2.3 Kriterien zum Vergleich der Eigenschaften von Automatisierungsstrukturen

Um die Vor- und Nachteile einer Automatisierungsstruktur bewerten zu können, werden in Abhängigkeit von der Zahl der Teilprozesse bzw. Automatisierungsfunktionen folgende Kriterien herangezogen:

- die Kosten für die Beschaffung der Geräte, der Verkabelung, der Software, der Pflege und Wartung,
- die Teilverfügbarkeit bei Hardware-Ausfällen oder Software-Fehlern, d.h. die Wahrscheinlichkeit, daß der Betrieb eines Prozesses bis zu einem betrachteten Zeitpunkt nicht durch Ausfälle einzelner Automatisierungseinrichtungen gestört ist,
- die Flexibilität bei Änderungen,
- die Koordinierung der Teilprozesse und Optimierung des Gesamtprozesses sowie
- die Bedienbarkeit.

Vergleicht man die Kosten für die Beschaffung eines zentralen Prozeßautomatisierungssystems mit denen einer dezentralen Struktur, so ergibt sich angenähert das in Bild 2.6 gezeigte Verhalten. Im Gegensatz zu den mit der Zahl der Teilprozesse und/oder der Automatisierungsfunktionen linear ansteigenden Kosten für dedizierte, dezentrale Automatisierungseinheiten sind für einen universellen, zentralen Prozeßrechner hohe Anfangskosten aufzuwenden. Die Möglichkeiten zum Anschluß von Prozeßsignal- und Prozeßbedienperipherie sowie die Fähigkeiten der Kommunikationsgeräte für den Informationsverkehr des zentralen Prozeßrechners sind meist überdimensioniert ausgelegt, so daß weitere Automatisierungsfunktionen ohne oder mit nur geringem zusätzlichen finanziellen Aufwand umgesetzt werden können.

Betrachtet man die Teilverfügbarkeit bei Hardware-Ausfällen oder Software-Fehlern und somit die Zuverlässigkeit des Betriebes, so ist bei zentralen Prozeßrechnern davon auszugehen, daß alle Störungen auf Grund ihrer seriellen Arbeitsweise zu Totalausfällen der Informationsverarbeitung führen können. Da zentrale Prozeßrechner schon bei der Beschaffung auf nachträgliche Erweiterung ihrer Automatisierungsfunktionalität hin ausgelegt sind, kann die Zuverlässigkeit des Betriebes, wie in Bild 2.7 dargestellt, in Abhängigkeit der Anzahl der Automatisierungsfunktionen als konstant angesehen werden.

Die Bewertung der Zuverlässigkeit einer dezentralen Struktur ist abhängig von den Auswirkungen, die eine Störung oder der Ausfall einer dezentralen Automatisierungseinheit bezüglich des gesamten technischen Prozesses mit sich bringt. In Bild 2.7 sind die Kurven zweier Beispiele eingezeichnet. In beiden Fällen nimmt die Zuverlässigkeit des Betriebes mit steigender Zahl von Teilprozessen ab, da das Gesamtsystem mit entsprechenden Automatisierungseinheiten erweitert werden muß, die wiederum Ursachen für Störungen enthalten können.

Dabei ergibt sich ein stärkerer Abfall der Zuverlässigkeit, wenn durch Ausfall einer Einheit der gesamte Prozeß gestört wird, denn ihr Wert berechnet sich als Produkt

