8 Kenngrößen eines Sicherheitssystems

Dieses Kapitel beschreibt die quantitativen Stufen der Sicherheit, die Erfüllung der notwendigen Maßnahmen zur Risikominderung und die hierzu verwendeten Kenngrößen. Diese Kenngrößen lassen sich in unterschiedlicher Abstufung zu einem Maßnahmenbündel zusammenfassen, so dass Sicherheitssysteme entstehen, die das notwendige Maß an Sicherheit garantieren und somit auch den Anforderungen der Norm entsprechen.

8.1 Quantifizierung der Sicherheit

Die Höhe der Anforderungen richtet sich nach dem Risiko oder dem Gefährdungspotenzial, das von der jeweiligen Anwendung ausgeht. Dies führt dazu, den größten Teil der sicherheitsgerichteten Anwendungen in Klassen einzuteilen. An diese Klassen werden die gleichen Anforderungen bezüglich der Sicherheit gestellt. Es gilt Kriterien zu finden, die exakt diese Klassen definieren. Ein mögliches Kriterium ist die Wahrscheinlichkeit für ein gefährliches Versagen, das bei einer bestimmten Anwendung noch toleriert wird. Im Bild 8.1 wird das tatsächlich verbleibende Risiko auch als „Restrisiko" bezeichnet.

Das heute in der Normung gewählte Verfahren zu einer anwendungsunabhängigen Klassenbildung basiert auf einer grundsätzlichen Risikobetrachtung, wie sie in der DIN VDE 31000 beschrieben ist, und aus dem Bild 8.1 hervorgeht.

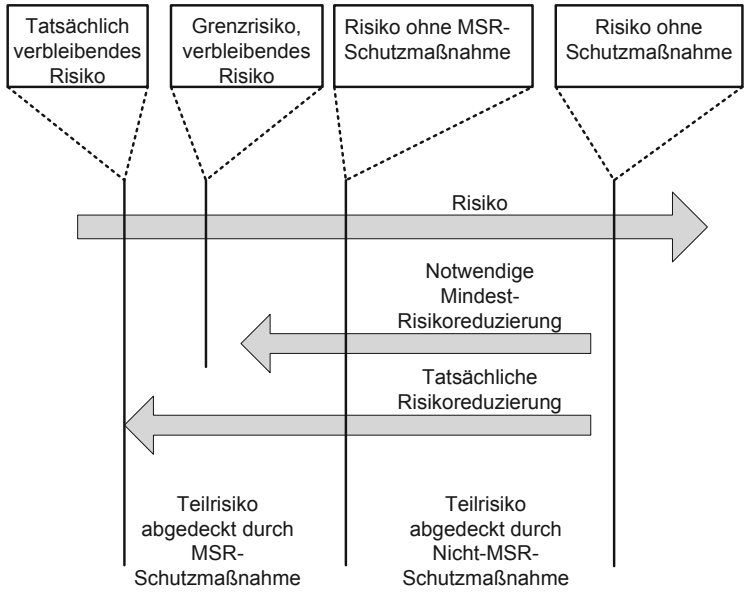

Bild 8.1 Risikoreduzierung durch Nicht-MSR- und MSR-Maßnahmen (MSR: Messen, Steuern, Regeln)

Das Risiko (*R*) ergibt sich dabei durch eine Wahrscheinlichkeitsaussage, die die zu erwartende Häufigkeit (*H*) des Eintritts eines Schadens und das zu erwartende Schadensausmaß (*S*) nach der folgenden Berechnung berücksichtigt[16]:

$$R = H \cdot S$$

Um nun eine Abstufung in unterschiedliche Anforderungsklassen zu erhalten, ist es erforderlich, ein Verfahren zur Bestimmung des Risikos einzuführen. Hierzu bieten sich mehrere Möglichkeiten an, die heute vorwiegend durch eine Analyse des Risikografen abgedeckt werden (siehe Abschnitte 7.1 und 7.2).

Die Sicherheitseinrichtung hat die Aufgabe, das Risiko einer Maschine oder Anlage soweit herabzusetzen, dass man mit einem verbleibenden Restrisiko leben kann. Dabei hat sich der SIL-Begriff durchgesetzt, der eine Risikoreduzierung jeweils um den Faktor 10 bringt. Die SIL-Angabe ist damit lediglich der Exponent zur Basis 10 desjenigen Faktors, den das Sicherheitssystem zur Risikominderung beiträgt.

