3 Kenngrößen für die Sicherheitsbewertung

Gegenüber Standardsystemen zeichnen sich Sicherheitssysteme durch die Einhaltung bestimmter Kriterien aus, die für die spezielle Applikation zur Einhaltung der Sicherheit notwendig sind. In der Regel enthalten Sicherheitssysteme fehlertolerante Strukturen, damit nicht jedes Versagen sofort zu einem fatalen Fehler führt. Im Grunde gibt es nur ganz wenige Kenngrößen, die über die Tauglichkeit eines Sicherheitssystems Auskunft geben.

Erstens ist die Struktur des Systems maßgeblich. Einkanalige Architekturen können bei jedem Fehler zum Ausfall führen. Wenn dieser Ausfall beispielsweise die Ausgangsstufe betrifft, kann ein notwendiges Abschalten nicht mehr durchgeführt werden und ein erhöhtes Sicherheitsrisiko ist nicht vermeidbar. Freilich entsteht nur dann dieses genannte Sicherheitsrisiko, wenn es überhaupt zu einem Ausfall oder einem Versagen kommt.

Zweitens gehört damit auch die Wahrscheinlichkeit für ein derartiges Versagen zu den wichtigen Kenngrößen. Aus der Erfahrung ist bekannt, dass Bauteile oder Komponenten eines Systems im Laufe der Zeit ausfallen können. Nicht alle diese Ausfälle werden sofort erkannt. Allerdings enthalten nicht erkannte Fehler ein latentes Risiko, da das gesamte System beim Auftreten einer Sicherheitsanforderung eventuell vollkommen unerwartet reagiert.

Daher spielt drittens neben der Wahl der Architektur und der Ausfallwahrscheinlichkeit auch die Möglichkeit der Fehleraufdeckung eine Rolle. Ganz abgesehen von den bis jetzt erkennbaren Kenngrößen gibt es auch noch Anteile, die durch systematische Fehler entstehen können.

Viertens sind daher die Fehler „gemeinsamer Ursache“ maßgeblich, die sich auch auf alle Einheiten mehrkanaliger Architekturen auswirken können und dann eine Reaktion auf eine Sicherheitsanforderung unterbinden.

3.1 Zusammenhang der Kenngrößen

Ein einfaches Beispiel soll die vier genannten Kenngrößen in einen Zusammenhang bringen: Ein Sicherheitssystem muss einen Antrieb abschalten, wenn man einen Not-Aus-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-Aus-Tasters oder der dazugehörigen Eingangsschaltung wird durch eine Zweikanaligkeit unterbunden.

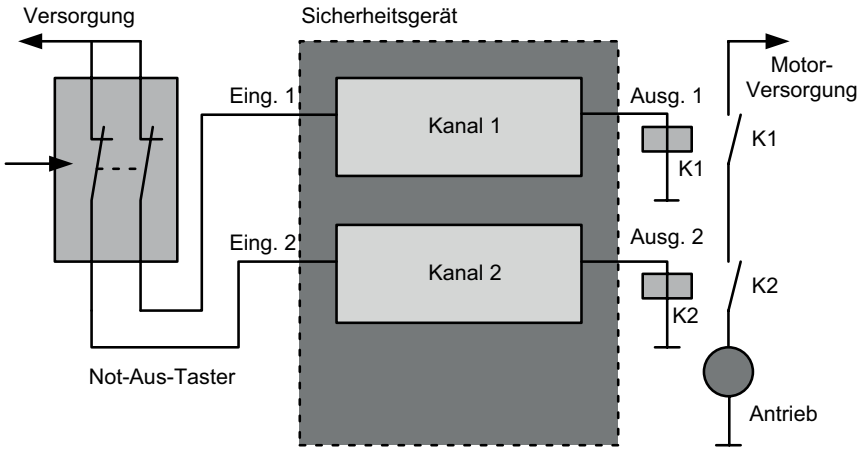

Bild 3.1: Zweikanaliges Sicherheitssystem

Wie Bild 3.1 darstellt, verwendet das Sicherheitssystem einen zweikanaligen Not-Aus-Taster zur Bedienung. Wenn ein Kontakt des Not-Aus-Tasters versagt, steht ein weiterer zur Verfügung. Gegen Fehler bei der 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 3.1 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 sich bei der dargestellten Schaltung um eine zweikanalige fehlertolerante Struktur. Ein einzelner Fehler führt nicht zum Verlust der Sicherheitsfunktion. Nach der Norm EN 954-1 würde diese Einheit der Kategorie 3 entsprechen [Lit 57]. Es ist eine besondere Eigenschaft der gezeigten Schaltung, dass im Fehlerfall immer eine Abschaltung erfolgt. 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 vom Kanal 1 und nach einem weiteren Zeitintervall der Ausgang vom Kanal 2 (Ausg. 2) ausfällt. Innerhalb dieser Fehlerkombination würde der obere Kanal (Kanal 1) die Sicherheitsanforderung des Not-Aus-Tasters nicht erkennen. Der untere Kanal (Kanal 2) stellt zwar die Not-Aus-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, so 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.