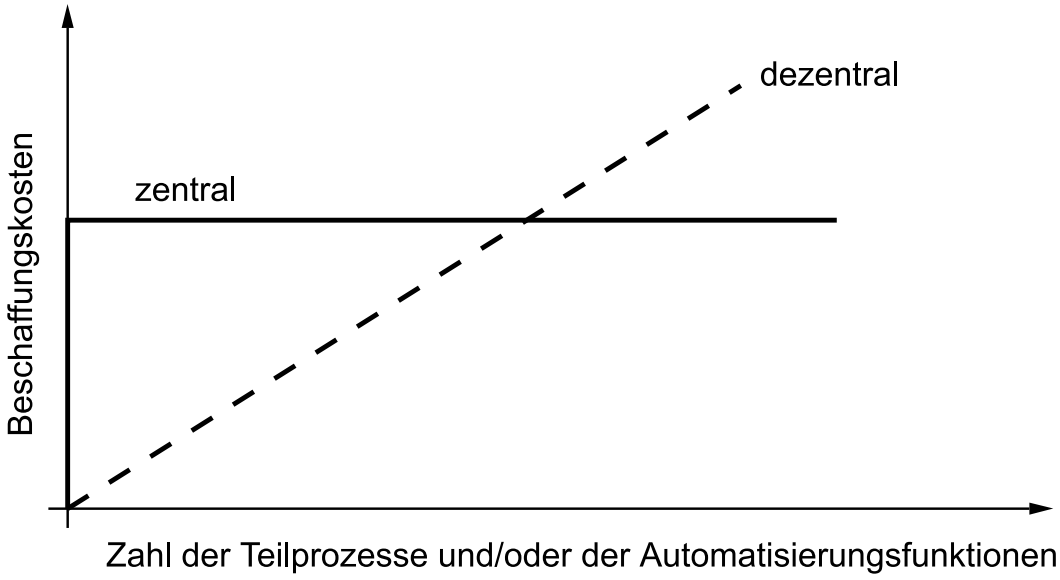

Bild 2.6: Vergleich der Beschaffungskosten

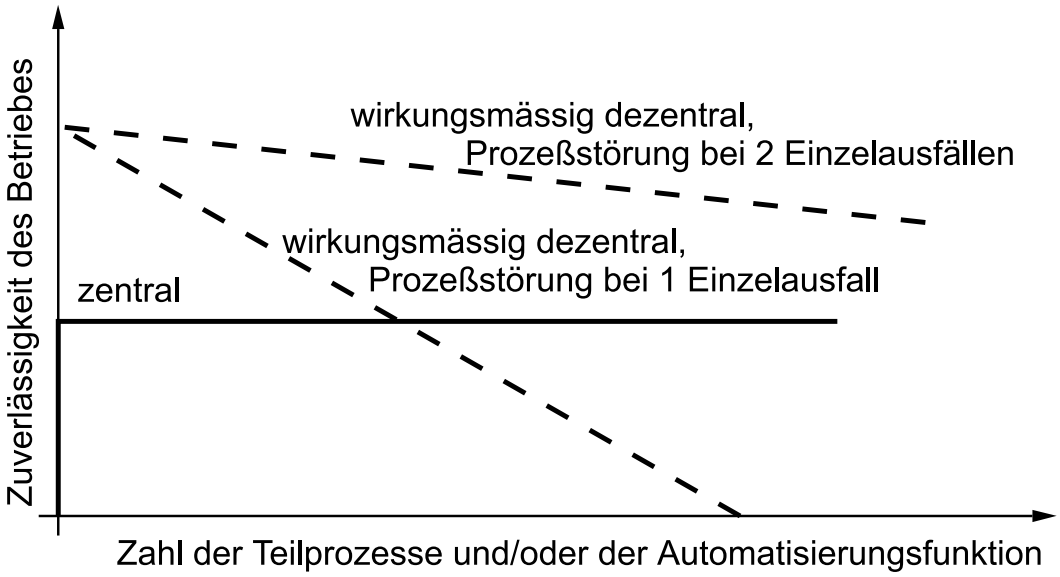

Bild 2.7: Vergleich der Zuverlässigkeit des Betriebes eines technischen Prozesses

der Zuverlässigkeitswerte der Einzelgeräte. Im zweiten Fall führt ein gestörtes Einzelgerät noch nicht zu einem völligen Betriebsausfall, weil z.B. die Auswirkungen der Störung gering sind oder Bedienungspersonal vorhanden ist, um die Aufgaben der gestörten Einheit von Hand wahrzunehmen. Erst wenn zwei Einzelgeräte gleichzeitig ausfallen — "gleichzeitig" kann hier auch bedeuten, daß nach dem Ausfall eines Einzelgerätes weitere Automatisierungseinheiten ausfallen, bevor das zuerst ausgefallene instandgesetzt ist —, kommt es zu einem Betriebsausfall. Ein Maß für die Zuverlässigkeit des Betriebes des technischen Prozesses ergibt sich in diesem Fall aus der Wahrscheinlichkeit, daß zwei oder mehr Einzelgeräte gleichzeitig gestört sind. Da diese Wahrscheinlichkeit äußerst gering ist, ist die Zuverlässigkeit des Betriebes für den zweiten Fall sehr hoch.

In den meisten praktischen Anwendungen ist die Verkopplung von Teilprozessen nicht so stark, als daß der Ausfall von zwei oder mehr Automatisierungseinheiten einen Totalausfall zur Folge hätte. Daher ist in der Regel die Zuverlässigkeit des Betriebes eines technischen Prozesses mit einer dezentralen Automatisierungsstruktur höher als beim Einsatz eines zentralen Prozeßrechners.

Wird dagegen ein zentraler Prozeßrechner vorgesehen, der auch die Überwachung, Steuerung und Regelung der Einzelanlagen teilweise oder ganz übernimmt, so sind die Teilprozesse vom Zusammenwirken der Einzelanlagen mit dem Prozeßrechner abhängig. Für zentral strukturierte Prozeßautomatisierungssysteme gilt damit:

- die Teilaufgaben des Prozesses werden von den gerätetechnischen Anlagenteilen und von den Programmen des zentralen Prozeßrechners bestimmt und
- durch den zentralen Prozeßrechner werden bisher autonome Teilprozesse miteinander verknüpft, die dadurch voneinander abhängig werden können.

