Fehlertolerante Systeme in der Automatisierungstechnik

Hubert Kirrmann, Karl-Erwin Großpietsch

Vor zehn Jahren war die Welt des industriellen Einsatzes fehlertoleranter Rechner noch in zwei weitgehend getrennte Fachgebiete unterteilt: Sicherheit und Verfügbarkeit.

Sichere Rechner werden eingesetzt, wo resultierenden Unfällen die Hauptsorge gilt, also in traditionell sicherheitsbewussten Gebieten, wie bei Druckpressen, chemischen und nuklearen Reaktoren oder bei der Eisenbahnsignalisierung. Von sicheren Rechnern wird erwartet, dass sie bei Ausfall keine falsche Daten liefern, wobei ein Ausbleiben der Funktion in Kauf genommen wird.

Verfügbare Rechner kommen dort zum Einsatz, wo Ausfälle das Hauptproblem sind, also dort, wo große wirtschaftliche Verluste durch Ausbleiben der Rechnerfunktion entstehen würden, wie in Telefonzentralen, Energieunternehmen oder Lagerhäusern. Von verfügbaren Rechnern wird erwartet, dass sie bei Ausfall die Funktion innerhalb kurzer Zeit wieder herstellen, wobei falsche Daten kurzzeitig in Kauf genommen werden.

Auch die Fachleute trafen sich auf getrennten Tagungen, auf der Safecomp-Konferenz wurde über Sicherheit, Nachweis und Validierung diskutiert, während auf der FTCS (Fault-Tolerant Computing Symposium) – Konferenz Themen der Verfügbarkeit, des Tests und der Diagnose im Vordergrund der Betrachtung standen.

Die Fachgebiete griffen stärker ineinander, als Rechner in Anwendungen eingesetzt wurden, bei denen der Ausfall des Rechners nicht nur die Verfügbarkeit beeinträchtigt, sondern auch die Sicherheit, und dies selbst dann, wenn der Rechner nur kurzzeitig aussetzt. Die ersten, frühen Beispiele von zugleich verfügbaren und sicheren Rechnern kamen aus der Raumfahrt, wie z. B. der Saturn V – Rechner der Mondflüge. Bei diesen kurzen Missionszeiten wurden Fehler durch 2-aus-3-Auswahl maskiert, ohne Reparaturmöglichkeit. Beim Space Shuttle war die Missionszeit länger, es wurde mit massiver Redundanz gearbeitet und zum ersten Mal wurde diversitär programmiert, eine Methode, die sonst nur Sicherheitssysteme kannten.

Mit dem Fly-by-wire (Airbus 320 und einige Jahre danach Boeing 777) entstand eine Generation von Rechnern, bei welcher das Zeitintervall, in dem der Rechner auf Grund eines Ausfalls ganz aussetzen oder falsche Daten liefern darf, sehr kurz (einige 100 ms) wurde. Hier kamen sowohl diversitäre Software wie maskierende Hardware zum Zuge.

In der Eisenbahnsignalisierung verbreitete sich nach dem Brand im Ärmelkanaltunnel am 18. November 1996 (welcher hätte vermieden werden können, wenn die Lok weitergefahren wäre) die Einsicht, dass es nicht genügt, bei Versagen des Rechners die Notbremse zu ziehen – Sicherheit kann durch Stillstand auch gefährdet werden. Ein Beispiel, das bei einem primär auf Sicherheit ausgelegten System auch die Verfügbarkeits-Probleme in der Automatisierungstechnik deutlich machte, war der spektakuläre Ausfall des neuen, von Siemens entwickelten Steuerungssystems für das Stellwerk des Bahnhofs Hamburg-Altona im März 1995, wenige Tage nach der Inbetriebnahme: Dieses Ereignis hatte monatelange Behinderungen des Eisenbahnverkehrs im Hamburger Raum zur Folge und führte dadurch auch einer breiteren Öffentlichkeit vor Augen, wie sich Systemfehler in hochkomplexen Steuerungssystemen auf die Verfügbarkeit von Diensten des Alltagslebens wie etwa Eisenbahn-Linien auswirken können. Fehlertoleranz-Lösungen für die Automatisierungstechnik sollten in der Zukunft also beiden Aspekten, Sicherheit und Verfügbarkeit, in integrierter Weise Rechnung tragen.

Rechner mit Sicherheitscharakter finden eine immer größere Verbreitung, so hielten sie in den neunziger Jahren ihren Einzug in Straßenfahrzeuge im Zusammenhang mit dem Airbag, dann mit dem Antiblockier-System (ABS) und anderen elektronischen Stabilitäts-Programmen (ESPs), unter steigenden Anforderungen. Die Einwirkung des Rechners auf die Bremsen ist eine kritische Funktion, welche in erster Linie von den Rechnern Integrität (keine Aktion bei Ausfall) verlangt.

