



CH 675563 A5



SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

⑪ CH 675563 A5

⑤① Int. Cl.⁵: B 60 L 15/42
B 60 R 16/02

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

⑫ PATENTSCHRIFT A5

⑫① Gesuchsnummer: 1275/88

⑫② Anmeldungsdatum: 07.04.1988

⑫③ Priorität(en): 30.04.1987 DE 3714960

⑫④ Patent erteilt: 15.10.1990

⑫⑤ Patentschrift
veröffentlicht: 15.10.1990

⑦③ Inhaber:
Licentia Patent- Verwaltungs-GmbH, Frankfurt a.M.
70 (DE)

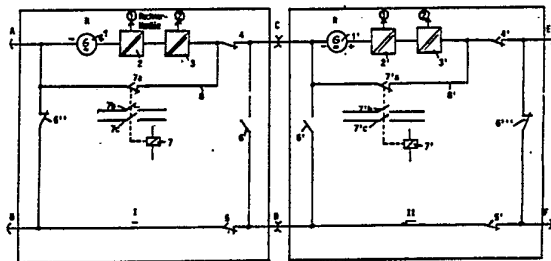
⑦② Erfinder:
Rapoen, Klaus, Berlin 44 (DE)

⑦④ Vertreter:
Kirker & Cie SA, Genève

⑤④ Anordnung zur sicheren Erfassung von Prozesszuständen innerhalb frei miteinander kuppelbarer Einheiten und Verfahren zur Durchführung.

⑤⑦ Zur sicheren Erfassung von Prozesszuständen innerhalb frei miteinander kuppelbarer Einheiten, die jeweils von miteinander koppelbaren Rechnern bedient werden, wird nach der Erfindung eine Anordnung mit folgenden Merkmalen vorgeschlagen:

- jede von n kuppelbaren Einheiten (hier z.B. I, II) bildet für jeden zu überwachenden Prozess mit einer steuerbaren Stromquelle (1 bzw. 1') sowie wenigstens zwei Stromerfassungsgliedern (2, 3 bzw. 2', 3') eine eigene interne Strommeldeschleife mit in Reihe liegenden vom Prozess auslösbaren Prozesskontakten (4, 5 bzw. 4', 5');
- beim Kuppeln mehrerer solcher Einheiten (I + II) werden die internen Strommeldeschleifen dieser Einheiten elektrisch aufgetrennt und jeweils für gleichartige Prozesse gemeinsame, alle Einheiten durchlaufende Strommeldeschleifen gebildet,
- jede der zu jeder Einheit gehörenden Stromquellen (1, 1') einschliesslich ihrer Stromerfassungsglieder (2, 3; 2', 3') ist durch eine Subschleife (8, 8') überbrückbar, die für Testzwecke durch einen Schalter aktivierbar ist, dessen Stellung sicherheitstechnisch durch besondere Tests über zusätzliche stellungsabhängige Stromschleifen überwacht wird.



Beschreibung

Die Erfindung bezieht sich auf eine Anordnung zur sicheren Erfassung von Prozesszuständen, wie sie im Oberbegriff des Anspruches 1 näher definiert ist.

Sicherheitstechnische Überwachung wird nach einem Grundprinzip der Steuerungstechnik im Ruhestromverfahren durchgeführt. Es wird dazu eine Meldestromschleife gebildet. Jegliche Stromunterbrechung ist als Störung zu deuten und lässt z. B. ein Relais abfallen, wodurch Meldung und ggf. Abschaltung erfolgt.

Bei miteinander kuppelbaren Einheiten, wie sie z. B. durch Fahrzeuge gegeben sein können, führt man zur Gewährleistung der Sicherheit Meldestromschleifen durch alle Fahrzeuge hindurch. In Reihenschaltung können darin z.B. jeweils alle Notschalter oder Notbremsschalter oder Türverriegelungen oder Kupplungskontakte etc. in separaten Schleifen liegen. Einspeisung und Stromrücklauf erfolgt z. B. vom Führerstand aus. Wird einer dieser Prozessschalter geöffnet, wird das Fahrzeug stillgesetzt.

