ÜBER HARDWAREIMPLEMENTIERBARE FEHLERTOLERANZ BEI INDUSTRIELLEN AUTOMATISIERUNGSSYSTEMEN MIT SEHR HOCHINTEGRIERTEN PROZESSOREN

Albrecht Weinert
Siemens AG, Karlsruhe
Systemtechnische Entwicklung

Kurzfassung

Die auch historisch bedingte Trennung zwischen sicherheitsgerichteter "Failsafe-" Technik und der übrigen, auch der fehlertoleranten, Automatisierungstechnik scheint bei zunehmendem Einsatz der Mikrorechnertechnik und komplexeren Prozessen immer weniger gerechtfertigt. Die Gründe hierfür werden zusammengestellt.

Serienmäßige industrielle Automatisierungssysteme bieten eine Basis für untereinander vollkompatible nichtfehlertolerante Standard- sowie für sicherheitsgerichtete und hochverfügbare Konfigurationen. Sie können diese Trennung und die damit verbundenen Nachteile überwinden. Ein Vorteil einer solchen durchgängigen Kompatibilität - auch unter Sicherheitsaspekten - ist es, daß sicherheitsrelevante Automatisierungssysteme bei Beobachtung, Bedienung und Wartung für die Benutzer praktisch genauso aussehen wie die gewohnten übrigen Systeme einer Anlage.

Diese Ziele wurden bei einem serienmäßigen, industriellen Automatisierungssystem mit hardware-implementierbarer Fehlertoleranz erreicht. Bestimmte Merkmale dieses beispielhaft angeführten Systems, wie die Verwendung besonderer Bit-Slice-Prozessoren, begünstigten eine solche hardwareorientierte Lösung. Die Anwendbarkeit dieses bewährten Ansatzes auch bei Automatisierungssystemen mit hochintegrierten Prozessoren wird im Beitrag erörtert.

Stichworte

Verfügbarkeit, Sicherheit, industrielle Automatisierungssysteme, VLSI-Prozessoren, Diversität, hardwareimplementierte Fehlertoleranz.

1. Fehlertoleranz und Sicherheit bei Automatisierungssystemen

Redundanz wird bei Automatisierungssystemen mit zwei Zielrichtungen eingesetzt:

- o das sicherheitsgerichtete oder "Failsafe-"Verhalten, im folgenden i. a. einfach mit "F" bezeichnet oder
- o die erhöhte Verfügbarkeit, im weiteren "H" genannt.

F : Ein F-Automatisierungssystem soll bei Anwesenheit (innerer) Fehler in einen einfachen stationären "Aus"-Zustand übergehen.
Der gesteuerte Prozeß muß so angeschlossen sein, daß der Auszustand des Automatisierungssystems ihn in einen sicheren Zustand überführt. Das Prinzip ist auf solche Prozesse beschränkt, bei denen immer ein so einfach erreichbarer sicherer Zustand existiert.

H : Ein H-Automatisierungssystem soll auch bei Anwesenheit zu tolerierender Fehler (im Automatisierungssystem selbst) seine spezifizierten Prozeßführungsdienste aufrecht erhalten. Dabei kann eine Leistungsminderung im Sinne einer sog. "graceful degradation" bei Echtzeitsystemen i. a. nicht hingenommen werden. Häufig wird von H-Systemen die ("on-line"-) Reparierbarkeit im ungestört weiterlaufenden Betrieb gefordert. Derartige on-line-reparierbare H-Automatisierungssysteme können über Jahre hinweg ununterbrochen in Betrieb sein.

Sicherheit im Sinne eines Failsafe-Verhaltens (F) und eine erhöhte Verfügbarkeit (H) der normalen Prozeßsteueraufgaben erscheinen als unterschiedliche und widersprüchliche Anforderungen an ein Automatisierungssystem. Und so werden beide Bereiche, H und F, vielfach mit unterschiedlichen Forschungs- und Entwicklungsansätzen und mit verschiedenen Produkten abgedeckt. Diese teilweise strenge Trennung geht auch noch auf die nicht-elektronische Automatisierungstechnik zurück. In der konventionellen Technik ließ sich für Prozesse, die einen jederzeit einfach erreichbaren, sicheren Aus-Zustand haben, ein hochwertiges, verläßliches Failsafe-Verhalten mit oft vergleichsweise geringem Zusatzaufwand erreichen. Ein dabei wesentliches und konsequent anzuwendendes Prinzip ist es, Zuständen mit niedrigerer (potentieller, kinetischer, magnetischer) Energie des Automatisierungs- oder Steuersystems sicherere Prozeßzustände zuzuordnen.

