3.1.3 Realisierung mit Mikroelektronik

Ausfallsicherheitsgerichtetes Verhalten läßt sich mit Mikroelektronik einkanalig eigentlich nicht realisieren. Der Grund hierfür ist die Vielfalt von Ausfällen, die in hochintegrierten Schaltungen auftreten können. Trotzdem werden einkanalige, mikroelektronische Systeme zur sicheren Prozeßautomatisierung in Form speicherprogrammierbarer Steuerungen industriell angeboten. Wir betrachten daher jetzt als Fallstudie Struktur, Programmierung und Betrieb sicherheitsgerichteter SPSen, um zu zeigen, wie weit die vorgestellten Konzepte Eingang in die Praxis gefunden haben. Diesem Abschnitt liegen Auszüge aus [122] zu Grunde.

Sicherheitsgerichtete SPSen

Sicherheitsgerichtete speicherprogrammierbare Steuerungen sind elektronische Systeme, die zur Lösung sicherheitsrelevanter Automatisierungsaufgaben herangezogen werden können und mit Hilfe anwendungsorientierter Logiksprachen programmiert werden. Das Hauptproblem, das sich beim Einsatz sicherheitsgerichteter SPSen stellt, ist, daß es ihre komplexe Hardware nicht erlaubt, a priori alle Fehlermöglichkeiten zu berücksichtigen. Ebensowenig kann in der Regel für die Software wegen ihres großen Umfanges und der Zahl möglicher Systemzustände Fehlerfreiheit nachgewiesen werden. Deshalb sind Funktionstests für alle Systemkomponenten einschließlich der Ein-/Ausgangsebene ständig durchzuführen. Sicherheitsgerichtete SPSen müssen Anforderungen an Hardware, Software sowie den Systementwurf erfüllen, die über jene an gewöhnliche SPSen weit hinausgehen. Sie werden vom TÜV nach Anforderungsklassen gemäß DIN V 19250 zertifiziert. Aus den im folgenden genannten Gründen sind sie trotz aller Probleme dabei, festverdrahtete Steuerungen langsam abzulösen.

Gegenüberstellung sicherheitsgerichteter VPS und SPS

Beim Vergleich sicherheitsgerichteter VPSen und SPSen schneiden letztere auf Grund ihrer besseren Funktionalität günstiger ab. Die Sicherheit beider Steuerungsarten erscheint jedoch zunehmend gleichwertig. Die wesentlichen Vorteile sicherheitsgerichteter SPSen gegenüber sicherheitsgerichteter VPSen können wie folgt zusammengefaßt werden.

- Mit sicherheitsgerichteten SPSen können Lösungen realisiert werden, die mit VPSen nicht praktikabel sind.
- Analogverarbeitung ist möglich.
- Höhere Verfügbarbeit ist einfach projektierbar.
- Hohe Funktionalität, z.B. Rechenfunktionen, Vergleicher und Ablaufsteuerungen, ist leicht zu verwirklichen.
- Hohe Flexibilität, d.h. im Ausnahmefall können SPSen schnell an Schutzaufgaben angepaßt werden.
- Koppelbarkeit an Fremdsysteme.

- Projektierung mit integrierten CAD-Werkzeugen.
- Dokumentation erfolgt in Funktionsplandarstellung, automatische Rückdokumentation ist möglich.
- Geringer Platzbedarf.
- Inbetriebnahme und Wartung:
  - Möglichkeiten der Signalverfolgung und Simulation in dynamischen Funktionsplänen.
  - Fehler werden als Information gespeichert.
  - Peripheriestromkreise werden mit überwacht.
  - Bei redundanter Auslegung ist es möglich, Baugruppen oder Software im laufenden Betrieb auszutauschen, ohne das die zugehörige Anlage abgefahren werden muß.
- SPSen sind, bei komplexeren Aufgabestellungen, kostengünstiger als VPSen. Ab etwa 20 – 25 Ein-/Ausgängen lohnt es sich, die Kosten beider Steuerungsarten zu vergleichen.

Baumusterprüfung und Anlagenabnahme

Rein theoretisch ist auch in sicherheitsgerichteten Anwendungen mit geringerem Gefahrenpotential der Einsatz "normaler" speicherprogrammierbarer Steuerungen möglich, wenn die sehr weitgehenden Forderungen der DIN VDE 0801 [30] an das Ausfallverhalten der Steuerungen durch erhebliche zusätzliche Maßnahmen bei Konstruktion, Projektierung und Programmierung der Anlagen berücksichtigt werden. Dieses Vorhaben scheitert jedoch häufig schon an der Tatsache, daß den Anwendern die internen Strukturen der Steuerungen nicht zugänglich sind und somit die diesbezüglichen Maßnahmen zur Fehlersicherheit nicht nachgerüstet werden können. Aus wirtschaftlichen Überlegungen ist eine solche Vorgehensweise auch wenig sinnvoll, da der zusätzliche Aufwand zur sicherheitstechnischen Ertüchtigung einer normalen SPS die Mehrkosten für eine TÜV-geprüfte SPS um ein Vielfaches übersteigt.

Zum Erwerb einer Betriebsgenehmigung für eine Steuerungsanlage ist deren Begutachtung durch einen Sachverständigen erforderlich. Grundlage dieser Abnahme ist das Merkblatt "Leitlinie für die Prüfung sicherheitsrelevanter MSR-Einrichtungen in Anlagen" des Verbands der Technischen Überwachungsvereine. Beim Einsatz einer sicherheitsgerichteten SPS ist der wesentliche Bestandteil dieser Abnahme durch die Baumusterprüfung beim Hersteller bereits erbracht. Der Gutachter überprüft "nur" noch die SPS-Programmierung und ob das eingesetzte Steuerungssystem für die festgelegte Anforderungsklasse zugelassen ist sowie ob die Auflagen des Prüfberichtes eingehalten sind. Brennersteuerungen bilden hier eine Ausnahme. Da die Anwendungsnorm DIN VDE 0116 "Elektrische Ausrüstung von Feuerungsanlagen" aus historischen Gründen bereits detaillierte Anforderungen an Steuerungen stellt, ist in diesem Fall die Festlegung einer Anforderungsklasse dann nicht erforderlich, wenn eine verwendete SPS bei der Baumusterprüfung zusätzlich nach DIN VDE 0116 geprüft wurde.