Bei einem Fahrzeugverband, der variabel aus mehr oder weniger, z. T. auch verschiedenen Fahrzeugen, oft ohne Führerstand, zusammenstellbar ist, liegen bereits Einspeisungsprobleme vor, dies vor allem bei redundanten Systemen, wo ein Fahrzeug die Steuerfunktion eines anderen mit übernehmen soll und zum störungsfreien Verhalten des Gesamtsystems (Zuges) bei Ausfall eines Fahrzeuges alle Fahrzeugeinheiten parallel arbeiten.

Bei signaltechnisch sicheren Rechnersystemen muss die Funktion des Rechners durch ständige Tests zusätzlich überprüfbar und dazu vom Prozess abkoppelbar sein. Dazu ist es bekannt, die Einspeisung einer durch mehrere Fahrzeuge hindurchgehenden Schleife nur von einem Rechner durchzuführen. Schaltet dieser den Prozess ab, z.B. wegen On-Line Tests zur Überprüfung, gibt es keine Prozessinformation mehr. Haben die anderen Fahrzeuge auch bordeigene Rechner, werden die Meldungen auch der anderen Rechner zumindest gestört und die Datenerfassung behindert. Nachteilig ist auch, dass nur der einspeisende Rechner einen On-Line Test durchführen kann.

Zweck der Erfindung ist es, die geschilderten Mängel zu beheben. Dabei liegt die Aufgabe in einer sicheren Erfassung von sicherheitsrelevanten Prozesszuständen bei durch mehrere Rechner verkoppelten Systemen ohne Beeinflussung des Gesamtsystems bei Ausfall oder Abschalten eines Rechners. On-Line Tests sollen dabei ohne Unterbrechung der allgemeinen Datenerfassung durchgeführt werden können. Bei Ausfall eines Rechners (bei Redundanzbetrieb) muss durch unterbrechungsfreies Umschalten ein echter Parallelbetrieb erfolgen, bei dem wichtige Funktionen des ausfallbehafteten Fahrzeuges zeitweilig von einem anderen Rechner übernommen werden können.

Diese Aufgabe wird nach der Erfindung gemäss den kennzeichnenden Merkmalen des Anspruches 1 gelöst. Weitere vorteilhafte Ausgestaltungen sind den abhängigen Ansprüchen entnehmbar.

Anhand schematischer Darstellungen wird die Erfindung im nachstehenden näher erläutert. Es zeigen:

- 5 Fig. 1 einen Zugverband aus zwei Fahrzeugen
Fig. 2 ein Funktionsschema.

Fig. 1 zeigt einen Fahrzeugverband mit zwei gekuppelten Einheiten, hier den Fahrzeugen I und II. Jedes Fahrzeug, das durch einen eigenen nicht näher dargestellten sicheren Bordrechner gesteuert wird, weist eine der Anzahl der zu überwachenden, d. h. zu erfassenden Prozesse entsprechende Anzahl von elektrisch getrennten Meldestromschleifen auf. Dargestellt ist der Übersichtlichkeit halber jedoch jeweils nur eine Meldestromschleife. Diese enthält als wesentliche Elemente eine vom Rechner R steuerbare zum Fahrzeugnetz potentialgetrennte Stromquelle 1 (bzw. 1') mit niedrigem Innenwiderstand (z. B. 15 mA bei max. 30 V), sowie zwei ebenfalls potentialgetrennte Stromerfassungsglieder 2 und 3 (bzw. 2', 3') für die Überwachungsmeldungen an zwei separate Rechnerkanäle ① und ②. Ferner gehören zur jeweiligen fahrzeugeigenen Meldestromschleife noch Prozessmeldekontakte, hier z. B. die Notschaltkontakte 4, 5 (bzw. 4', 5' im anderen Fahrzeug).

