen der Maschinenrichtlinie möglich ist und nicht im Widerspruch zu den harmonisierten Normen ISO 13849 bzw. IEC 62061 steht.

Ein Betrieb im degradierten Zustand bricht – normkonform – mit dem Dogma der sofortigen Energietrennung im Fehlerfall. Dies erhöht die Sicherheit und Verfügbarkeit von Maschinen und Anlagen:

- Verringerung von Manipulationsanreizen.
- Keine Folgeschäden durch Abschalten zur Unzeit.
- Steigerung der Produktivität.
- Anlassbezogene Wartung ohne Ausfallzeiten.

In diesem Dokument ist die Basis für die Umsetzung einer qualifizierten Diagnose und eines Entscheiders in sicherheitsbezogenen Produkten beschrieben, um den Betrieb einer Maschine/Anlage im degradierten Zustand zu ermöglichen.

Anwender und Hersteller sind aufgefordert, diese Vorteile in Maschinen umzusetzen.

Anhang A Funktionsbaustein „Off-Delay Timer“

A.1 Funktionsbaustein

Abb. A.1: FB „Off-delay Timer“

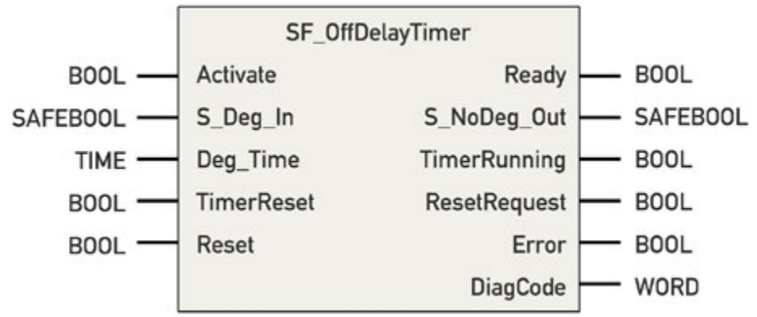


Tabelle A.1: Interfacebeschreibung

FB Name	SF_OffDelayTimer		
Ein FB SF_OffDelayTimer ermöglicht es, applikationsbezogen kürzere Zeiten als ΔT_{max} für den degradierten Betrieb zu realisieren. Das Ausgangssignal des FBs wird nach Ablauf der parametrierten Zeit ausgeschaltet. Die Zeit ΔT_{max} ist fest vorgegeben mit 48h.			
VAR_INPUT			
Name	**Data Type**	**Initial Value**	**Description, Parameter Values**
Activate	BOOL	FALSE	Siehe PLCOpen Dokumentation
S_Deg_In	SAFE-BOOL	FALSE	Variable. Eingang des Entscheiders FALSE: Degradierter Betrieb ist nicht angewählt. TRUE: Degradierter Betrieb ist angewählt, Timer läuft ab.
Reset	BOOL	FALSE	Siehe PLCOpen Dokumentation
TimerReset	BOOL	FALSE	Eingang zum Rücksetzen des Timers von der Auswertelogik her (optional).
DegTime	TIME	T#0h	Wertebereich: 0 … 48h (2880min) Countdown degradierte Betriebszeit.
VAR_OUTPUT			
Ready	BOOL	FALSE	Siehe PLCOpen Dokumentation
S_NoDeg_Out	SAFE-BOOL	TRUE	Safety related output signal. TRUE: Timer ist abgelaufen, maximale Betriebszeit ist erreicht. FALSE: Timer ist nicht gestartet oder läuft.
TimerRunning	BOOL	FALSE	FALSE: Timer ist nicht gestartet TRUE: Timer läuft
ResetRequest	BOOL	FALSE	Optional. Siehe PLCOpen Dokumentation
Error	BOOL	FALSE	Siehe PLCOpen Dokumentation
DiagCode	WORD	#0000	Siehe PLCOpen Dokumentation
Notes: 1. Reset-Eingang, da Baustein optional per Software zurückgesetzt werden können soll. 2. Ausgang TimerRunning als Meldeausgang für den Benutzer, um rechtzeitig Korrekturmaßnahmen einleiten zu können.			

