Sicherheitsanalyse technischer Systeme

Autor(en): **Birolini, A.**

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: **09.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-903684

Sicherheitsanalyse technischer Systeme

A. Birolini

Die steigende Komplexität technischer Systeme erhöht die Gefahr für überkritische Ausfälle. Der Entwicklungsingenieur muss deshalb konsequent die Auswirkung von Ausfällen untersuchen und Massnahmen zu ihrer Milderung treffen. Eine 100%ige Sicherheit kann aber im allgemeinen Fall nicht erreicht werden. Nach einer kurzen Einführung in die Begriffe der Zuverlässigkeitstheorie werden die Methoden der Sicherheitsanalysen und -prüfungen technischer Systeme dargelegt. Der Aspekt menschlicher Zuverlässigkeit kommt im Schlusskapitel zur Sprache.

L'augmentation de la complexité des systèmes techniques fait croître le danger de défaillances hypercritiques. L'ingénieur de développement doit analyser systématiquement la conséquence de défaillances et prendre les actions nécessaires à limiter leur effet. Une sécurité de 100% n'est toutefois pas possible dans le cas général. Après une courte introduction dans les concepts de base de la théorie de la fiabilité, les méthodes d'analyse et de test de la sécurité des systèmes techniques sont exposées.

Adresse des Autors
Prof. Dr. *A. Birolini*, Fachgruppe Zuverlässigkeitstechnik, ETH, 8092 Zürich.

Die steigende Komplexität technischer Systeme, der Zwang, diese in immer kürzerer Zeit zu entwickeln, und der ständige Kostendruck vergrössern die Gefahr für überkritische Ausfälle, d.h. für Ausfälle, welche die Sicherheit beeinträchtigen. Es wird heute akzeptiert, dass komplexe technische Systeme nicht 100%ig sicher sein können; die Frage nach ihrer Sicherheit soll deshalb lauten: *Wie sicher ist eigentlich sicher genug?* Bei einer solchen Fragestellung besteht die Gefahr, dass aus Gewohnheit, Bequemlichkeit oder aus anderen Gründen die Warnsignale, die sich aus einem Unfall oder einer Katastrophe ergeben, ungenügend wahrgenommen werden. Sagt man z.B. von einer Anlage, die Wahrscheinlichkeit für einen überkritischen Ausfall sei 10^{-4} pro Jahr, und liegt dazu die Anlage weit weg vom eigenen Lebensraum, so wird ein solches Risiko oft a priori akzeptiert. Erst wenn mehrere Ausfälle in einer bestimmten Zeitspanne aufgetreten sind, merkt man, dass das Risiko zu hoch war. 10^{-4} pro Jahr ist bei einem einzelnen System gewiss eine genügend kleine Zahl (im Falle eines Dauerbetriebs entspricht sie einer Ausfallrate von etwa 10^{-8} h^{-1}). Liegen aber 1000 solcher (oder ähnlicher) statistisch unabhängiger Anlagen vor, so ergibt sich für die Wahrscheinlichkeit eines überkritischen Ausfalls der Wert 0,09 pro Jahr[1]. 9% pro Jahr heisst aber im Mittel ein überkritischer Ausfall etwa alle 10 Jahre (mit $5 \cdot 10^{-4}$ pro Jahr hätte man im Mittel einen überkritischen Ausfall alle 2 Jahre).

Obiges Zahlenbeispiel soll nicht den Eindruck erwecken, dass das Risiko für überkritische Ausfälle eines technischen Systems genau berechnet werden kann. In den meisten Fällen ist nur eine grobe Schätzung möglich. Es soll aber zeigen, dass es gefährlich ist, kleine Risiken a priori zu akzeptieren oder Warnsignale nicht rechtzeitig zu erkennen, vor allem, wenn eine relativ grosse Anzahl ähnlicher Systeme vorhanden ist.

Für technische Systeme sollen die Analysen der Sicherheit eng gekoppelt mit jenen der Zuverlässigkeit durchgeführt werden. Dies, weil Zuverlässigkeitsanalysen neben den Ausfallratenanalysen punktuell auch *Ausfallartenanalysen* beinhalten müssen, und diese bereits zu den Sicherheitsanalysen gehören. Nach einer kurzen Einführung der Grundbegriffe werden die Methoden der Zuverlässigkeits- und Sicherheitsanalysen dargelegt. Auf Prüfungen sowie auf den Einfluss der menschlichen Faktoren wird in den letzten beiden Kapiteln eingegangen. Anstatt von technischen Systemen wird, wie in der Zuverlässigkeitstechnik üblich, von Betrachtungseinheiten gesprochen.

Grundbegriffe

Zuverlässigkeit

Zuverlässigkeit ist die Eigenschaft einer Betrachtungseinheit, funktionstüchtig zu bleiben. Sie wird mit R bezeichnet und durch die Wahrscheinlichkeit ausgedrückt, dass die Betrachtungseinheit die geforderte Funktion unter vorgegebenen Arbeitsbedingungen während einer festgelegten Zeitdauer T ausfallfrei ausführt.

Unter einer Betrachtungseinheit versteht man eine Anordnung beliebiger Komplexität (z.B. Bauteil, Baugruppe, Gerät, Anlage, System), welche für die Untersuchungen und Analysen als Einheit interpretiert wird (dabei kann es sich um eine Funktions-

[1] Binomialverteilung (Gl. 10) mit $n = 1000$, $k = 1$ und $p = 10^{-4}$ oder aus der Poissonschen Näherung

$$p_k = \frac{(np)^k}{k!} e^{-np}$$

oder Konstruktionseinheit handeln). Die geforderte Funktion spezifiziert die Aufgaben der Betrachtungseinheit; für gegebene Eingänge dürfen beispielsweise die Ausgänge vorgeschriebene Toleranzbänder nicht verlassen. Die Arbeitsbedingungen haben einen direkten Einfluss auf die Zuverlässigkeit und müssen gut spezifiziert werden[2]. Geforderte Funktionen und Arbeitsbedingungen können auch zeitabhängig sein. In solchen Fällen wird mit einem Anforderungsprofil operiert.

Oft interessiert in den Anwendungen der Verlauf der Zuverlässigkeit R, wenn die Missionsdauer T variiert, d.h. die Zuverlässigkeitsfunktion $R(t)$. Ferner gibt es Fälle, wo die Betrachtungseinheit nur eine einmalige Mission ausführen muss (Raketen, Geschosse usw.). Hier verwendet man in der Regel den Begriff der geforderten Mission.