Sicherheit Anforderungsklasse	AK 1...4	AK 1...5	AK 1...6
Verfügbarkeit	normal	hoch	sehr hoch
Konfiguration			
Zentralbaugruppe	einkanalig	redundant	redundant
E/A-Baugruppen	einkanalig	einkanalig	redundant
E/A-Bus	einkanalig	einkanalig	redundant

Tabelle 3.1: Forderungen der Normen an die Struktur speicherprogrammierbarer Steuerungen

Forderung der Normen an die SPS-Systemstruktur

Für sichere speicherprogrammierbare Steuerungen ergeben sich aus der Norm DIN VDE 0801 [30] gemäß Tabelle 3.1 drei unterschiedliche Systemstrukturen, mit denen die maximalen Anforderungsklassen 4, 5 und 6 erreichbar sind. Zur Verwendung in den Klassen 7 und 8 (z.B. in Kernkraftwerken) ist eine SPS allein aus Sicherheitsgründen nicht ausreichend. In diesen Fällen müssen diversitäre Steuerungssysteme aus unterschiedlichen Einheiten eingesetzt werden (z.B. eine sichere SPS und parallel dazu eine bauteilfehlersichere verdrahtungsprogrammierte Steuerung). Durch teilweise oder komplette Redundanz (zweifache Auslegung) der verwendeten Baugruppen lassen sich Sicherheit und Verfügbarkeit kombinieren. Hierbei gilt "sehr hohe" Verfügbarkeit für den Einsatz in den Anforderungsklassen 1 – 5, in denen über 95% der Anwendungsfälle liegen. Für sicherheitstechnische Aufgaben sind komplexere Systemstrukturen nicht erforderlich, da sie kein höheres Maß an Sicherheit bieten. Sie führen im Gegenteil zu einer Senkung der Anlagenverfügbarkeit, da umfangreichere Hardware häufiger ausfällt.

Aufbau sicherheitsgerichteter SPSen

Der maximale Aufbau einer sicherheitsgerichteten SPS ist in Bild 3.1 dargestellt. Welche Komponenten hiervon im Einzelfall redundant vorhanden sein müssen, ergibt sich nach Tabelle 3.1 aus der geforderten Sicherheit und der gewünschten Verfügbarkeit. Darüberhinaus müssen Sensoren, Aktoren, Transmitter und die zugehörigen Ein-/Ausgänge redundant ausgeführt sein, wenn diese Komponenten nicht über eine Baumusterprüfung zum sicherheitsgerichteten Einsatz abgenommen sind. Zur Erhöhung der Verfügbarkeit kann zusätzlich zu den sicherheitstechnisch geforderten Kanälen ein weiterer Ein-/Ausgang nach dem Prinzip "1 von 2" bzw. "2 von 3" vorhanden sein. Nach Ausfall eines Kanals ist dann immer noch die von der Norm geforderte Anzahl von Ein-/Ausgängen verfügbar, so daß die Steuerung unterbrechungsfrei in Betrieb bleibt.

Anforderungsklasse 1...4 Den einfachsten Fall stellen einkanalige Steuerungen bis zur Anforderungsklasse 4 mit normaler Verfügbarkeit dar. Diese sind entsprechend der linken Hälfte der in Bild 3.1 dargestellten Steuerung aufgebaut: eine Zentralbaugruppe ist über einen EA-Bus mit einfach ausgelegten Ein- und Ausgabebaugruppen verbunden. Doch schon eine solche Steuerung unterscheidet sich ganz erheblich von normalen SPSen. Durch umfangreiche Selbsttests des Zentralteils und

