Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 80 (1989)

Heft: 11

Artikel: Sicherheit oder Verfügbarkeit?

Autor: Kirrmann, H.

DOI: https://doi.org/10.5169/seals-903683

Sicherheit oder Verfügbarkeit?

H. Kirrmann

Neue technische Verfahren in Fabrikation, Transport oder Handel bringen neue Risiken mit sich. Der Erfolg einer technischen Anlage hängt davon ab, ob sie das Vertrauen des Publikums und der Anlagebetreiber gewinnt. Für das Publikum ist in erster Linie die Sicherheit (= kein Unfall) wichtig, für den Betreiber liegt die Verfügbarkeit (= kein Ausfall) an erster Stelle. Beide bestimmen die Wirtschaftlichkeit einer Anlage.

Die *Verfügbarkeit,* d.h. das Verhältnis der Produktionszeit zur Lebenszeit der Anlage, beeinflusst die Wirtschaftlichkeit auf vielfältige Weise. Die Produktionskosten pro Stunde lassen sich gut abschätzen. Steht jedoch eine Anlage still, so übersteigen die Verluste die Produktionskosten des gleichen Zeitraumes. Zum Beispiel haben die Elektrizitätswerke in Frankreich ausgerechnet, dass eine nicht produzierte Kilowattstunde etwa 40- bis 60mal teurer kommt als eine produzierte.

Die *Sicherheit* ist noch schwieriger zu bewerten. Eine Anlage gilt als sicher, wenn die Wahrscheinlichkeit eines Unfalles unter einem vertretbaren Wert liegt. Was «Unfall» oder «vertretbar» heisst, wissen – das ist leider so – am besten die Versicherungen. Grob ausgedrückt: die Sicherheit einer Anlage kann wirtschaftlich durch die Höhe ihrer Versicherungsprämien ausgedrückt werden.

Selbstverständlich sind die Anlagebauer bemüht, sowohl Sicherheit wie Verfügbarkeit durch eine hohe Zuverlässigkeit der Elemente einer Anlage zu steigern. Nun stösst aber die Erhöhung der Qualität der Elemente bald einmal auf wirtschaftliche Grenzen. Reicht nun für eine bestimmte Anwendung die Zuverlässigkeit der Anlagenelemente nicht aus, so werden Elemente redundant angelegt, wobei entschieden werden muss, ob die Redundanz zur Erhöhung der Sicherheit oder zur Erhöhung der Verfügbarkeit dienen soll.

Sicherheit und Verfügbarkeit sind nämlich gegensätzliche Forderungen; beide zerren an den Reserven der Anlage. Das Ersetzen der Sicherungen durch Kupferdrähte erhöht zwar die Verfügbarkeit der Stromversorgung, senkt aber die Sicherheit. Die Vermehrung von Sicherheitsvorschriften vermindert zwangsläufig die Verfügbarkeit. Schutzsysteme stoppen die Anlage häufiger als nötig, sei es durch eigenes Versagen oder aus übermässiger Vorsicht des Betreibers. Total sichere Flugzeuge bleiben am Boden, total sichere Fabriken produzieren nichts.

Umgekehrt können Anlagen gar nicht in Betrieb genommen werden, wenn ihre Sicherheit zweifelhaft ist. Bei grosstechnischen Projekten, die erhebliche Risiken bergen, werden immer strengere Auflagen gestellt. Diese erschweren zwar die Arbeit der Ingenieure, ermöglichen aber auch ihren Auftrag. Noch vor wenigen Jahren haben Kernkraftwerkingenieure mit Wehmut nach dem Osten geschaut, der ungehindert vom Publikumsdruck effiziente Kernkraftwerke bauen konnte, während sie selbst mit unmöglichen Sicherheitsreglementen zu kämpfen hatten. Es wurde sogar behauptet, jene Kraftwerke seien sicherer, weil sie weniger komplex seien. Die Ernüchterung kam mit dem Reaktorunfall in Tschernobyl.' Sicherheit und Verfügbarkeit müssen also gegeneinander abgewogen werden, und zwar schon sehr früh im Lebenszyklus eines technischen Produktes, z.B. bei einfachen Entscheidungen, wie sich eine Schaltung bei Stromausfall zu verhalten hat.

Die Spezifikationen einer Anlage bestehen heute aus zwei Teilen. Die eine besagt, was die Anlage machen soll (Verfügbarkeit), die andere, was sie nicht machen darf (Sicherheit). Diese Funktionsteilung wird in den meisten Anlagen beachtet: Die Schutztechnik wird von der Leittechnik streng getrennt. Bereits bei den ersten Dampfmaschinen wurde der Fliehkraftregler vom Überdruckventil getrennt. Heute üben Menschen die Leitfunktion aus, während Automaten die Schutzfunktion wahrnehmen. Die zunehmend komplexen Sicherheitsnormen können nicht mehr durch die blosse Abgabe von Betriebsvorschriften an das Bedienungspersonal erfüllt werden. Es wird dem Menschen nicht mehr zugetraut, über der Technik zu stehen. Die Eisenbahnen sind hier wegweisend gewesen. Heute überwachen in Öltankern und Kraftwerken Rechner die Zulässigkeit der Handlungen des Personals.