Ausfall

Ein Ausfall tritt auf, wenn die Betrachtungseinheit aufhört, ihre geforderte Funktion auszuführen. Die Betriebszeit kann dabei sehr kurz gewesen sein, denn Ausfälle können auch durch transiente Vorgänge beim Einschalten verursacht werden. Bei der Beurteilung eines Ausfalls wird davon ausgegangen, dass zum Beanspruchungsbeginn die Betrachtungseinheit fehlerfrei war. Die Bewertung erfolgt dann unter den folgenden drei Gesichtspunkten:

1. *Art:* Es wird unterschieden zwischen Sprungausfall, Driftausfall und intermittierendem Ausfall.
2. *Ursache:* Eine übliche Klassierung unterscheidet Anwendungsfehlerausfall, inhärenten Ausfall, Verschleissausfall, Primärausfall und Folgeausfall.
3. *Auswirkung:* Abhängig davon, ob man sich auf die direkt betroffene oder auf eine übergeordnete Betrachtungseinheit bezieht, wird unterschieden zwischen keiner Auswirkung, Teilausfall, Vollausfall und überkritischem Ausfall (bei überkritischen Ausfällen ist die Sicherheit nicht mehr gewährleistet).

[2] Die Erfahrung zeigt z.B., dass sich die Ausfallrate elektronischer Bauteile verdoppelt, wenn die Umgebungstemperatur um 10 bis 20 °C erhöht wird.

Ausfallrate

Die Ausfallrate spielt in den Zuverlässigkeitsanalysen eine wichtige Rolle. Sie ist gleich der Wahrscheinlichkeit, bezogen auf die Zeitspanne δt, dass die Betrachtungseinheit im Intervall $(t, t + \delta t)$ ausfallen wird, unter der Bedingung, dass sie zur Zeit $t = 0$ eingeschaltet wurde und im Intervall $(0, t)$ nicht ausgefallen ist. Sie wird mit $\lambda(t)$ bezeichnet. Zwischen der Ausfallrate und der Zuverlässigkeitsfunktion besteht die Beziehung

$$\lambda(t) = -\frac{1}{R(t)}\,\frac{dR(t)}{dt} \qquad (1)$$

Mit $R(0) = 1$ ergibt sich daraus

$$R(t) = e^{-\int_0^t \lambda(x)\,dx} \qquad (2)$$

In der Praxis weist die Ausfallrate einer Gesamtheit statistisch identischer Betrachtungseinheiten den typischen Verlauf einer Badewannenkurve [1;...;5] auf. Für die Zuverlässigkeitsuntersuchungen wird in der Regel angenommen, dass durch geeignete Vorbehandlung die schwachen Betrachtungseinheiten eliminiert worden sind und zur Zeit $t = 0$ die Ausfallrate einen konstanten Wert hat. Für viele elektronische Bauteile bleibt dann die Ausfallrate während der ganzen Brauchbarkeitsdauer näherungsweise konstant. Mit $\lambda(t) = \lambda$ ergibt sich aus (2)

$$R(t) = e^{-\lambda t}. \qquad (3)$$

Der Mittelwert der ausfallfreien Arbeitszeiten τ ist gegeben durch

$$E\{\tau\} = MTTF = \int_0^\infty R(t)\,dt, \qquad (4)$$

wobei $MTTF$ für Mean Time To Failure steht. Im Falle einer konstanten Ausfallrate gilt

$$E\{\tau\} = \int_0^\infty e^{-\lambda t}\,dt = 1/\lambda. \qquad (5)$$

Es ist üblich, $1/\lambda$ als Mean Time Between Failures zu bezeichnen:

$$MTBF = 1/\lambda \qquad (6)$$

Sicherheit

Die Sicherheit ist die Eigenschaft einer Betrachtungseinheit, keine Gefahr für Menschen, Sachen oder Umwelt darzustellen. Sie muss unter folgenden zwei Gesichtspunkten untersucht werden:

- die Betrachtungseinheit funktioniert korrekt und wird korrekt betrieben
- die Betrachtungseinheit oder ein Teil davon ist ausgefallen.

Der erste Aspekt wird durch die *Unfallverhütung* abgedeckt, die vielfach durch gesetzliche Vorschriften geregelt ist. Der zweite Aspekt ist Gegenstand der *technischen Sicherheit* und wird mit den Methoden der Zuverlässigkeitstheorie untersucht. Dabei müssen auch die Einwirkungen äusserer Einflüsse (Katastrophe, Sabotage usw.) berücksichtigt werden. Prinzipiell soll zwischen technischer Sicherheit und Zuverlässigkeit unterschieden werden. Während die Sicherheitstheorie Massnahmen untersucht, die es gestatten, bei einem Ausfall die Betrachtungseinheit in einen *sicheren Zustand* zu bringen (Fail Safe), untersucht die Zuverlässigkeitstheorie Massnahmen, um ganz allgemein die Anzahl Ausfälle zu vermindern.

Produkthaftung

Eng verbunden mit dem Begriff der Sicherheit ist der Begriff der Produkthaftung. Produkthaftung ist die rechtliche Verantwortung des Herstellers für Personen-, Sach- oder Vermögensschäden, die durch den Gebrauch fehlerhafter, defekter oder ausgefallener Betrachtungseinheiten entstehen. Die rasche Zunahme der Produkthaftpflichtfälle in den USA (50 000 im Jahr 1960, 500 000 im Jahr 1970, über eine Million im Jahr 1980) darf von einem exportorientierten Unternehmen nicht ignoriert werden. Der Grund für diese geradezu chaotischen Verhältnisse liegt wohl in der Besonderheit der prozessualen Verfahren der USA. Ein gut ausgebautes Konfigurationsmanagement [1] und die Durchführung von Sicherheitsanalysen sind die notwendigen Voraussetzungen, um Produkthaftpflichtfälle zu verhindern.

Zuverlässigkeitsanalysen

Zuverlässigkeitsanalysen in der Entwicklungsphase dienen in erster Linie der rechtzeitigen Erkennung und Beseitigung von Schwachstellen und der Durchführung von Vergleichsstudien. Sie sollen vom Entwicklungsingenieur in Zusammenarbeit mit dem Zuverlässigkeitsingenieur durchgeführt wer-

den. Ein wichtiger Teil dieser Analysen besteht in der Untersuchung der *Ausfallraten* und der *Ausfallarten* der Betrachtungseinheit. Auf die Ausfallartenanalyse wird weiter hinten eingegangen.