Bei der mechanischen Fahrzeugkupplung werden die fahrzeugeigenen Meldestromschleifen elektrisch aufgetrennt und durch Umschaltung eine gemeinsame Meldestromschleife geschaffen. Die Anzahl der gekuppelten Fahrzeuge bestimmt letztlich die Grösse der Meldestromschleife; wegen der reihengeschalteten Stromquellen (Spannungssumma- tion) ist die Grösse begrenzt.

Bei der Kupplung der dargestellten Fahrzeuge I und II erfolgt die nötige Umschaltung der Meldestromschleife durch nicht näher dargestellte Signalrelais (Kupplungsauswertung).

Diese Relais weisen zwangsgeführte Kontakte 6, 6' auf, deren Schaltstellungen – jetzt geöffnet – sicher überwacht werden. Die entsprechenden Kontakte 6'' und 6''' am Anfang und Ende des Fahrzeugverbandes sind zur Zeit geschlossen. Prinzipiell können hier natürlich auch direkte mechanische Schalter an den Kupplungen Verwendung finden.

Im vorliegenden ergibt sich damit folgende Strommeldeschleife durch den Zugverband:

50 1+, 2, 3, 4, C, 1', 2', 3', 4', 6'', 5', D, 5, 6'', 1-.

Der Prozess muss derart auf die Meldeschleife einwirken, dass das zu meldende Ereignis die Stromschleife signaltechnisch sicher unterbricht. Für die Ausführung des Meldekontaktes sind folgende Varianten denkbar.

- 60 1. Entweder ein vom Prozess zwangsöffnender Kontakt oder
2. zwei in Reihe geschaltete Kontakte, die unabhängig voneinander den Prozess erfassen.

Die Funktion beider Kontakte muss dann inner-

halb der Ausfalloffenbarungszeit (AOZ) der Melde-
einrichtung überprüft werden. Zur Festlegung der
Ausfalloffenbarungszeit werden beide Kontakte
und ihre Auslösemechanismen als eine Betracht-
ungseinheit gesehen. Hierbei wird als sicher ange-
nommen, dass nach erfolgter Prüfung auf Funktion
der beiden Einzelkontakte und ihrer Auslösemecha-
nismen innerhalb der Ausfalloffenbarungszeit min-
destens ein Kontakt bei Eintritt eines Prozessereig-
nisses die Stromschleife unterbricht.

Die Auswertung erfolgt jeweils durch die vonein-
ander und gegenüber anderen Meldestreifen unab-
hängigen Stromerfassungsglieder 2, 3 bzw. 2', 3'.
Vorteilhaft sind z. B. Optokoppler einsetzbar. Die
Ausgangssignale der Stromerfassungsglieder gehen
jeweils an die zugeordneten Rechnerkanäle

① und ② des bordeigenen sicheren Rech-
ners. Dabei sind die Meldungen der Stromschleifen
an die jeweiligen Rechner als Prozessmeldungen
nur gültig, wenn ein zwangsgeführtes Meldungs-
auswertungsrelais 7 (bzw. 7') rechnergesteuert an-
gezogen hat, d. h. der Ruhekontakt 7a (bzw. 7'a) ge-
öffnet ist. Das Kommando zur Öffnung wird vom
Rechner zwar mit einem Signal «Meldungs-
auswertung Ein» gegeben, die Stellung des Mel-
dungsauswertungsrelais 7 muss jedoch überwacht
werden. Das geschieht jeweils mit zwei sparaten
Stromschleifen über eigene zwangsgeführte Ar-
beitskontakte 7b und 7c (bzw. 7'b und 7'c). Die Not-
schaltkontakte 4, 5 (bzw. 4', 5') als Meldek-
ontakte des Prozesses sind zweckmässig als Zwangsöff-
ner (VDE 0113) ausgebildet, d. h. sie öffnen zwangs-
weise abhängig vom Prozess. Erfolgt dies, wird von
den Stromerfassungsgliedern 2, 3 «O»-Signal über
die Kanäle ① und ② dem Bordrechner mitge-
teilt, der daraufhin z. B. die Bremsen löst.