In der konventionellen Technik sind der Einsatz hochwertiger Bauelemente und Materialien sowie bei nichtelektronischer Technik auch die vorbeugende Wartung wirksame und gängige Maßnahmen zur Erhöhung der Verfügbarkeit. Fehlertoleranzmaßnahmen hingegen sind für die konventionelle Technik weniger adäquat und auch ungebräuchlich. Daß die konventionelle Technik reine F-Lösungen begünstigt, Fehlertoleranzverfahren hingegen eher behindert, ist einer der Gründe für die erwähnte Eigenständigkeit bzw. Abtrennung des Failsafe- oder Sicherheitsbereiches von der übrigen, auch der der fehlertoleranten Automatisierungstechnik. Das Ausgehen vom erreichten Stand der Technik und den entsprechenden Vorschriften führte nach Einzug der Elektronik in die Automatisierungstechnik bei vielen Anwendungen zu ganz speziellen F-Systemen. Auch ohne die begünstigten Voraussetzungen der konventionellen Technik wird mit z. T. erheblichem Aufwand das in der konventionellen Technik übliche reine F-Verhalten erreicht. Solche speziellen F-Systeme erfüllen dann die an sie gestellten hohen Sicherheitsanforderungen, sind aber i. a. mit anderen betrieblichen Anforderungen und mit der übrigen (Nicht-F-) Automatisierungstechnik schlecht vereinbar.

Die auch historisch bedingte Abtrennung des Sicherheits- oder F-Bereichs von der übrigen Automatisierungstechnik erscheint aber bei Einsatz der Mikrorechnertechnik und bei komplexeren Prozessen nicht mehr im traditionellen Maße gerechtfertigt:

- Ganz spezielle und in kleinen Stückzahlen eingesetzte F-Systeme haben einige, teilweise nicht unproblematische Besonderheiten. Für Entwicklung, Test, Dokumentation, Wartung, Ersatzteilversorgung etc. muß ein großer Aufwand getrieben werden; dennoch wird die bei großen serienmäßigen Automatisierungssystemen mögliche Breite und Durchdringung doch nicht erreicht werden. Genausowenig können Spezialsysteme die umfassende Betriebsbewährung serienmäßiger Automatisierungssysteme in zahlreichen, unterschiedlichen Anwendungen erlangen. Werden neben einem serienmäßigen Automatisierungssystem spezielle F-Systeme eingesetzt, so muß das Personal deren Bedienung, Beobachtung und Wartung zusätzlich lernen. Die mit dem ständigen Umgang mit den serienmäßigen Systemen gewonnenen und aufrechterhaltenen Erfahrungen kommen so (gerade) dem Sicherheitsbereich nicht zugute.

- Ein (reines) F-System neigt dazu, aufgrund von Fehlern im Automatisierungssystem den betreffenden ungestörten (!) Prozeß häufig bzw. zu häufig sicherheitsgerichtet stillzusetzen. Die durch dieses Verhalten vergleichsweise verminderte Verfügbarkeit beeinträchtigt die Sicherheit primär nicht; je strenger die Sicherheitsvorschriften sind, desto stärker ist i. a. der genannte Effekt. Falls die Genehmigungsvorschriften und -behörden dies in einer praktikablen Form zulassen, sind viele Betreiber bereit, für eine höhere Verfügbarkeit (H) unter Beibehaltung des geforderten sicherheitsgerichteten Verhaltens (F), d. h. für ein "HF"-System, auch mehr zu investieren.

- Solche "H-Erweiterungen" werden den Betreibern gestattet, sofern sie das (genehmigungsrelevante) F-Verhalten nicht beeinträchtigen. Es wird gelegentlich übersehen, daß ein solches als nicht sicherheitsschädlich zugestandenes H-Verhalten in eine auch unter Sicherheitsaspekten richtige Richtung geht. Solange durch geeignete H-Maßnahmen und vielfach auch On-line-Reparaturen, die spezifizierten Funktionen des Automatisierungssystems vollkommen aufrechterhalten werden können, besteht keine Notwendigkeit sicherheitsgerichtete Abschaltungen herbeizuführen. Ein Automatisierungssystem mit theoretisch 100 %iger Verfügbarkeit aller seiner spezifizierten Prozeßsteuerfunktionen wäre auch 100 %ig sicher. Zudem ist diese Art "Sicherheit durch Verfügbarkeit" eines Automatisierungssystems unabhängig von der Existenz eines einfachen, sicheren Prozeßzustandes. Man kann durchaus sagen, daß ein sehr zuverlässiges H-Verhalten gegenüber dem F-Verhalten die höherwertige und umfassendere Eigenschaft ist. Dem theoretischen Grenzfall einer solchen 100 %igen Verfügbarkeit kann man heute durch geeignete Strukturen und Online-Reparierbarkeit praktisch sehr nahe kommen; für höchste Sicherheitsanforderungen wird man aber nach wie vor Automatisierungssteme mit gezielten Failsafe-Eigenschaften brauchen.

