Grundlagen eines modernen Sicherheitskonzeptes für Steuerungen

Autor(en): **Retsch, T. / Vondracek, G.**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **80 (1989)**

Heft 11

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-903688

Grundlagen eines modernen Sicherheitskonzeptes für Steuerungen

T. Retsch und G. Vondracek

Je gefährlicher technische Systeme sind – das heisst, je mehr Energie sie speichern und umsetzen –, desto sicherer müssen sie sein. Soll ein technisches System mit Hilfe einer Steuerung gesichert werden, so muss diese entsprechend gebaut sein. Der vorliegende Artikel zeigt, wie eine Steuerung konzipiert sein muss, damit sie die sicherheitsrelevanten Aufgaben mit dem erforderlichen Sicherheitsgrad erfüllt. Dabei werden auch grundsätzliche Überlegungen zur Arbeitssicherheit bei technischen Anlagen und Geräten angestellt.

Les systèmes techniques doivent être d'autant plus sûrs qu'ils sont dangereux – c'est-à-dire plus ils accumulent et transforment de l'énergie. S'il faut protéger un système technique par une commande, celle-ci doit être de construction adéquate. L'article montre comment doit être la conception d'une commande pour qu'elle remplisse ses tâches en fonction de la sécurité et de la fiabilité requises. Des considérations fondamentales sont faites quant à la sécurité du travail des installations et appareils techniques.

Adresse der Autoren

Toni Retsch, dipl. Ing. ETH, und
Georg Vondracek, dipl. Ing.,
Schweizerische Unfallversicherungsanstalt,
Fluhmattstrasse 1, 6002 Luzern.

Technische Systeme bestehen aus verschiedenen Einheiten, zum Beispiel aus mechanischen Bauteilen, die von einer Steuerung Befehle erhalten und diese ausführen. Alle Steuerungen – ob sie nun elektrisch, elektronisch, pneumatisch, hydraulisch, biologisch oder mechanisch funktionieren – verarbeiten und bearbeiten Informationen. Der jeweilige Zustand des Systems wird mit Sensoren erfasst. Diese Informationen werden in der Steuerung verarbeitet und in Form von Befehlen wieder ans System abgegeben. Die nun folgenden Überlegungen sind grundsätzlicher Natur und gelten für alle Arten von Steuerungen.

Grundsätze

Wenn wir uns Gedanken zur *Personensicherheit* machen, dann stellen wir fest, dass es zwei Grundsätze zu beachten gilt.

1. Technische Systeme müssen so konzipiert oder gesichert werden, dass bei ihrer bestimmungsgemässen Verwendung Personen nicht gefährdet werden.

2. Alle technischen Systeme neigen zum Zerfall. Es sind deshalb Vorkehren zu treffen, damit auch beim Ausfall von Teilen des technischen Systems Personen nicht geschädigt werden.

Beide Aussagen gelten sowohl für das ganze technische System als auch für dessen Subsysteme, wie z.B. die Steuerung. Denn technische Systeme können einen geforderten Sicherheitsgrad nur erreichen, wenn all ihre Bestandteile und Subsysteme den gleichen oder einen höheren Sicherheitsgrad aufweisen als das Gesamtsystem.

Will man Grundsatz 1 mit Hilfe der Steuerung verwirklichen, so übernimmt die Steuerung Sicherheitsaufgaben. Sie muss in diesem Fall so aufgebaut sein, dass sie diese Sicherheitsaufgaben erfüllt. Eine Steuerung, die sicherheitsrelevante Aufgaben übernehmen muss, muss nicht nur funktionieren; sie muss vielmehr eine *Sicherheitsfunktion* erfüllen, und zwar mit dem im voraus zu definierenden Grad an Zuverlässigkeit oder – wie es im Fachjargon heisst –, mit der *geforderten* oder *vereinbarten* Sicherheit. Zu beachten ist dabei, das nicht die Steuerung schlechthin diese Sicherheitsbedingungen erfüllen muss, sondern nur der sicherheitsrelevante Teil der Steuerung. Dem Grundsatz 2, dass beim Ausfall von Teilen des technischen Systems keine Personen geschädigt werden dürfen, kann durch Redundanz entsprochen werden.