Durch die letztgenannte Verkopplung von Teilprozessen entstehen neuartige Probleme hinsichtlich folgender Gesichtspunkte:

Zuverlässigkeit, Verfügbarkeit und Sicherheit: Wegen der Zentralisierung und Serialisierung der Aufgabenbearbeitung ist davon auszugehen, daß alle Störungen zu einem Totalausfall der Informationsverarbeitung führen können, der einen Gesamtausfall des Prozesses nach sich zieht.

Projektierung und Systementwicklung: Die bisher angewandten empirischen Verfahren zur Projektierung von Einzelanlagen genügen nicht mehr den Anforderungen, die sich bei der Projektierung komplexer Prozeßautomatisierungssysteme stellen. Fehlplanungen und wirtschaftlich unbefriedigende Ergebnisse sind die Folge dieses Mangels.

Fehlerdiagnose und Wartung: Mit der Komplexität der Automatisierungssysteme wachsen die Schwierigkeiten der Fehlerdiagnose und Wartung. Schon die Abgrenzung zwischen Geräte- und Programmierfehlern ist oft nicht leicht.

Organisatorische Abwicklung: Die Verknüpfung autonomer Einzelanlagen zu großen Systemen erzeugt neuartige organisatorische Probleme für die Abwicklung von Prozeßautomatisierungsvorhaben.

Beim Aufbau komplexer zentralrechnergeführter Anlagen tritt an die Stelle der Verantwortlichkeit für Einzelanlagen die Verantwortlichkeit für Untersysteme, die aus Geräten und Rechnerprogrammen bestehen. Wegen der engen Verkopplung zwischen den Untersystemen können nun Konfliktsituationen dadurch auftreten, daß eine Beschränkung der Funktionen eines Untersystems im Interesse der optimalen Auslegung des Gesamtsystems erforderlich wird.

Vergleicht man Automatisierungsstrukturen hinsichtlich der Flexibilität bei Änderungen, der Koordination der Teilprozesse und der Optimierung der Gesamtprozesse, so erweisen sich auch hier dezentrale Struktur als vorteilhaft. Allerdings erfordern dezentrale Strukturen zusätzlichen Aufwand zur Kommunikation der einzelnen Automatisierungseinheiten.

Ein nicht zu unterschätzendes Kriterium zum Vergleich von Automatisierungsstrukturen ist das der Bedienbarkeit und Benutzerfreundlichkeit, denn es steht heute oft im Mittelpunkt des Anwenderinteresses. Dies führte zur Entwicklung entsprechend komfortabler Prozeßbedienperipherien und entsprechender Software. Solche Benutzerschnittstellen lassen sich sowohl für zentrale als auch für dezentrale Strukturen verwirklichen. Durch Zuordnung einer dezentralen Automatisierungseinheit zu einem Teilprozeß kann jedoch die Transparenz eines komplexen Prozeßgeschehens für den Bediener erhöht werden. Die Ursachen von Störungen lassen sich dann sowohl örtlich als auch funktionell besser lokalisieren, abgrenzen und beheben. Dies trägt sehr wesentlich zur Bedienbarkeit und Wartbarkeit komplexer technischer Prozesse in Störfällen bei.

Aus obigen Betrachtungen läßt sich als Schlußfolgerung für die geeignete Wahl einer Struktur für die Automatisierung eines technischen Prozesses ziehen:

So dezentral wie möglich, so zentral wie nötig.

In entsprechenden Kombinationen lassen sich damit die jeweiligen Vorteile einer Struktur nutzen, während die jeweiligen Nachteile vermieden werden. Die in einer späteren Kurseinheit vorgestellten Automatisierungshierarchien sind Beispiele für solche Kombinationen. Die Wahl dezentraler Strukturen wird sehr stark durch die Entwicklung immer kostengünstigerer und leistungsfähigerer Mikroprozessoren begünstigt, die auch auf der untersten Prozeßebene eine sehr hohe Flexibilität mit sich bringen.

2.4 Redundante Konfigurationen

Es gibt mehrere Methoden, um der mangelnden Zuverlässigkeit der Zentralrechnerstruktur zu begegnen:

- Schaffung einer Umschaltmöglichkeit auf redundante Einzelgeräte,
- Anwendung redundanter Prozeßrechensysteme (Doppel- oder Mehrrechner) mit Umschaltmöglichkeit im Störungsfalle oder
- Einführung dezentraler Prozeßrechensysteme mit weitgehend paralleler Informationsverarbeitung.

