



PATENTAMT

In der vom Anmelder eingereichten Fassung veröffentlicht

(21) WP G 06 F / 323 586 3

(22) 21.12.88

(44) 02.05.90

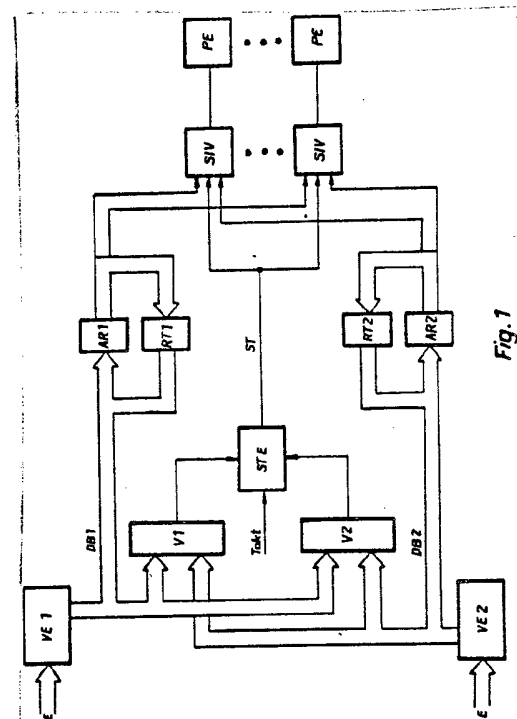
(71) VEB Werk für Signal- und Sicherungstechnik, Elsenstraße 87/96, Berlin, 1193, DD

(72) Grünher, Jochen, Dipl.-Ing.; Klaus, Jürgen; Postler, Johann Georg, Dipl.-Ing.; Schwarz, Ralf, Dipl.-Ing., DD

(54) Schaltungsanordnung zur signaltechnisch sicheren Ausgabe von Prozeßdaten

(55) Redundant, Prozeßdaten, Rücklesen, Sicherungstechnik, sicherer Takt, Verarbeitungseinheit, Vergleich, Prüfzeit

(57) Schaltungsanordnung zur signaltechnisch sicheren Ausgabe von Prozeßdaten. Die Eingangsdaten sind auf redundante, nach gleichem Programm arbeitende Verarbeitungseinrichtungen geschaltet. Sie findet Anwendung in sicherungstechnischen Einrichtungen (Eisenbahnsicherungstechnik). Aufgabe der Erfindung ist eine einfache Anordnung, die für das Rücklesen der Daten und deren Prüfung nur eine geringe zeitliche Belastung darstellt. Die Anordnung soll im wesentlichen mit handelsüblichen Bauelementen und Baugruppen auskommen. Erfindungsgemäß liegen die Ausgangsdatenbusse beider Verarbeitungseinheiten redundant an Vergleichern und an Ausgaberegistern an, deren Datenausgänge bitparallel konjunktiv miteinander und mit dem in einer Stauseinheit gebildeten fehlersicheren Takt verknüpft ist, so daß die Prozeßdaten bei Fehlerfreiheit sofort ausgegeben werden. Das Rücklesen der Daten zu Prüfzwecken und Eigendiagnose erfolgt in Abhängigkeit von der Fehleroffenbarungszeit. Fig. 1



Patentansprüche:

1. Schaltungsanordnung zur signaltechnischen sicheren Ausgabe von Prozeßdaten, deren Eingangsdaten auf gleich aufgebaute redundante, nach einem gleichen Programm arbeitende Verarbeitungseinheiten geschaltet sind und deren Ausgangsdaten mittels Vergleicher auf Übereinstimmung geprüft und die Vergleicherausgangssignale mit einem Eingangstaktsignal zur Bildung eines sicheren Taktes verknüpft werden, **gekennzeichnet dadurch**, daß die Ausgangsdatenbusse (DB 1; DB 2) der Verarbeitungseinheiten (VE 1; VE 2) auch auf Ausgaberegister (AR 1; AR 2) geschaltet sind, deren Datenausgänge einerseits bitparallel konjunktiv mit einem sicheren Takt (ST) verknüpft sind und andererseits auf Rücklesetore (RT 1; RT 2) geführt sind, die in einem durch die Fehleroffenbarungszeit bestimmten Zeitraster aktiviert werden.
2. Schaltungsanordnung nach Anspruch 1, **dadurch gekennzeichnet**, daß zur Erzielung einer kurzen Fehleroffenbarungszeit die Ausgabedaten der Ausgaberegister (AR 1; AR 2) abgeschaltet, von den Verarbeitungseinheiten (VE 1; VE 2) zurückgelesen und wie Eingangsdaten verglichen und ausgewertet werden.

Hierzu 3 Seiten Zeichnungen

Anwendungsgebiet der Erfindung

Die Erfindung betrifft eine Schaltungsanordnung zur signaltechnisch sicheren Ausgabe von Prozeßdaten. Die Eingangsdaten sind auf gleich aufgebaute redundante Verarbeitungseinheiten geschaltet, deren Ausgangsdatenbusse mittels Vergleicher auf Übereinstimmung geprüft werden. Die Programmbearbeitung ist grundsätzlich in beiden Verarbeitungseinrichtungen gleich. Die Anwendung der Erfindung erfolgt in sicherungstechnischen Einrichtungen, insbesondere der Eisenbahnsicherungstechnik.

Charakteristik des bekannten Standes der Technik

In vielen Bereichen der Schaltungstechnik ist es notwendig, die Ausgabe von Daten und damit die Ansteuerung von Prozeßelementen nach sicherungstechnischen Grundsätzen auszuführen. Das bedeutet, daß fehlerhafte Daten, fehlerhafte Schaltzustände oder Bauelementedefekte immer so wirken müssen, daß angeschlossene Prozeßelemente einen Zustand einnehmen, der als ungefährlich definiert ist.

Diese Forderung läßt sich bei der Anwendung von Mikrorechnern für die Verarbeitung von Daten und Ableitung von Ausgabedaten für Prozeßelemente oft nur durch komplizierte Verarbeitungsverfahren oder durch die zusätzliche Anwendung komplizierter, meist signaltechnisch sicherer Zusatzschaltungen oder auch durch die Anwendung zusätzlicher fail-safe Bauelemente realisieren.

So ist es beispielsweise bekannt (Signal u. Draht, 1978, Bd. 70, Heft 4, Seiten 82-86), ein Mikrocomputersystem aus zwei Teilsystemen aufzubauen, die jeweils eigene Busleitungen besitzen. Zwischen die Busleitungen ist ein Vergleicher geschaltet, dem die Impulse eines Taktgebers zugeführt werden und die er als Takt für den nächsten Verarbeitungsschritt durchschaltet, wenn der Vergleicher die Übereinstimmung der Daten feststellt. Wird durch den Vergleicher ein Fehler festgestellt, dann wird der Taktgeber gestoppt und damit das gesamte System gesperrt. Eine Fehlerprüfung, zum Beispiel zum Zwecke der Fehlertoleranz gegenüber Störimpulsen ist dann nicht mehr möglich, ebensowenig eine Eigendiagnose von Teilsystemen zur Fehlerlokalisierung.

In der US-PS 4049957 ist ein Doppelrechnersystem beschrieben, bei dem nur bestimmte Daten beider Teilsysteme auf Übereinstimmung geprüft werden. Diese Daten werden in Registern abgespeichert und bei Fehlerfreiheit über einen Vergleicher ausgegeben. Der Vergleich führt daher zu einer zeitlichen Belastung des Systems.