Sicherheit durch Redundanz

Typische Beispiele für Redundanz sind das Überdimensionieren (damit das Bauelement nicht während seiner Nutzungszeit ausfällt) oder das doppelte Ausführen der Bauteile. Ein Bauteil, bei dem beide Lösungsansätze in der Praxis angewendet werden, ist das Seil. Oft wird versucht, die Sicherheit eines Seils durch Überdimensionieren zu erreichen (z.B. Sicherheitsfaktor 12). In anderen Fällen behilft man sich durch die Verwendung von zwei Seilen. Es ist klar, dass bei der zweiten Lösung die Sicherheit nur dann erhöht wird, wenn der Bruch des einen Seiles erkannt und der Fehler behoben wird. Dabei stellt sich die Frage, ob das Erkennen des eingetretenen Fehlers durch den Menschen (organisatorische Massnahmen) oder durch das technische System selbst (technische Massnahmen) erfolgen soll.

Organisatorische oder technische Sicherheitsmassnahmen?

Wird der Mensch (bzw. sein Verhalten) in die Gewährleistung der Sicherheit miteinbezogen, muss beachtet werden, dass damit ein relativ unzuverlässiges Element in den Sicherheitskreis eingeführt wird. Wird die gleiche Aufgabe durch die Technik erfüllt, so ist die Zuverlässigkeit um Grössenordnungen besser.

Mit zunehmender Komplexität der Systeme nimmt die Fehlerhäufigkeit beim Menschen zu, weil er durch diese Systeme überfordert wird. Daraus kann zusammenfassend der Grundsatz abgeleitet werden:

Zur Gewährleistung der geforderten Sicherheit haben technische Lösungen gegenüber organisatorischen Massnahmen den Vorrang.

Zwingend sind technische Massnahmen dort, wo das erforderliche Verhalten vom Menschen praktisch nicht mehr erbracht werden kann (Überforderung) oder wo Ereignisse verhindert werden müssen, die durch das Verhalten des Menschen nicht beeinflussbar sind. Allgemein gilt der Grundsatz, das organisatorische Massnahmen zum Abwenden von Gefahren zugelassen sind, wenn technische Massnahmen wirtschaftlich nicht mehr vertretbar erscheinen. Dabei sollte aber immer beachtet werden, dass organisatorische Massnahmen nicht kostenneutral sind. Das geforderte Verhalten muss den betroffenen Personen beigebracht werden (Information und Training) und durch die Vorgesetzten kontrolliert werden. Dies muss nicht nur einmal gemacht werden, sondern während der ganzen Lebensdauer der Anlage gewährleistet sein (auch bei Personalwechsel, Ferienabwesenheit, Krankheit usw.). Unter Berücksichtigung des höheren Restrisikos dieser Lösung kann die scheinbar kostengünstige organisatorische Massnahme schnell zur teureren Lösung werden.

Investitionen für Sicherheitsmassnahmen lohnen sich

Aus den bisherigen Ausführungen geht klar hervor, dass zur Gewährleistung der Sicherheit von Personen zusätzliche Massnahmen erforderlich sind, d.h. Massnahmen, die über das hinausgehen, was zum Erfüllen des Einsatzauftrages des technischen Systems notwendig wäre. Daraus könnten folgende Schlussfolgerungen gezogen werden:

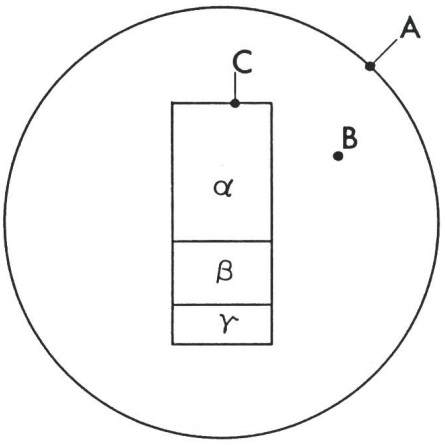
- Die Sicherheit verteuert die Produktion, weil die notwendigen redundanten Mittel Kosten verursachen, die für die Produktion im eigentlichen Sinne nicht notwendig sind.
- Die Sicherheitsmassnahmen behindern oft den Menschen beim Umgang mit der Maschine (Zeitverlust, zusätzliche Aufgaben usw.).
- Die Sicherheitsmassnahmen reduzieren unter Umständen die Zuverlässigkeit der Anlage.

Diese Betrachtungsweise ist zu einseitig. Die praktische Erfahrung gibt vielmehr dem folgenden Slogan recht: «Nur ein sicheres Produktionsmittel ist auch ein wirtschaftliches Produktionsmittel.» Aber es ist natürlich richtig, wenn zum Erreichen der geforderten Sicherheit (Schutzziele) optimale Lösungen gesucht werden, also Lösungen, die beim Arbeiten möglichst wenig behindern und die auf möglichst einfachen Sicherheitskreisen aufbauen, so dass die Zuverlässigkeit der Gesamtanlage möglichst wenig tangiert wird.

Es seien hier noch zwei weitere Bemerkungen gestattet. Im Leitbild fast jeder Firma steht heute, dass der Mitarbeiter das höchste Gut des Unternehmens sei; man wird wohl für dieses höchste Gut auch entsprechende Sicherheitsmassnahmen ergreifen wollen, damit es möglichst lange erhalten bleibt. Ausserdem dürfte die neue Gesetzgebung im Bereich der Produktehaftung (EG) dazu führen, dass die billige Lösung sehr schnell zur sehr teuren Lösung wird.

Sicherheitstechnische Beurteilung einer Steuerung

Damit können wir uns nun der eigentlichen *Sicherheitstechnik* zuwenden. Als Sicherheitstechnik bezeichnen wird die Anwendung von technischen Massnahmen zur Erhöhung der Betriebssicherheit von Geräten, Maschinen und Anlagen mit dem Ziel, Menschen vor den negativen Folgen von Ausfällen oder vor fehlerhaftem Verhalten technischer Einrichtungen zu schützen. (Die Begriffe «Ausfall» und «Fehler» werden in DIN 40042 definiert, der «Fehler einer Steuerung» in DIN 19347.)



Figur 1 Fehlerkategorien

A Menge aller Fehler im betrachteten System

B Menge aller Fehler, welche keinen Einfluss auf die Sicherheit von Personen haben

C Menge aller Fehler, welche einen Einfluss auf die Sicherheit von Personen haben (Fehler, die im Sicherheitskreis auftreten)

α Untermenge der Menge *C*, nämlich die zu berücksichtigenden Fehler

β Untermenge der Menge *C*, nämlich die begründet auszuschliessenden Fehler (z.B. Schalter mit zwangsunterbrechenden Kontakten)

γ Untermenge der Menge *C*, nämlich die nicht bekannten Fehler. Die Fehler der Untermengen β (teilweise) und γ gehen ins Restrisiko ein

Die Sicherheit eines technischen Systems lässt sich am besten beurteilen, wenn man das Verhalten des Systems beim Auftreten eines Fehlers überprüft. Die möglichen Fehler werden sinnvollerweise nach Figur 1 in die folgenden Kategorien aufgeteilt (vgl. dazu VDE 3541):

Muss ein Gerät sicherheitstechnisch beurteilt werden, so sind dafür klare Bedingungen zu definieren.

1. Es müssen die *Kanäle* der Steuerung bestimmt sein, welche die sicherheitstechnisch relevanten Informationen übertragen und verarbeiten. Nur in diesen Kanälen müssen die Fehlereinflüsse studiert werden (Fig. 2).