Drive-by-Wire, oder die direkte Radauslenkung durch Rechner, ohne mechanische oder hydraulische Rückfallebene, ist eine der anspruchsvollsten Anwendungen. Dies mag erstaunen, denn Straßenfahrzeuge sind einfacher aufgebaut als Flugzeuge. Der Grund liegt in der benötigten aktiven Spurführung, welche nur sehr kurzes Aussetzen der Funktion und noch kürzere Zeitintervalle, in denen ausfallbedingt Daten verfälscht werden, erlaubt. Ein Auto legt bei 144 km/h eine Distanz von 4 m in 100 ms zurück, bei einer fehlerhaften Vollauslenkung bleiben für eine Korrektur wenige Millisekunden übrig. Ein Flugzeug dagegen, außer in der kurzen Zeit vor dem Aufsetzen, hat einen viel größeren Manövrierraum. Neue fehlertolerante Rechnerarchitekturen der Autoindustrie, die zur Erfüllung der Sicherheitsanforderungen für Drive-by-Wire-Systeme entwickelt wurden, sind hier wegweisend: Sie könnten in industriellen Steuerungen die gleiche Bedeutung erlangen, wie der CAN-Bus (ursprünglich auch für die Automobilindustrie entwickelt) bei den Feldbussen.

Eine weitere Tendenz der gegenwärtigen Entwicklung ist der zunehmende Anteil an herkömmlichen (Commercial Off-the-Shelf) Komponenten in Sicherheitsanwendungen. Die Erkenntnis verbreitet sich, dass Rechnersysteme so komplex geworden sind, dass niemand mehr für ihr Verhalten Gewährleistung übernehmen kann. Dies trifft ebenso für die spezialisierten Steuerungen zu, die traditionell im Sicherheitsbereich eingesetzt werden. Abgesehen von kritischen, aber simplen Komponenten wie Vergleichern macht es wenig aus, ob Komponenten speziell (d. h. teuer) für die Sicherheitstechnik entwickelt wurden, oder ob sie aus anderen Industriebranchen wie der Prozessautomatisierung kommen: Es kommt auf die Art und Weise an, wie sie eingesetzt werden. In der Tat wurden viele spezialisierte Sicherheitsrechner durch Zusammenschaltung von herkömmlichen Industriesteuerungen und Netzwerken (mit etwas Zusatz) ersetzt. Darum sind auch sogenannte ,,Sicherheitsbusse“ vor allem ein Marketingbegriff. Sicherheit kann kein Bus und keine Steuerung gewähren, sondern erst die Gesamtheit einer Leitanlage für eine bestimmte Strecke. Für herkömmliche Komponenten spricht ihr millionenfachen Einsatz in verschiedenen Anwendungen. Ihre Tücken sind vorhanden, aber bekannt. Hingegen fehlt bei speziellen Sicherheitsrechnern die Erfahrung, weil ihre Menge viel kleiner ist. Man kann auch zwischen Riffen sicher segeln – man muss nur wissen, wo sie sind.

Eine weitere Entwicklung ist die zunehmende Normung. Verschiedene Einsatzgebiete haben schon lange ihre eigenen Normen, wobei Deutschland Vorreiter mit den VDE-Normen spielte. Vermehrt nehmen Hersteller Bezug auf die IEC-Norm 61508 oder auf ähnliche Europa-Normen. Dem Anwender sollte aber bewusst sein, dass diese Normen lockere Richtlinien sind, und dass der Nennung eines Sicherheitsniveaus (SIL) nicht mehr Bedeutung zugemessen werden darf als einer ISO 9001-Zertifizierung. Hingegen ist der IEC-Standard 61508 ein Türöffner für zukünftige, griffigere Normen. Die Zertifizierung einer Steuerung gemäß einer Norm ist eine gute Voraussetzung, jedoch keine Garantie, dass die Anlage sicher betrieben wird. Letztlich bestimmt die Anwendung, wieviel Redundanz und Fehlertoleranz notwendig und zumutbar sind.

Um für Steuerungssysteme der Praxis sowohl hohe Sicherheit und als auch hohe Verfügbarkeit zu erreichen, müssen also im Allgemeinen Maßnahmen auf unterschiedlichen Ebenen ineinandergreifen:

- Benutzung grundlegender Redundanz-Techniken,
- Anpassung an spezifische System-Bedingungen, z. B. an die Situation in den industriell immer wichtigeren eingebetteten Systemen (wie z. B. Airbag-Systeme) aus digitalen und nicht-digitalen Komponenten,
- Entwicklung von modular aufgebauten Systemlösungen aus Standardbausteinen und durch Kombination unterschiedlicher, miteinander verträglicher Methodiken,
- Testen und Verifikation, z. B. auch in Hinblick auf die geforderte Zertifizierung von Systemen.