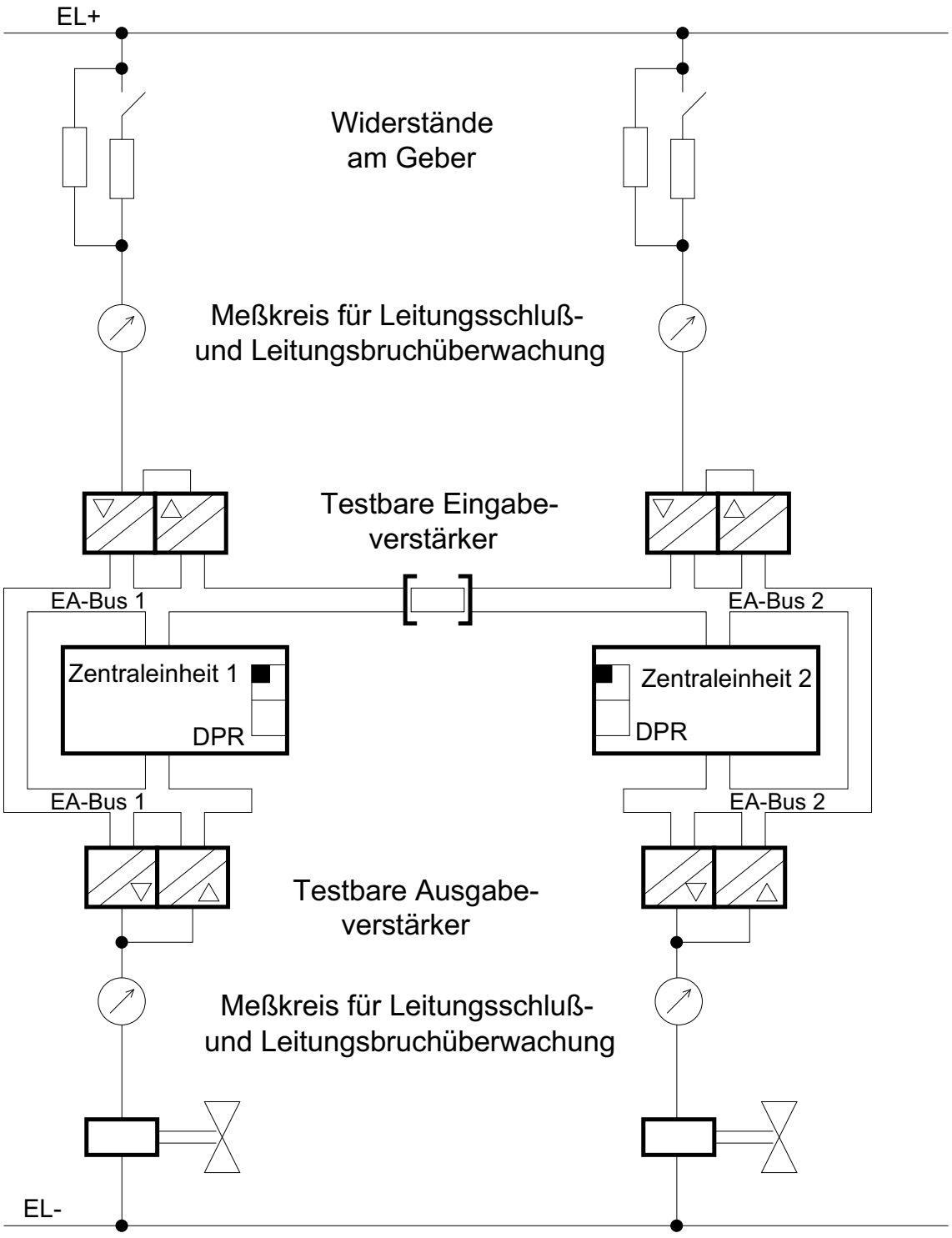

Bild 3.1: Systemstruktur sicherheitsgerichteter speicherprogrammierbarer Steuerungen

testbare EA-Baugruppen deckt diese Ausführung bei bestimmten Herstellern bereits die Anwendungsnorm DIN VDE 0116 für Brennersteuerungen ab.

Anforderungsklasse 1...5 Wird entweder hohe Verfügbarkeit oder Sicherheit bis zur Anforderungsklasse 5 (oder beides) benötigt, so ist eine zweite Zentralbaugruppe erforderlich. Es werden dann wie in Bild 3.1 gezeigt zwei Zentralbaugruppen über einen gemeinsamen EA-Bus mit den einfach ausgelegten EA-Baugruppen verbunden. In beiden Zentralbaugruppen wird parallel das gleiche Programm abgearbeitet. Über eine schnelle Datenverbindung tauschen die Prozessoren während des Verarbeitungszyklus den Zustand der Ein- und Ausgänge untereinander aus und kontrollieren sich so gegenseitig. Hat eine der Zentralbaugruppen einen Defekt, kann die andere den Betrieb in vollem Umfang allein aufrechterhalten. Die defekte Baugruppe kann mit wenigen Handgriffen während des Betriebes ausgetauscht werden. Obwohl die Norm beim Einsatz in Anforderungsklasse 5 eine redundante Zentraleinheit fordert, ist auch hier wegen des hohen Sicherheitsniveaus der einzelnen Zentralbaugruppen einkanaliger Betrieb bis zu 72 Stunden Dauer erlaubt. Somit ist ununterbrochener Betrieb von Anlagen auch über Wochenenden hinweg gewährleistet.

Anforderungsklasse 1...6 Für Sicherheit in Anforderungsklasse 6 oder höchste Verfügbarkeit bis AK 5 sind voll redundante Systeme erforderlich. Hierbei werden pro Ein- und Ausgang zwei EA-Punkte auf unterschiedlichen Baugruppen über zwei getrennte EA-Busse mit den je zwei Zentralbaugruppen verbunden. In AK 6 führt der Ausfall einer Zentralbaugruppe im Normalfalle zu einer Systemgesamtabschaltung. Bei geeigneten begleitenden organisatorischen Maßnahmen ist anlagenabhängig einkanaliger Betrieb bis zu 1 Stunde Dauer zum geregelten Anlagenabfahren möglich. Wenn innerhalb dieser Zeit die defekte Einheit ausgetauscht wird, ist auch hier unterbrechungsfreier Betrieb garantiert.

Tests in sicherheitsgerichteten SPSen

Betriebssysteme sicherheitsgericheter SPSen sind so ausgelegt, daß — im Rahmen der technischen Möglichkeiten — jeder Fehler innerhalb der anlagenabhängigen Sicherheitszeiten (1 – 200 sec) erkannt wird und zur Abschaltung der fehlerhaften Komponente oder zur Gesamtabschaltung führt. Neben diesen aktiven Fehlern kann in einem System auch ein Defekt latent vorhanden sein, der zwar nicht direkt zu einer gefährlichen Situation führt, aber bei Auftreten eines zweiten Fehlers die sichere Reaktion der Steuerung verhindern kann. Solche passiven Fehler werden innerhalb der Zweitfehlereintrittszeit erkannt, die im Normalfall zwischen 1 und 24 Stunden liegt. Diese Zeiten — und damit die Testintervalle — sind anlagenabhängig konfigurierbar, um SPS-Zykluszeiten möglichst gering zu belasten. Bei der Baumusterprüfung wird die als Firmware installierte komplette Software eines Betriebssystems vom TÜV auf Fehlerfreiheit untersucht. Im Steuerungsbetrieb überprüft sich die Software ständig selbst und überwacht dabei alle intern verwendeten Parameter auf zulässige Werte. Somit ist ein wesentlicher Teil der in einem System vorhandenen Software ständig damit beschäftigt, zufällige Fehler der Hardware und systematische Fehler der Software aufzuspüren. Daher ist das Sicherheitsniveau einer solchen SPS trotz des Vorhandenseins von Software und trotz ihrer Problematik mit

den Prinzipien einer verdrahtungsprogrammierten, bauteilfehlersicheren Steuerung vergleichbar. Dabei erweist sich als Vorteil, daß Software erlaubt, gezielt nach Fehlern in der Hardware zu suchen, diese zu lokalisieren und dem Bedienungspersonal zu melden.

Test der Zentralbaugruppen In sicherheitsgerichteten SPSen werden alle Komponenten der Zentralbaugruppen ständig auf ihre Funktionsfähigkeit hin geprüft. Teilweise werden diese Tests per Software durchgeführt, teilweise sind hierfür Hardware-Einrichtungen wie Watchdogs oder Speicherkomparatoren vorhanden. Zu diesem Zweck sind auch die Speicher doppelt vorhanden. Daten werden aus Sicherheitsgründen normal und zusätzlich invertiert abgelegt. Ab Anforderungsklasse 5 wird die Funktionsfähigkeit außerdem über den Vergleich mit einer redundanten Zentralbaugruppe geprüft.