In der PS-DE 3310975 ist eine Einrichtung zur sicheren Prozeßsteuerung beschrieben, bei der Prozeßsteueraufträge von einem nicht sicheren Mikrocomputer in Kommandodaten eingesetzt werden und in einer Ausgabeeinrichtung gespeichert. Diese Kommandodaten werden laufend zu Prüfzwecken rückgelesen. Das Rücklesen erfolgt in den Mikrocomputer, der die Kommandodaten ausgegeben hat und parallel dazu in einen zweiten Mikrocomputer. Nur wenn beide Mikrocomputer übereinstimmend klassifizieren, erfolgt die Freigabe der gespeicherten Daten in Richtung Prozeßperipherie. Auch bei dieser Anordnung entsteht ein erheblicher zeitlicher Aufwand für die Klassifizierung der rückgelesenen Daten. Außerdem müssen Teile der Einrichtung, so die Auswerteschaltung der beiden Mikrocomputer, die Freigabeschaltung für die Ausgabeeinrichtung sowie zumindest Teile der Ausgabeeinrichtung selbst nach sicherungstechnischen Prinzipien aufgebaut werden.

Weiterhin ist in der DE-OS 2931280 eine redundante Steueranordnung mit mehreren programmierbaren Rechnern vorgeschlagen worden, bei welcher die über die Ausgangsbusleitungen übertragenen Signale in den peripheren Einheiten verknüpft und die verknüpften Signale parallel über mehrere Eingangsbusleitungen zu den Zentraleinheiten rückgeführt werden. Dort findet der Vergleich der rückgeführten Signale mit den Solldaten statt und im Falle einer Abweichung wird ein Fehlersignal abgegeben.

Alle diese bekannten Anordnungen arbeiten derart, daß entweder getaktete Vergleichseinrichtungen bei einer Antivalenz bzw. Nichtübereinstimmung der überprüften Signale oder bei Ausfall der Vergleichseinrichtung die Datenausgabe abschalten und einen Prüftakt sperren. Das bewirkt dann eine Sicherheitsreaktion in der Prozeßperipherie und/oder auch eine Abschaltung der Verarbeitungseinheiten selbst. Andere Anordnungen arbeiten derart, daß sie Ausgabedaten auf Ausgaberegister schalten, rücklesen, prüfen und bei Übereinstimmung durch Vergleichseinrichtungen die Durchschaltung der Daten zur Prozeßperipherie bewirken.

Diese Arbeitsweisen erfordern neben einem hohen technischen Aufwand immer eine erhebliche zeitliche Belastung der Verarbeitungseinrichtung. Weiterhin ist bei den Einrichtungen, bei denen durch Ausbleiben des Prüftaktes die Abschaltung der Verarbeitungseinrichtung selbst erfolgt, keine Eigendiagnose der Verarbeitungseinheiten mehr möglich, und es ist auch nicht das Prinzip der Fehlertoleranz anwendbar.

Ziel der Erfindung

Ziel der Erfindung ist die signaltechnisch sichere Ausgabe von Daten mit minimalem technischem Aufwand und insbesondere geringer zeitlicher Belastung der Verarbeitungseinheiten.

Darlegung des Wesens der Erfindung

Der Erfindung liegt die Aufgabe zugrunde, eine Schaltungsanordnung zur signaltechnisch sicheren Ausgabe von Prozeßdaten zu schaffen, bei der die durch redundante Verarbeitungseinheiten gebildeten Prozeßdaten Vergleichen zugeführt und über Ausgaberegister zur Prozeßperipherie ausgegeben werden und bei der die ausgegebenen Prozeßdaten zu Prüfzwecken rückgelesen werden. Der Aufwand der gesamten Schaltung soll im wesentlichen mit handelsüblichen, nicht fehlersicheren Bauelementen und Baugruppen erfolgen.