Die einfachste Form von Redundanz liegt bereits vor — ohne daß sie allerdings von Betreibern als solche bezeichnet wird — wenn Bedienpersonal parallel zu eingesetzten Rechnern Prozeßgrößen überwacht und im Notfall eingreifen kann. Die Aufgaben des Bedienpersonals bezüglich Prozeßüberwachung und -sicherung spielen bei Zuverlässigkeits- und Sicherheitsbetrachtungen eine wesentliche Rolle.

Im folgenden soll jedoch nur die Auslegung der Hard- und Software von Automatisierungssystemen betrachtet werden. Hierbei können folgende Formen von Redundanz unterschieden werden:

- redundante Hardware,
- redundante Software,
- Erfassung redundanter Meßgrößen, wozu auch auf Grund der Funktion eines technischen Prozesses voneinander abhängige Größen wie z.B. Weg, Zeit und Geschwindigkeit gehören, und
- zeitliche Redundanz, z.B. durch mehrfaches Abfragen des gleichen Meßwertes in bestimmten Zeitabständen oder mehrmalige Ausführung des gleichen Programmstückes.

Die beiden letztgenannten Formen der Redundanz sind mit relativ geringem Aufwand zu realisieren und werden häufig in Automatisierungssystemen eingesetzt. Hard- und Software-Redundanz erfordern dagegen merklich höheren Aufwand. Letzterer kann jedoch gerechtfertigt sein, wenn dadurch Kosteneinsparungen durch erhöhte Prozeßverfügbarkeit erreicht werden. Erhöhter Aufwand muß immer getrieben werden, wenn Ausfälle eine Gefährdung von Menschen mit sich bringen können.

Für die Hardware-Redundanz können verschiedene Einteilungsgesichtspunkte gewählt werden. Bei Betrachtung des Einsatzprinzips unterscheidet man

statische oder m-von-n-Redundanz: die Ergebnisse von n Einheiten, die dieselben Aufgaben bearbeiten, werden miteinander verglichen und Ausgabewerte werden durch m-von-n-Mehrheitsentscheide bestimmt. Die Ergebnisse werden erst dann falsch, wenn mindestens m Einheiten defekt sind, was sehr unwahrscheinlich ist.

dynamische Redundanz: tritt ein Fehler bei einem im Eingriff befindlichen Gerät auf, so wird auf eine Reserveeinheit umgeschaltet.

Betrachtet man die Hardware-Redundanz nach der Arbeitsweise im fehlerfreien Fall, so kommt man zur Unterteilung in

blinde Redundanz: die redundante Einheit ist im fehlerfreien Fall nicht tätig und

funktionsbeteiligte Redundanz: die redundante Einheit führt im fehlerfreien Fall Aufgaben aus.

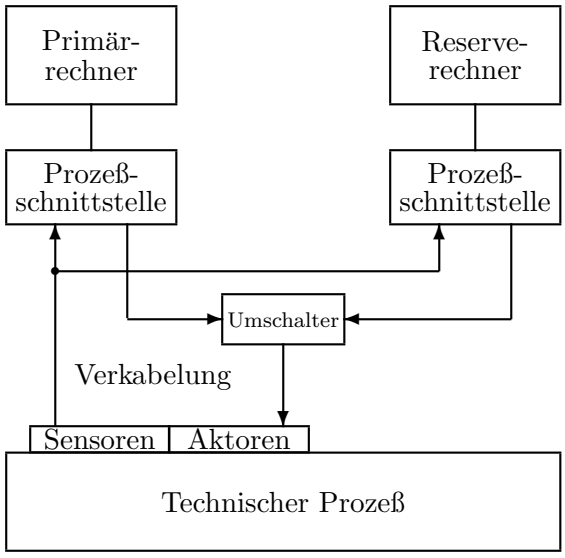

Bild 2.8: Zentralisiertes Automatisierungssystem mit einem Reserverechner

Methoden zur Steigerung der Zuverlässigkeit von Automatisierungssystemen durch Hardware-Redundanz basieren alle auf der Idee, Reservemodule an den kritischsten Systemstellen vorzusehen. Wenn ein Primärmodul ausfällt oder nicht länger angemessen arbeiten kann, übernimmt ein Reservemodul seine Funktionen. In einem zentralisierten Prozeßrechnersystem ist der Rechner selbst das kritischste Element. Vor diesem Hintergrund wurde die Architektur mit einem redundanten **Reserverechner** nach Bild 2.8 entwickelt.

Das System umfaßt zwei Rechner und einen Ausgabeumschalter. Es gibt folgende Möglichkeiten zum Betrieb eines solchen Doppelrechnersystems:

Parallelbetrieb: Beide Rechner lesen dieselben Prozeßdaten ein und führen dieselben Programme parallel aus. Jedoch sendet nur einer von ihnen Steuerungssignale zum automatisierten Prozeß durch den Ausgabeumschalter. Wenn dieser Rechner ausfällt, wird der Umschalter betätigt und der sekundäre Rechner übernimmt. Es bleibt festzuhalten, daß ein Reserverechner den Systemdurchsatz nicht erhöht, da er genau dieselben Verarbeitungen wie der primäre Rechner durchführt.