- Auch bei typischen Anwendungsfällen für reine F-Systeme, können neben den wirtschaftlichen auch Sicherheitsgründe für ein zusätzliches H-Verhalten des Automatisierungssystems sprechen.
  In diesen typischen Anwendungsfällen existiert ein vom F-System jederzeit leicht erreichbarer Aus-Zustand des Prozesses, der für sich betrachtet auch vollkommen sicher und unkritisch ist. Bei einer über den betreffenden Prozeß hinausgehenden, umfassenden Betrachtung können aber häufig sekundäre Effekte des Prozeßstillstandes erkannt werden, die an ganz anderer Stelle sicherheits-

mindernd wirken. Beispiele für diese Situation lassen sich u. a. bei Transportsystemen finden, deren Stillstand i. a. ein unkritischer sicherer Aus-Zustand ist. Insofern spricht scheinbar nichts gegen die bisher notwendige Lösung, diesen Stillstand wegen innerer Fehler eines F-Automatisierungssstems herbeizuführen. Erst die Betrachtung von Sekundäreffekten, wie die Verlagerung von Transportaufgaben auf andere, dann überlastete Systeme, kritische Phasen des notwendigen Wiederanlaufs etc. können Sicherheitsbedenken gegen solche "F"-Abschaltungen aufwerfen.

Es erscheint grundsätzlich anstrebenswert, die Abspaltung des Sicherheitsbereichs, die zu besonderen F-Automatisierungssystemen führt und alle damit verbundenen Nachteile zu überwinden. Dies kann mit einem großen, serienmäßigen, industriellen Automatisierungssystem erreicht werden, das eine gemeinsame Basis für folgende untereinander vollkompatible Lösungen bietet:

- o nicht fehlertolerante oder sicherheitsgerichtete Standardsysteme und
- o höherverfügbare H-Systeme
- o für sicherheitskritische, genehmigungspflichtige Anlagen geeignete F-Lösungen

sowie auch

- o H- und F-Charakteristiken geeignet in sich vereinigende HF-Systeme.

2. Ein industrielles Automatisierungssystem mit hardwareimplementierbarer Fehlertoleranz als Beispiel und Ausgangspunkt

Es soll im weiteren gezeigt werden, daß dieses Ziel gerade durch die Bereitstellung hardwareimplementierbarer Fehlertoleranz erreicht werden kann. Dieser Weg wurde beim Siemens-Automatisierungssystem TELEPERM M erfolgreich beschritten /4/.

Die neben dem einkanaligen Standard (1 von 1) möglichen Redundanzstrukturen sind:

F : 2 von 2
H : 1 von 2 und
HF : 2 von 3

Bei den fehlertolerant projektierten Konfigurationen bearbeitet die vervielfachte Standard-Hardware taktsynchron die gleiche Standard-Software. Die Erkennung, Lokalisierung und ggf. das Maskieren von Fehlern übernimmt die einzige spezielle (Nicht-Standard-) Hardware in dem modularen System. Selbstverständlich sind solche Voter-, Synchronisierungs- etc. -baugruppen auch redundierbar und sie werden in ihrer Funktion ständig geprüft.

Das hier als ein Beispiel eines realisierten Konzeptes mit projektierbarer, hardwareimplementierbarer Fehlertoleranz betrachtete industrielle Seriensystem hat u. a. folgende hier wesentliche Eigenschaften:

A) Bei den H- und HF-Konfigurationen werden Fehler in nur einem von zwei bzw. drei redundanten Teilsystemen stoßfrei (d. h. ohne zeitaufwendige Error-Recovery-Maßnahmen) toleriert.

B) Solche tolerierten Fehler führen zu keiner Leistungsminderung des Automatisierungssystems (no degradation).

C) Solchermaßen tolerierte Teilsystemdefekte können ohne Beeinträchtigung der Prozeßführungsfunktion des Automatisierungssystems, d. h. on-line, repariert werden. Diese On-Line-Reparatur schließt natürlich das Aktualisieren und Synchronisieren eines reparierten Teilsystems ein. Dies geschieht bei nur transienten Störungen weitgehend selbsttätig.

D) Die fehlertoleranten Konfigurationen verwenden weitgehend bis vollkommen unverändert vervielfachte Standardhardware und -software; sie sind damit durchgehend nicht-diversitär.

E) Die Hardwareimplementierung von Synchronisierung, Vergleichen etc. nutzt u.a. aus, daß die zentrale TELEPERM M-Verarbeitungseinheit (CPU) ein spezieller Bit-Slice-Prozessor mit vergleichsweise wenigen und vor allem gut sicht- und kontrollierbaren inneren Zuständen ist.

Die Eigenschaften A bis C, d.h. stoßfreies Weiterlaufen bei Fehlereintritt oder Störungen, On-Line-Reparierbarkeit etc., können für ein serienmäßiges, industrielles H-Automatisierungssystem mit universeller Einsetzbarkeit als unabdingbar gelten. Mit der hardware-implementierten Fehlertoleranz ließen sich diese Eigenschaften bei sehr strengen Zeitanforderungen realisieren; künftige andere Lösungen und insbesondere software-orientierte Lösungen werden sich daran messen lassen müssen.