Test der EA-Ebene Betrachten wir hierzu die Flammenüberwachung einer Gasfeuerungsanlage, bei der — unter allen denkbaren Umständen — spätestens eine Sekunde nach Erlöschen der Flamme das Gasventil schließen muß. Abgeschaltet werden muß auch dann, wenn die Steuerung auf Grund eines Defektes den Zustand der Flamme nicht mehr kennt. Sollte in diesem Falle die Eingangskarte fälschlicherweise den Wert “0” (Flamme aus) liefern und damit eine unnötige Abschaltung auslösen, so ist dieser aktive Fehler sicherheitstechnisch unkritisch. Gefährlich ist in diesem Zusammenhang nur der passive Fehler, daß die Baugruppe unabhängig vom Eingangswert immer den Wert “1” (Flamme an) meldet. Eine Steuerung muß also die Möglichkeit besitzen, diese Fehler zu erkennen.

Für sicherheitsgerichtete Ein- und Ausgänge müssen demnach testbare EA-Baugruppen eingesetzt werden. In solchen Einheiten ist für Prüfzwecke zu jedem Eingang ein zusätzlicher Ausgang und zu jedem Ausgang ein Eingang vorhanden. Über die Prüfausgänge wird bei testbaren binären Eingabebaugruppen in jedem Zyklus festgestellt, ob die Eingangskanäle in der Lage sind, beide Signalpegel unabhängig vom anstehenden Eingangssignal durchzuschalten. Bei testbaren binären Ausgabebaugruppen werden in jedem Zyklus die Ausgangspegel zurückgelesen und mit den Ausgabesignalen der Logik verglichen. Zusätzlich wird für maximal 0,2 msec (damit keine Aktoren ansprechen) ein Schaltbarkeitstest durchgeführt. Analoge Baugruppen werden entsprechend kontrolliert, nur daß hier durch Rampentests die kompletten Wertebereiche der Ein- und Ausgänge durchgeprüft werden. Baugruppen mit Leitungsüberwachung können zusätzlich über Strommessungen Drahtbruch und Kurzschluß auf den Leitungen feststellen.

Alle diese automatischen Funktionen sind in den Betriebssystemen sicherheitsgericheter SPSen realisiert und haben keinen Einfluß auf die Anwenderlogik. Daher erscheint eine solche Steuerung bei der Programmierung wie jede andere SPS. Alle festgestellten Fehler werden auf Diagnoseanzeigen der Zentralbaugruppen anwendergerecht ausgegeben und können zusätzlich auf Programmiergeräten und Prozeßleitsystemen dargestellt werden. Weiterhin erfolgt je nach Konfigurierung eine Teil- (was bei redundanter Auslegung unterbrechungsfreien Betrieb garantiert) oder Gesamtabschaltung. Durch diese Möglichkeit zur differenzierten Reaktion einer SPS auf Fehler in der EA-Ebene können neben sicherheitsgerichteten Aufgaben auch unkritische Funktionen mit TÜV-geprüften Steuerungen realisiert werden. Obwohl

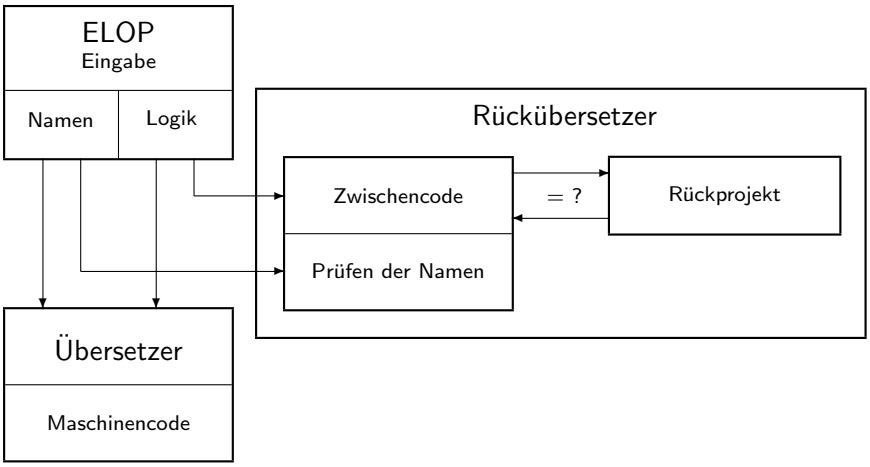

Bild 3.2: Funktionsweise eines Rücksübersetzers

hierfür preisgünstige, nicht testbare EA-Karten eingesetzt werden können, ist auch in diesem Fall die Verwendung testbarer Baugruppen sinnvoll, da die Diagnosemöglichkeiten schnellen und gezielten Austausch defekter Komponenten unterstützen.

Programmierung sicherheitsgerichteter SPSen

Speicherprogrammierbare Steuerungen, insbesondere sicherheitsgerichtete, werden graphisch in Funktionsplan programmiert. Dabei laufen die Programmierumgebungen nicht auf den Zielmaschinen, sondern auf Standard-PCs. Bei der Eingabe steht die Funktion im Vordergrund, während die internen Maßnahmen (Speicherverwaltung, Systemtests, Synchronisierung der redundanten Zentralbaugruppen) Aufgabe der Betriebssysteme sind. Binäre, digitale und mathematische Grundfunktionen werden mit Symbolen nach DIN 19 239 unter Verwendung symbolischer Namen für Ein-, Ausgänge und Merker erfaßt.

Funktionspläne werden von Übersetzern in die Maschinensprachen von SPS-Prozessoren übersetzt und dann in die Steuerungen geladen. Da dieser Vorgang auf PCs und damit auf keiner "sicheren" Hardware abläuft, müssen Programme im Rahmen von Anlagenabnahmen auf fehlerfreie Übersetzung hin geprüft werden. Schließlich können Speicherfehler in PCs, Viren oder Fehler in den PC-Betriebssystemen die Übersetzungen stören, so daß generierte Steuerungsprogramme nicht mehr den eingegebenen Funktionsplänen entsprechen. Entsprechende Überprüfungen können durch sehr aufwendige vollständige Funktionstests nach jeder Übersetzung oder die Anwendung eines TÜV-geprüften Rücksübersetzers vorgenommen werden, der wie in Bild 3.2 dargestellt aus einem Objektprogramm wieder einen Funktionsplan erzeugt und diesen mit dem Original vergleicht. Solch ein Rücksübersetzer kann auch zur Vereinfachung der Anlagenabnahme eingesetzt werden, indem bei Änderungen dem TÜV gegenüber die entsprechenden Stellen nachgewiesen werden.