SIL 1 Faktor 10

SIL 2 Faktor 100

SIL 3 Faktor 1 000

SIL 4 Faktor 10 000

Um eine messbare Größe zur unabhängigen Sicherheitsbeurteilung zu erhalten, verbindet man die Anforderungsrate mit einer Zeiteinheit. Dabei wird angenommen, dass eine Sicherheitsanforderung höchstens einmal pro Jahr auftritt. Damit sollte ein SIL-2-System höchstens eine gefahrvolle Ausfallrate von 10^{-2} pro Jahr haben[17]. Anders ausgedrückt: Die mittlere Lebenszeit, bevor ein Versagen auftritt, sollte größer als 100 Jahre sein. Häufig wird das Zeitintervall auch mit dem Begriff MTTF verbunden (MTTF: Mean Time To Failure). Hier ist die mittlere Zeitdauer gemeint, die vergeht, bis ein Fehler auftritt,

SIL 2: Höchstens ein gefahrvolles Versagen innerhalb von 100 Jahren,
$MTTF_d$: 100 Jahre[18]

Freilich gibt es auch zahlreiche Sicherheitssysteme, die öfter als einmal pro Jahr gebraucht werden oder gar ununterbrochen arbeiten. Beispielsweise muss ein Lichtgitter dauernd prüfen, ob nicht eine Person ihre Hände oder Arme im gefahrvollen Bereich hat, bevor ein Schneid- oder Pressvorgang gestartet wird. Bei derartigen Anwendungen macht es keinen Sinn mehr, eine Versagensrate pro Anforderung anzugeben. Hier verwendet man den sogenannten PFH-Wert, der die Ausfallrate pro Sunden angibt (PFH: Probability Failure per Hour)[19].

---

16) Die Bewertung des Risikos wurde bereits ausführlich in Abschnitt 2.1 beschrieben.

17) In manchen Normen wird der Begriff PFD (Probability for Failure on Demand) verwendet. Hierbei ist die Wahrscheinlichkeit gemeint, dass ein System auf eine Anforderung nicht reagiert.

18) In der Sicherheitstechnik ist man bei allen Berechungen in der Regel an den „gefahrvollen" Kenngrößen interessiert. Sie tragen den Index „d".

19) Die Zuordnung zwischen dem PFD- und dem PFH-Wert gelingt dann durch die Zuordnung zwischen der Zeiteinheit Jahr und Stunde. Da ein Jahr ca. 10000 Stunden (oder genau 8 760) hat, liegt zwischen dem PFD- und PFH-Wert ein Faktor von 10^4.

Hier ist anzumerken, dass sowohl der PFD- als auch der PFH-Wert dimensionslos sind. Im Gegensatz hierzu ist die Ausfallrate (λ) auf ein Zeitintervall bezogen und hat damit die Dimension 1/h.

Der Begriff SIL als Maß der Risikoreduzierung für das Sicherheitssystem wird nicht von der Norm DIN EN ISO 13849 verwendet. Allerdings lässt sich zumindest für die tolerable maximale Ausfallrate zwischen den Normen IEC 61508, DIN EN IEC 62061 und DIN EN ISO 13849 ein Vergleich herstellen. Dieser Zusammenhang wird in der folgenden Tabelle 8.1 dargestellt. Dabei ist anzumerken, dass die Gegenüberstellung der maximalen Ausfallraten von SIL und PL mit Vorsicht zu genießen ist. So gibt es für SIL 4 kein Pendant als Performance Level. Ferner fehlen für die PL „a" und „b" zugehörige SIL-Einstufungen. Außerdem bezieht sich die PL-Einstufung stets auf das gesamte Sicherheitssystem mit Mechanik und Elektrik. Bei der Einstufung nach SIL ist nur die Elektrik oder Elektronik einbezogen.