Diese Überwachung des Menschen durch die Maschine birgt bereits Konfliktstoff in sich. Einerseits ist das Personal versucht, durch Ausschalten der Sicherheitsvorschriften die Verfügbarkeit zu erhöhen. Tatsächlich ist «Dienst nach Vorschrift» eine Möglichkeit, die Produktion zum Erliegen zu bringen. Dabei hätte der automatische Schutz viele technische Katastrophen in den letzten Jahren (Bhopal, Tschernobyl, Three Miles Island) verhindern können, wenn er nicht absichtlich ausser Betrieb gesetzt worden wäre. Anderseits fühlt sich das Personal bevormundet oder verlässt sich übermässig auf die Schutzeinrichtungen. Beides kann verheerende Folgen haben. Typisch dafür war der Absturz eines Airbus, dessen Pilot aus Bravour die Automatik ausgeschaltet hat, um tiefer und langsamer zu fliegen als erlaubt, im Vertrauen darauf, dass die

Adresse des Autors

Dr. *Hubert Kirrmann,* dipl. El.-Ing. ETH, Asea Brown Boveri Forschungszentrum, 5405 Dättwil.

restlichen Schutzmechanismen ausreichen würden. Die fortschreitende Automatisierung und Informatisierung von Fahrzeugen, Flugzeugen, Banken und industriellen Anlagen verwischt die Funktionstrennung zwischen Schutz- und Leitsystem.

Wenn Automaten die Leitfunktion übernehmen, dann wird sofort nach deren Sicherheit gefragt: «Was passiert, wenn der Rechner versagt?» Die umgekehrte Frage «Was passiert, wenn der Mensch versagt?» wird seltener gestellt, sie ist auch schwieriger zu beantworten. Zeitungen registrieren jedes Versagen eines Rechners in einer kritischen Aufgabe mit publizistischer Freude. Wieviele Unfälle durch den Einsatz von Rechnern verhindert wurden, können sie hingegen nicht erwähnen. Diese Skepsis stammt zum Teil aus einem Konkurrenzdenken zwischen Mensch und Maschine. Der Mensch ist versucht, wenigstens auf dem Gebiet der Sicherheit eine Überlegenheit zu zeigen, die in der Praxis nicht nachweisbar ist. Bei jedem Schritt in Richtung Personaleinsparung durch Automaten wird das Argument der Sicherheit in den Vordergrund geschoben. Dies galt für die Bremser auf den englischen Dampflokomotiven, für die Funker an Bord von Propellerflugzeugen und tritt jetzt wieder in Zusammenhang mit dem Ersatz des Bordmechanikers im Cockpit des Airbus A320 auf.

Dort, wo sich die Leitautomatik durchgesetzt hat, hat sich das Publikum allen Unkenrufen zum Trotz dem menschenlosen Betrieb anvertraut. Bei den Aufzügen sind die Liftboys schon längst verschwunden. Befragungen der Passagiere des VAL (Metro der Stadt Lille in Frankreich) zeigen, dass die Abwesenheit des Führers keine besondere Beunruhigung hervorruft. Dafür hält die Vollautomatisierung die Betriebssicherheit hoch und senkt die Betriebskosten, so dass der VAL einer der wenigen selbsttragenden öffentlichen Verkehrsmittel ist. Die Verantwortung für die Sicherheit in vollautomatischen Systemen wird also nicht mehr dem Personal, sondern dem Ingenieur überlassen. Früher konnte sich der Ingenieur noch darauf verlassen, dass das Personal unvorhergesehene Situationen abfangen konnte. Jetzt müssen alle Situationen bereits in der Planungsphase berücksichtigt werden. Weiter besteht die Gefahr, dass die saubere Trennung zwischen Schutz- und Leitsystem verlorengeht, wenn die gleiche Maschine beide Funktionen übernimmt. Hier kommt die Verantwortung des Projektleiters hinzu, der beide Aufgaben unabhängigen Gruppen zuweisen sollte.

Das weitere Vordringen der Automatisierung hängt vorwiegend davon ab, ob beide Anforderungen, Sicherheit und Verfügbarkeit, ausgewogen erfüllt werden. Letzthin verstellt der Mensch die Waage. Er kann bei gleichem Risiko mehr produzieren, oder das Gleiche sicherer produzieren. Dabei verhält es sich wie beim Anti-Blokkier-System (ABS) auf Autos, das sich negativ auf die Sicherheit ausgewirkt hat: es verleitet die Fahrer eher dazu, bei gleichem Risiko schneller zu fahren als bei gleicher Geschwindigkeit sicherer zu fahren. Das übermässige Vertrauen in die eigene Fähigkeit ist die Achillesferse der Sicherheitstechnik.