Quelle: ZVEI

Abb. A.2: Zustandsübergangsdiagramm

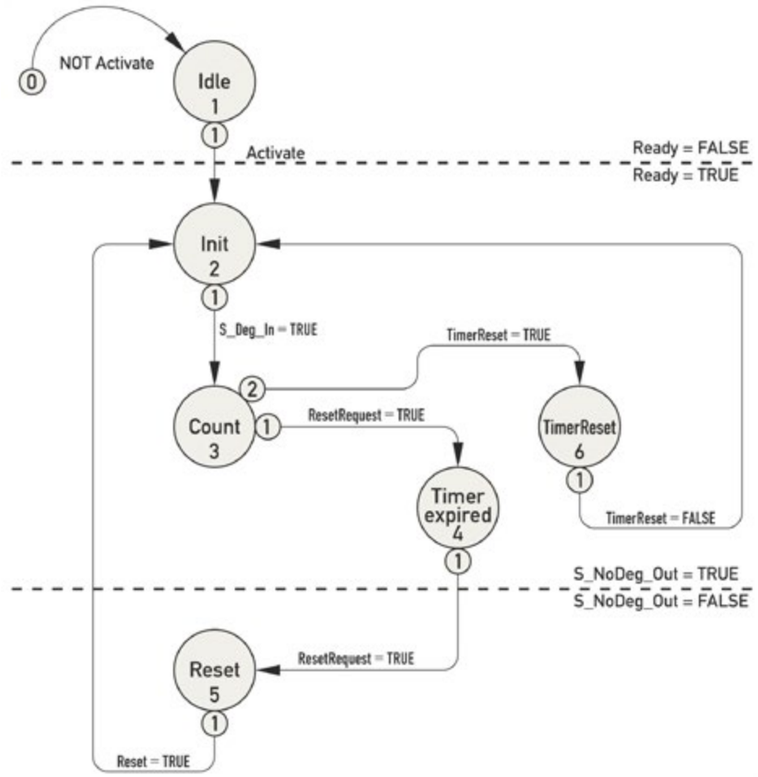
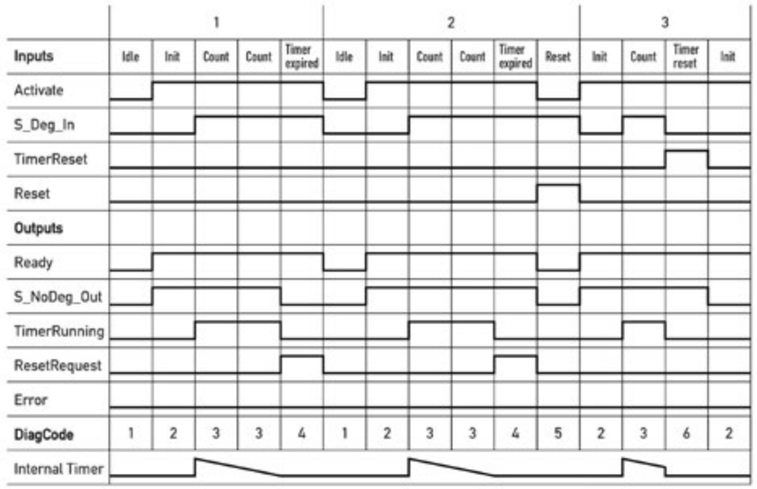


Tabelle A.2: Spezifische Fehlercodes

DiagCode	Name Status	Statusbeschreibung und Ausgangszustand
1	Idle	Der Funktionsblock ist inaktiv (Initialstatus) Ready = FALSE S_NoDeg_Out = FALSE TimerRunning = FALSE ResetRequest = FALSE
2	Init	Der Entscheider ist bereit, degradierter Betrieb ist nicht aktiviert Ready = TRUE S_NoDeg_Out = TRUE TimerRunning = FALSE ResetRequest = FALSE
3	Count	Degradierter Betrieb wurde aktiviert, Zeit läuft ab Ready = TRUE S_NoDeg_Out = TRUE TimerRunning = TRUE ResetRequest = FALSE
4	Timer expired	Zeit ist abgelaufen, Anforderung der Abschaltung Ready = TRUE S_NoDeg_Out = FALSE TimerRunning = FALSE ResetRequest = TRUE
5	Reset	Rücksetzen des Bausteins nach Ablauf des Countdowns Ready = FALSE S_NoDeg_Out = FALSE TimerRunning = FALSE ResetRequest = FALSE
6	Timer reset	Countdown wird zurückgesetzt und kann neu gestartet werden Ready = TRUE S_NoDeg_Out = FALSE TimerRunning = FALSE ResetRequest = FALSE

Abb. A.3: Timingdiagramm



Legende:
1: Ablauf des Timers nach Aktivierung S_Deg_In und Reset der Steuerung
2: Ablauf des Timers nach Aktivierung S_Deg_In und Reset des Funktionsbausteins
3: Rücksetzen des Timers vor Ablauf

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