Die Nichtdiversität (Eigenschaft D) ist eine zwangsläufige Folge der Hardwareimplementierung der Fehlertoleranzmaßnahmen mit CPU-Taktsynchronlauf. Im folgenden wird gezeigt, daß mögliche (oder behauptete) Vorteile diversitärer Lösungen durch andere Systemeigenschaften erreicht werden können, während alle gravierenden Nachteile und auch Gefahren diversitärer Lösungen natürlich vollkommen vermieden werden /5/.

Die an sich allgemein weniger interessante TELEPERM M-Besonderheit E, das ist die Vewendung von Bit-Slice-Prozessoren, hat die gewählte Hardware-Fehlertoleranzlösung sehr begünstigt. Die Konsequenzen für entsprechende Lösungen mit höherintegrierten Prozessoren werden weiter unten behandelt.

3. Zur Nicht-Diversität serienmäßiger Automatisierungssysteme

Von immer weiter wachsenden Kreisen vor allem der Sicherheitstechnik wird Diversität bei der Software als **das** Heilmittel gegen die als unvermeidbar geltenden Softwarefehler angesehen und ihr Einsatz z. T. sehr pauschal und unkritisch gefordert. Die Nichtvereinbarkeit mit diversitäten Lösungen erscheint von diesem Standpunkt aus als ein grundsätzlicher Nachteil von hardwareimplementierter Fehlertoleranz. Eine genauere Betrachtung zeigt jedoch, daß sich für große, serienmäßige Automatisierungssysteme die möglichen Vorteile einer Softwarediversität kaum, deren erhebliche Nachteile jedoch umso gravierender auswirken. Insofern wird man bei solchen industriellen Automatisierungssystemen ohnehin auf die Diversität verzichten müssen, so daß kein Nachteil von hardwareimplementierter Fehlertoleranz in ihrer Nichtvereinbarkeit mit Diversität zu sehen ist.

Anmerkung: Softwarediversität, bei der verschiedene Programmversionen nacheinander bearbeitet werden, d. h. sog. Zeitdiversität ist mit hardware-implentierter Fehlertoleranz vereinbar, denn dies könnte auch taktsynchron auf zueinander redundanten Teilsystemen geschehen. Ein solches Vorgehen ist bei zeitkritischen Automatisierungsaufgaben aber nicht als allgemeines Bearbeitungsprinzip, sondern höchstens für besondere Ausnahmefälle sinnvoll. In diesem Sinne ist die Nichtvereinbarkeit von Diversität und Hardwarefehlertoleranzlösungen zu verstehen.

Das Auftreten physikalischer Fehler im Betrieb ist prinzipiell unvermeidbar. Solche Fehler können also nur durch besondere Fehlertoleranzmaßnahmen toleriert oder durch Failsafe-Maßnahmen beherrscht werden. Aus den o. g. Forderungen A bis C (stoßfreies Weiterlaufen etc.) ergibt sich zumindest für H-Systeme mit strengen Echtzeitanforderungen die Notwendigkeit gleichzeitiger, mehrfach-redundanter Bearbeitung der selben Aufgabe auf vervielfachter Hardware. Systematische Entwurfs- oder Realisierungsfehler sind hingegen von vornherein und während des Betriebes des Systems unveränderlich vorhanden. Maßnahmen zu deren Vermeidung oder Aufdeckung vor dem Betrieb sind immer sinnvoller als Maßnahmen zu deren Tolerierung während des Betriebs, d. h. sinnvoller als Diversität. Dies gilt eigentlich ganz grundsätzlich. Bei den hier betrachteten Großserien-Automatisierungssystemen fällt natürlich noch besonders in Gewicht, daß neben dem erheblichen Entwicklungsaufwand, den diversitären Lösungen zusätzlich erfordern, weitere große Aufwendungen im laufenden Betrieb entstehen, die quasi mit der großen Anzahl verkaufter Systeme und mit deren Lebensdauer zu multiplizieren sind. Allein der über die gesamte Lebensdauer aller verkauften Systeme zu erbringende, erheblich erhöhte, teilweise vervielfachte Aufwand bei Dokumentation, Wartung, Versionsverwaltung, Handhabung etc. ist i. a. weder beim Hersteller noch beim Kunden über lange Systemlebensdauern (10 bis 40 Jahre) tragbar. Noch so große Anstrengungen zur Vermeidung und Aufdeckung systematischer Fehler sind dagegen nur einmaliger Entwicklungsaufwand und damit tragbar.
Neben ihrer schlechten Vereinbarkeit mit Großserien haben diversitäre Lösungen noch eigene, z. T. auch sicherheitskritische Nachteile:

- Auch diversitäte Lösungen müssen ab einem bestimmten Niveau der Verallgemeinerung von einer gemeinsamen Spezifikation ausgehen. Diese Spezifikation muß bei Automatisierungsanwendungen schon sehr detailliert sein. Gegen entsprechende Fehlermöglichkeiten auf dieser Ebene ist Diversität sowieso wirkungslos.