Im Ruhezustand des Meldungsauswertungsrelais
7 bzw. nach einem Abschalten desselben ist der
Kontakt 7a geschlossen. Das bewirkt ein Kurz-
schliessen und Bilden einer vom Prozess unabhän-
gigen Subschleife 8 (bzw. 8') über der Stromquelle 1
und den Stromerfassungsgliedern 2, 3 (bzw. 1' und
2', 3'). In diesem Zustand werden On-Line Tests
vorgenommen, für beide Fahrzeuge zu unterschied-
lichen Zeiten. Eine Beeinträchtigung der Prozess-
auswertung im jeweils anderen Fahrzeug (hier z. B.
II) findet dabei nicht statt. Durch rechnergesteu-
ertes Zu- und Abschalten der Stromquelle 1 kann da-
bei die Funktion der sicheren Signalerfassung über-
prüft werden.

Im Rahmen der Rechner On-Line Tests werden
auch die Eingaben für die sicheren Signale inner-
halb der Ausfalloffenbarungszeit (AOZ) geprüft.
Diese Prüfung umfasst die Auswerteschaltung der
Stromschleifen (Optokoppler) und die Datenpfade
der Eingabekarten. Der Test erkennt stuck-at-1
(gefährlich), stuck-at-0 (ungefährlich) und Mitzieh-
effekte zwischen zwei beliebigen Eingangsbits je ei-
nes Kanals. Während des Tests können keine Pro-
zesszustände abgefragt werden.

Mit Hilfe des Signals «Meldungsauswertung Ein»
kann zwischen On-Line Testbetrieb oder Prozess-

erfassung gewählt werden. Die Überwachung der
Ausführung des Befehls Meldungsauswertung
«Ein», d. h. die Stellung dieses für die Sicherheit
verantwortlichen Meldungsauswertungsrelais 7
(bzw. 7') muss jedoch zusätzlich sicher überwacht
werden. Dies geschieht über sichere Signaleingab-
en über Kontakt 7b und Kontakt 7c. Diese beiden
Signale unterliegen einem besonderen On-Line-
Test, der während der Prozesserrfassung durchge-
führt wird.

Fig. 2 zeigt in einem Funktionsschema den Pro-
zess mit Ankopplung an den Rechner.

Über eine Rechner-Ausgabekarte III (es genügt
ein Rechnerkanal ① oder ②) für z. B. hier 24
Testausgaben (an Port 0 bis Port 23) werden die On-
Line-Tests durchgeführt nach Abkopplung der ver-
schiedenen Prozesse und Bildung von Subschleifen
über die Schalter 7a.

Wie hier für Anschluss 0 dargestellt, werden für
alle Prozesse die entsprechenden Stromquellen 1
nach einem überdeckenden Testmuster mit log. 1 an-
gesteuert und die zugeordneten Stromerfassungsg-
lieder 2, 3 müssen das Muster gleichzeitig und
gleichwertig erfassen und an die beiden Eingabe-
karten IV, V für die beiden Rechnerkanäle 1 und 2
weitergeben, wo das Bit-Muster sicher wiederer-
kannt werden muss. Die Testausgaben (einkanalig)
selbst sind nicht sicher. Sie speisen über die Strom-
quelle 1 in die Prozessmeldeschleifen ein und bilden
mit den Prozessen Und-Verknüpfungen. Zur Ab-
frage der Prozesszustände müssen die Testausga-
ben auf «1» stehen, d. h. die ersten 22 Anschlüsse
(0 bis 21) müssen zur Einspeisung der Prozessmel-
deschleifen eine «1» ausgeben. Darüberhinaus
muss vom Rechner das nicht sichere Signal
«Meldungsauswertung ein» zur Ansteuerung des
Relais 7 (vgl. Fig. 1) ausgegeben werden. Darüber-
hinaus werden die beiden verbleibenden Testan-
schlüsse (Port 22 und Port 23) mit einer besonderen
Signalfolge beschickt. Während die Anschlüsse 0
bis 21 während der Prozesserrfassung fest eine «1»
ausgeben, erfolgt an Port 22 und Port 23 eine «1»-
«0»-Wechselfolge mit einem Tastverhältnis 1:1
(künstliche Dynamisierung). Dabei sind Port 22 und
Port 23 immer antivalent, d. h. wenn Anschluss 22
eine «1» ausgibt, gibt Anschluss 23 eine «0» aus
und umgekehrt. Die Taktzeit kann zwischen einigen
Millisekunden und mehreren Sekunden liegen. Wird
der ausgegebene Wechseltakt, der bei Rückmel-
dung über die Kontakte 7b und 7c an den Eingaben
des Rechners nicht mehr erkannt, so sind alle siche-
ren Eingaben ungültig.