Die Untersuchung der *Ausfallrate* führt zur Berechnung der vorausgesagten Zuverlässigkeit, d.h. jener Zuverlässigkeit, die anhand der Struktur der Betrachtungseinheit und der Zuverlässigkeit ihrer Elemente rechnerisch bestimmt werden kann. Die Voraussage ist wichtig, um Schwachstellen frühzeitig zu erkennen, Alternativlösungen zu untersuchen, Zusammenhänge zwischen Zuverlässigkeit, Instandhaltbarkeit, logistischer Unterstützung und Verfügbarkeit quantitativ zu erfassen sowie Zuverlässigkeitsforderungen an Unterlieferanten stellen zu können. Wegen

- der getroffenen Vereinfachung bei der Festlegung der Modelle,
- der ungenügenden Berücksichtigung der Auswirkung innerer und äusserer Störeinflüsse (Schaltvorgänge, EMV usw.),
- der Unsicherheit der verwendeten Daten (die Ausfallraten der Bauteile liegen im Bereich 10^{-9} bis 10^{-7} h^{-1} und können praktisch nur noch mit Hilfe zeitraffender Prüfungen ermittelt werden) und
- der Schwierigkeit, zuverlässige Daten aus der Nutzungsphase zu erhalten,

kann die vorausgesagte Zuverlässigkeit lediglich eine Schätzung der wahren Zuverlässigkeit darstellen. Diese kann nur mit Hilfe von Zuverlässigkeitsprüfungen ermittelt werden. Bezogen auf die Ausfallrate der Betrachtungseinheit können mit der nötigen Erfahrung - falls in der Fertigungsphase geeignete Massnahmen gegen Vorschädigungen getroffen werden - die Differenzen zwischen der vorausgesagten und der wahren Zuverlässigkeit klein gehalten werden (etwa Faktor 2).

Die Berechnung der vorausgesagten Zuverlässigkeit elektronischer und elektromechanischer Betrachtungseinheiten erfolgt gemäss folgenden Schritten:

1. Definition der geforderten Funktion und des Anforderungsprofils,
2. Aufstellung des Zuverlässigkeitsblockdiagramms (ZBD),
3. Bestimmung der Arbeitsbedingungen für jedes Element im ZBD,
4. Bestimmung der Ausfallrate für jedes Element im ZBD,
5. Berechnung der vorausgesagten Zuverlässigkeit für jedes Element im ZBD,
6. Berechnung der vorausgesagten Zuverlässigkeit der Betrachtungseinheit,
7. Behebung der Schwachstellen und Wiederholung der Schritte 2 bis 6, falls die Zuverlässigkeitsziele nicht erreicht worden sind.

Eine ausführliche Darlegung der obigen Schritte kann in [1] gefunden werden. Wichtig für die Betrachtungen über die Sicherheit technischer Systeme sind die Überlegungen betreffend der *Redundanz*. Redundanz entsteht in ihrer einfachsten Form durch das Einführen von zusätzlichen Elementen (Reserveelemente), welche dieselbe Funktion wie andere Elemente ausführen und dadurch die Zuverlässigkeit, die Verfügbarkeit oder die Sicherheit der Betrachtungseinheit erhöhen. Im Zuverlässigkeits-Blockdiagramm wird eine Redundanz als Parallelschaltung erscheinen, in der Hardware je nach Ausfallart als Parallel- oder Serieschaltung. Es werden prinzipiell drei Redundanzarten unterschieden:

- *Heisse Redundanz* (aktive oder parallele Redundanz): Das Redundanzelement ist von Anfang an der gleichen Belastung wie das arbeitende Element ausgesetzt.
- *Warme Redundanz* (leicht belastete Redundanz): Das Redundanzelement ist bis zum Ausfall des arbeitenden Elements oder bis zu seinem eigenen Ausfall einer kleineren Belastung ausgesetzt.
- *Kalte Redundanz* (Standby-, unbelastete Redundanz): Das Redundanzelement ist bis zum Ausfall des arbeitenden Elements keiner Belastung ausgesetzt.

Aus den obigen Darlegungen könnte man schliessen, dass eine Redundanz lediglich aus der Verdoppelung der schwachen Teile besteht. Das ist aber nur teilweise richtig, denn oft werden raffiniertere Entwicklungs- oder Konstruktionsmassnahmen (wie beispielsweise fehlerkorrigierende Kodierung oder Parallelausführung der gleichen Funktion mit anderen Elementen) verwendet. Es kann auch vorkommen, dass die Redundanz nicht genau die gleiche Funktion ausführt wie das Element, welches nach Ausfall ersetzt werden soll (Pseudoredundanz). Ausserdem bedingt die Redundanz oft eine Aufteilung der Last und das Einführen von Zusatzeinrichtungen zur Überwachung und Umschaltung, die in den Zuverlässigkeitsberechnungen berücksichtigt werden müssen.

Sind hohe Sicherheitsforderungen zu erfüllen, empfiehlt es sich, die redundanten Elemente verschieden zu realisieren (andere Bauteile, andere Fertigung, andere Software). Die Tabelle I gibt die Zuverlässigkeitsfunktionen einiger einfacher Redundanzstrukturen für den Fall heisse Redundanz, unabhängige Elemente, nicht reparierbar, wieder. Die Resultate dieser Tabelle werden im nächsten Abschnitt diskutiert.

Ein weiterer wichtiger Aspekt, der beim Einsatz von Redundanz überprüft werden muss, ist die Ausfallart der betreffenden Elemente. Sie bestimmt, ob bei der Hardwarerealisierung die Redundanz serie- oder parallelzuschalten ist. Ihre Untersuchung ist damit eine Voraussetzung für die korrekte Aufstellung des Zuverlässigkeits-Blockdiagramms. Die Ausfallart wird im Rahmen der Sicherheitsanalysen nicht nur für die redundanten Elemente, sondern allgemein untersucht.

Sicherheitsanalysen

Zur Ausfallratenanalyse (vorausgesagte Zuverlässigkeit) kommt bei kritischen Elementen einer Betrachtungseinheit (insbesondere bei Schnittstellen, wo Redundanz erscheint) stets auch eine *Ausfallartenanalyse* hinzu. Diese wird mit FMEA (Failure Modes and Effects Analysis) oder mit FMECA (Failure Modes, Effects and Criticality Analysis) bezeichnet und besteht in der systematischen Untersuchung der möglichen Ausfälle bezüglich ihrer Auswirkung auf die Funktionstüchtigkeit und auf die Sicherheit des betreffenden Elements und der von diesem beeinflussten Elemente. [1;...;4;6;...;9] Die Untersuchung berücksichtigt die verschiedenen Ausfallarten und Ausfallursachen. Sie ermöglicht die Bestimmung der potentiellen Gefahren und damit die Analyse der Vorkehrungen zur Verkleinerung der Auftrittswahrscheinlichkeit der Ausfälle und zur Beseitigung oder Milderung der Auswirkungen. Bei der FMEA/FMECA werden oft nicht nur Ausfälle, sondern auch Fehler und Defekte berücksichtigt. Die Abkürzung FMEA/FMECA steht dann für Fault Modes and Effects Analysis/Fault Modes, Effects and Criticality Analysis. Eine FMEA/FMECA wird vom