- Die Tolerierbarkeit zufälliger physikalischer Fehler durch Redundanz und die gleichzeitige Tolerierung systematischer Fehler durch Diversität schränken sich zumindet gegenseitig ein.

- Die Organisation einer diversitäten Lösung bedingt an sich Einschränkungen und auch neue Fehlerquellen.

- Diversitäres Vorgehen schließt korrelierte Fehler der erstellten Versionen keineswegs aus.

Beim Hersteller werden Hardware- und Softwareentwurfs- und Realisierungsfehler durch Maßnahmen und Gegebenheiten aufgedeckt, die einer Diversität mindestens gleichwertig sind. Hierzu sind u. a. der nur bei einem großen Hersteller und bei einem Großseriensystem mögliche Umfang hochwertiger Qualitätssicherungsmaßnahmen im allgemeinsten Sinne zu zählen sowie auch die sehr zahlreichen, unterschiedlichen - "diversen" - Einsatzerfahrungen mit einem Seriensystem.

Die Vorteile der Großserie kommen der Programmierung und Konfiguration eines einzelnen Systems oder weniger Systeme für eine bestimmte Anwendung durch Projektierungsingenieure und Benutzer nicht in dem Maße wie der Systemprogrammierung, dem Systementwurf etc. zugute. Bei der Programmierung und Projektierung einzelner Anwendungen könnte man sich von einem diversitären Vorgehen vielleicht doch Vorteile versprechen. Beim o. g. beispielhaft genannten TELEPERM M-Automatisierungssystem gibt es jedoch praktisch keine Programmierung (im eigentlichen Sinne) eines Systems für eine bestimmte Anwendung; es werden ledig-

lich serienmäßig gelieferte Software-"Bausteine" in einer Projektierungssprache konfiguriert und parametriert; eine solche Softwarearchitektur wird bei künftigen Automatisierungssystemen überwiegend eingesetzt werden. Die vom Automatisierungssystem "direkt verstandene" Projektierungssprache bewegt sich etwa auf dem Detaillierungsniveau, das bei diversitären Lösungen für Automatisierungssysteme die gemeinsame Projektierung haben würde. Bei Automatisierungssystemen mit einer solchen Softwarearchitektur ist ein diversitätes Vorgehen auch für die einzelne Anwendung sinnlos und unnötig.

Bei dem hier kurz vorgestellten Automatisierungssystem bedingen und stützen sich die Nichtdiversität und die besondere Hardwareimplementierung der Fehlertoleranz auf glückliche Weise gegenseitig:

Die Nichtdiversität ist einerseits eine Grundvoraussetzung für die hardwareimplementierbare Fehlertoleranz; andererseits wird sie nicht nur von den Nachteilen eines diversitären Vorgehens sondern auch von der durchgängigen Kompatibilität der dargestellten Hardwarelösung besonders gerechtfertigt. Die H-, HF- und F-Systeme mit besonderen Verfügbarkeits- und Sicherheitsanforderungen gleichen im wesentlichen den weitverbreiteten, bewährten nichtfehlertoleranten Automatisierungssystemen und erlangen somit bei Hardware und Software deren Betriebsbewährung. Diese durchgängige Kompatibilität zwischen Standard-, H-, F- und HF-Systemen geht über eine Nichtdiversität der fehlertoleranten Konfigurationen noch hinaus; sie bietet unter anderem den Vorteil, daß sich alle Automatisierungssysteme einer größeren Anlage, von den i. a. zahlreichen Standardsystemen bis hin zu sicherheitsrelevanten F- und HF-Systemen, für den Benutzer bei Handhabung, Bedienung, Beobachtung etc. weitgehend gleich darstellen. Eine solche nicht künstlich darübergelegte gleiche Benutzeroberfläche bei allen Systemen einer Anlage hat u. a. auch Vorteile für die Sicherheit insbesondere in Ausnahmesituationen:

- Der Benutzer wird nicht durch die Verschiedenartigkeit seiner Automatisierungssysteme verwirrt.

- Seine mit den zahlreichen Standardsystemen gewonnene Routine und Erfahrung kommt auch dem Sicherheitsbereich zugute.

Die Abbildung 1 zeigt überblickartig die geschilderten Zusammenhänge und die gegenseitige Bedingtheit zwischen Anforderungen, Softwarearchitektur, Großserieneinsatz sowie Nichtdiversität und hardwareimplementierbarer Fehlertoleranz. Diesen bei TELEPERM M bewährten, aber auch in vieler Hinsicht ganz allgemein vorteilhaften Weg der Hardwareimplementierung der Fehlertoleranzmaßnahmen auch bei Automatisierungssystemen mit sehr hoch integrierten Prozessoren, wie beispielsweise mit dem SAB 80 286, zu beschreiten, kann sinnvoll und erstrebenswert sein, vgl. Abb. 2. Schon um die Nichtdiversität zu stützen, erscheint die grundsätzliche Beibehaltung der wesentlichen Eigenschaften der geschilderten Softwarearchitektur, wie die Anwenderprogrammierung des Einzelsystems direkt in einer Projektierungssprache, sinnvoll.

