Redundanz entscheidet über Sicherheit : Einsatz von elektronischen Sicherheitssystemen

Autor(en): **Wydler, Ulrich**

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): **87 (1996)**

Heft 3

PDF erstellt am: **08.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-902299

Alle Errungenschaften der Elektronik, welche zur Steigerung der Sicherheit beitragen, sind nur unter der Voraussetzung nutzbar, dass sie zuverlässig funktionieren und eine hohe Verfügbarkeit aufweisen. Es hat sich gezeigt, dass die Mehrfachausführung von Bauteilen – Redundanz – die einzige gangbare Methode ist, elektronische Systeme wirksam vor Totalausfällen zu schützen. Sie kommt allerdings aus Kostengründen nur dann in Frage, wenn menschliche Unversehrtheit oder unverhältnismässige materielle Werte auf dem Spiel stehen.

Redundanz entscheidet über Sicherheit

Einsatz von elektronischen Sicherheitssystemen

■ Ulrich Wydler

Begonnen hat die Erforschung der Zuverlässigkeit elektronischer Komponenten mit der bemannten Raumfahrt. Die Anforderungen an Steuerung, Navigation und Systemüberwachung waren ohne Elektronik nicht zu bewältigen. Jedoch erwies sich die Elektronik im Vergleich zur robusten Mechanik als überaus empfindlich und störanfällig. Konnten dank Computereinsatz die ballistischen und steuertechnischen Probleme simuliert und mit der Zeit gelöst werden, so blieb doch das erhebliche Risiko, dass ein wichtiges elektronisches System versagte, zumal unter der extremen physischen Belastung während des Fluges. Da bessere Komponenten nicht kurzfristig verfügbar waren, musste das Problem der Verfügbarkeit und Zuverlässigkeit mit anderen Methoden gelöst werden.

Bei der Lösung dieser Schwierigkeit diente die Natur als Vorbild. Im Bereich der Fortpflanzung – welche über Weiterbestand oder Aussterben einer Art entscheidet – werden Befruchtungskeime im Überfluss produziert. Mit Millionen von Samen wird die Wahrscheinlichkeit, dass einer ein Ei befruchtet, so gross, dass der Fortbestand über Jahrmillionen sichergestellt ist. Der Einsatz einer Vielzahl von gleichartigen Elementen erhöht offenbar die Wahrscheinlichkeit, dass mindestens eines seine Aufgabe erfüllt. Diese Technik der Mehrfachausführung nennt man Redundanz.

Berechnung der Ausfallwahrscheinlichkeit

Auf die Technik übertragen heisst das, dass durch redundante Ausführung von Bauteilen, Baugruppen oder ganzen Systemen offenbar die Wahrscheinlichkeit wächst, dass immer eines einsatzfähig ist. Natürlich konnte man sich in der Raumfahrt mit einer solchen Wahrscheinlichkeit allein nicht zufriedengeben. Deshalb mussten Berechnungsgrundlagen erarbeitet werden, damit die statistische Ausfallwahrscheinlichkeit rechnerisch ermittelt werden konnte. Voraussetzung dafür war, dass über das Ausfallverhalten von Einzelkomponenten ausreichende Kenntnisse vorlagen. Darauf aufbauend, konnte in einem synthetischen Prozess die Ausfallwahrscheinlichkeit von Schaltungen, Subsystemen und Systemen berechnet werden. Auf dieser Grundlage hat sich die Zuverlässigkeitsanalyse elektronischer Systeme etabliert.

Erschwert wird die Sache allerdings dadurch, dass elektronische Bauteile empfindlich auf verschiedene Einsatzfaktoren reagieren, wie:

Adresse des Autors:
Ulrich Wydler, Leiter Unternehmensbereich Systemintegration + Service, Kaba Holding AG, 8153 Rümlang.