2. Es ist eine *Vereinbarung* zu treffen, welche Fehler berücksichtigt werden müssen (mögliche Fehler für elektrische Bauelemente sind z.B. auf BIA Blatt 340220 aufgeführt). Für die sicherheitstechnische Beurteilung einer konkreten Steuerung muss deshalb je nach angewendeten Bauelementen eine Fehlerliste erstellt werden.

3. Es muss eine *Vereinbarung* getroffen werden, welche Fehler ausge-

schlossen werden dürfen (z.B. das Wegfallen eines verschraubten und verstifteten Überwachungsschalters oder das Nichtöffnen eines zwangsläufig wirkenden Kontaktes).

4. Es muss eine *Verhaltensliste* des Gerätes erstellt werden, welche die Funktionsweise des Systems beim Auftreten der vereinbarten Fehler beschreibt.

Unter diesen Voraussetzungen sollte es dem Konstrukteur (Elektroniker) wie auch der die Sicherheit beurteilenden Stelle klar sein, welche Anforderungen an eine Steuerung zu stellen sind.

Fehlereffektanalyse

Nun muss die Sicherheit eines Gerätes oder der Steuerung einer Anlage gemäss den festgelegten Kriterien nachgewiesen werden. Das geschieht am besten mit einer Fehlereffektanalyse (Tab. I). Die Fehlereffektanalyse ist eine systematische Untersuchung der Auswirkungen aller vereinbarten Fehler in den sicherheitsrelevanten Kanälen der Steuerung. Die Analyse liefert den Nachweis, dass sich die Steuerung beim Auftreten von Fehlern so verhält wie vereinbart. Die Fehlereffektanalyse zeigt letztlich auf, dass das Auftreten der vereinbarten Fehler in der Steuerung nicht zu einem gefährdenden Betriebszustand des technischen Systems führt. Eine Fehlereffektanalyse kann z.B. wie folgt aussehen:

Wird eine Steuerung lediglich nach funktionellen Gesichtspunkten konzipiert, so wird die Fehlereffektanalyse in sehr vielen Fällen in der Kolonne «gefährlich» ein *Ja* haben. Dies bedeutet, dass die vorgeschlagene Lösung den sicherheitstechnischen Anforderungen nicht genügt. Die Steuerung muss dementsprechend geändert und danach mit einer zweiten Fehlereffektanalyse überprüft werden. Kennt ein Konstrukteur aber die Regeln, wie eine sichere Steuerung aufgebaut wird, so gibt ihm die Fehlereffektanalyse direkt die Bestätigung dafür, dass die von ihm entworfene Steuerung die Sicherheitsanforderungen erfüllt.

Bauelement im sicherheitsrelevanten Kanal	Fehlerart	Reaktion der Steuerung	gefährlich
Relais K	wird nicht anziehen	...	nein
	wird nicht abfallen	...	nein
Transistor T	Unterbruch	...	nein
	durchlegiert	...	ja
usw.	usw.	usw.	usw.

Tabelle I Beispiel einer Fehleffektanalyse

Die Fehlereffektanalyse bildet daher einen integrierenden Bestandteil des Sicherheitsnachweises eines Gerätes oder einer Anlage.

Redundanz bei Steuerungen

Mit welchen Mitteln kann die geforderte (vereinbarte) Sicherheit einer Steuerung erreicht werden?

Dazu gibt es drei Lösungsansätze:

1. Bauelemente verwenden, bei denen die zur Diskussion stehenden Fehler ausgeschlossen werden dürfen oder bei denen das Auftreten dieses Fehlers dazu führt, dass das Bauelement *sicheres Verhalten* zeigt, d.h. *qualitative Redundanz* durch Verwenden von *qualifizierten* Bauelementen.

2. Redundante Informationsdarstellung anwenden. Statt «statischer Signale (JA [1], NEIN [0]) werden *dynamische*, also redundante *Signale* angewendet (mäander-, impulsartige oder codierte Signale).