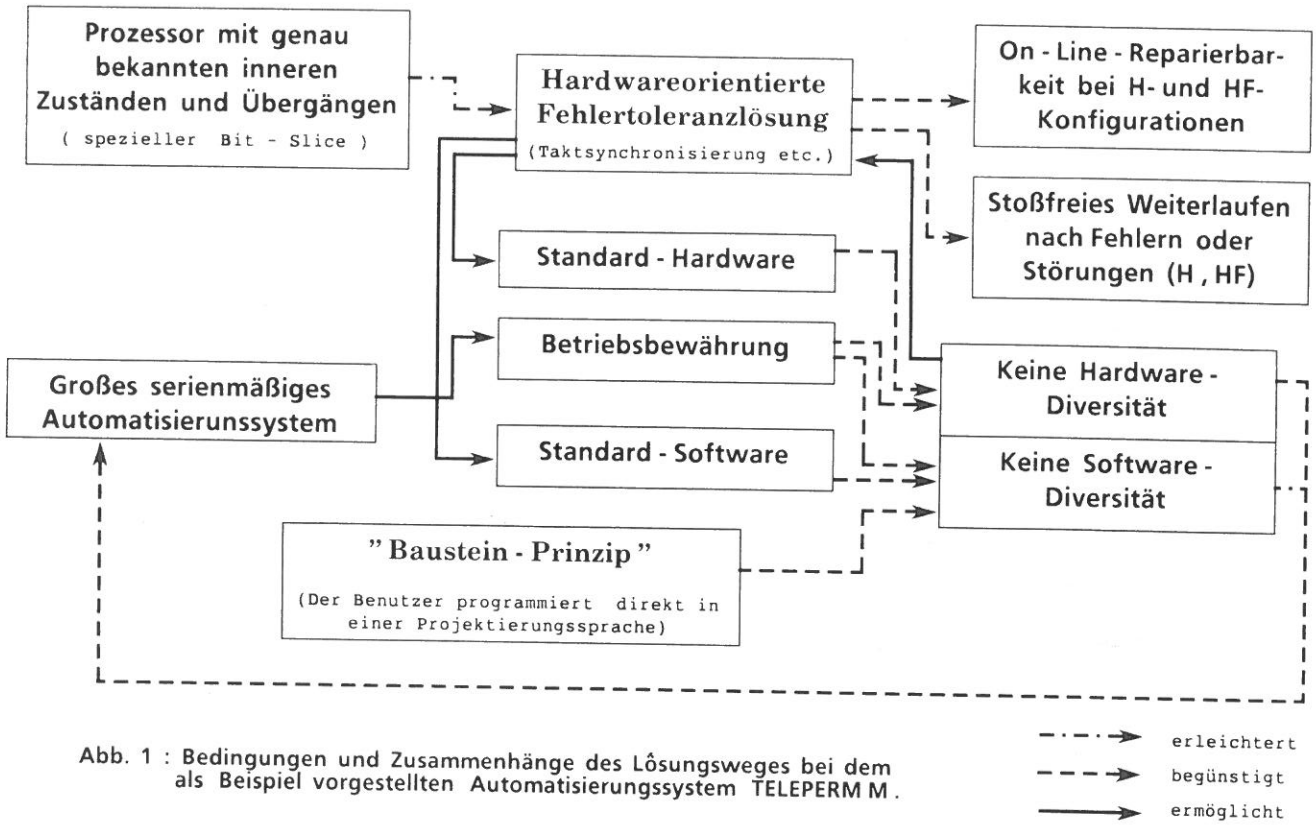

Abb. 1 : Bedingungen und Zusammenhänge des Lösungsweges bei dem als Beispiel vorgestellten Automatisierungssystem TELEPERM M .

