(19) Republik Österreich Patentamt

(11) Nummer: AT 402 909 B

(12) PATENTSCHRIFT

(21) Anmeldenummer: 578/93

(22) Anmeldetag: 23. 3.1993

(42) Beginn der Patentdauer: 15. 2.1997

(45) Ausgabetag: 25. 9.1997

(51) Int.Cl.[6] : B61L 25/08
G06F 11/00

(30) Priorität:

30. 4.1992 CH 1399/92 beansprucht.

(56) Entgegenhaltungen:

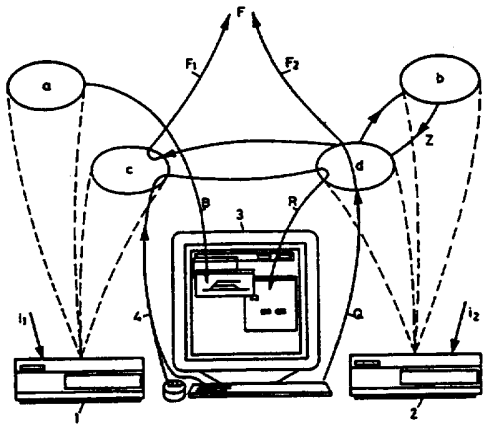
HALFPAP, H. ET AL.: SAFE L 90. SIGNAL + DRAHT 77(1985), HEFT 4, S. 67-72
GB 2149540A DE 3522418C2 DE 3127363A1 DE 3137450C2
DE 3211265C2 DE 3938501A1

(73) Patentinhaber:

SIEMENS INTEGRA VERKEHRSTECHNIK AG
CH-8304 WALLISELLEN (CH).

(54) VERFAHREN ZUR GEWÄHRLEISTUNG DER SIGNALTECHNISCHEN SICHERHEIT DER BENUTZEROBERFLÄCHE EINER DATENVERARBEITUNGSANLAGE

(57) Die signaltechnische Sicherheit wird durch einen Bildaufbau durch einen ersten Rechner (1) und eine Ueberprüfung des **Elementzustands** durch einen zweiten Rechner (2) gewährleistet. Der erste Rechner (1) bekommt eine externe Information (i_1), aus der er das anzuzeigende Bild (B) aufbaut, das an ein X-Terminal (3) ausgegeben wird. Das angezeigte Bild (B) ist im Grundzustand nicht sicher. Der zweite Rechner (2) bekommt eine externe Information (i_2), aus der er ein Prozessabbild für die Sicherheitsprüfung bildet. Diese Verfahrensschritte können simultan durchgeführt werden. Dann verarbeitet der erste Rechner (1) Befehle (4), die von einer Maus oder der Tastatur eingeleitet werden, und der zweite Rechner (2) überprüft den Zustand aller Elemente, die einen Einfluss auf die Zulässigkeit des kritischen Befehls haben könnten, mit seinem eigenen Prozessabbild (Z). Für alle Elemente, die einen Zustand einnehmen, der zu einer gefährlichen Handlung des Fahrdienstleiters führen könnte, generiert der zweite Rechner (2) eine Rückfrage (R) in Textform und verlangt eine Quittierung (Q).



AT 402 909 B

Die vorliegende Erfindung betrifft ein Verfahren zur Gewährleistung der signaltechnischen Sicherheit der Benutzeroberfläche einer Datenverarbeitungsanlage gemäss dem Oberbegriff des Patentanspruchs 1.

In den heute eingesetzten Anzeigen für die signaltechnischsichere Darstellung des Prozessabbilds von Eisenbahnanlagen werden die Farbsichtgeräte zweikanalig von zwei verschiedenen Rechnern angesteuert, um für den Prozesszustand eine Anzeige mit signaltechnischer Sicherheit zu gewährleisten. Bierbei wird speziell für diesen Zweck entwickelte Hard- und Software verwendet. Häufig wird ein spezieller Bildschirm-Controller verwendet. Dieser beinhaltet zwei Bildspeicher, welche je von einem separaten Rechner beschickt werden. Die Anzeige wird im Sekundentakt zwischen den beiden Bildspeichern umgeschaltet. Dadurch entsteht auf der Anzeige ein Blinken im Sekundenrhythmus, falls die beiden Bildspeicher nicht den gleichen Inhalt haben.

Solchermassen realisierte Anzeigen weisen zwar eine dauernde signaltechnische Sicherheit auf. Es handelt sich hierbei jedoch um Spezialentwicklungen. Dadurch wird die Verwendung von normierten grafischen Oberflächen mit einer vollgrafischen Anzeige verunmöglicht.

Ein Verfahren, das die vorhergehend beschriebenen Probleme und Nachteile aufweist, ist aus der Druckschrift "Signal + Draht, Heft 4, 1985, S. 67 bis 72, bekannt. Insbesondere ist dabei die Tatsache als nachteilig zu werten, dass solche Speziallösungen sehr teure Lösungen darstellen.

Ein spezielles Verfahren zur technischen Realisierung eines sicheren Rechners, jedoch unter Verwendung spezieller Prüfsummen, ist in der GB-PS-2 149 540 beschrieben.