Durch die Erfindung kann auf einfache Weise ei-
ne sichere Prozesserrfassung gewährleistet wer-
den.

Patentansprüche

1. Anordnung zur sicheren Erfassung von Pro-
zesszuständen innerhalb frei miteinander kuppelba-
rer Einheiten, die jeweils von miteinander koppelba-
ren Rechnern bedient werden, unter Anwendung

- von Strommeldeschleifen und Prüftests, gekennzeichnet durch folgende Merkmale
- jede von kuppelbaren Einheiten (I, II) bildet für jeden zu überwachenden Prozess mit einer steuerbaren Stromquelle (1 bzw. 1') sowie wenigstens zwei Stromerfassungsgliedern (2, 3 bzw. 2', 3') eine eigene interne Strommeldeschleife mit in Reihe liegenden vom Prozess auslösbaren Prozesskontakten (4, 5 bzw. 4', 5'); 5
 - beim Kuppeln mehrerer solcher Einheiten (I + II) werden die internen Strommeldeschleifen dieser Einheiten elektrisch aufgetrennt und jeweils für gleichartige Prozesse gemeinsame, alle Einheiten durchlaufende Strommeldeschleifen gebildet, 10
 - jede der zu jeder Einheit gehörenden Stromquellen (1, 1') einschliesslich ihrer Stromerfassungsglieder (2, 3; 2', 3') ist durch eine Subschleife (8, 8') überbrückbar, die für Testzwecke durch einen Schalter aktivierbar ist, dessen Stellung sicherheitstechnisch durch besondere Tests über zusätzliche stellungsabhängige Stromschleifen überwacht wird. 15
2. Anordnung nach Anspruch 1, dadurch gekennzeichnet, dass die Subschleife (8) über den Ruhekontakt (7a) eines zwangsgeführten Meldungsauswertungs-Relais (7) geführt wird, das von einem Rechnersignal «Meldungsauswertung Ein» ansteuerbar ist und damit die Subschleife (8) unterbricht, wobei zwei zwangsgeführte Arbeitskontakte (7b, 7c) des Meldungsauswertungs-Relais geschlossen werden und über die damit gebildeten zusätzlichen Stromschleifen die besonderen Tests erfolgen. 20
3. Verfahren zur Testdurchführung für eine Anordnung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die besonderen Tests als On-Line Tests während der Prozesserfassung erfolgen, bei der neben der Einspeisung der gemeinsamen Strommeldeschleifen mit festem Dauersignal «1» (über Bit 0 bis 21) die zwei zusätzlichen Stromschleifen von je einem nicht sicheren Ausgang des Rechners (über Bit 22, 23) mit einer dynamisch abwechselnden «1»–«0»-Folge versorgt werden, die wiedererkannt werden muss. 25
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass das Tastverhältnis der antivalenten Wechseltaktfolge 1 : 1 beträgt. 30
5. Verfahren nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass die Taktzeit einstellbar ist und zwischen einigen Millisekunden und mehreren Sekunden liegt. 35
6. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass im Rahmen der On-Line Tests des Rechners in einer kuppelbaren Einheit (I bzw. II) periodisch die zugehörige Subschleife (8 bzw. 8') aktiviert und damit diese Einheit aus der Prozesserfassung herausgenommen wird, wobei über den verbleibenden Stromdurchgang über die Subschleife (8 bzw. 8') mittels der steuerbaren Stromquelle (z. B. 1) die sicheren Signale innerhalb der Ausfallöffnungszeit prüfbar sind, ohne die Prozesserfassung oder den On-Line-Test der weiteren gekuppelten Einheiten zu beeinflussen. 40
7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass die Prüfung der Stromerfassungsglieder (2, 3) die Auswerteschaltung und die Datenpfade der Eingabekarten (3) einschliesst. 45