Bereitschaftsbetrieb: Bei diesem Verfahren werden der Primärrechner als Arbeits- und der Reserverechner als Bereitschaftsrechner bezeichnet. Der Arbeitsrechner nimmt im normalen, ungestörten Betrieb die Automatisierungsaufgaben wahr. Der Bereitschaftsrechner führt Überwachungsrechnungen durch und erhält in kurzen Zeitabständen vom Arbeitsrechner Informationen über aktuelle Prozeßzustände und Zwischenergebnisse. Wird bei der Überwachung ein Fehler erkannt oder meldet sich der Arbeitsrechner nach einer vorgegebenen Zeit nicht mehr, so schaltet der Bereitschaftsrechner den Arbeitsrechner ab und übernimmt dessen Aufgaben an einem festgelegten Einsatzpunkt. Gleichzeitig wird natürlich eine Meldung an das Bedienungspersonal gegeben, um die Prüfung und Instandsetzung des Arbeitsrechners zu veranlassen.

Aufteilung der Automatisierungsaufgaben: Zur Verringerung der Kosten, die

beim Bereitschaftsbetrieb wegen der Auslegung beider Rechner für den gesamten Aufgabenumfang sehr hoch sind, werden bei dynamischer funktionsbeteiligter Redundanz die Automatisierungsaufgaben auf beide Rechner aufgeteilt:

- der Primärrechner führt diejenigen Automatisierungsaufgaben aus, die zur Aufrechterhaltung der Prozeßfunktion unbedingt notwendig sind, z.B. Grenzwertüberwachung, Steuerung und Regelung, während
- der Reserverechner im normalen, ungestörten Betrieb zwei Arten von Aufgaben wahrnimmt:
  1. er bearbeitet zum einen diejenigen weniger dringlichen Automatisierungsaufgaben, bei deren Ausfall die Funktion des Prozesses zwar beeinträchtigt, aber nicht völlig eingestellt wird, z.B. Optimierungsrechnungen oder Auswertung von Prozeßergebnissen, und
  2. zum anderen überwacht er ständig den ersten Rechner. Wird nun bei der Überwachung ein Fehler im Primärrechner festgestellt, so übernimmt der zweite Rechner voll dessen Aufgaben, wobei er einen Teil seiner eigenen regulären Aufgaben abwirft. Diese Aufgabenübernahme erfolgt allerdings nur einseitig. Bei einem Ausfall des Reserverechners fallen dessen Aufgaben nämlich völlig aus, denn der erste Rechner bearbeitet weiterhin nur seine Aufgaben und übernimmt keine Aufgaben des zweiten Rechners.

Während zum Parallel- und Bereitschaftsbetrieb beide Rechner für die Bearbeitung aller Automatisierungsaufgaben und zur Ein- und Ausgabe aller Prozeßsignale ausgelegt sein müssen, genügt bei dynamischer funktionsbeteiligter Redundanz ein Ausbau für die jeweils vorgesehenen Teilaufgaben, wodurch Kosten gespart werden.

Obwohl im Prinzip einfach, ist die Idee der Verdopplung eines Automatisierungssystems außergewöhnlich schwer zu implementieren und die Kosten der Implementierung sind sehr hoch. Ein genauerer Blick auf Bild 2.8 zeigt, daß es eine Anzahl möglicher Störungsquellen im System gibt. Diese sind

–Sensoren und Aktoren,

–Verkabelung (gewöhnlich fällt ein Kabel nicht aus, aber es kann aufgerissen oder durchgeschnitten werden — versehentlich oder böswillig),

–Umschalter,

–Prozeßschnittstelle,

–Zentralrechner und

–zusätzliche Elemente wie Stromversorgung oder Kühlung (sofern benötigt).

Alle diese Elemente müssen ordnungsgemäß funktionieren, um korrekten Betrieb des Automatisierungssystems zu gewährleisten, und jedes defekte Gerät kann einen Prozeßstillstand verursachen. Um die Systemzuverlässigkeit real zu erhöhen, müssen alle Elemente, oder zumindest alle sicherheitskritischen, verdoppelt werden. Jedoch können weder der Umschalter noch die Aktoren verdoppelt werden. Es ist zum Beispiel nicht möglich, ein Ventil durch Montage eines zweiten am selben Rohr abzusichern: werden sie eines hinter dem anderen am selben Rohr montiert, dann schließt bereits eines von ihnen das Rohr; werden sie anderenfalls parallel an zwei

Zweigen des Rohres montiert, dann öffnet bereits eines von ihnen permanent den Fluß durch das Rohr.