3. Zum Übertragen oder Verarbeiten eines sicherheitsrelevanten Signals kein einzelnes Bauteil, sondern parallel mehrere Bauteile verwenden, d.h. *quantitative Redundanz* durch mehrkanaligen Aufbau einer Schaltung, oder durch zusätzliche Schaltungskreise (Testen).

Im folgenden werden die drei Lösungsansätze näher erläutert:

Sicherheit durch qualitative Redundanz

1. Durch konstruktive Massnahmen werden die Bauelemente so gestaltet, dass gewisse *Fehler ausgeschlossen* werden können.

Erstes Beispiel eines Fehlers mit gefährlichem Verhalten: Kurzschluss zwischen zwei sicherheitsrelevanten Leitungen.

Lösung: Leitungen getrennt führen und isolieren sowie Klemmen genügend weit auseinanderlegen. Dieser Fehler kann damit ausgeschlossen werden.

Zweites Beispiel eines Fehlers mit gefährlichem Verhalten: Klebenbleiben des Kontaktes eines Überwachungsschalters (Schalterkontakte öffnen sich nicht und unterbrechen daher den Schaltkreis nicht).

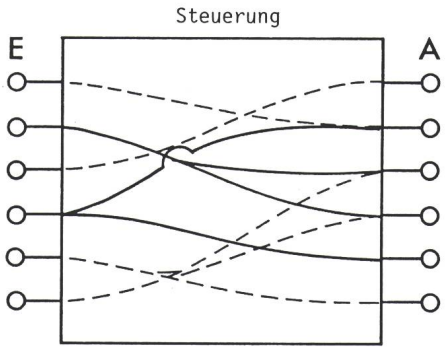
Lösung: Verwenden eines Schalters, dessen Kontakte zwangsläufig geöffnet werden. Bedingung: Dieser Schalter muss mechanisch zwangsläufig betätigt werden. Unter diesen Voraussetzungen wird auch ein verklebter Schalterkontakt aufgedrückt und damit der Schaltkreis unterbrochen. Dieser Fehler kann also ausgeschlossen werden.

2. Die Bauteile werden so gestaltet, dass diese bei Auftreten des Fehlers *sicheres Verhalten* zeigen.

Drittes Beispiel eines Fehlers mit gefährlichem Verhalten: Bruch einer Feder im Endschalter.

Lösung: Feder so einsetzen, dass Schaltkontakte mit Federkraft geschlossen werden. Damit bleibt der Schaltkreis geöffnet, d.h. der sichere Zustand gewährleistet.

Viertes Beispiel eines Fehlers mit gefährlichem Verhalten: Ausfall eines Transistors in einem elektronischen Überwachungsgerät.



Figur 2 Sicherheitsrelevante Kanäle einer Steuerung

------- sicherheitsunrelevante Funktionen
——— sicherheitsrelevante Funktionen
E Eingänge
A Ausgänge

Lösung: Dynamische Signale verwenden, so dass das Überwachungsgerät bei diesem Fehler das sichere Signal «Null» angibt (Fail-Safe-Prinzip).

Sicherheit durch Informationsredundanz

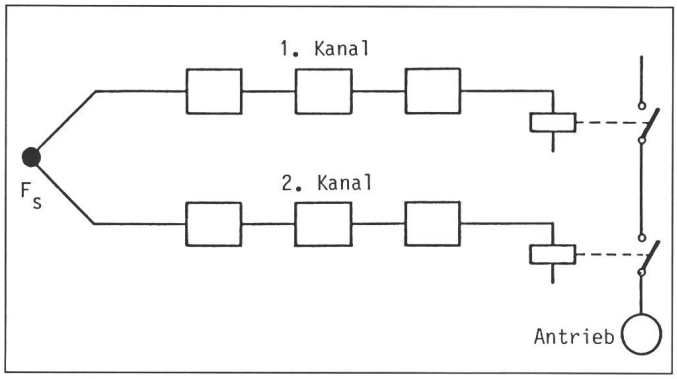
Als Beispiel für eine redundante Informationsdarstellung kann das Fail-Safe-Prinzip dienen. Bei diesem überträgt eine einkanalige Schaltung ein *dynamisches*, also redundantes Signal. Sowohl beim Ausfall des Signals als auch beim Fehler in der Schaltung wird ein sicherer Zustand eingeleitet. (Typische Anwendungen bei Funkfernsteuerungen.)