Glossar

Qualität: Mass für das Erreichen der gestellten Anforderungen.

Verlässlichkeit: Oberbegriff, der die Fähigkeit einer Einheit umschreibt, ihre beabsichtigte Funktion frei von eigenen Fehlern zu erfüllen. Die Verlässlichkeit kann erhöht werden durch Verbesserung der Qualität des Entwurfs oder der Bauelemente (Fehlervermeidung) oder durch Redundanz (Fehlertoleranz). Verlässlichkeit ist damit ein Mass für die Voraussehbarkeit des Verhaltens einer Einheit bei Funktion und Ausfall. Sicherheitsprobleme entstehen, wenn die Verlässlichkeit überschätzt wird [sûreté de fonctionnement, dependability].

Zuverlässigkeit: Wahrscheinlichkeit, dass ein anfänglich funktionsfähiges Element eine geforderte Funktion unter vorgegebenen Arbeitsbedingungen während einer festgelegten Zeit ausfallfrei ausführt (gilt für nichtreparierbare Elemente). Die Zuverlässigkeit R wird ausgedrückt als Wert (z.B. R = 95% in 5 Jahren), als Funktion der Zeit (z.B. $R(t) = e^{-\lambda t}$) oder als deren Integral, die mittlere Funktionszeit (MTTF = Mean Time To Fail), z.B. MTTF = $1/\lambda$ [fiabilité, reliability].

Verfügbarkeit: Die Verfügbarkeit ist die Wahrscheinlichkeit, dass ein reparierbares Element zu einer Zeit t funktionstüchtig ist. Bei nicht reparierbaren Elementen fällt Verfügbarkeit mit Zuverlässigkeit zusammen. Die stationäre Verfügbarkeit A ist das Verhältnis der Funktionszeit zur Lebenszeit einer Einheit. Sie hängt von der Zuverlässigkeit des Elementes ab (mittlere Funktionszeit MUT = Mean Up Time) und von der Ausfalldauer (MDT = mittlere Ausfalldauer = Mean Down Time). Die Summe MUT + MDT wird als MTBF bezeichnet (MTBF = Mean Time Between Failure).

Ausgedrückt wird die Verfügbarkeit als: A = MUT/(MUT + MDT) = MUT/MTBF [disponibilité, availability].

Sicherheit: Wahrscheinlichkeit, dass der Ausfall eines Elementes nicht zu Schäden führt, die ein erträgliches Mass übersteigen. Wenn die gefährlichen Zustände der Anlage definierbar sind (z.B. als solche, wo das Risiko höher ist als das Grenzrisiko), kann die Sicherheit als die Wahrscheinlichkeit ausgedrückt werden, dass diese gefährlichen Zustände nicht erreicht werden [sécurité, safety].

Redundanz: Zusätzliche Betriebsmittel, welche für den normalen Betrieb nicht notwendig sind und ohne den Fehlerfall nicht nötig wären [redondance, redundancy].

Fehlertoleranz: In weitem Sinn die Fähigkeit einer Anlage, sich beim Auftreten eines Fehlers in ihren Teile definiert zu verhalten. Als spezifiziertes Verhalten kann die Anlage ihre Funktion aufrechterhalten oder sicher stoppen. Fehlertoleranz braucht dazu die in der Anlage vorhandene Redundanz.

Im engen Sinn ist Fehlertoleranz die Fähigkeit einer Anlage, ihre Funktion bei Ausfall eines ihrer Teile weiterzuführen (Überlebensfähigkeit).

Die *Fehlertoleranz einer Strecke* ist deren Fähigkeit, Ausfälle des Leitsystems während einer bestimmten Zeit (Toleranzzeit) zu ertragen [tolérance aux fautes, fault-tolerance].

Die Begriffsbildung auf dem Gebiet der Verlässlichkeit ist im Fluss. Unterschiedliche Definitionen sind zu finden in DIN 40041/42, NTG 3004, EWICS TC7, IFIP WG 10.4, IEEE und ISO.

Integrität: Fähigkeit einer Einheit, eine bestimmte Anzahl beliebiger Ausfälle eigener Teile zu überwinden, ohne falsche Daten auszugeben. In der Kodierungstheorie ist die Integrität gleich der Hamming-Distanz, die zwei gültige Kodewörter trennt (diese wird auch durch die Restfehlerwahrscheinlichkeit ausgedrückt) [intégrité, integrity].

Stetigkeit: Fähigkeit einer Einheit, eine bestimmte Anzahl beliebiger Ausfälle eigener Teile zu überwinden, ohne die Funktion einzustellen. In der Kodierungstheorie entspricht die Stetigkeit der Hamming-Distanz, innerhalb welcher Fehler korrigiert werden [persistance, persistency].