Die Anwesenheit eines Ausgabeumschalters schafft das Problem der Steuerung seiner Position. Es ist offensichtlich, daß der Schalter nicht vom Primärrechner gesteuert werden kann, da bei seinem Ausfall umgeschaltet werden soll. Aber er kann auch nicht vom Reserverechner gesteuert werden, denn dann könnte er als Ergebnis einer Fehlfunktion dieses Rechners umgeschaltet werden. Es sollte auch wie bemerkt berücksichtigt werden, daß der Schalter selbst versagen kann.

In der industriellen Praxis wird die Konfiguration mit einem Reserverechner nicht als kosteneffektiv angesehen und deshalb selten benutzt. In den seltenen Fällen des Einsatzes eines Reserverechners kann das Umschalterproblem abhängig von den Anwendungsmerkmalen in einer von zwei Weisen gelöst werden. Eine dieser Methoden ist dann anwendbar, wenn die erforderliche Geschwindigkeit der Rechnerreaktion relativ gering ist, so daß der Umschalter manuell von einem menschlichen Bediener betätigt werden kann, von dem erwartet wird, daß er eine Rechnerfehlfunktion erkennt. Andernfalls wird eine spezielle Umschaltersteuerung verwendet, die beide Rechner überwacht — z.B. indem sie von beiden in regelmäßigen Zeitabständen Bereitschaftsmeldungen empfängt. Wenn eine Bereitschaftsmeldung nicht rechtzeitig kommt, dann wird der entsprechende Rechner als ausgefallen angesehen. Man kann sich klarmachen, daß diese Methode relativ sicher ist, da eine Fehlfunktion der Umschaltersteuerung nicht gefährlich ist, sofern weder der Primär- noch der Reserverechner ausgefallen sind. Soweit es den Umschalter betrifft, wird angenommen, daß seine Zuverlässigkeit höher als die der Rechner ist.

Ein alternativer Ansatz ist nützlich, wenn ein System logisch in eine Anzahl von Regelkreisen aufgespalten werden kann. Nach Bild 2.9 besteht er darin, nur einzelne Kreise anstelle des ganzen Automatisierungssystems zu verdoppeln. Der Ansatz ist sehr flexibel, da in der Regel nicht alle Teilaufgaben des Systems von gleicher Relevanz sind. Gewöhnlich können nämlich einige von ihnen vorübergehend zurückgestellt werden, wenn ein Ausfall auftritt. Grundsätzlich kann diese Methode auf kontinuierliche Regelkreise und zur binären Steuerung angewandt werden. Jedoch wird sie meistens für kontinuierliche Regelkreise benutzt, für die PID-Regler einsetzbar sind. Gelegentlich werden nicht nur die Regler, sondern auch die Sensoren und Kabel verdoppelt. Ein einzelner Kreis kann dann manuell von einem Bediener oder automatisch von einer speziellen Steuerung umgeschaltet werden.

Die Idee, *Einzelgeräte als Reserve* vorzuhalten, ist nicht auf zentralisierte Rechnersysteme beschränkt, sondern kann ebensogut in jeder anderen Systemarchitektur angewandt werden, z.B. der Einzelgerätetechnik selbst. Sie hat sich als kosteneffektiv erwiesen und wird in der industriellen Praxis häufig angewandt.

Eine mit Doppelrechnersystemen angestrebte hohe Zuverlässigkeit des Betriebes technischer Prozesse genügt nicht, wenn bei Ausfällen Gefahren für Menschen eintreten können. Zusätzlich wird in diesen Fällen die Forderung gestellt, daß gefährliche Einzelfehler nicht auftreten dürfen. Als gefährlich werden dabei solche Fehler bezeichnet, die die Ausgabe falscher Prozeßsignale verursachen oder eine Sicherheitsoperation wie eine Abschaltung oder Störungsmeldung verhindern könnten. Ähnliches gilt für Raumfahrt- und Militäranwendungen, z.B. zur Luftverteidigung oder Steuerung ballistischer Raketen, wo höchste Zuverlässigkeit verlangt wird und Kosten als weniger wichtiger Faktor betrachtet werden.