Sicherheit durch quantitative Redundanz

Fünftes Beispiel eines Fehlers mit gefährlichem Verhalten: Klebenbleiben des Kontaktes eines Relais oder Schützen (Relaiskontakte öffnen sich nicht und unterbrechen daher den Schaltkreis nicht.)

Lösung: Verwenden eines Relais mit zwanggeführten Kontakten: Ist einer der Ruhekontakte geschlossen, so sind *alle Arbeitskontakte geöffnet*. Ist einer der Arbeitskontakte geschlossen, so sind *alle Ruhekontakte geöffnet*. Damit ist aber noch nicht gewährleistet, dass die Kontakte des Relais sich tatsächlich öffnen, selbst wenn sie zum Beispiel verklebt sind. Eine Zwangöffnung der Relaiskontakte lässt sich nicht erreichen.

Ein Relais mit zwanggeführten Kontakten (oft auch Sicherheitsrelais genannt) unterbricht also den Schaltkreis nicht sicherer als jedes andere Relais. Deshalb darf dieser Fehler *nicht* ausgeschlossen werden. Ein Relais mit zwanggeführten Kontakten kann aber getestet werden. Sollen z.B. die Arbeitskontakte (Schliesser) gegen Ende des Arbeitszyklus öffnen, so kann über die Gegenkontakte (Öffner) überprüft werden, ob dies tatsächlich geschehen ist und umgekehrt. Die geforderte Sicherheit kann nur durch mehrkanaligen Schaltungsaufbau erreicht werden. Bei dieser Lösung wird eine bestimmte Sicherheitsfunktion über zwei (oder mehrere) parallel geschaltete Kanäle übertragen und verarbeitet. Damit führt ein Fehler in einem Bauteil - zum Beispiel im ersten Kanal - nicht zum gefährlichen Verhalten des Systems, denn die Sicherheitsfunktion wird über den zweiten, noch intakten Kanal weiterhin gewährleistet. Die Sicherheit bleibt aber nur gewährleistet, wenn der aufgetretene Fehler im ersten Kanal *entdeckt* und *behoben* wird oder das System in einen sicheren Zustand übergeführt wird, bevor ein zweiter Fehler im System auftritt (Fig. 3).



Figur 3
Sicherheit durch mehrkanaligen Schaltungsaufbau
F_s Sicherheitsfunktion

Wenn ein Fehler zwar entdeckt wird, es aber nicht möglich ist, den Fehler zu beheben oder das System in einen sicheren Zustand zu überführen (das kann z.B. bei chemischen Prozessen der Fall sein oder bei einem Flugzeug, das weiterfliegen muss), so muss die Funktion auch nach dem Eintreten des Fehlers weiterhin mit der geforderten Sicherheit erbracht werden. Dies bedeutet, dass in diesem Fall ein zweikanaliger Schaltungsaufbau nicht genügt, sondern eine 3- oder *n*-kanalige Ausführung notwendig wird. Anders ausgedrückt heisst das, dass wir nach dem Eintreten eines Fehlers im System damit rechnen müssen, dass ein weiterer Fehler eintritt, bevor das System in einen sicheren Zustand übergeführt werden kann. Wir bezeichnen solche Fehler als *gleichzeitig* auftretende Fehler, wobei gleichzeitig als prozessabhängig zu verstehen ist und nicht als durch ein fixes Zeitmass gegeben.