Besonders bei der Realisierung risikobehafteter Anlagen ist übersichtliche, modulare Programmierung erforderlich, um logische Fehler zu vermeiden. Hierzu verfügen sicherheitsgerichtete SPSen über umfangreiche Bibliotheken mit Standardfunktionen, die vom TÜV zur Anwendung für sicherheitsgerichtete Aufgaben geprüft sind. Weiterhin können eigene Funktionsbausteine definiert werden, die bestimmte spezifische

Bezeichnung	Signaldarstellung			Logischer Wert	
	Logik	Valenz	Kanal	Null	Eins
A	positiv	Äquivalenz	1	L	H
			2	L	H
B	positiv	Antivalenz	1	L	H
			2	H	L
C	negativ	Äquivalenz	1	H	L
			2	H	L
D	negativ	Antivalenz	1	H	L
			2	L	H

Tabelle 3.2: Statische Signaldarstellungen

Teilaufgaben erfüllen. Diese können einmaliger, anwendungsunabhängiger TÜV-Abnahme unterworfen werden, so daß bei einer Anlagenbegutachtung nicht mehr die programmierte Logik, sondern nur noch die anlagenabhängige Parametrierung geprüft werden muß.

3.2 Zweikanalige Hardware-Systeme

3.2.1 Realisierung mit konventioneller Technik

In Eisenbahnsignalanlagen werden oft redundante Überwachungskreise mit Relais realisiert. Diese redundanten Überwachungskreise stellen eine zweikanalige Signalverarbeitung dar.

3.2.2 Realisierung mit Elektronik

Zweikanalige Signaldarstellung

Zweikanalige Signalverarbeitung läßt sich mit verschiedenen Signaldarstellungen realisieren. Es wird zwischen statischen und dynamischen Signalen unterschieden. Die Signale auf den beiden Kanälen können äquivalente oder antivalente Werte annehmen. Man kann weiter zwischen positiver und negativer Logik unterscheiden. Bei positiver Logik ist dem Wert "Logisch Null" das niedrige Signal L und dem Wert "Logisch Eins" das hohe Signal H auf dem Kanal 1 zugeordnet. Bei negativer Logik ist die Zuordnung vertauscht. Tabelle 3.2 zeigt die möglichen statischen Signaldarstellungen für zweikanalige Signalverarbeitung.

Eine dynamische Signaldarstellung erhält man durch ständiges Umschalten zwischen zwei oder mehreren statischen Darstellungen. Tabelle 3.3 zeigt 5 ausgewählte dynamische Signaldarstellungen für die zweikanalige Signalverarbeitung.

Die Bezeichnungen I, II und IV wurden nach der Zahl der zugrundeliegenden statischen Darstellungen gewählt, die als Index mitaufgeführt sind (z.B. II_{AC}). Die Darstellung I_A bedeutet, daß in jedem Takt dieselbe statische Darstellung verwendet ist. Sie kann z.B. in Form von Impulsen realisiert sein.

Bezeichnung	Folge statischer Darstellungen (aus Tab. 3.2)	Zahl der Takte	Kanal	Logischer Wert	
				Null Takt: 1 2 3 4 ...	Eins Takt: 1 2 3 4 ...
I_A	A-A-A-A- ...	1	1	LLLL ...	HHHH ...
			2	LLLL ...	HHHH ...
II_{AC}	A-C-A-C- ...	2	1	LHLH ...	HLHL ...
			2	LHLH ...	HLHL ...
II_{BD}	B-D-B-D ...	2	1	LHLH ...	HLHL ...
			2	HLHL ...	LHLH ...
IV_{ABCD}	A-B-C-D ...	4	1	LLHH ...	HHLL ...
			2	LHHL ...	HLLH ...
IV_{ACBD}	A-C-B-D ...	4	1	LHLH ...	HLHL ...
			2	LHHL ...	HLLH ...

Tabelle 3.3: Dynamische Signaldarstellungen

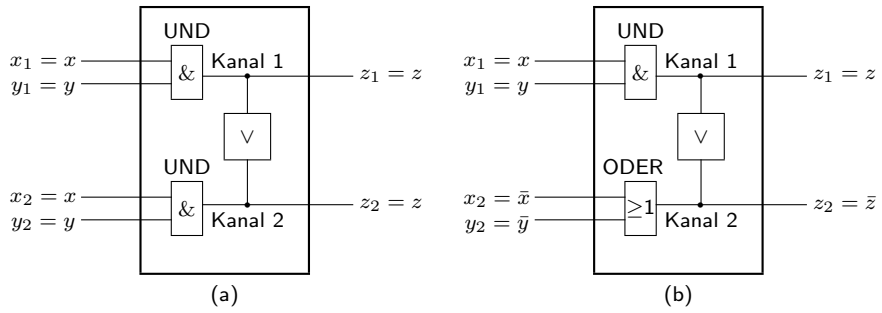

Bild 3.3: Realisierung der Und-Funktion in zweikanaliger Signalverarbeitung

Realisierung einer logischen Grundfunktion

Ein Beispiel für zweikanalige Signalverarbeitung zeigt das Bild 3.3. Für die Realisierung der logischen Und-Funktion ist in Bild 3.3 (a) die Signaldarstellung A und in Bild 3.3 (b) die Darstellung B der Tabelle 3.2 verwendet.

Bei der Signaldarstellung B werden im Kanal 2 komplementäre Signale verarbeitet. Daher tritt anstelle der Und- die Oder-Funktion auf. Ständige Umschaltung der Signaldarstellung zwischen zwei statischen Darstellungen erfordert auch die ständige Umschaltung der logischen Funktionen (zwischen Und und Oder). Eine Lösung bietet hier ein 2-aus-3-Verknüpfungsbaustein, an dem der dritte Eingang ständig zwischen "Null" (Und-Funktion) und "Eins" (Oder-Funktion) umgeschaltet wird [88].