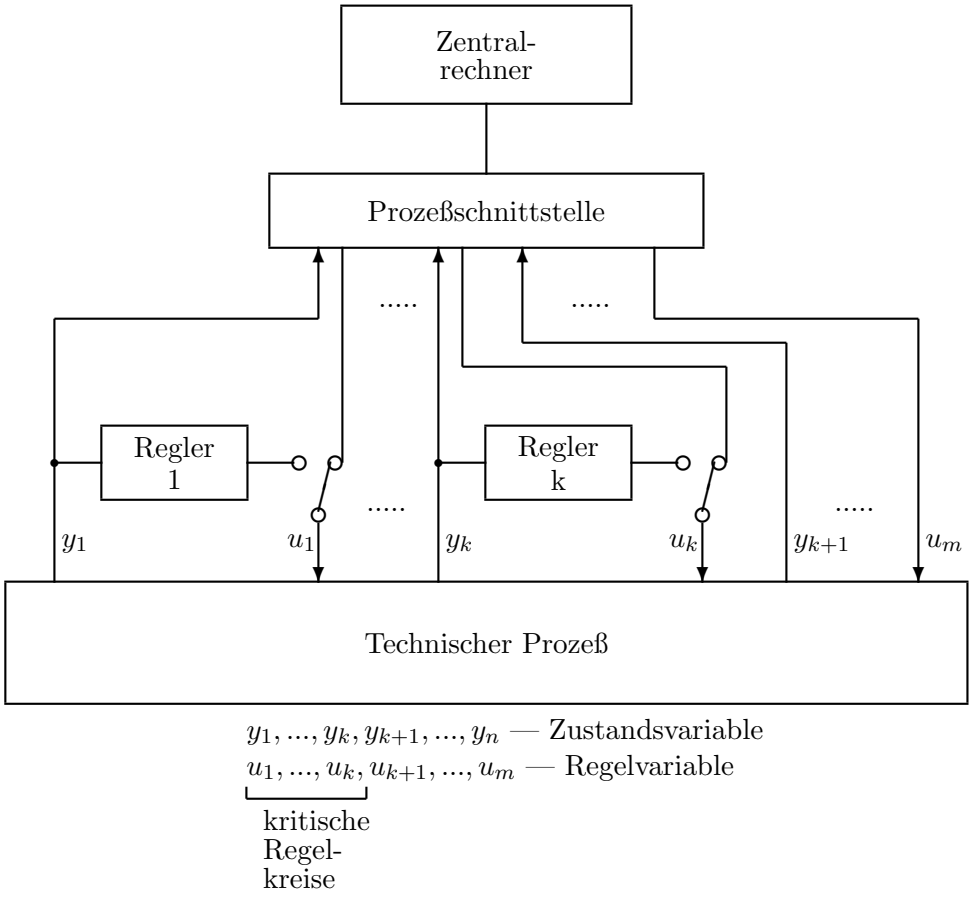

Bild 2.9: Automatisierungsstruktur mit Einzelgerätereserve

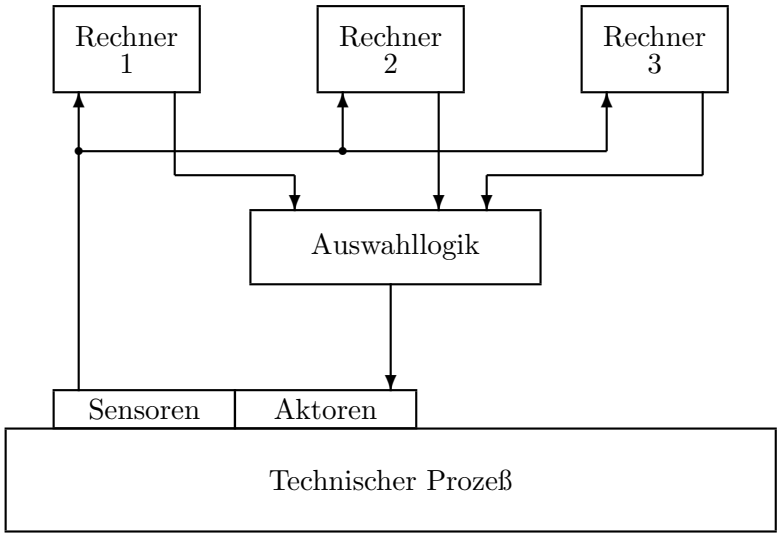

Bild 2.10: Parallele Rechner mit Ergebnisauswahl

Die geforderte Zuverlässigkeit und Sicherheit kann dann durch Einsatz von drei oder mehr unabhängigen Rechnern erreicht werden, die wie in Bild 2.10 gezeigt parallel arbeiten. Alle Rechner erhalten dieselben Daten von einer gemeinsamen Umgebung und müssen auf dieselben Anforderungen antworten. Ihre Ergebnisse werden verglichen und die, die von der Mehrheit der Rechner geliefert wurden, werden von einer Auswahllogik ausgewählt (*m-von-n-Redundanz*). Die Wahllogik kann zwar per Programm durchgeführt werden, wird aber als kritischer Teil des Systems üblicherweise durch spezielle ausfallsicherheitsgerichtete Techniken implementiert, die bei Fehlfunktionen auf jeden Fall einen sicheren Zustand herbeiführen.

Es ist wert festzuhalten, daß die Rechner in einem Auswahlsystem nicht vom selben Typ zu sein brauchen. Sie müssen nur dieselbe Verhaltensfunktionalität implementieren, während die Einzelheiten der Hardware wie auch die Software-Implementierung verschieden sein können. Dies erhöht die Immunität des Systems gegen Entwurfs- und Codierungsfehler.