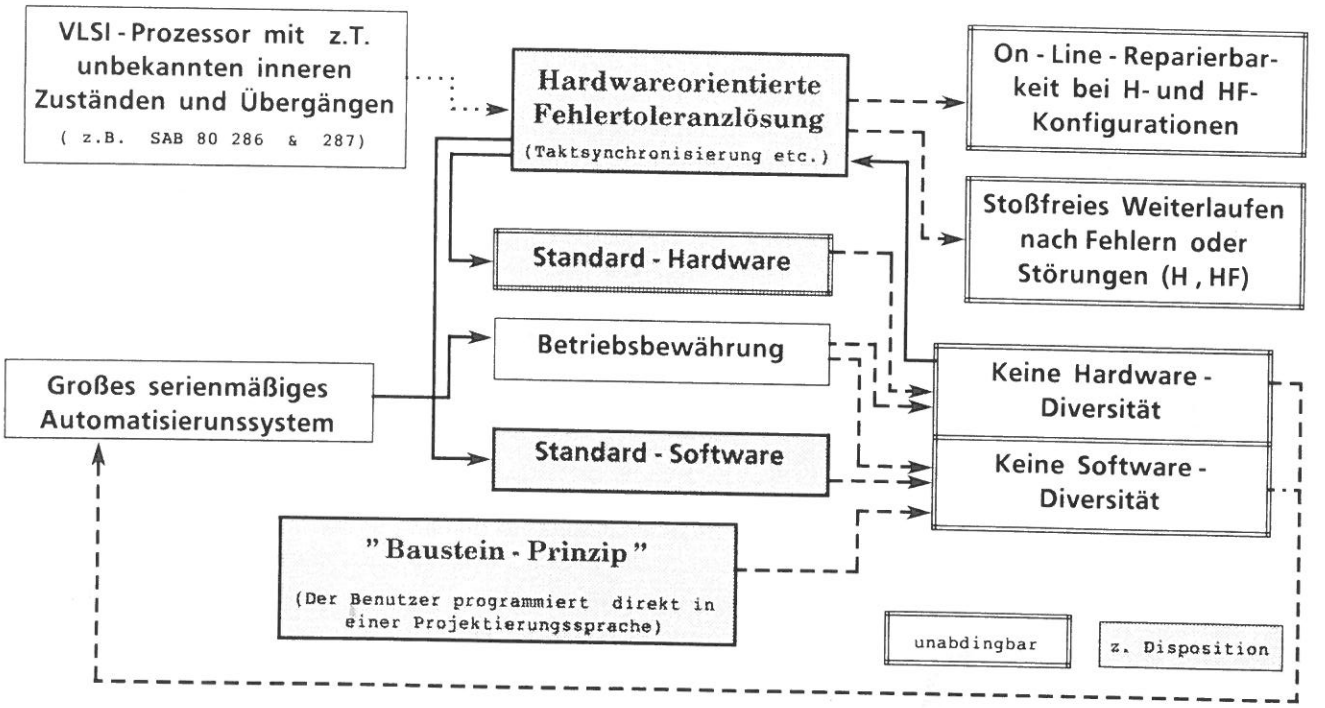

Abb. 2 : Zur Übertragbarkeit des u.a. in Abb. 1 dargestellten Lösungswegs auf Automatisierungssysteme mit sehr hoch integrierten Prozessoren.

4. Zum Einsatz von sehr hochintegrierten Prozessoren

Die geschilderte Hardwareimplementierung der Fehlertoleranzmaßnahmen, von Synchronisierung, Vergleichen etc. erfordert u. a.:

- Die Bit- oder Taktsynchronisierung mehrerer Prozessoren muß mit rückwirkungsfreien Kopplungen erreicht werden.

- Das Einsynchronisieren eines rückgesetzten Prozessors auf einen ungestört weitergelaufenen und weiterlaufenden muß bewirkt werden können. Dies benötigt man z. B. nach der On-line-Reparatur eines Teilsystems.

Die Lösung u. a. dieser Aufgaben wurde in dem als realisiertes Beispiel herangezogenen TELEPERM M-Automatisierungssystem durch einige Eigenschaften der dort eingesetzten Bit-Slice-Prozessoren wirksam unterstützt:

- Ihre inneren Zustände und Operationen sind übersichtlich und vollkommen bekannt; und weiter

- sind die inneren Zustände sichtbar und kontrollierbar.

Die zukünftig wohl einzusetzenden VLSI-Prozessoren haben hingegen i. a. folgende Eigenarten:

- Sie besitzen z. T. mehrere, absichtlich möglichst lose gekoppelte Speicher- und Verarbeitungswerke, Befehlswarteschlangen etc., die evt. zueinander asynchron oder unklar synchronisiert arbeiten.

- Es gibt sehr zahlreiche, von außen z. T. unsichtbare, evt. auch unbekannte innere Zustände und Übergänge.

- Teilweise sind einige innere Zustandsübergänge nach Abschluß der Hardware-Resetphase irreversibel; ein Beispiel hierfür ist der Wechsel des Adressierungsmodes beim SAB 80 286 /6/.

Die bei den ersten beiden Punkten angedeuteten möglichen Unklarheiten können durch eine mangelhafte Dokumentation des Prozessorherstellers oder durch dessen absichtliche "Geheimhaltungspolitik" verursacht werden.

Ein iAPX 80286/80287-Doppel-System mit Hardwaresynchronisierung und -vergleichen etc. wurde als Versuchsmuster entwickelt und untersucht. Die genannten Schwierigkeiten erwiesen sich dabei als überwindbar, so daß es möglich erscheint, hardwareimplementierbare Fehlertoleranz auch für Systeme mit solchen VLSI-Prozessoren darzustellen. Dabei ergeben sich gewisse Einschränkungen für den Entwurf des Systems, das zu verwendende Rückwandbussystem etc. U. a. lassen beispielsweise die "prozessornahen" Synchronisations- und Vergleichseinrichtungen eine von den üblichen Single-Board-Computerlösungen abweichende Aufteilung des Systems auf Baugruppen erforderlich erscheinen.