Erfindungsgemäß liegen die Ausgangsdatenbusse beider Verarbeitungseinrichtungen redundant an den Vergleichen und direkt an den Eingängen von Ausgaberegistern. Deren Datenausgänge werden konjunktiv miteinander und mit dem in einer Stauseinheit gebildeten fehlersicheren Takt verknüpft und bei Fehlerfreiheit sofort auf die Prozeßelemente durchgeschaltet. Die Datenausgänge der Ausgaberegister sind gleichfalls auf Rücklesetore geführt, deren Abfrage und Auswertung in den Verarbeitungseinheiten zu Prüfzwecken in einem durch die Fehleroffenbarungszeit bestimmten Zeitraster erfolgt. Zeitpunkt und Häufigkeit des Rücklesens werden durch das Programm festgelegt.

Zur Erzielung einer kurzen Fehleroffenbarungszeit werden die Ausgabedaten kurzzeitig abgeschaltet, rückgelesen und dann wie Eingangsdaten behandelt. Wird ein Fehler ermittelt, so führt dieses Ergebnis ebenfalls zur Abschaltung des sicheren Taktes.

In der fehlersicheren Verknüpfung der Ausgabedaten mit dem sicheren Taktsignal werden immer die äquivalenten Ausgabedaten beider Verarbeitungseinrichtungen mit dem sicheren Takt verknüpft. Dadurch ist bei ungleichen Daten aus den Verarbeitungskanälen bereits keine fehlerhafte Ansteuerung der Prozeßelemente möglich, auch wenn die Verarbeitungseinheiten die Ausgabedaten noch nicht rückgelesen und bei der Auswertung und dem Vergleich dieser Daten eine Nichtübereinstimmung festgestellt haben.

Die Verarbeitungseinrichtungen, denen die gleichen Eingangsdaten zugeführt werden, arbeiten die gleichen Programme ab. Somit erarbeiten sie auch die gleichen Ausgabedaten. Jeder Verarbeitungseinheit ist ein Vergleich zugeordnet, der die Daten auf den Busleitungen der eigenen Einheit mit den äquivalenten Daten auf den Busleitungen der anderen Verarbeitungseinheit vergleicht. Die Ausgänge der Vergleiche werden auf Fehlerflipflops geschaltet. Alle diese Schaltungsdetails arbeiten nicht fehlersicher. Die Ausgänge der Vergleiche (Fehlerflipflops) beider Kanäle werden in einer Stauseinheit, einer besonderen fehlersicheren Schaltung, mit einem Taktsignal verknüpft. Am Ausgang der Stauseinheit steht immer dann ein fehlersicheres Taktsignal an, wenn der Eingangstakt vorhanden ist und die Vergleicherausgänge die Stellung – kein Fehler – haben. Die Verarbeitungseinheiten werden hier, wenn sie bei der Kontrolle der rückgelesenen Daten einen Fehler festgestellt haben, nicht abgeschaltet, so daß sie noch eine Eigendiagnose der Verarbeitungseinheit selbst und der angeschlossenen Baugruppen durchführen können.

Die fehlerhaften Daten werden für die Diagnose selbst genutzt.

Durch das Rücklesen in Abhängigkeit von der Fehleroffenbarungszeit werden die Verarbeitungseinheiten zeitlich entlastet.

Ausführungsbeispiel

Die Erfindung soll nachstehend anhand eines Ausführungsbeispiels näher erläutert werden.

Fig. 1: zeigt die erfindungsgemäße Schaltungsanordnung

Fig. 2 und 3: zeigen die Einfügung von Prüfzyklen in den Programmablauf.

Die Anordnung besteht aus den beiden Verarbeitungseinheiten VE 1 und VE 2, die die gleichen Eingangsdaten E zugeführt bekommen und die gleichen Programme abarbeiten. Jeder Verarbeitungseinheit ist ein Vergleich V 1; V 2 zugeordnet, der die Daten auf den Busleitungen DB 1; DB 2 der eigenen mit den Daten auf den Busleitungen der anderen Verarbeitungseinheit vergleicht. Den Ausgang der Vergleiche bilden Fehlerflipflops, die bei einem durch den Vergleich festgestellten Fehler sofort umschalten. Die Stellungen der Fehlerflipflops werden in einer Stauseinheit STE mit einem Taktsignal fehlersicher verknüpft. Am Ausgang der Stauseinheit STE liegt immer dann ein fehlersicherer Takt ST an, wenn das Eingangstaktsignal vorhanden ist und die Vergleiche V 1; V 2 keinen Fehler festgestellt haben. Im Fehlerfall wird der sichere Takt abgeschaltet.