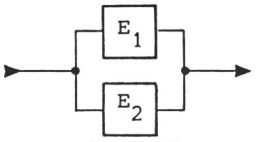
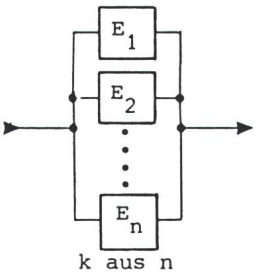
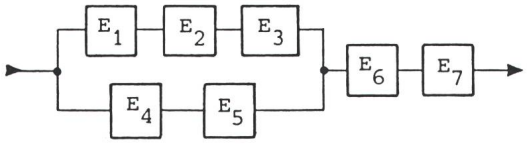
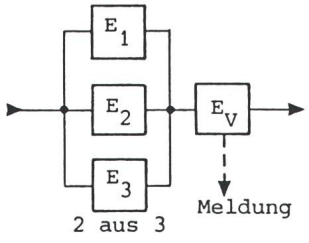
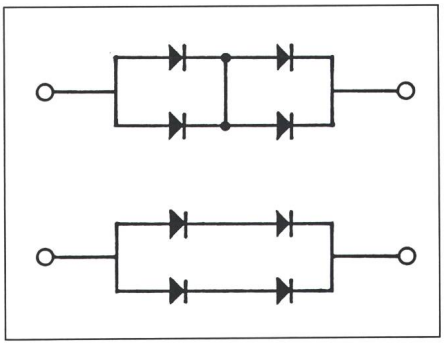
Zuverlässigkeitsblockdiagramm	Zuverlässigkeitsfunktion ($R_B = R_B(t)$, $R_i = R_i(t)$)	Bemerkungen
 1 aus 2	$R_B = R_1 + R_2 - R_1 R_2$	Redundanz 1 aus 2 für $R_1(t) = R_2(t) = e^{-\lambda t}$ gilt $R_B(t) = 2e^{-\lambda t} - e^{-2\lambda t}$
 k aus n	$R_1 = R_2 = \ldots = R_n = R$ $R_B = \sum_{i=k}^{n} \binom{n}{i} R^i (1-R)^{n-i}$	Redundanz k aus n für k = 1 gilt $R_B = 1-(1-R)^n$
	$R_B = (R_1 R_2 R_3 + R_4 R_5 - R_1 R_2 R_3 R_4 R_5) R_6 R_7$	Serien-/Parallelstruktur
 2 aus 3	$R_1 = R_2 = R_3 = R$ $R_B = (3R^2 - 2R^3) R_V$	Majoritäts-Redundanz (allg.Fall n+1 aus 2n+1)

Tabelle I Einfache Redundanzstrukturen und entsprechende Zuverlässigkeitsfunktionen
Heisse Redundanz mit unabhängigen Elementen, nicht reparierbar (bis Systemausfall)

Entwicklungsingenieur in Zusammenarbeit mit einem Zuverlässigkeitsspezialisten *bottom-up* durchgeführt. In der Regel beschränkt man sich auf die Schnittstellen und auf die kritischen Elemente. Die Prozedur ist in Tabelle II angegeben. Für die Untersuchung mechanischer Betrachtungseinheiten stellt die FMEA/FMECA eines der wichtigsten Analysewerkzeuge dar.

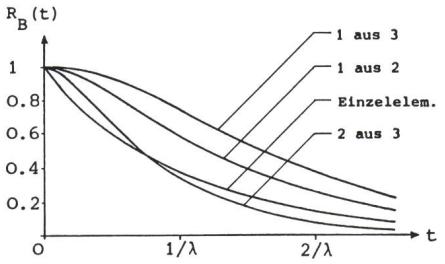
Neben der FMEA/FMECA ist auch die Fault Tree Analysis (FTA) bekannt, welche eine systematische Untersuchung der Auswirkung von Ausfällen und Fehlern erlaubt [1; 2; 10; 11; 12]. Dabei geht man *top-down* vom unerwünschten Ereignis (Top Event) aus und setzt es mit UND- bzw. ODER-Verknüpfungen von internen Ausfällen oder auch von externen Einflüssen zusammen. Ein Vorteil der FTA ist, dass sie auch Situationen behandeln kann, in welchen das unerwünschte Ereignis auf der Ebene der Betrachtungseinheit durch das Zusammenwirken mehrerer Ausfälle oder Fehler zustandekommt. Sie ist aber weniger systematisch als die FMEA/FMECA und gibt weniger Gewähr, dass alle Ausfall- und Fehlerarten berücksichtigt worden sind. Die Erfahrung zeigt, dass die FMEA/FMECA und die FTA sich gegenseitig ergänzen. Im übrigen gibt es auch Kombinationen von FMEA/FMECA und FTA.



Figur 1 Quadredundanz mit Dioden (mit oder ohne Brücke)

Oft muss eine Redundanz realisiert werden, welche zwei Ausfallarten (z.B. Kurzschluss und Unterbrechung) berücksichtigt. Eine Möglichkeit, die sich hier bietet, ist die Verwendung der Quadredundanz wie sie Figur 1 für den Fall einer Diode zeigt. Die Quadredundanz toleriert mindestens einen Ausfall irgendwelcher Art (Kurzschluss oder Unterbrechung). Sie wird mit der Methode des *Zustandsraums* untersucht [1].

Unter der Annahme, dass die betreffende Betrachtungseinheit die Bedingung für die Aufstellung des Zuverlässigkeits-Blockdiagramms erfüllt (pro Element eine Ausfallart und nur zwei Zustände), können die Gleichungen



Figur 2 Zuverlässigkeitsfunktion für das Einzelelement und für eine heisse Redundanz 1 aus 2, 1 aus 3, 2 aus 3, gemäss Tabelle I
konstante Ausfallrate λ

der Tabelle I für Sicherheitsanalysen herangezogen werden. Ist die Ausfallrate jedes Elements konstant $\lambda(t) = \lambda$, so gibt die Figur 2 den Verlauf der Zuverlässigkeitsfunktionen für das Einzelelement (G1.3) sowie für die Redundanzen 1 aus 2, 1 aus 3 und 2 aus 3. Wie aus Figur 2 ersichtlich ist, bleibt für kurze Missionen ($t \ll 1/\lambda$) die Ausfallwahrscheinlichkeit $(1 - R_B(t))$ bei den redundanten Strukturen praktisch Null. Um sehr kleine Ausfallwahrscheinlichkeiten zu erreichen, muss man also mit Redundanz operieren und eine möglichst kurze Missionsdauer anstreben.