Parallele Systeme mit Auswahl sind selten in industriellen Prozeßautomatisierungsanwendungen, insbesondere in der kontinuierlichen Regelung, zu finden. Jedoch können sie in natürlicherer Weise in Umgebungen mit diskreten Ereignissen und in Kommandosystemen eingesetzt werden.

Beim Einsatz redundanter Prozeßrechensysteme muß immer gewährleistet sein, daß nach Ausfall einer Einheit

- der Ausfall von den anderen Einheiten erkannt wird,
- Daten gesichert werden,
- die Automatisierungsfunktionen durch andere Einheiten übernommen werden,
- eine Meldung an das Bedienpersonal ausgegeben wird.

Bis jetzt hat sich die Diskussion in diesem Abschnitt auf Methoden zur Gewährleistung kontinuierlicher Betriebsbereitschaft von Prozeßautomatisierungssystemen

beim Auftreten von Ausfällen konzentriert. Implementierungen dieses Ansatzes der Fehlertoleranz haben sich als schwierig und teuer herausgestellt. Der zweite Ansatz ist der, einen automatisierten Prozeß in einem sicheren Zustand und zu minimalen Kosten anzuhalten. Dies stimmt mit dem in Abschnitt 1.7 in groben Zügen dargestellten Nothaltansatz überein.

Als Beispiel betrachten wir den in Bild 2.5 gezeigten chemischen Prozeß. Nach der in Abschnitt 1.3 gegebenen Prozeßbeschreibung ist der kritischste Teil des Automatisierungssystems der Temperaturregelkreis, da Überhitzung den Prozeß zur Explosion bringen kann. Dies kann durch einen zusätzlichen *Schutzkreis* verhindert werden, der, wie in Bild 2.11 eingezeichnet, aus einem Sensor für einen Temperaturschwellwert und einem zusätzlichen Heizungsschalter besteht. Der Schalter ist an, wenn die Temperatur unter dem Schwellwert liegt, und aus, wenn die Temperatur das Schwellwertniveau überschreitet. Das Abschalten der Heizung kann von einem Alarmsignal an einen menschlichen Bediener begleitet sein. Gewöhnlich ist der Auszustand permanent und kann nur durch manuelle Bedienung zurückgesetzt werden.

Obiges Beispiel soll verdeutlichen, daß ein Schutzkreis kein redundanter Regelkreis ist. Insbesondere übernimmt er keine Automatisierungsfunktionen im Falle einer Rechnerfehlfunktion. Statt dessen hält er den Prozeß als letzten Ausweg an, um ernsten Schaden und Unfallopfer zu verhindern. Dies kann mit der Rolle elektrischer Sicherungen in elektrischen Stromversorgungsanlagen verglichen werden. Es ist auch wichtig festzuhalten, daß ein Schutzkreis von Natur aus zwei Zustände hat und daß er unter Benutzung einer logischen Steuerung zur Verarbeitung binärer Signale implementiert werden kann.

Die Verwendung von Schutzkreisen ist allgemein üblich und ist Teil der Automatisierungstechnik geworden. Die Methode ist mit anderen Verfahren zur Steigerung der Systemzuverlässigkeit kompatibel und kann deshalb in jeder Automatisierungssystemarchitektur benutzt werden.

2.5 Mehrstufige Automatisierungssysteme

Die Vor- und Nachteile der Einzelgerätetechnik und der Zentralrechnerstruktur können wie in Bild 2.12 gezeigt im Rahmen einer zweistufigen hierarchischen Architektur ausgeglichen werden. Die untere, prozeßnahe Ebene besteht aus kleinen Prozeßrechnern oder Einzelgeräten für einzelne Regelkreise und ähnelt der klassischen Prozeßautomatisierungsstruktur. Die obere Ebene besteht aus einem Zentralrechner, der die Regler der unteren Ebene überwacht. Man bezeichnet die in Bild 2.12 dargestellte Verarbeitungsstruktur häufig auch als “Satelliten-” oder “Sternsystem”, da die Informationswege sternförmig vom zentralen, übergeordneten Prozeßrechner ausgehen. Das Hauptkriterium für die Zerlegung eines Automatisierungssystems in zwei Ebenen ist die Dringlichkeit der Aufgaben, welche auf jeder Ebene ausgeführt werden. In der Regel werden die zeitkritischen Aufgaben der eigentlichen Automatisierung von Geräten der unteren Ebene ausgeführt, während die obere Ebene für langfristige Optimierung und Mensch-Maschine-Kommunikation verantwortlich ist. Die meisten sicherheitskritischen Funktionen werden an die Einzelgeräte delegiert. Der Zentralrechner überwacht jedoch den Prozeßzustand und informiert den