Da die Verarbeitungseinheiten VE die gleichen Programme abarbeiten, bilden sie auch die gleichen Ausgabedaten für die Ansteuerung der Prozeßelemente PE. Diese Ausgabedaten werden jeweils auch über den Datenbus in Ausgaberegister AR 1; AR 2 geschrieben. Die Schaltungen zur Adreßkodierung und Verknüpfung der Steuersignale, die auf die Ausgaberegister und Rücklesetore RT 1; RT 2 wirken, sind nicht dargestellt.

Die einander entsprechenden Daten der Ausgaberegister AR 1; AR 2 werden mit dem sicheren Takt ST konjunktiv in einer fehlersicheren Verknüpfungsschaltung SIV verknüpft. Diese stellt wiederum nur ein Ausgangssignal zur Ansteuerung der Prozeßelemente PE bereit, wenn die Ausgabedaten beider Verarbeitungseinheiten die notwendige Sollstellung haben, gleich sind und das sichere Taktsignal ST vorhanden ist. Das Ausgangssignal der sicheren Verknüpfungsschaltung SIV ist ein Taktsignal. Es kann z.B. gleichgerichtet werden zur Ansteuerung der Prozeßelemente oder zur Ansteuerung fehlersicherer

Leistungsverstärker dienen. Die auf die Ausgaberegister ausgegebenen Daten liegen gleichzeitig am Eingang der Rücklesetore RT 1; RT 2 an und werden auf Anforderung der Verarbeitungseinheiten VE 1; VE 2 in diese zur Kontrolle zurückgelesen.

Der Ablauf sämtlicher Programmteile der Verarbeitungseinheiten VE wird durch ein Steuerprogramm organisiert. Dieses bestimmt auch den Zeitpunkt, zu dem in den normalen Ablauf Testprogramme eingefügt werden, um die Fehleroffenbarungszeit einzuhalten. In den Figuren 2 und 3 sind Ausschnitte von Einfügungen von Prüfprogrammen dargestellt, die mit Hilfe des Rücklesens der Ausgabedaten durchgeführt werden.

Stimmen die auf den Bussen liegenden Ausgabedaten überein, werden aber am Ausgang der Ausgaberegister AR 1; AR 2 z. B. durch Bauelementedefekte verfälscht, so kann ebenfalls in sicherungstechnischer Verknüpfung kein Ausgangssignal zur Ansteuerung der Prozeßelemente PE mehr gebildet werden, weil in dieser Verknüpfungsschaltung SIV die Ungleichheit der Daten bei VE erkannt wird. Außerdem werden die verfälschten Daten in die Verarbeitungseinheiten zurückgelesen und wie Eingangsdaten behandelt. Die beim nachfolgenden Vergleich bemerkte Verfälschung führt ebenfalls zur Abschaltung des sicheren Taktes der Stauseinheit. Dadurch fehlt ein weiteres Signal für die Verknüpfung in der Verknüpfungsschaltung SIV. Da, wie oben beschrieben, schon kein Ausgangssignal für die Prozeßelemente mehr erzeugt werden kann, wenn die Ausgabedaten beider Ausgaberegister unterschiedlich sind, brauchen das Rücklesen und die Auswertung der Daten nur in solchen zeitlichen Abständen erfolgen, die durch eine notwendige Fehleroffenbarungszeit gegeben sind.