Einfluss der Missionsdauer und der Wartung

Ist die Mission kurz und repetitiv (z.B. Flugzeug), so kann jede Mission für sich betrachtet werden und, wenn T die Missionsdauer und zu Beginn jeder Mission die Betrachtungseinheit neuwertig ist, so gibt

$$p = 1 - R(T) \qquad (7)$$

die Ausfallwahrscheinlichkeit in jeder einzelnen Mission wieder.

Ist die Missionsdauer lang, so kann mit der periodischen Wartung während der Mission die Ausfallwahrscheinlichkeit unter bestimmten Bedingungen reduziert werden. Zur Untersuchung sei hier eine Betrachtungseinheit mit der Zuverlässigkeitsfunktion $R(t)$ gegeben. Die Wartung erfolgt periodisch mit der Periode T_{PM}. Nach jeder Wartung sei die Betrachtungseinheit wieder neuwertig (d.h., verborgene Ausfälle sowie Verschlechterungen infolge Verschleisses oder Ermüdung werden während der Wartung entdeckt und behoben). Gesucht ist nun die Wahrscheinlichkeit für keinen Ausfall im ganzen Intervall $(0,t)$. Bezeichnet man diese Wahrscheinlichkeit mit $R_{PM}(t)$ und nimmt man an, die Dauer der Wartung sei vernachlässigbar, so gilt [1]:

$$R_{PM}(t) = R(t), \text{ für } 0 \leq t < T_{PM}$$

und (8)

$$R_{PM}(t) = R^n(T_{PM})\, R(t - n T_{PM}), \text{ für}$$

$$n\, T_{PM} \leq t < (n+1)\, T_{PM},\ n \geq 1.$$

Die Figur 3 zeigt den Verlauf von $R_{PM}(t)$, links für eine beliebige und rechts für eine konstante Ausfallrate. Man erkennt, dass nur im Falle einer beliebigen Ausfallrate (auf Systemebene) die Wartung einen Gewinn bringt. Unter Berücksichtigung der Gleichungen der Tabelle I wird ersichtlich, dass für Systeme mit Redundanz die Wartung einen Beitrag zur Erhöhung der Sicherheit leisten kann. Wichtig für alle Betrachtungen in Zusammenhang mit Redundanz bleibt aber auch die Untersuchung der Ausfallart.

1. Laufende *Numerierung* der Schritte.
2. *Bezeichnung* des betreffenden Elementes (z.B. Transistor, Speisung, Ventile usw.) und Kurzbeschreibung seiner Funktionen. Wenn möglich Referenzangabe zum Zuverlässigkeitsblockdiagramm.
3. Annahme einer möglichen *Ausfallart*. Dabei ist oft zu berücksichtigen, in welcher Betriebsphase einer Mission sich die Betrachtungseinheit befindet, denn ein Ausfall oder ein Fehler in einer früheren Betriebsphase kann einen Einfluss auf die gerade untersuchte Betriebsphase haben. Für jedes Element gemäss Punkt 3 sind nacheinander alle möglichen Ausfallarten zu betrachten.
4. Kurzbeschreibung der möglichen *Ursachen* für die in Punkt 3 angenommene Ausfallart. Die Identifikation der Ursachen ist notwendig, um die Auftrittswahrscheinlichkeit schätzen oder berechnen zu können (Punkt 9) und um Verhütungs- oder Kompensationsmassnahmen zu untersuchen (Punkt 7). Eine Ausfallart (Kurzschluss, Unterbrechung, Drift usw.) kann mehrere Ursachen haben. Ferner kann es sich um einen Primär- oder um einen Folgeausfall handeln. Alle unabhängigen Ursachen müssen identifiziert und untersucht werden.
5. Beschreibung der *Symptome*, durch welche sich die in Punkt 3 angenommene Ausfallart manifestiert, sowie der Möglichkeiten zur Lokalisierung des Ausfalls (Hinweise zur Instandhaltbarkeit). Ferner Kurzbeschreibung der lokalen Auswirkung des Ausfalls auf das betreffende Element und auf die Elemente, die in Beziehung mit diesem stehen (beispielsweise Input/Output).
6. Kurzbeschreibung der *Auswirkungen* der in Punkt 3 angenommenen Ausfallart auf die ganze Betrachtungseinheit in bezug auf die Sicherheit und auf die Erfüllung der geforderten Funktion.
7. Kurzbeschreibung der *Vorkehrungen*, welche die Auswirkung des Ausfalls mildern, die Auftrittswahrscheinlichkeit verkleinern oder die Weiterführung der Mission oder der geforderten Funktion erlauben.
8. *Gewichtung* der Auswirkung der angenommenen Ausfallart auf die Sicherheit und auf die Erfüllung der geforderten Funktion der ganzen Betrachtungseinheit. Die Bewertungsziffer wird in der Regel gemäss folgender Skala festgelegt: 1 = praktisch keine Auswirkung (sicher), 2 = Teilausfall (unkritisch), 3 = Vollausfall (kritisch), 4 = überkritischer Ausfall (katastrophal). Die Bewertung erfolgt mit Ingenieurgefühl.
9. Berechnung oder Schätzung der *Auftrittswahrscheinlichkeit* der in Punkt 3 angenommenen Ausfallart unter Berücksichtigung der in Punkt 4 identifizierten Ursachen. (Anstelle der Auftrittswahrscheinlichkeit kann auch die Ausfallrate angegeben werden.) Eine für Sicherheitsanalysen übliche Abstufung der Auftrittswahrscheinlichkeit ist A = häufig, B = wahrscheinlich, C = wenig wahrscheinlich, D = unwahrscheinlich, E = sehr unwahrscheinlich.
10. Zusammenfassung von Bemerkungen und *Anregungen* zu den Angaben der früheren Punkte, zur Einführung von Korrekturmassnahmen usw.

Tabelle II Prozedur für die Durchführung einer Failure Modes, Effects and Criticality Analysis (FMECA)

Sicherheitsprüfungen

Sicherheitsprüfungen sind notwendig, um die bei einer Betrachtungseinheit erreichte Sicherheit beurteilen zu können. Je früher damit begonnen wird, desto schneller können Schwachstellen, die in den Analysen nicht zum Vorschein kamen, entdeckt und mit geringem Aufwand behoben werden. Bei den Sicherheitsprüfungen werden in der Regel die Aspekte der Unfallverhütung und der technischen Sicherheit getrennt geprüft. Während sie für die Unfallverhütung oft einen deterministischen Charakter haben, stützen sich die Prüfungen der technischen Sicherheit auf die Methoden der

statistischen Qualitätskontrolle. Bei diesen geht es um die Ermittlung oder den Nachweis einer unbekannten Wahrscheinlichkeit p, die ähnlich der Gleichung (7) folgendermassen definiert werden kann

$$p = 1 - \text{Sicherheit} = 1 - Pr\{\text{kein überkritischer Ausfall}\}\ . \qquad (9)$$

Zur Ermittlung oder zum Nachweis von p geht man in der Regel von der Binomialverteilung aus. Für diese gibt

$$p_k = \binom{n}{k} p^k (1-p)^{n-k} \qquad (10)$$

die Wahrscheinlichkeit an, dass in n unabhängigen Versuchen genau k Misserfolge auftreten werden. Dabei wird p als bekannt vorausgesetzt. Im Falle einer Sicherheitsprüfung ist aber p unbekannt, und Zweck der Prüfung ist eben, p zu ermitteln oder nachzuweisen.