Zusammenhang zwischen Signaldarstellung und Fehlererkennbarkeit

Der Vergleicher V (Bild 3.3) prüft ständig oder wechselweise die Ausgangssignale auf Äquivalenz oder Antivalenz. Ist die durch die jeweilige Darstellung definierte Äquivalenz bzw. Antivalenz der Signale nicht gegeben, so wird diese Abweichung als ein Fehler des Bausteins interpretiert. Bemerkenswert ist die Fehlererkennbarkeit zweikanaliger Systeme, die von der verwendeten Signaldarstellung abhängig ist. Tabelle 3.4 zeigt diese Unterschiede für die 4 statischen und 5 dynamischen Dars-

Signaldarstellung		Fehlererkennbarkeit				
		Einfach-fehler	Doppelfehler			
			Kanal 1:	L	H	L	H
			Kanal 2:	L	H	H	L
Statisch	A	JA		NEIN	NEIN	JA	JA
	B	JA		JA	JA	NEIN	NEIN
	C	JA		NEIN	NEIN	JA	JA
	D	JA		JA	JA	NEIN	NEIN
Dynamisch	I_A	JA		NEIN	NEIN	JA	JA
	II_{AC}	JA*		NEIN	NEIN	JA*	JA*
	II_{BD}	JA*		JA*	JA*	NEIN	NEIN
	IV_{ABCD}	JA*		JA*	JA*	JA*	JA*
	IV_{ACBD}	JA*		JA*	JA*	JA*	JA*

Tabelle 3.4: Fehlererkennbarkeit bei verschiedenen Signaldarstellungen

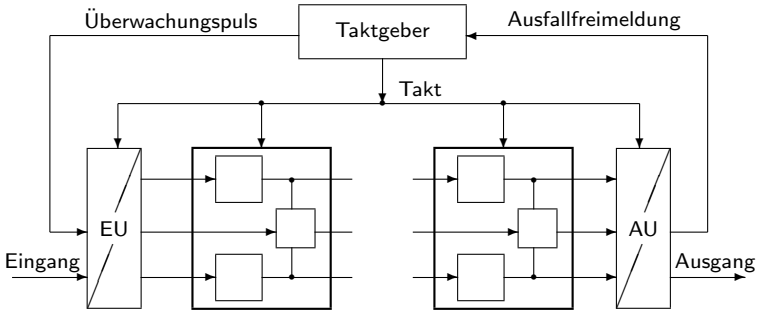

Bild 3.4: Blockschaltbild des URTL-Systems

tellungen aus Tabelle 3.2 und 3.3.

Die Unterschiede in der Fehlererkennbarkeit zeigen wiederum, wie komplex der Zusammenhang zwischen verwendeter Diversitätsart und damit erkennbarer Fehler ist. Durch die Signaldarstellung ist die Art des Einsatzes der Verknüpfungsbausteine in Kanal 1 und 2 bestimmt (statisch, dynamisch, antivalent usw.). Die letzten zwei Signaldarstellungen zeichnen sich durch vollständige und datenflußunabhängige (mit * gekennzeichnet) Fehlererkennung aus.

Das System URTL

Das zweikanalige ausfallsicherheitsgerichtete System URTL wurde in [88] beschrieben. Ein Blockdiagramm des Systems zeigt Bild 3.4. Die Ausgangsignale der Bausteine werden in jedem Takt durch die Überwachungsverstärker geprüft. Hier wird die antivalente dynamische Signaldarstellung (II_{BD} in Tabelle 3.3) angewendet. Nur bei antivalenten Ausgangssignalen an allen Bausteinen, die den Überwachungsverstärkern als Stromversorgung dienen, kann ein Überwachungspuls den Überwachungskreis vollständig durchlaufen und als Ausfallfreimeldung zum Taktgeber zurückkommen.

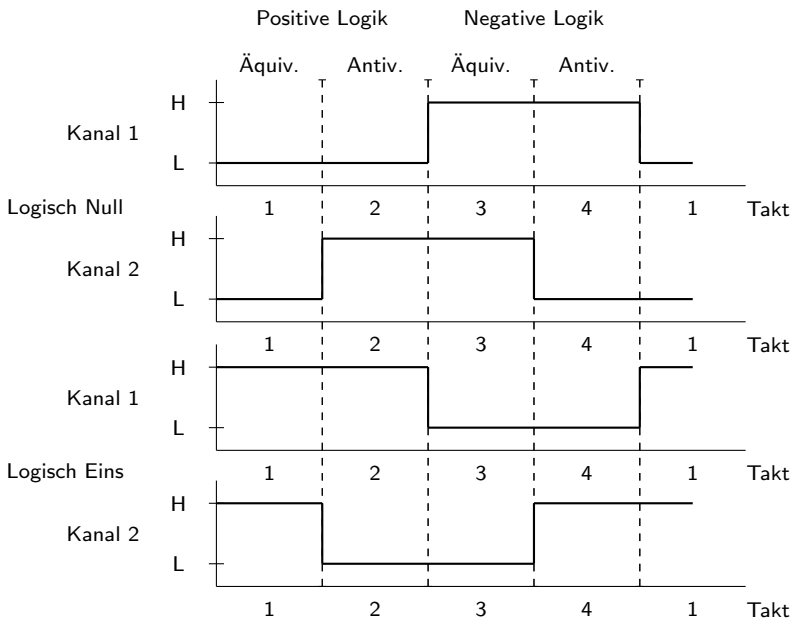

Bild 3.5: Zeitdiagramm für die Signalpaare “Logisch Null” und “Logisch Eins”

Ein System mit vollständiger Ausfallerkennung

In [80] wurde ein Verfahren, das vollständige Ausfallerkennung gewährleistet, entworfen. Mit diesem Verfahren lassen sich nicht nur Einfach-, sondern auch Doppelausfälle in einem zweikanaligen Schaltkreissystem erkennen. Mehrfachausfälle, die in einem Kanal auftreten, sind wie Einfachausfälle, und solche, die auf beiden Kanälen verteilt auftreten, wiederum wie Doppelausfälle erkennbar. Dadurch ist die Vollständigkeit der Ausfallerkennung erreicht [76].

Signaldarstellung Zur vollständigen Ausfallerkennung wurde die Signaldarstellung IV_{ABCD} aus Tabelle 3.3 verwendet. Bild 3.5 zeigt diese Signaldarstellung im Zeitdiagramm. Das Blockbild des zweikanaligen Schaltkreissystems entspricht dem Diagramm nach Bild 3.4. Die Ausgangssignale werden an jedem Baustein nicht nur auf Antivalenz (in den Takten 2 und 4), sondern auch auf Äquivalenz (in den Takten 1 und 3) geprüft. Dafür ist ein Überwachungskreis zur wechselweisen Prüfung von Antivalenz und Äquivalenz erforderlich.