Nach dem in Fig. 3 dargestellten Ablaufplan werden, wenn sich die Ausgabedaten betriebsmäßig über längere Zeiten nicht ändern, zur Erzielung einer kurzen Fehleroffenbarungszeit, die Ausgabedaten kurzzeitig abgeschaltet, rückgelesen, verglichen und bei Fehlerfreiheit wieder angeschaltet. Anderenfalls wird eine Fehlerbehandlung eingeleitet, die die normale Arbeit der Einrichtung beendet.

Dieses Prinzip der Ausgabe kann für die Ansteuerung einer Vielzahl von Prozeßelementen benutzt werden, da die Ausgaberegister zur Erzielung einer größeren Verarbeitungsbreite kaskadiert werden können.

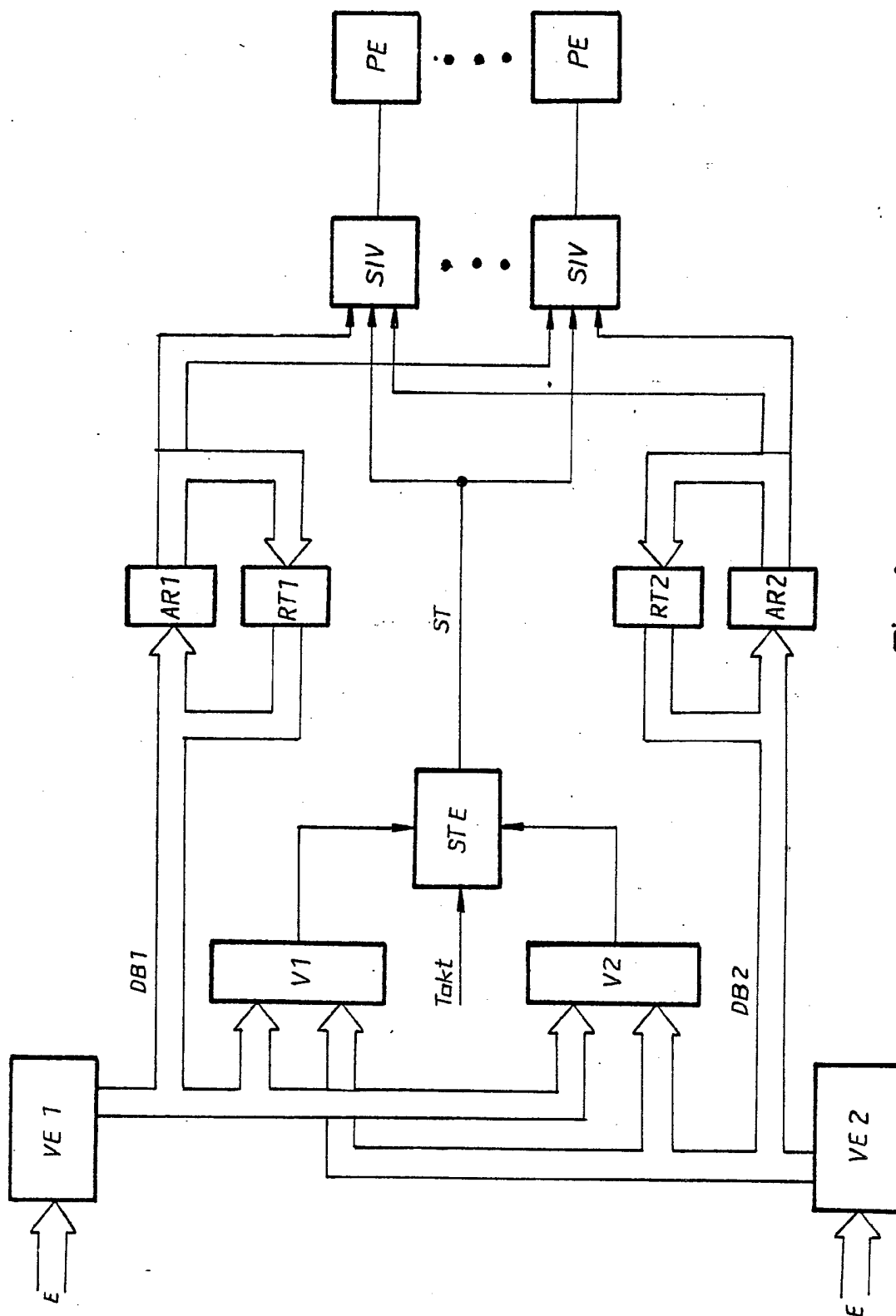


Fig. 1

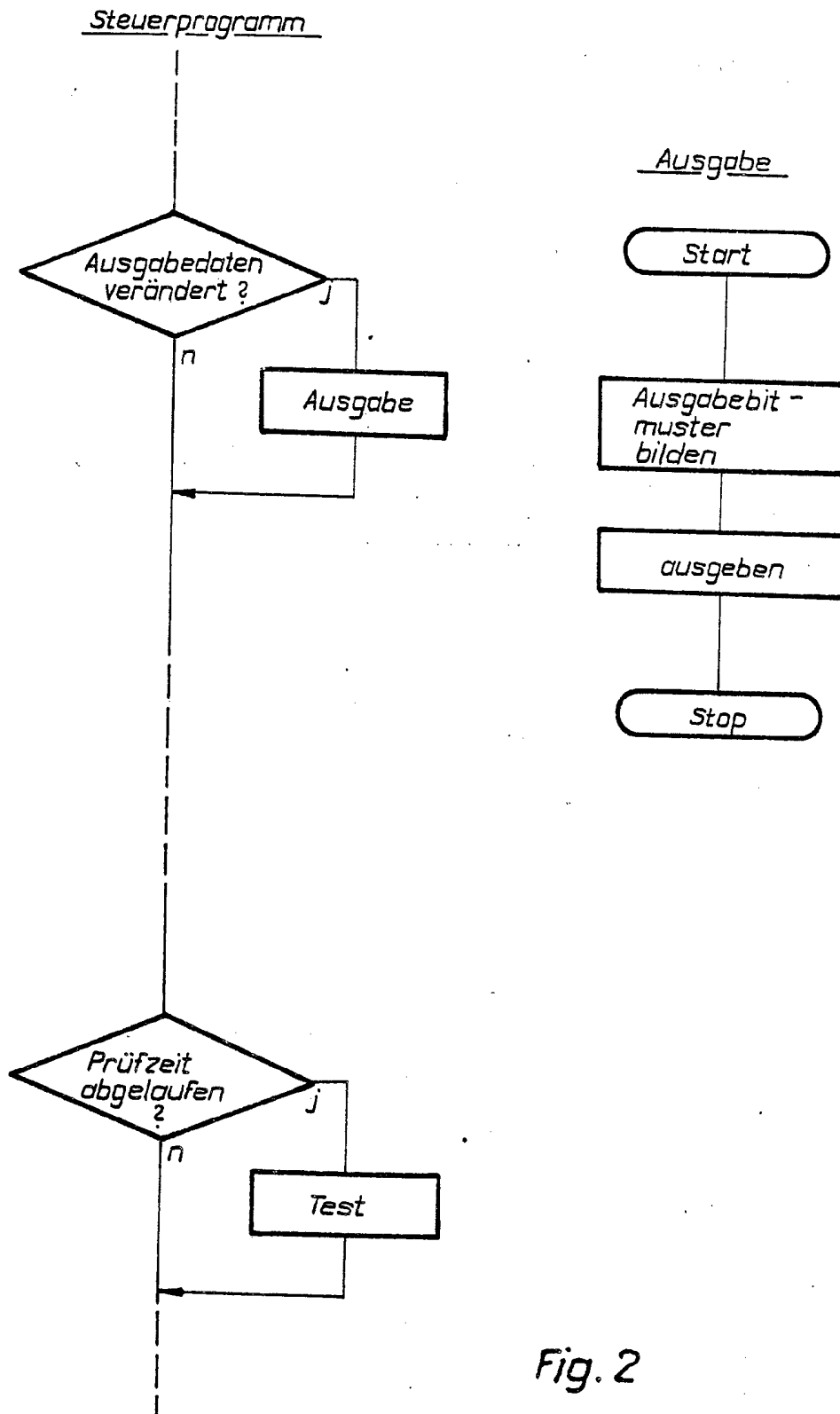


Fig. 2

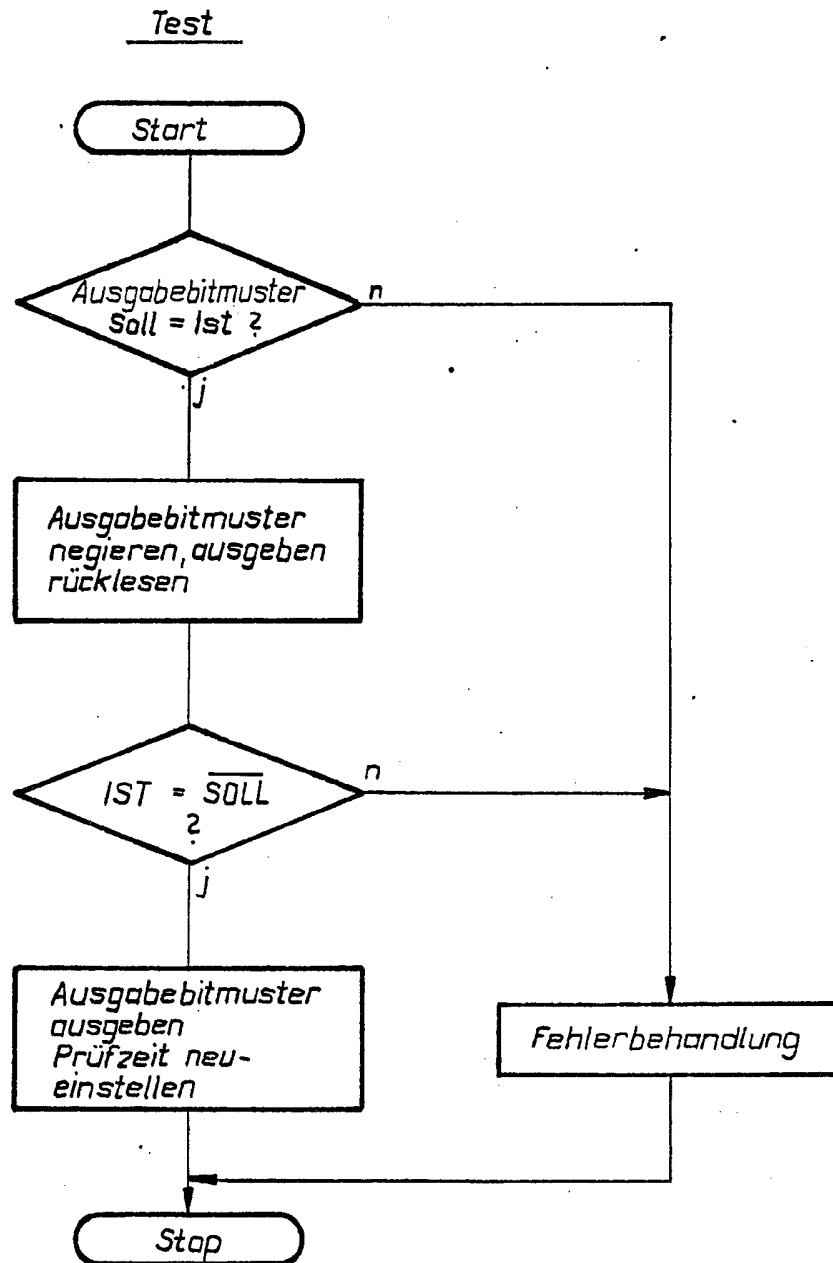


Fig. 3