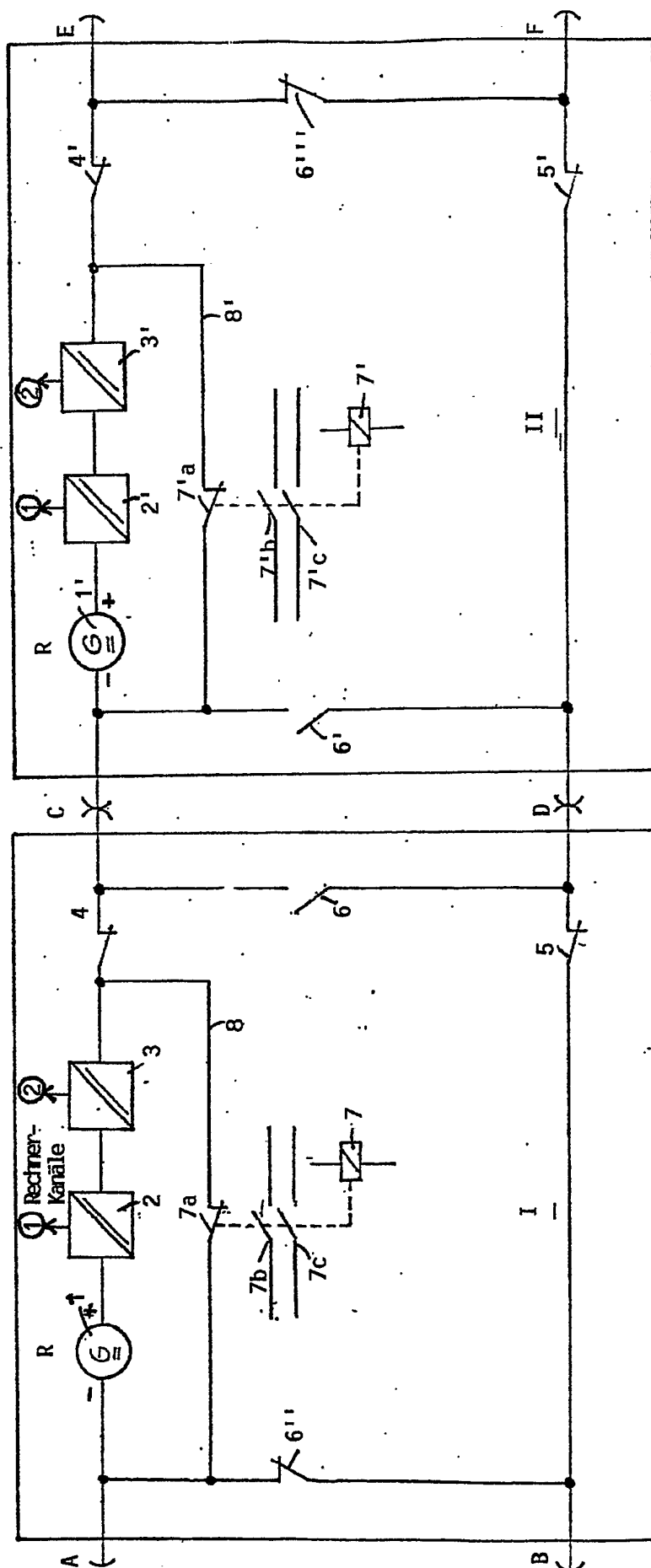


Fig. 1