Verknüpfungsbaustein Zur Erprobung des Verfahrens kann man auf die Bausteine des URTL-Systems zurückgreifen. Für die Überwachung äquivalenter Signale (Takt 1 und 3) muß man entweder einen neuen Überwachungsverstärker entwerfen oder den im URTL-System vorhandenen Überwachungsverstärker verwenden und die Äquivalenz- auf die Antivalenzüberwachung zurückführen. In Bild 3.6 ist die letztere Lösung zur Realisierung des Verknüpfungsbausteins gewählt. Dabei werden vier Antivalenzüberwachungsverstärker verwendet.

Die Verknüpfungselemente G_1 und G_2 realisieren eine negierte 2-aus-3-Mehrheitslogik. Wird dem Eingangspaar $Z_1,\ Z_2$ logisch Null (Eins) aufgeprägt, so läßt sich mit den übrigen zwei Eingangspaaren X und Y die NAND-(NOR)-Verknüpfung realisieren. Durch Verwendung der negierten Ausgänge ergibt sich

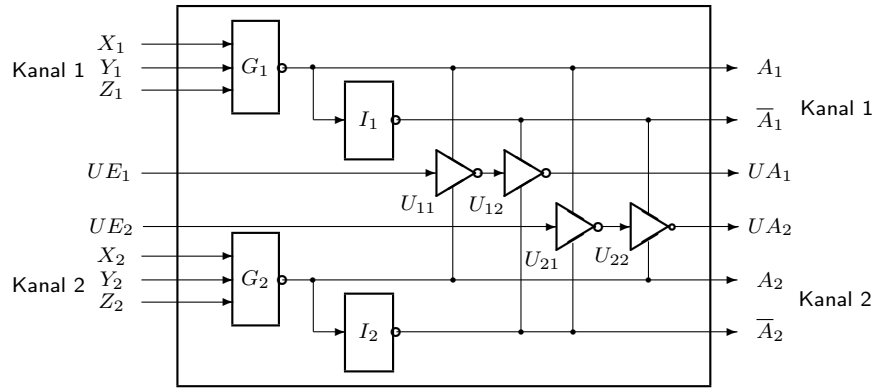

Bild 3.6: Verknüpfungsbaustein

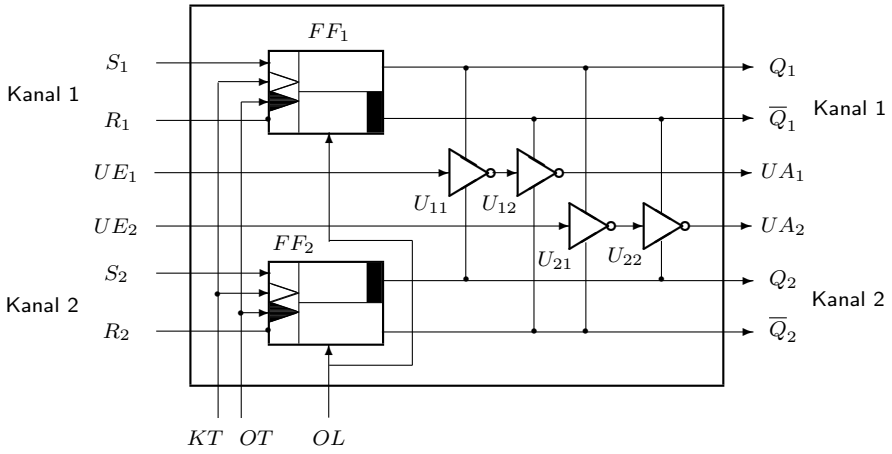

Bild 3.7: Speicherbaustein

daraus die Und-(Oder)-Verknüpfung. Vertauschen der Kanäle führt hier nicht wie beim URTL-System zur Inversion. Mit diesem Verknüpfungsbaustein läßt sich also eine der 7 logischen Grundfunktionen Oder, NOR, Und, NAND, $2v3$, $\overline{2v3}$ und Nicht realisieren. Für die Inversion (Nicht-Funktion) ist kein gesonderter Baustein erforderlich, da die negierten Signale an jedem Baustein zur Verfügung stehen (I_1 und I_2 sind Inverter). Die Überwachungsverstärker sind für Überwachungspulse nur dann durchlässig, wenn sie an antivalente Signale angeschlossen sind. Das trifft bei U_{11} und U_{12} dann zu, wenn die Ausgänge an G_1 und G_2 (und daher auch an I_1 und I_2) antivalent sind. Dagegen sind die Überwachungsverstärker U_{21} und U_{22} bei äquivalenten Signalen an G_1 und G_2, d.h. bei antivalenten Signalen an G_1, I_2 bzw. G_2, I_1 (an denen sie auch angeschlossen sind), durchlässig. Ein zu den Takten 2 und 4 am Eingang UE_1 angelegter Überwachungspuls erscheint am Ausgang UA_1. Dasselbe gilt für UE_2 und UA_2 zu den Takten 1 und 3.

Speicherbaustein Für die Speicherung von Daten wird eine bistabile Kippstufe (Flip-Flop-Baustein FF) mit zwei getakteten RS-Master-Slave-Flip-Flops (FF_1 und FF_2) verwendet (Bild 3.7).

Beide Flip-Flops, FF_1 und FF_2, werden durch zwei Taktsignale (Äquivalenz- und Antivalenztaktsignal OT bzw. KT) gesteuert. Die Funktion der beiden Flip-Flops wird im nächsten Bild 3.8 in Form eines Zeitdiagramms verdeutlicht. Es werden die mit Nr. 1 gekennzeichneten Werte (vor dem Äquivalenztaktsignal) invertiert und die