Einige der oben beschriebenen unterschiedlichen Aspekte werden in den sechs Beiträgen dieses Schwerpunktheftes vertieft. Der erste Aufsatz gibt eine Übersicht über die in der Praxis gegenwärtig benutzten Techniken zum Erreichen von Fehlertoleranz bei Steuerungen im Automatisierungswesen. Zunächst werden mögliche Arten von Ausfällen beschrieben, und es wird ihr Einfluss auf gesteuerte industrielle Strecken diskutiert. Dann werden die wesentlichen Redundanzmethoden vorgestellt, um verschiedene Grade von Fehlertoleranz zu erreichen. Abschließend wird auf Standardisierungsbemühungen für fehlertolerante industrielle Steuerungen eingegangen, und es werden Beispiele gesteuerter Strecken aus der industriellen Praxis einschließlich der hierfür jeweils gewählten Fehlertoleranz-Lösungen aufgeführt.

Der nachfolgende Beitrag von *E. Dilger* und *W. Dieterle* von der Robert Bosch GmbH gibt einen Überblick über die Verlässlichkeits-Anforderungen an neue Architekturen für die gegenwärtig zunehmend zum Einsatz kommenden X-by-wire-Steuerungen. Fehlertoleranz-Lösungen für diese Probleme werden diskutiert. Ein zentraler Aspekt bei diesen Architekturen ist die geforderte hohe Verfügbarkeit der Kommunikationssysteme, wie sie beispielsweise durch eine zeitgetriggerte Betriebsweise des CAN-Busses erreicht wird.

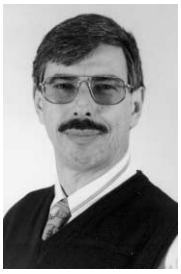
Ein Beitrag aus dem Bereich der Eisenbahnsignalisierung von *J. Braband* von der Siemens AG präsentiert eine Sicherheits-Analyse von Kommunikationssystemen, die aus kommerziellen Standard-Komponenten aufgebaut sind. Diese Analyse führt auf Lösungen, die eine Benutzung solcher Standard-Komponenten auch für sicherheitskritische Anwendungen ermöglichen.

Die systematische Kombinierbarkeit von Lösungsansätzen für den Entwurf eines fehlertoleranten Systems wird in dem Beitrag von *M. Auerswald*, *M. Herrmann*, *S. Kowalewski* und *V. Schulte-Coerne* von der Robert Bosch GmbH betrachtet. Die Autoren beschreiben ein Vorhaben, die bekannten Fehlertoleranztechniken im Hinblick auf ihre industrielle Einsetzbarkeit zu klassifizieren und zu bewerten.

Der abschließende Beitrag von *E. Pofahl* vom TÜV Rheinland erläutert die Techniken des TÜV zur Prüfung und Zertifizierung elektronischer Steuerungsssysteme.

Aus Platzgründen wird ein weiterer Beitrag von *R. Budde*, *A. Poigné*, und *K.-H. Sylla* von der Fraunhofer-Gesellschaft, der sich dem für komplexe sicherheitskritische Systeme ebenfalls immer wichtiger werdenden Aspekt der Verifikation von Systemen mittels formaler Methoden widmet, in einer späteren Ausgabe erscheinen; der Aufsatz baut dabei auf zwei vorangegangenen und einem in diesem Heft (unter der Rubrik ,,Theorie für den Anwender“) erscheinenden kurzen Einführungsbeitrag über die sogenannte synchrone Programmierung auf.

Insgesamt konnten bei der Vielschichtigkeit der behandelten Thematik natürlich nicht alle Aspekte im begrenzten Rahmen dieses Themenhefts diskutiert werden; wir glauben jedoch, dass die Auswahl der Beiträge die gegenwärtigen Schwerpunkte der Entwicklung bei fehlertoleranten Steuerungssystemen widerspiegelt.



Prof. Dr. Hubert Kirrmann ist Senior Scientist am ABB Forschungszentrum in Baden (Schweiz) und unterrichtet an der Eidgenössischen Technischen Hochschule in Lausanne. Seine Arbeitsgebiete sind industrielle, fehlertolerante Leitsysteme und Kommunikationsbusse. Er ist Editor des Standards IEC 61375 (Train Communication Network) und Member of the Editorial Board of IEEE MICRO.

Adresse: ABB Forschungszentrum, CH-5405 Dättwil, Schweiz. E-Mail: hubert.kirrmann@ch.abb.com

Dr. Karl-Erwin Großpietsch ist Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Autonome intelligente System (FhG-AiS) in St. Augustin-Birlinghoven. Seine Arbeitsgebiete sind Fehlertoleranz, Rechnerarchitektur und autonome Systeme; die Ergebnisse dieser Arbeiten sind in über 130 Veröffentlichungen dokumentiert. Seit März 1998 ist er Sprecher des GI/ITG-Fachausschusses „Verlässlichkeit und Fehlertoleranz“; seit September 2001 ist er außerdem Chairman des Board of Directors der Euromicro.

Adresse: Fraunhofer-Gesellschaft, Institut für Autonome intelligente Systeme, D-53754 St. Augustin.
E-Mail: grosspietsch@ais.fraunhofer.de