5. Zusammenfassung

Die in sicherheitskritischen Bereichen eingesetzten Automatisierungssysteme, die i. a. ein sogenanntes Failsafe-Verhalten, abgekürzt "F", haben, stellen z. Z ein eigenes Gebiet dar, das teilweise zu der übrigen, auch der fehlertoleranten, industriellen Automatisierungstechnik wenig Verbindung hat. Diese Trennung hat auch historische Gründe in der konventionellen Automatisierungstechnik. Die Abspaltung des Sicherheitsbereiches von der übrigen Automatisierungstechnik hat auch gravierende Nachteile und ist bei zunehmendem Einsatz der Mikrorechnertechnik und komplexeren Prozeßsteuerungen immer weniger zu rechtfertigen.

Die wichtigsten Gründe gegen diese Trennung sind:

- Die technische bzw. physikalische Begünstigung für die Verwirklichung eines (reinen) F-Verhaltens durch die konventionelle Automatisierungstechnik entfällt bei elektronischer Technik.

  Von der übrigen Automatisierungstechnik getrennt entwickelte, ganz spezielle F-Systeme, die nur in kleinsten Stückzahlen oder gar nur einmalig eingesetzt werden, können trotz des stückzahlbezogenen immensen Aufwands doch i. a. nicht die Breite der Tests, Qualitätssicherungsverfahren etc. großer, serienmäßiger Automatisierungssysteme, auf keinen Fall aber deren umfangreiche Betriebsbewährung erreichen.

- Das Bedienpersonal wird mit speziellen F-Systemen mit einer von der übrigen gewohnten Automatisierungstechnik abweichenden Bedienung, Beobachtung, Handhabung etc. konfrontiert.

- Reines F-Verhalten erzielt Sicherheit auf Kosten der Verfügbarkeit.

- Die von F-Systemen vorausgesetzten, einfach erreichbaren, sicheren Prozeß-Auszustände brauchen nicht jederzeit zu existieren. Außerdem können sie aufgrund sekundärer Effekte an anderen Stellen sicherheitsmindernd wirken.

Ein großes, serienmäßiges Automatisierungssystem, das eine gemeinsame Basis für untereinander voll kompatible Standard-, F-, H- und HF-Konfigurationen bietet, vermeidet alle diese Nachteile. Eine völlige Nichtdiversität aller fehlertoleranten Konfigurationen wird durch eine solche durchgängige Kompatibilität einerseits erfordert, andererseits durch diese auch gerade gestützt, da die "diverse" Betriebsbewährung der Standardsysteme auch den fehlertoleranten Konfigurationen zugutekommt. Diese so eröffnete Möglichkeit des völligen Verzichts auf Diversität ist wegen der zahlreichen Nachteile diversitärer Lösungen ein großer Vorzug.

Die geeignete Bereitstellung hardwareimplementierbarer Fehlertoleranz ist ein Weg, diese weitgehende Kompatibilität zu erreichen. Das Siemens-TELEPERM M-Automatisierungssystem ist ein praxiserprobtes Beispiel hierfür. Einige Besonderheiten der TELEPERM M-Software- und -Hardwarearchitektur unterstützten diese Lösung ganz besonders wirksam. Obwohl dies in dem Maße bei neuen Systemen mit VLSI-Prozessoren nicht mehr zu erwarten ist, ist dieser Lösungsweg weiterhin gangbar. Dies zeigten entsprechende Untersuchungen mit SAB 80 286-Systemen.

6. Literatur

/1/ T. Anderson & P.A. Lee
Fault-Tolerance
Principles and Practice
London 1981

/2/ Algirdas Avizienis
Fault-Tolerance
The Survival Attribute of Digital Systems
Proc. IEEE, 66 (1978), Nr. 10 (Oktober), S. 1109 bis 1125

/3/ Algirdas Avizienis & J. Kelly
Fault-Tolerance by Design Diversity
Concepts and Experiments
Computer 17 (1984), Nr. 8 (August), S. 67 bis 80

/4/ U. Kling & E. Schrodi
Redundantes hochverfügbares Automatisierungssystem AS 220 H
im dezentralen Prozeßleitsystem TELEPERM M
Siemens Energietechnik 5 (1983), H. 2

/5/ N.G. Leveson
Correlated Failures in Multi-Version Software
in Proceedings of the Fourth IFAC Workshop SafeComp '85
Oxford 1985

/6/ Siemens AG
SAB 80 286
Programmer's Reference Manual
including the SAB 80 286 Numeric Supplement
User's Manual 1984

/7/ J.H. Wenseley & al.
S I F T
Design and Analysis of a Fault-Tolerant Computer
for Aircraft Control

/8/ J.H. Wenseley
An Operating System for a TMR Fault-Tolerant Computer
FTCS-13 conf. Proc. (1983), S. 452 bis 455