Insgesamt stehen damit 4 Kenngrößen im Vordergrund, die in der folgenden Übersicht vorerst rein qualitativ beschrieben werden:

Kenngröße	**Definition**	**Bedeutung**
Architektur (HFT)	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.
λ	Der Lambda-Wert ist die Ausfallrate	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 1fit = 1 Ausfall / 10^9 Stunden.
DC	Diagnosedeckungsgrad (Diagnostic-Coverage)	Der Diagnosedeckungsgrad ist ein Maß für die Erkennung möglicher Fehler durch Tests.
β	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.

3.1.1 Fehlerausschlüsse

Nahezu jede Schaltung kann durch bestimmte Fehlerfälle zum Totalversagen gebracht werden. Es ist Aufgabe der Sicherheitstechnik diese Fehlerfälle entweder sofort zu erkennen oder sie von vorne herein auszuschließen. Auch die Schaltung nach Bild 3.1 beinhaltet derartige Fehler, die sofort zum Versagen führen. Beispielsweise kann ein Kabel, ein Kurzschluss im Stecker oder ein ähnlicher Fehler beide Kontakte der Relais überbrücken (Bild 3.2).

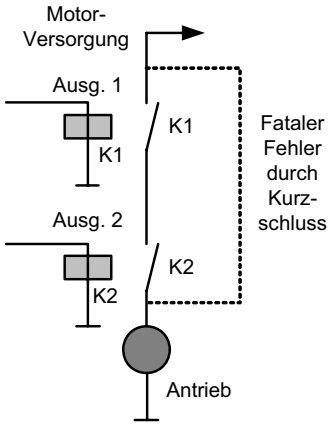

Bild 3.2: Fataler Fehler durch Kurzschluss

Ein derartiger Fehlerfall ist in jedem Fall dadurch zu vermeiden, indem man die Verdrahtung und die Anschlusstechnik fehlerfrei auslegt. Gegebenenfalls darf man die Versorgung des Motors nicht in die in die Nähe des Kontakts K2 bringen, damit ein loses Kabel oder ein defekter Stecker nicht zum Kurzschluss führt.

Wenn es gelingt, einen Anteil an möglichen Fehlern von vornherein auszuschließen, so gehen in die Fehlerbetrachtung nur noch die restlichen Fehler ein, für die kein Fehlerausschluss möglich ist.

3.1.2 Funktionstests

Die einwandfreie Funktion eines Sicherheitssystems kann durch Tests verifiziert werden. Standard-Funktionstests machen aber in der Regel keine hinreichend gute Aussage, ob das Sicherheitssystem auch noch im Fehlerfall richtig reagiert. Sie stellen lediglich eine Aussage über den momentanen Zustand im Bezug auf die gerade getestete Funktion dar. Falls beispielsweise ein Fehler innerhalb eines Kanals vorliegt, man aber das gesamte System testet, so fällt der Fehler nur selten auf. Bild 3.3 zeigt einen Fehler der in Bild 3.1 gezeigten Schaltung.

In der Schaltung nach Bild 3.3 liegt ein bösartiges Versagen im Kanal 1 vor. Entweder ist der Ausgang von Kanal 1 (Ausg. 1) derart ausgefallen, dass das Relais K1 stets angesteuert wird, oder der Kontakt des Relais K1 ist defekt und immer geschlossen. In beiden Fällen lässt sich der Kontakt K1 nicht mehr öffnen und der Strom über K1 fließt andauernd. Eine Person, die einen Funktionstest durchführt, betätigt den Not-Aus-Taster. Da der untere Kanal (Kanal 2) vollkommen intakt ist, fällt das Relais K2 ab und der Strom für den Antrieb wird durch den Kontakt des unteren Relais K2 unterbrochen. Das Betätigen des Not-Aus-Tasters führt also – wie erwartet – zum Stoppen des Antriebs. Man könnte daher meinen, die Sicherheitsschaltung wäre vollkommen in Ordnung. Dies ist aber nicht der Fall, da ein einzelner weiterer Fehler (z. B. der Ausfall des Ausgangs 2) zum Totalversagen führt. Die als „einwandfrei“ eingestufte Schaltung erfüllt damit nicht mehr die Anforderung, auf einen Fehlerfall immun zu reagieren.