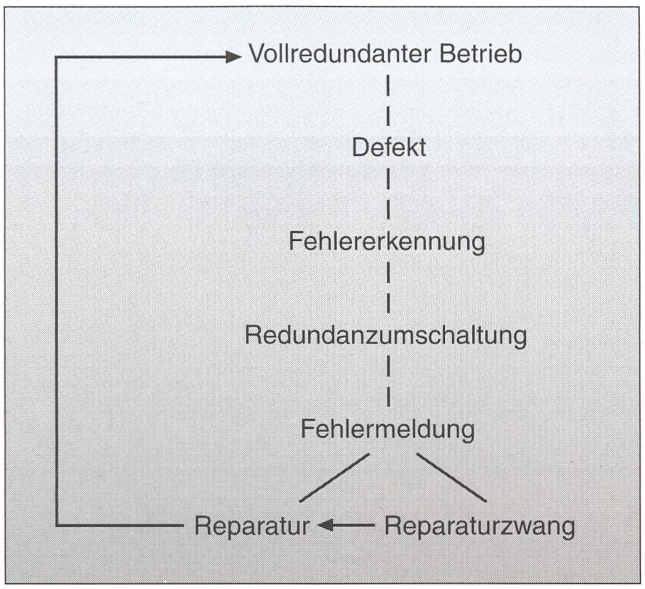

Bild 1 Ablaufzyklus für redundante Systeme

- Umgebungstemperatur
- physische Belastung (Vibration, Schock usw.)
- Verlustleistung
- Spannungsversorgung usw.

Es genügt also nicht, die Komponenten zu kennen; auch deren konkrete Einsatzkriterien müssen in die Rechnung eingehen. Das heisst, dass eine MTBF-Berechnung (Mean Time Between Failure) nur für einen konkreten Anwendungsfall in einer definierten Umgebung stimmt.

Enorme Reduktion der Ausfallwahrscheinlichkeit durch Redundanz

Am Beispiel eines doppelt redundanten Systems kann das enorme Steigerungspotential in der Systemzuverlässigkeit dargestellt werden. Die vereinfachte Berechnungsformel lautet:

$$MTTF = \frac{3\lambda + \mu}{2\lambda^2} \qquad (1)$$

Dabei bedeutet λ den Reziprokwert der Erwartungszeit für den Ausfall eines Systemteils und μ den Reziprokwert der Reparaturzeit. MTTF (Mean Time To Failure) wird als statistische Erwartungszeit für einen Totalausfall des redundanten Gesamtsystems definiert.

Offenkundig wird die Rechnung zusätzlich durch die Reparaturzeit erheblich beeinflusst. Dies ist auch sehr anschaulich: Wird ein doppelt redundantes System beim Defekt eines Systemteils nicht repariert, so führt der nächste Defekt am noch funktionierenden Teil zwangsläufig zu einem Totalausfall. Also kann man durch schnelle Reparatur die Wahrscheinlichkeit, dass zwei unabhängige Baugruppen ausfallen, erheblich senken. Könnte man die Reparatur in Null-Zeit durchführen, würde in der vereinfachten Formel (1) μ = unendlich, das heisst, die Erwartungszeit für einen totalen Systemausfall wäre unendlich lang: Es käme gar nie dazu, weil ja stets zwei vollständig funktionierende, redundante Systeme im Einsatz wären. Im anderen Extrem wird μ zu Null, wenn ein Defekt überhaupt nicht behoben wird. Dann lautet die Formel:

$$MTTF_{(\mu=0)} = \frac{3}{2\lambda} \qquad (2)$$

Das bedeutet, dass der Gewinn an Systemzuverlässigkeit für diesen Extremfall lediglich 50% beträgt. Für einen derart bescheidenen Gewinn wäre der Aufwand, Systeme und Baugruppen mehrfach auszuführen, viel zu gross.

Reparaturzeit entscheidet über Erwartungszeit für einen Systemausfall

Augenscheinlich hat die Reparaturzeit einen entscheidenden Einfluss auf die Ausfallwahrscheinlichkeit redundanter Systeme. Also muss die Reparatur so schnell wie möglich erfolgen. Reparieren kann man allerdings nur erkannte Fehler. Somit liegt in der Fehlererkennung ein zweiter Schlüssel zum zuverlässigen System. Hier wird der Ingenieur besonders gefordert, denn niemand kann jede Fehlermöglichkeit vorhersehen. Ein unerkannter Defekt – zum Beispiel ein Leck in einem Kernkraftwerk – kann fatale Folgen haben.

Auch für die systematische Fehlererkennung hat die Raumfahrt eine spezielle Methodik entwickelt, die FMEA (Failure Mode Effects Analysis). Hierbei wird jedes Bauteil auf seine möglichen Ausfallarten untersucht (ein Transistor verursacht im Defektfall z. B. einen Kurzschluss oder einen Unterbruch). Danach wird für jede Komponente und jede Ausfallart die Auswirkung auf das Gesamtsystem untersucht. Daraus ergeben sich die maximal möglichen Ausfallvarianten. Jetzt kann ein Fehlerdiagnoseprogramm entwickelt werden, welches auf jede Ausfallvariante reagiert. Bei vollautomatischen Systemen sind die Anforderungen an die Fehlererkennung besonders hoch, weil der Mensch als Überwachungsglied weitgehend wegfällt.