Eine *n*-kanalige Steuerung ist gegen $(n-1)$ gleichzeitig auftretende Fehler gesichert, wenn die Kanäle gegenseitig *überwacht* werden. Ist dies nicht der Fall, dann kann ein Fehler lange anstehen, ohne dass es das System bemerkt. Ohne gegenseitige Überwachung der Kanäle kann also die geforderte Sicherheit nicht erfüllt werden. Hier erhält nun das oben beschriebene Relais mit zwanggeführten Kontakten seine Bedeutung. Dieses, und nur dieses Relais kann auf seinen Zustand abgefragt werden. Das heisst, dass sich nur solche Relais gegenseitig überwachen können.

Es gilt also der folgende Grundsatz:

Die Sicherheit in mehrkanaligen Systemen ist nur gewährleistet, wenn ein Fehler entdeckt und behoben wird, bevor ein weiterer Fehler auftritt.

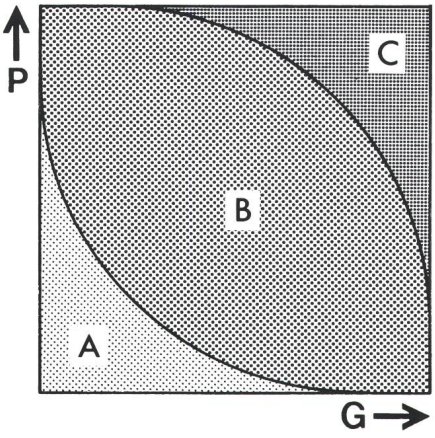
Je länger der Zyklus dauert, d.h. je länger das Zeitmass für die sogenannte Gleichzeitigkeit des Eintretens von Fehlern ist, um so höherkanaliger muss die Sicherheitsschaltung sein.

Erforderlicher Sicherheitsgrad

Der erforderliche Sicherheitsgrad (die geforderte Sicherheit einer technischen Einrichtung oder Anlage) hängt vom Verletzungsrisiko der betroffenen Personen ab. Mit Hilfe der Darstellung in Figur 4 und Tabelle II lässt sich dieses Risiko abschätzen. Bezieht man die vorher beschriebenen Fehler auf diese Darstellung, so kann man folgende Schlüsse ziehen:

Feld A: geringes (minimiertes) und deshalb akzeptiertes Risiko

Der Fehler tritt selten auf und führt zu einer geringen Gefährdung, allen-



Figur 4 Klassierung von Schadenrisiken
G Schadenumfang
P Eintrittshäufigkeit
→ = zunehmend (sehr klein, klein, gross, sehr gross)
A, B, C siehe Tabelle II

falls zu einer vernachlässigbaren Verletzung, z.B. zu einem leicht gequetschten Fingerglied. Hier werden keine Anforderungen an die Sicherheit gestellt. Eine rein funktionelle Steuerung genügt.

Feld B: mittleres (normales) Risiko

Der auftretende Fehler führt zu einer Gefährdung während einer gewissen Zeit (Zyklus), weil bis zur Behebung des Fehlers oder bis zur Herstellung eines ungefährlichen Zustandes die Sicherheitsfunktion nicht mehr gewährleistet ist. Der gefährdende Zustand ist aber erkennbar, und durch entsprechendes Verhalten des Personals ist ein Personenschaden vermeidbar.

Beispiel: Infolge Klebens eines Relais schaltet eine Produktionsmaschine beim Öffnen des Verdeckes nicht ab. Dadurch entsteht eine Gefährdung (die Maschine läuft nun bei geöffnetem Schutzverdeck). Aber erst wenn die Bedienungsperson sich falsch verhält, nämlich wenn sie trotz laufender Maschine in den Bearbeitungsraum greift, kommt es zum Unfall. Hier genügt eine Lösung, bei der die Sicherheitsfunktion für eine kurze Zeit, d.h. bis zum Zyklusende, nicht mehr gewährleistet ist. Das System muss aber den Fehler erkennen, und ein neuer Zyklusstart muss verhindert werden. Denn vom Eintritt des Fehlers an ist die Sicherheitsfunktion nicht mehr gewährleistet, wenn der Fehler nicht behoben wird. Diese Lösung bezeichnen wir als Massnahme mit normaler Schutzwirkung. Zulässig sind solche Lösungen zur Abwendung von Ereignissen mit normalem Risiko.