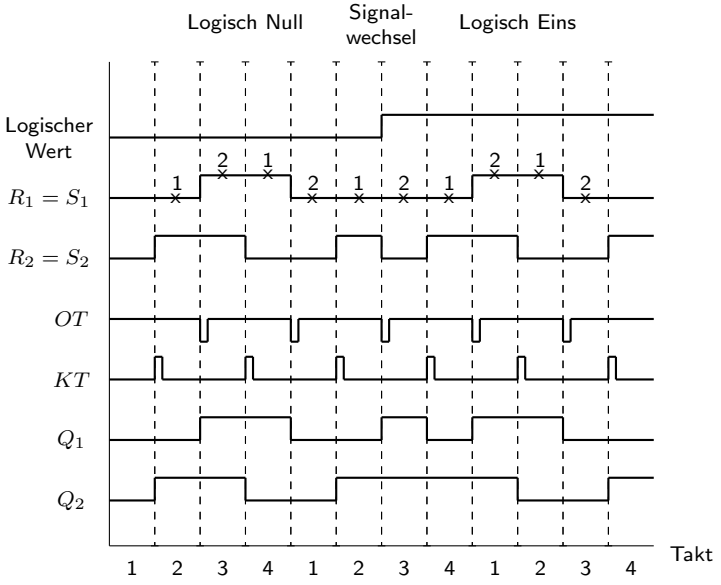

Bild 3.8: Zeitdiagramm der Signale am Speicherbaustein beim Signalwechsel

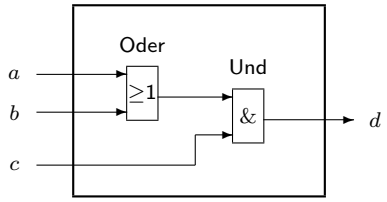

Bild 3.9: Einkanalige Implementierung

mit Nr. 2 gekennzeichneten Werte (vor dem Antivalenztaktsignal) nicht invertiert am Ausgang des Flip-Flops FF_1 (Q_1) im nächsten Takt wiedergegeben. Ähnliches gilt für die Signale am Flip-Flop FF_2. In diesem Bild ist ein Signalwechsel von logisch Null (erste 6 Zeitintervalle) auf logisch Eins (folgende 6 Zeitintervalle) zu erkennen. Ein solcher Signalwechsel ist in jedem Takt möglich.

Beispiel Mit Hilfe der Verknüpfungs- und Speicherbausteine lassen sich nun beliebige kombinatorische oder sequentielle logische Funktionen realisieren. Die Implementierung einer logischen Funktion sei an einem einfachen Beispiel gezeigt. Dabei sei die Funktion

$$d = (a + b) \cdot c = a \cdot c + b \cdot c$$

gewählt. Bild 3.9 zeigt die einkanalige Realisierung.

Die gleiche Funktion ist in Bild 3.10 durch Verwendung des obigen Verknüpfungsbausteins (Bild 3.6) zweikanalig realisiert.

Die Überwachungskreise zur Äquivalenz- und Antivalenzprüfung erhält man durch serielles Durchschalten der Überwachungsverstärker beider Verknüpfungsbausteine. Das neue Verfahren zur Erkennung von Einfach- und Doppelausfällen (der Verknüpfungs- sowie Speicherbausteine) wurde praktisch erprobt [41]. Die Erprobung bestätigte, daß ein zu einem beliebigen Zeitpunkt mittels Hardware simulierter (von Hand injizierter) Doppelausfall im gleichen oder darauffolgenden Takt erkannt wird. Das Verfahren der vollständigen Ausfallerkennung läßt sich auf drei- und

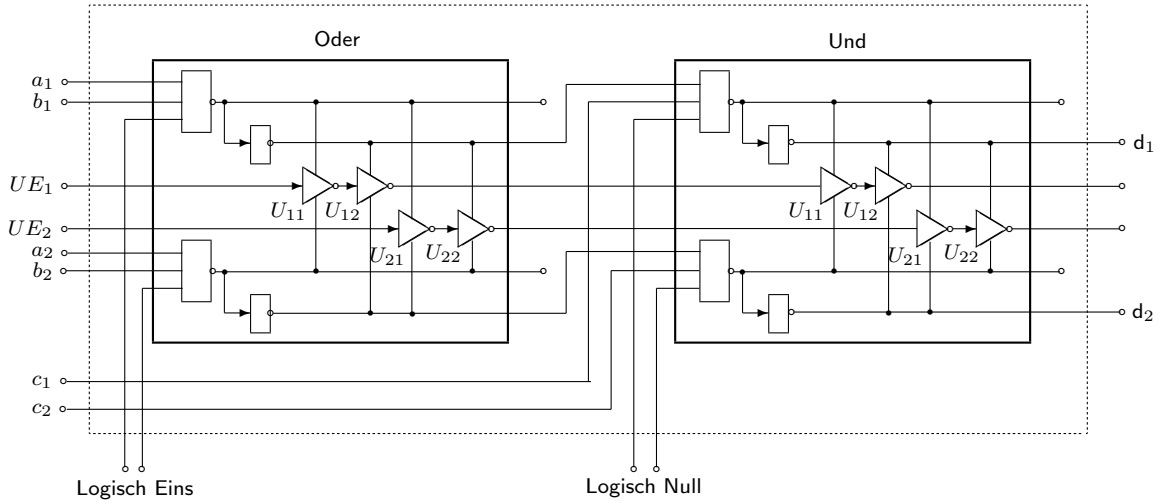

Bild 3.10: Zweikanalige Implementierung

mehrkanalige Signaldarstellung erweitern. Bausteine für ein dreikanaliges System sind in [76] beschrieben.

3.2.3 Realisierung mit Mikroelektronik

System mit Original- und Komplementärlogik

Um eine nahezu 100 %-ige Ausfallerkennung zu erreichen, wurde für die Realisierung eines fehlertoleranten Rechnersystems die Anwendung duplizierter Komplementärlogik vorgeschlagen [107]. Bild 3.11 zeigt die Grundstruktur eines solchen Schaltkreises. Die logische Funktion dieses VLSI-Bausteins ist zweimal implementiert: zum einen als Original- und zum anderen als Komplementärlogik. Für die Herstellung sind also zwei Masken erforderlich. Entwurfs- und Herstellungsfehler, die nur in einem Teil auftreten, lassen sich durch Vergleich der Signale der Original- und der Komplementärlogik erkennen. Nicht nur die Ein- und Ausgabesignale, sondern auch die Zwischenergebnisse, wie z.B. die Registerinhalte der Original- und der Komplementärlogik, tragen zur hohen Ausfallerkennbarkeit sowie zur kurzen Erkennungszeit bei. Dem Verfahren werden folgende Vorteile zugeschrieben:

- sofortige Erkennung von Einzelausfällen,
- sofortige Erkennung der meisten Mehrfachausfälle,
- sofortige Erkennung der meisten Brückenschlußausfälle,
- sofortige Erkennung von Stromversorgungs- und Taktversorgungsausfällen,
- große Wahrscheinlichkeit der Erkennung transienter Ausfälle,
- automatische Trennung (Isolierung) ausgefallener Bausteine bzw. interner Schaltungsbereiche eines Bausteins.