Tabelle 8.1 Bezug zwischen SIL und PL für die maximalen Ausfallraten

SIL	PL	PFH (pro Stunde)
4		10^{-9} bis < 10^{-8}
3	e	10^{-8} bis < 10^{-7}
2	d	10^{-7} bis < 10^{-6}
1	c	10^{-6} bis < 10^{-5}

8.2 Quantitative Kenngrößen

Zur Beurteilung der Sicherheit eines Systems oder einer Komponente gibt es aus technischer Sicht lediglich die bereits in Abschnitt 7.3 genannten Kenngrößen:

Tabelle 8.2 Kenngrößen zur Beurteilung der Sicherheit

Kenngröße	Definition	Bedeutung
Architektur, Struktur	Architekturen bestimmen die Eignung für die Applikation.	Die gewählte Architektur bestimmt die Fehlertoleranz. Eine einkanalige Struktur reagiert bei jedem Fehlerfall mit einem Ausfall. Ein Großteil dieser Ausfälle führt zu Sicherheitsversagen der gesamten Schaltung. HFT: Hardwarefehlertoleranz
λ, MTTF	Der Lambda-Wert ist die Ausfallrate. Der MTTF-Wert gibt die mittlere Lebensdauer an.	Die Ausfallrate (λ) ist eine der signifikanten Kenngrößen von Sicherheitssystemen. Sicherheitssysteme sollten nur Bauteile mit sehr niedrigen λ-Werten enthalten, damit Fehler nur selten auftreten. Die Ausfallraten werden in fit (fit: Failure in Time) angegeben. Dabei ist 1 fit = 1 Ausfall/10^9 Stunden.

Tabelle 8.2 (Fortsetzung) Kenngrößen zur Beurteilung der Sicherheit

Kenngröße	Definition	Bedeutung
		Ausfallrate und Lebensdauer sind zueinander reziprok. Wobei sich der λ-Wert zumeist auf das Zeitintervall von einer Stunde, der MTTF-Wert aber auf ein Intervall von einem Jahr bezieht.
DC	Diagnosedeckungsgrad (Diagnostic Coverage)	Der Diagnosedeckungsgrad ist ein Maß für die Erkennung möglicher Fehler durch Tests.
β, CCF	Fehler mit gemeinsamer Ursache (Common-Cause-Fehler)	Ein Design für Sicherheit sollte einen niedrigen β-Wert aufweisen, damit ein Fehler nicht zum Gesamtversagen der Sicherheitsfunktion führt.

Die Kombination der Kenngrößen in geeigneter Form führt zum geforderten Sicherheitssystem, das eine Reduzierung des vorhandenen Risikos garantiert.

Ein einfaches Beispiel soll die vier genannten Kenngrößen in einen Zusammenhang bringen: Ein Sicherheitssystem muss einen Antrieb abschalten, wenn man einen Not-Halt-Taster betätigt. Damit die Möglichkeit besteht, auch eine Abschaltung zu erwirken, wenn ein Abschaltweg ausgefallen ist, soll ein zweiter Abschaltweg existieren. Ein eventuelles Versagen des Not-Halt-Tasters oder der dazugehörigen Eingangsschaltung wird durch eine Zweikanaligkeit unterbunden (Bild 8.2)[20].

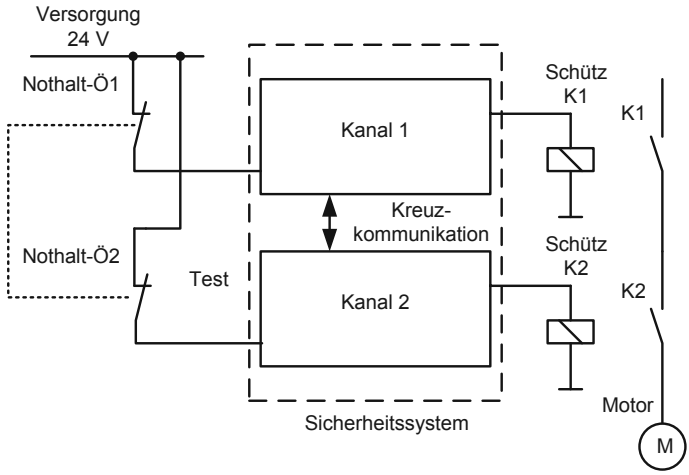

Bild 8.2 Beispiel eines zweikanaligen Sicherheitssystems

Wie Bild 8.2 darstellt, verwendet das Sicherheitssystem einen zweikanaligen Not-Halt-Taster zur Bedienung. Wenn ein Kontakt des Not-Halt-Tasters versagt, steht ein weiterer zur Verfügung.