Ermittlung der Sicherheit

Wenn in n Versuchen genau k Misserfolge aufgetreten sind, so liefert

$$\hat{p} = k/n \qquad (11)$$

eine *Maximum-Likelihood-Schätzung* der unbekannten p. Zur besseren Eingrenzung des wahren Werts von p (Intervallschätzung) können aus Figur 3 die untere und die obere Vertrauensgrenze $\hat{p}_u$ und $\hat{p}_0$ für eine Aussagewahrscheinlichkeit $\gamma = 0{,}8$ oder $\gamma = 0{,}9$ bestimmt werden [1].

Nachweis der Sicherheit

Beim *Nachweis* von p geht es prinzipiell um die Prüfung der gleichen Vereinbarung, wie sie zwischen Lieferanten und Abnehmer im Falle der Eingangskontrolle besteht: Die Betrachtungseinheiten sollen mit einer Wahrscheinlichkeit $\geq 1-\alpha$ akzeptiert werden, falls die wahre (unbekannte) Wahrscheinlichkeit p (Gl. 9) kleiner als ein spezifizierter Wert p_0 ist, und sie sollen mit einer Wahrscheinlichkeit $\geq 1-\beta$ zurückgewiesen werden, falls p grösser als der maximal akzeptierbare Wert p_1 ist. α ist das Lieferantenrisiko (Fehler 1. Art), d.h. die Wahrscheinlichkeit, eine wahre Hypothese ($p<p_0$) zu verwerfen. β ist das Abnehmerrisiko (Fehler 2. Art), d.h. die Wahrscheinlichkeit, eine falsche Hypothese ($p<p_1$) anzunehmen. Die Überprüfung obiger Abmachung ist ein Problem der statistischen Hypothesenprüfung und kann mit Hilfe der zweiseitigen Einfach-Stichprobenprüfung erfolgen. Die Prozedur lautet:

1. Aus p_0, p_1, α und β bestimme man die kleinsten Zahlen c und n, für welche gilt

$$\sum_{i=0}^{c} \binom{n}{i} p_1^i (1-p_1)^{n-i} \leq \beta \qquad (12)$$

$$\sum_{i=0}^{c} \binom{n}{i} p_0^i (1-p_0)^{n-i} \geq 1-\alpha \qquad (13)$$

2. Man führe n Versuche durch und
   - verwerfe die Hypothese $p < p_0$ falls $k > c$
   - nehme die Hypothese $p < p_0$ an, falls $k \leq c$

   wobei k die Anzahl Misserfolge in den n Versuchen ist.

Die Lösung des Gleichungssystems (12) gibt z.B. für $p_1/p_0 = 2$ [1]:

$$c = 14,\ n = 10{,}17/p_0 \quad \text{für } \alpha \approx \beta \approx 0{,}093 < 0{,}1 \qquad (14)$$

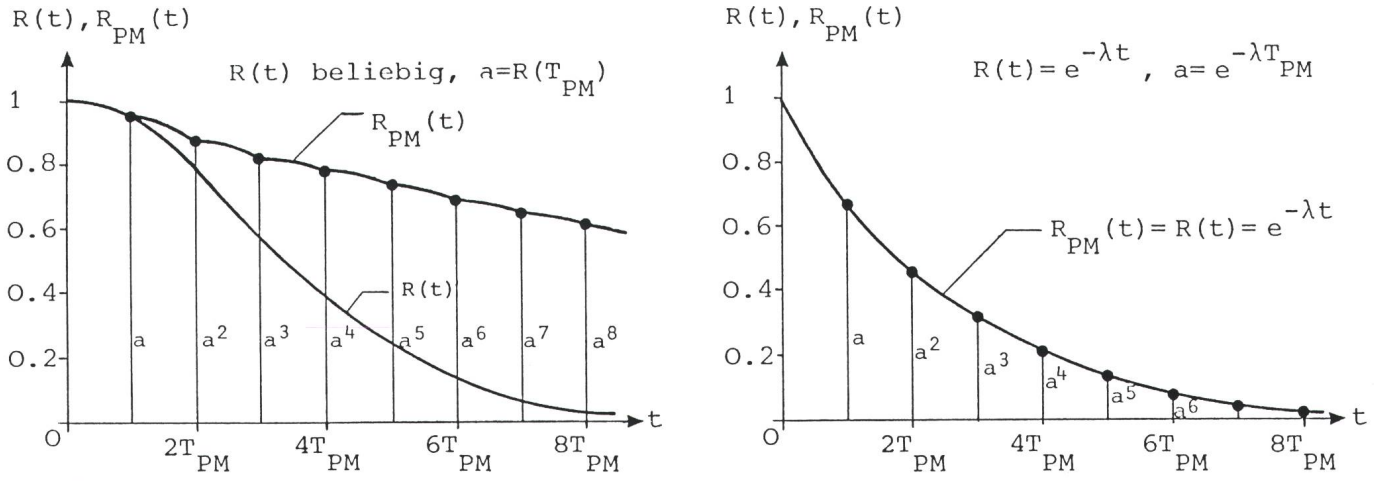
$$c = 6,\ n = 4{,}62/p_0 \quad \text{für } \alpha \approx \beta \approx 0{,}185 < 0{,}2.$$

Eine einseitige Prüfung der Form $p < p_0$ mit Wahrscheinlichkeit $1-\alpha$ oder $p < p_1$ mit Wahrscheinlichkeit β ist auch möglich[3]. Im Falle, das aus Kosten- oder anderen Gründen die Anzahl Versuche n begrenzt ist, muss man sich bei der Auswertung der Daten für Sicherherheitsprüfungen bemühen, auch die Resultate früherer Versuche oder Erfahrungen zu berücksichtigen.