	Risiko	Sicherheit	Schutzmassnahme	Merkmal
Feld A	minimiert	gewährleistet	nicht nötig	Schadenumfang sehr klein bis klein bei kleiner und sehr kleiner Eintrittshäufigkeit
Feld B	normal	nicht gewährleistet	nötig, normale Schutzwirkung	Schadenumfang sehr klein bis gross bei grosser bzw. sehr kleiner Eintrittshäufigkeit
Feld C	erhöht	nicht gewährleistet	nötig, erhöhte Schutzwirkung	Schadenumfang klein bis sehr gross bei sehr grosser bzw. kleiner Eintrittshäufigkeit

Tabelle II

Feld C: erhöhtes Risiko

Der auftretende Fehler führt direkt zum Unfall.

Beispiel: Bei einer teleskopierbaren Arbeitshebebühne wird die Standsicherheit dadurch gewährleistet, dass die Steuerung dafür sorgt, dass die Hebebühne in einem bestimmten Bereich nicht ausgefahren werden kann. Dies muss durch eine Sicherheitsschaltung gewährleistet werden. Fährt die Bühne nur ein einziges Mal in diesen Bereich, so kippt sie, und das Personal im Arbeitskorb hat keine grosse Überlebenschance.

Hier gilt deshalb die Bedingung, das auch beim Auftreten eines Fehlers im Sicherheitskreis die Sicherheitsfunktion erhalten bleiben muss, d.h. dass trotz des Fehlers die Bewegung der Hebebühne sofort unterbrochen werden muss. Wenn es sich beim möglichen Fehler wiederum um das Kleben eines Relais handelt, so führen hier nur noch mehrkanalige, überwachte Sicherheitskreise zum Ziel. Ob sie zwei-, drei-, oder *n*-kanalig sein müssen, hängt von der Länge des «Zyklus» ab, also von der Frage, ob vor Erreichen des sicheren Zustandes weitere Fehler zu erwarten sind.

In diesem Artikel wurde dargestellt, mit welchen Überlegungen ein Konstrukteur zu einer sicherheitsgerechten Steuerung gelangen kann. Vieles von dem, was gesagt wurde, ist nicht neu. Bereits Bekanntes wurde aber in die richtigen Zusammenhänge eingeordnet. Die Autoren hoffen, damit einen Beitrag zur Klärung kontroverser Fragen geleistet zu haben.

Unfälle an elektrischen Starkstromanlagen in der Schweiz in den Jahren 1985 bis 1987

In den Jahren 1985 bis 1987 wurden dem Starkstrominspektorat in Zürich gesamthaft 630 Elektrounfälle gemeldet. 44 Unfälle verliefen tödlich. Rund die Hälfte der Unfälle wurde durch Elektrofachleute verursacht. Ein ausführlicher Bericht wird im SEV-Bulletin Nr. 13 vom 1. Juli 1989 (Energietechnik) erscheinen, in dem diese Elektrounfälle statistisch erfasst, analysiert, ausgewertet und mit den Ergebnissen früherer Jahre verglichen werden. Der Bericht enthält auch einen Querschnitt durch das gesamte Unfallgeschehen und gibt Einblick in die Vielfalt der Unfallsituationen. Mehrere bemerkenswerte Unfälle werden beschrieben, deren Ursachen erläutert und Massnahmen erwähnt, um ähnliche Ereignisse zu verhüten.

Sonderdrucke in deutscher und französischer Sprache können ab Anfang September bei der Drucksachenverwaltung des SEV, Postfach, 8034 Zürich, Tel. 01/384 91 11, bestellt werden.

E. Lamprecht, Starkstrominspektorat