Erst Plausibilität entscheidet über Funktionstüchtigkeit

Nun arbeitet aber auch die Diagnose elektronisch, das heisst auch sie kann fehlerbehaftet sein. Deshalb muss die Schlussfolgerung «funktionstüchtig» oder «defekt» oft aus der Plausibilität gefunden werden. Plausibilität basiert auf dem Mehrheitsprinzip. Wenn beispielsweise von drei Diagnostikprogrammen zwei «funktionstüchtig» melden und das dritte «defekt», so ist anzunehmen, dass das Gesamtsystem «funktionstüchtig» ist, also das dritte System einen Diagnosefehler macht. Aus diesen Gründen werden vollautomatische Systeme oft drei- bis fünffach redundant ausgeführt (z. B. Flugregler bei Flugzeugen, Brennstabsteuerungen in Kernkraftwerken usw.).

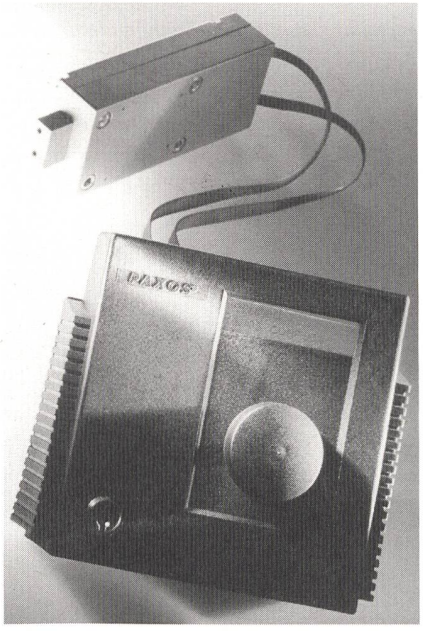

Bild 2 Beispiel einer vollredundanten Applikation: Hochsicherheitsschloss Paxos compact

Zwang zur Reparatur schliesst den Regelkreis der Redundanz

Die ganze Fehlererkennung nützt nichts, wenn die defekte Komponente nicht repariert wird. Bei Flugzeugen herrschen aus diesem Grund sehr strenge Vorschriften für die Meldepflicht von defekten Baugruppen. Neuerdings wird die Diagnostik sogar nach der Landung direkt vom Flugzeug «abgezapft». Bei anderen Systemen, wenn keine Menschenleben auf dem Spiel stehen, kommt eine Sperre für die Benutzung zum Einsatz, wenn ein Fehler nicht innert nützlicher Frist behoben wird. Erst wenn ein Reparaturzwang besteht, schliesst sich der Regelkreis, welcher eine Unterbrechung der Redundanz nur für einen kurzen Zeitraum zulässt.

Beispiel

An einem praktischen Beispiel soll der mit dieser Methode erreichbare Gewinn an Zuverlässigkeit gezeigt werden. Ein elektronisches Schloss ohne Systemredundanz erreicht einen angenommenen Wert *MTTF* = 5×10^4 h. Bei einem doppelt redundanten Schloss wird vom gleichen Wert für jedes redundante Teil ausgegangen. Die angenommene Reparaturzeit beträgt 72 h (mit Reparaturzwang). Nach Formel (1) errechnet sich eine $MTTF = 15\times10^6$ für das redundante System. Gemessen am nicht redundanten System bedeutet dies – bei doppeltem Aufwand – eine um einen Faktor 300 gesteigerte Erwartungszeit für einen Totalausfall.

Doppelt ist der Aufwand allerdings nur in der Herstellung des Produktes. In der Entwicklung steigert sich dieser um das 5- bis 10fache. Aus wirtschaftlichen Erwägungen lohnt sich deshalb die Redundanz nur dort, wo Menschenleben in Gefahr sind (Flugzeugelektronik, Zweikreisbremssystem beim Auto usw.) oder wo der totale Systemausfall unverhältnismässige Folgekosten generiert (Satelliten, Tresortüren usw.). Die Redundanz ist die einzige Methode, um ein elektronisches System wirksam vor dem Totalausfall zu schützen.

Literatur

Alessandro Birolini: Qualität und Zuverlässigkeit technischer Systeme, Springer-Verlag.

La redondance est déterminante pour la sécurité

Tous les progrès de l'électronique qui concourent à augmenter la sécurité ne sont exploitables que si leur fonctionnement est fiable et que s'ils présentent une haute disponibilité. Il s'est avéré que l'exécution multiple de composants – redondance – est la seule méthode praticable pouvant assurer une protection efficace des systèmes électroniques contre les défaillances totales. Cependant, pour des raisons de coûts, elle n'entre en ligne de compte que si l'intégrité humaine ou des valeurs matérielles particulièrement élevées sont en jeu.