Schlussfolgerungen, Ausblick

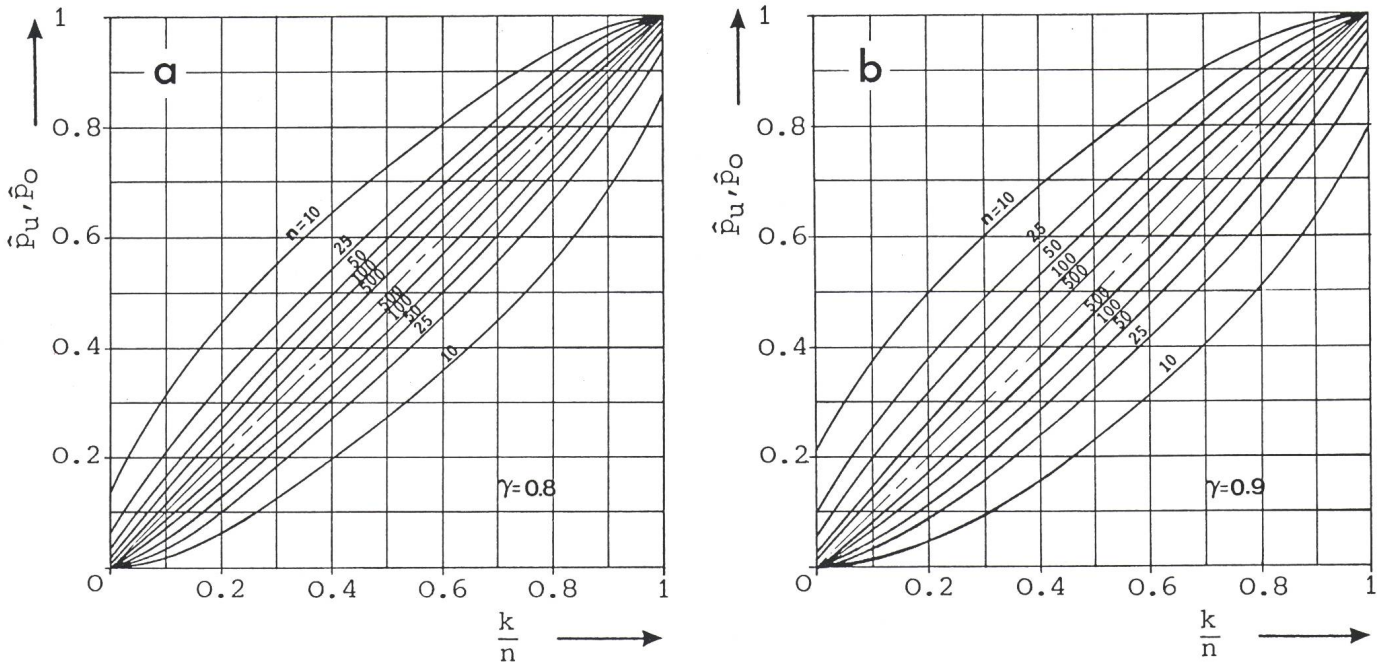
Die Analyse der technischen Sicherheit in Ergänzung zu klassischen Untersuchungen im Rahmen der Unfallverhütung drängt sich für viele Pro-

[3] Ähnlich der Eingangsprüfung nach AQL oder LTPD.



Figur 3 Verlauf der Zuverlässigkeit eines Einzelelements mit periodischer Wartung (Periode T_{PM}) für zwei Verteilungsfunktionen der ausfallfreien Arbeitszeit

Links beliebige, rechts konstante Ausfallrate



Figur 4 Vertrauensgrenzen $\hat{p}_u$ und $\hat{p}_o$ für eine unbekannte Wahrscheinlichkeit p in Funktion der beobachteten relativen Häufigkeit k/n, mit dem Stichprobenumfang n und der Aussagewahrscheinlichkeit γ als Parameter

a $\gamma = 0{,}8$ b $\gamma = 0{,}9$

dukte, insbesondere für technische Systeme, immer mehr auf. Dadurch soll die Gefahr für überkritische Ausfälle und damit auch das Risiko für einen Produkthaftpflichtfall unter eine tragbare Schwelle reduziert werden. Die genaue Berechnung einer solchen Gefahr ist praktisch nicht möglich. Eine Schätzung kann mit Hilfe der Werkzeuge der Zuverlässigkeitstechnik erfolgen, indem man sich bei der Berechnung der vorausgesagten Zuverlässigkeit auf die überkritischen Ausfälle beschränkt und den Auswirkungen der Ausfälle (Ausfallart) besondere Beachtung schenkt.

Bei den bis hierhin angestellten Überlegungen wurde der Einflussfaktor «Mensch» nicht berücksichtigt. Als irrationales Wesen bleibt der Mensch meist unberechenbar in seinen Reaktionen und Handlungen. Analysen von Unglücksfällen und Katastrophen zeigen, dass in vielen Fällen nicht technische Mängel ausschlaggebend waren, sondern menschliches Versagen vorlag [13,...15]. Untersucht man die Gründe, die zu diesem Versagen führten, findet man verschiedene Einflussquellen:

- sprachliche Fehlinterpretationen,
- mangelnde oder fehlerhafte Kommunikation,
- mangelnde oder fehlerhafte Instruktion,
- durch Routine herabgesetzte Aufmerksamkeit,
- Herabsetzung der kognitiven Fähigkeiten durch Stressbelastung,
- irrational-affektives Handeln infolge unbewusster Mechanismen,
- situative Affekthandlungen usw.

Die unbekannte Grösse «Mensch» spielt sowohl beim Herstellungsprozess eines technischen Systems als auch bei dessen Benützung eine wesentliche Rolle. In der Produktion beeinflusst die menschliche Komponente die Produktqualität und somit auch die Ausfallrate und die Unfallquote eines technischen Systems. Durch eine systematische Qualitätssicherung [1] können diese Faktoren weitgehend eliminiert werden. Im Gegensatz dazu besteht auf der Benützerseite keine vergleichbare Kontrollmöglichkeit, welche Anwenderfehler ausschalten könnte. Aus diesem Grunde ist es wesentlich, dass technische Systeme so konzipiert werden, dass eine missbräuchliche Verwendung beinahe ausgeschlossen bleibt. Ebenso entscheidend ist, dass unmissverständliche, klare und einfache Bedienungsanweisungen, die keine Fehlinterpretationen offenlassen, zur Verfügung gestellt werden. Trotz allem muss akzeptiert werden, dass das perfektionieren technischer Systeme an der Schnittstelle «Mensch» seine Grenzen findet.

Literatur

[1a] *A. Birolini:* Qualität und Zuverlässigkeit technischer Systeme. Theorie, Praxis, Management. Berlin u.a., Springer-Verlag, 2. Aufl. 1988.