[20] Anstatt des Not-Halt-Tasters kann man auch einen oder zwei Türschalter anschließen und so eine Abschaltung des Antriebs erreichen, wenn die Türe geöffnet wird.

Gegen Fehler bei der logischen Verarbeitung (Sicherheitsgerät) hilft auch hier eine Zweikanaligkeit. Wenn – einmal angenommen – der Eingang 1 (Eing. 1) ausfällt, kann dann noch eine sichere Abschaltung über den anderen Kanal (Kanal 2 mit Eing. 2) erfolgen. Auch ein mögliches Versagen eines der beiden Ausgänge (Ausg. 1 oder Ausg. 2) hat keine fatalen Folgen, da stets noch ein weiterer Kanal mit dem noch intakten Ausgang zur Verfügung steht. In dem Schaltungsbeispiel nach Bild 8.2 steuern die beiden Ausgänge (Ausg. 1 und Ausg. 2) jeweils getrennte Relais an (K1 und K2), deren Kontakte den Antrieb über eine Serienschaltung mit Strom versorgen.

Wenn alle Bauteile und Komponenten einwandfrei funktionieren, dann handelt es sich bei der dargestellten Schaltung um eine zweikanalige fehlertolerante Struktur. Ein einzelner Fehler führt nicht zum Verlust der Sicherheitsfunktion. Nach der Norm DIN EN ISO 13849-1 würde diese Einheit der Kategorie 3 entsprechen. Es ist eine besondere Eigenschaft der gezeigten Schaltung, dass im Fehlerfall immer eine Abschaltung erfolgt. Ein Kanal alleine kann das System in den sicheren Zustand versetzen, auch wenn der andere versagt hat. Die Technik ist damit für Sicherheitsapplikationen, nicht aber für Verfügbarkeitsapplikationen geeignet.

Natürlich garantiert die Immunität gegenüber einem Einzelfehler noch keine extrem hohe Eignung für alle Sicherheitseinrichtungen. Es besteht ja die Möglichkeit, dass nach einer gewissen Zeit zuerst der Eingang 1 von Kanal 1 und nach einem weiteren Zeitintervall der Ausgang von Kanal 2 (Ausg. 2) ausfällt. Innerhalb dieser Fehlerkombination würde der obere Kanal (Kanal 1) die Sicherheitsanforderung des Not-Halt-Tasters nicht erkennen. Der untere Kanal (Kanal 2) stellt zwar die Not-Halt-Anforderung fest, er ist aber nicht mehr in der Lage, den Antrieb abzuschalten, da sein Ausgang defekt ist. Eine derartige Fehleranhäufung ist zwar unwahrscheinlich, aber sie kommt durchaus vor und hängt von der Ausfallrate der verwendeten Bauteile ab.

Wenn die Ausfallrate der Bauteile nicht allzu hoch ist, besteht durchaus die Möglichkeit, die sicherheitskritischen Bauteile der Schaltung auf Fehlerfreiheit zu prüfen. Sollte also der Eingang des Kanals 1 ausgefallen sein und wird dieses erkannt, bevor der Ausgang von Kanal 2 versagt, besteht kein Sicherheitsrisiko. Man erkennt hierbei recht leicht den fundamentalen Zusammenhang zwischen der Ausfallrate von Bauteilen und der Häufigkeit der Prüfung: Je unwahrscheinlicher ein Bauteilausfall ist, desto seltener muss man das Bauteil in der Sicherheitskette prüfen.

Jegliches Prüfen von Bauteilen oder Komponenten versagt genau an denjenigen Stellen, an denen ein einzelner Ausfall zu einer völligen Blockade der Sicherheitsfunktion führt. Beispielsweise können sich die beiden Relais K1 und K2 in einer Einheit befinden, die durch eine äußere Einwirkung beide Relais zerstört. Dies kann eventuell dadurch geschehen, dass ein externer Schock (Schlag) beide Relais schädigt oder dass in die Einheit eine klebrige Flüssigkeit hineinläuft, die beide Relais gleichzeitig festsetzt. Derartige Fehler mit gemeinsamer Ursache (Common-Cause-Fehler) sind daher besonders kritisch zu betrachten und in jedem Fall zu vermeiden.