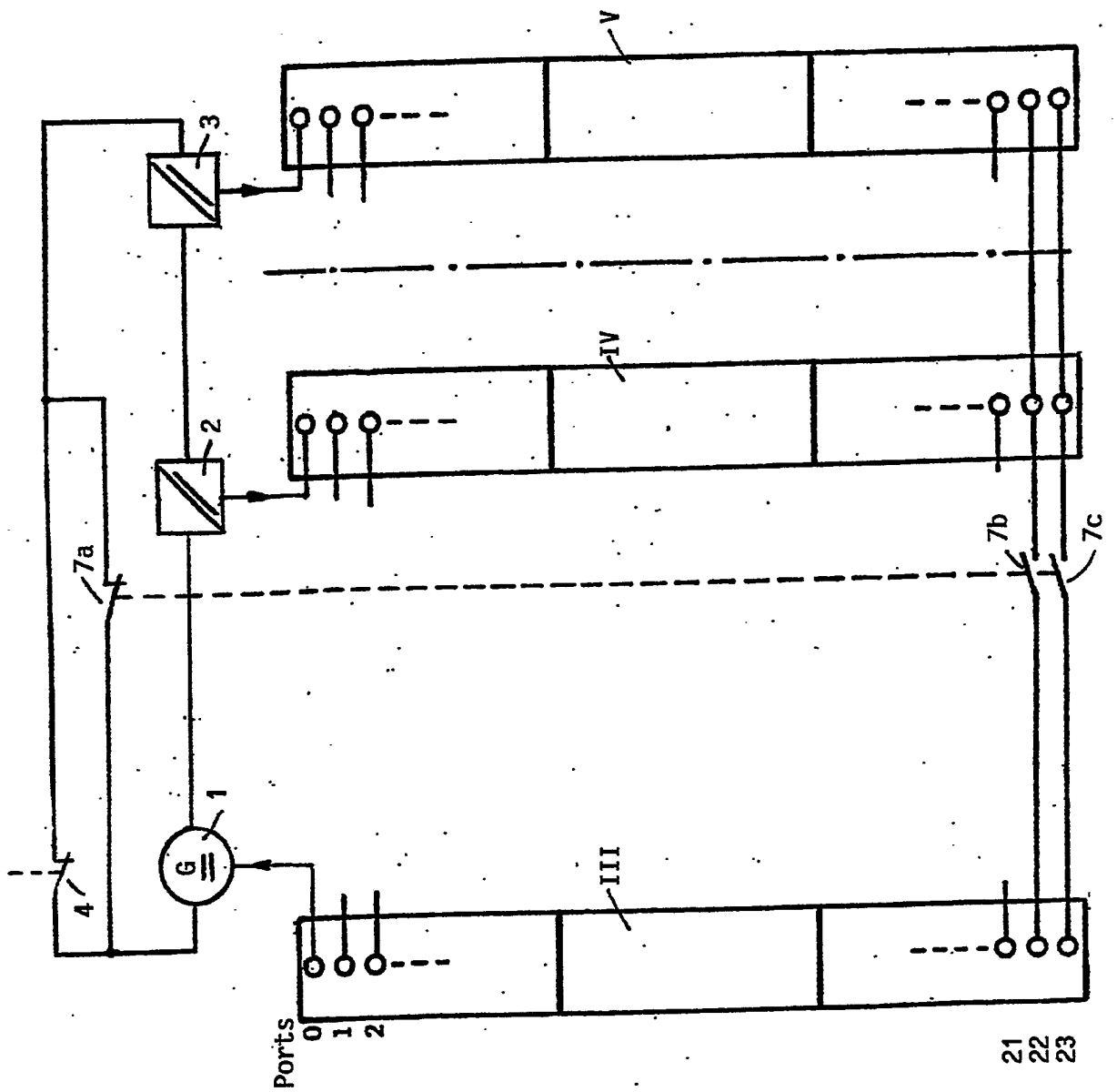


Fig. 2