[1b] *A. Birolini:* Zuverlässigkeitssicherung technischer Systeme. Bull. SEV/VSE 77(1986)7, S. 347...360.

[2] *Dhillon B.S.:* Human Reliability. New York a.o., Pergamon, 1986.

[3] Electronic reliability handbook. MIL-HDBK-338, 1984.

[4] Procedures for performing a failure mode, effects and criticality analysis. MIL-Standard 1629, edition A 1980.

[5] *F. Sevcik:* Current and future concepts in FMEA. Proc. Ann. Rel. & Maint. Symp., 1981, p. 414...421.

[6] Ausfalleffektanalyse. DIN 25448/06.80.

[7] *Hall F. a.o.:* Hardware/Software FMECA. Proc. Ann. Rel. & Maint. Symp., 1983, pp. 320...327.

[8] *Jackson T.:* Integration of sneak circuit analysis with FMEA. Proc. Ann. Rel. & Maint. Symp., 1986, pp. 408...414.

[9] *Jordan W.E.:* Failure modes, effects and criticality analysis. Nat. Symposium, 1972, pp. 30...37.

[10] Störfallablaufanalyse. Teil 1: Störfallablaufdiagramm, Methode und Bildzeichen. Teil 2: Auswertung des Störfallablaufdiagramms mit Hilfe der Wahrscheinlichkeitsrechnung. DIN 25419, Teil 1/06.77, Teil 2/02.79.

[11] Fehlerbaumanalyse; Methode und Bildzeichen. DIN 25424, Teil 1/09.81.

[12] IEEE Trans. Rel.: Special issue on nuclear system reliability and safety. 25 (1976), pp. 130...202.

[13] *A. Wildavsky:* Die Suche nach einer fehlerlosen Risikominderungsstrategie. In S. Lange u.a.: Ermittlung und Bewertung industrieller Risiken. Berlin u.a., Springer Verlag, 1984, S. 224...233.

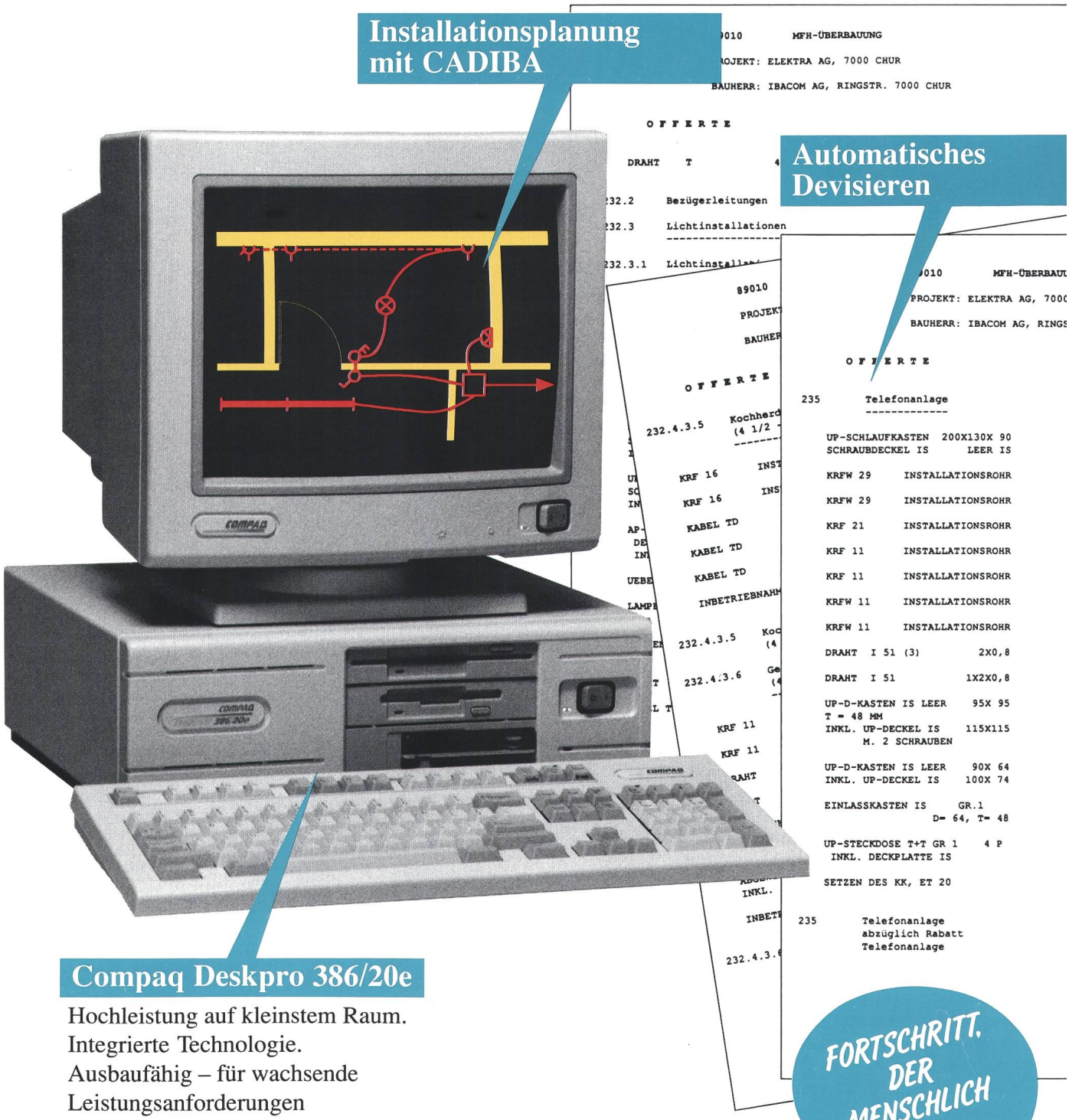
[14] *B. Umiker, P. Bisang:* Wie lassen sich grosse Industriekatastrophen verhüten? IO-Management Zeitschrift 56(1987)1, S. 15...22.

[15] *B.L. Whorf:* Sprache - Denken - Wirklichkeit. Hamburg, Rowohlt Verlag, 1984.

Überlassen Sie die Elektroinstallations-Planung COMPAQ und CADIBA®

Installationsplanung mit CADIBA

Automatisches Devisieren



Compaq Deskpro 386/20e

Hochleistung auf kleinstem Raum.
Integrierte Technologie.
Ausbaufähig – für wachsende
Leistungsanforderungen
professioneller Anwender.

FORTSCHRITT, DER MENSCHLICH IST.

IBACOM SOFTWARE AG
Ringstrasse 34
CH-7000 Chur
Telefon 081 25 11 55
Telefax 081 24 35 34

Software-Entwicklung

IBACOM
für Computer.

COMPAQ