8.2.1 Die Struktur des Sicherheitssystems

Die Struktur eines Sicherheitssystems stellt die wichtigste Kenngröße dar. Einkanalige Strukturen bestehen aus eine Kette hintereinander gereihter Einheiten, die in ihrer Gesamtheit die Sicherheitsfunktion bestimmen (Bild 8.3).

Die Sicherheitsfunktion besteht dabei oftmals aus dem Sensor, der die Messgröße für die Sicherheit erfasst, der Eingangsschaltung, der Logik, die für die Verarbeitung sorgt, der Ausgabe und schließlich aus dem Aktuator, der für die Ausführung der Sicherheitsfunktion verantwortlich ist.

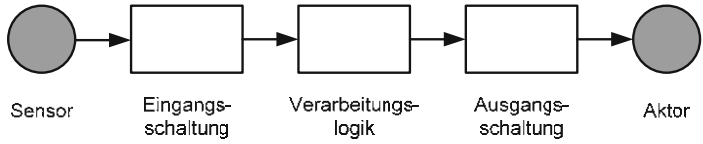

Bild 8.3 Typische Ausprägung einer einkanaligen Struktur

Einkanalige Strukturen können in fataler Art und Weise ausfallen, so dass eine sichere Abschaltung (als gewünschte Sicherheitsfunktion) nicht mehr funktioniert.

Daher ist eine einkanalige Struktur gegenüber Fehlern nicht immun. Die Hardwarefehlertoleranz (HFT) hat den Wert 0: HFT = 0.

Eine zweikanalige Struktur ist (im Gegensatz zu einer einkanaligen Struktur) gegenüber Fehlern immun. Im Falle eines Ausfalls oder eines Versagens ist der jeweils andere Kanal noch in der Lage eine Sicherheitsfunktion auszuführen (Bild 8.4).

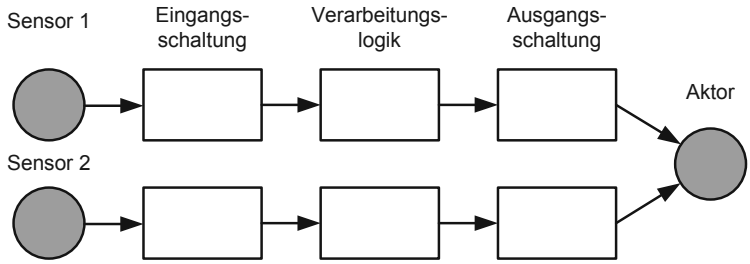

Bild 8.4 Typische Ausprägung einer zweikanaligen Struktur

Die Hardwarefehlertoleranz ist damit 1, weil ein einzelner Fehler nicht direkt zu einem Versagen führt: HFT = 1.

Die Grafik in Bild 7.5 (nach der Norm DIN EN ISO 13849) zeigt in den Kategorien B, 1 und 2 einkanalige und in den Kategorien 3 und 4 zweikanalige Strukturen[21)].

Die Ausprägung einer Struktur wird auch manchmal mit Nummernbezeichnungen dargestellt. Hierbei verwendet man:

XooY: X Kanäle, die notwendig für die Abschaltung sind, und
Y Kanäle, die überhaupt vorhanden sind

[21)] Auch das Auftreten eines einzelnen oder gar mehrerer Fehler in einer einkanaligen Struktur führt nicht unbedingt in einen fatalen Zustand. Es besteht auch die Möglichkeit, dass die Struktur im sicheren Zustand ausfällt. Dann ist sie zwar „sicher" aber nicht mehr „verfügbar". Auch zweikanalige Strukturen können durch einen Einzelfehler fatal ausfallen. Beispielweise kann sich ein Fehler auf beide Kanäle gleichzeitig auswirken und diese gemeinsam in einen fatalen Zustand versetzen. Diese Fehler werden „Fehler gemeinsamer Ursache" genannt (vgl. Abschnitt 8.2.4).