Weiters ist aus der DE-C2-35 22 418 eine Einrichtung zur Gleisfreimeldung im Bereich eines Stellwerks bekannt, welche jedoch mit einem Gleisstrom-Kreissender und einem oder mehreren Gleisstrom-Kreisempfängern arbeitet.

Weiters ist aus der DE-A1-31 27 363 ein rechnergesteuertes Stellwerk bekannt, das jedoch unter Verwendung sicherer Rechner arbeitet.

Weiters ist aus der DE-C2-31 37 450 eine Sicherheits-Ausgabeschaltung für eine Datenverarbeitungsanlage bekannt, die jedoch nicht unter Verwendung von Standard-Hardware, sondern mit einer speziellen Taktversorgung arbeitet.

Weiters ist aus der DE-C2-32 11 265 ein zweikanaliges Fail Safe-Mikro-Computerschaltwerk für Eisenbahnsicherungsanlagen bekannt, das jedoch mit Mikrocomputern arbeitet, die in zwei Kanälen dieselben Informationen verarbeiten.

Schliesslich ist aus der DE-A1-39 38 501 ein Verfahren zu Betrieb eines mehrkanaligen Fail Safe-Rechner-Systems bekannt, bei dem jedoch Daten, die auf zwei mit der gleichen Software arbeitenden Kanäle erzeugt werden, mit Hilfe einer speziellen Hardware auf Übereinstimmung geprüft werden.

Für die Realisierung normierter grafischer Oberflächen auf vollgrafischen Bildschirmen wird heute häufig die X-Window-Technik eingesetzt. Die Anzeige erfolgt hierbei durch ein X-Terminal oder eine Datenverarbeitungsanlage mit entsprechender Funktionalität. Bei einem solchen X-Terminal als Anzeige lässt sich jedoch das bewährte Konzept nicht mehr in der bisherigen Form realisieren. Es stellen sich folgende Probleme:

Die Hard- und Software im X-Terminal weist eine gewisse Komplexität auf. Sie kann nicht als fehlerfrei im Sinne von signaltechnischer Sicherheit gewertet werden. Die Ausführung nur mit einem Prozessor im Terminal und die Ansteuerung des Terminals von 2 Rechnern erreicht daher nicht die gleiche Wirkung wie bei den bekannten Systemen, weil damit die signaltechnische Sicherheit nur bis zum Eingang des X-Terminals gewährleistet wird. Eine Verdoppelung des X-Terminal-Prozessors wäre technisch schwierig zu realisieren. Insbesondere aber stellt sich das Problem, dass hierbei wieder eine nicht genormte Speziallösung entwickelt werden müsste. Dies wäre aufgrund der steigenden Komplexität moderner Technologie sehr aufwendig. Bei grafischen Oberflächen erfolgt die Bedienung nicht nur über die Tastatur, sondern auch über ein Zeigegerät. Die Position des Zeigegeräts wird auf dem Bildschirm durch einen Zeiger dargestellt. Bei jeder Bewegung des Zeigegeräts muss die Position des Zeigers auf dem Bildschirm sofort nachgeführt werden. Bei einem zyklischen Umschalten der Anzeige zwischen zwei Kanälen müssten die beiden Kanäle auf sehr aufwendige Art synchronisiert werden, damit der Zeiger bei den regelmässigen Umschaltungen auch während einer Bewegung des Zeigegeräts keine die Bedienung störenden Sprünge vollführt.

Der Erfindung liegt demgemäß die Aufgabe zugrunde, ein Verfahren gemäß dem Oberbegriff des Anspruchs 1 derart weiterzubilden, daß die signaltechnische Sicherheit mit möglichst geringem Aufwand erzielbar ist.

Diese Aufgabe wird erfindungsgemäß mit den im Kennzeichnungsteil des Anspruchs 1 angegebenen Verfahrensschritten gelöst.

Die angegebenen Verfahrensschritte ermöglichen es, zwei Standardrechner zu verwenden, die entsprechend preiswert sind. Darüber hinaus wird keine aufwendige Datenkopplungsvorrichtung für diese beiden Rechner benötigt. Somit entstehen bei der Durchführung des erfindinngsgemäßen Verfahrens wesentlich

geringere Kosten als bei dem bekannten Verfahren.

Weitere vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Die Erfindung wird nun beispielsweise anhand einer Zeichnung näher beschrieben. Es zeigt:

Fig. 1 eine schematische Darstellung zur Erläuterung der Ueberprüfung des Elementzustands durch den zweiten Rechner gemäss einer ersten Variante des erfindungsgemässen Verfahrens, und

Fig. 2 eine schematische Darstellung zur Erläuterung der Anzeigesicherung durch Rücklesen des Bildes gemäss einer weiteren Variante des erfindungsgemässen Verfahrens.

Gemäss einer ersten Variante des Verfahrens nach der vorliegenden Erfindung wird die signaltechnische Sicherheit durch einen Bildaufbau durch einen ersten Rechner 1 (Fig. 1) und eine Ueberprüfung des Elementzustands durch einen zweiten Rechner 2 gewährleistet. Der erste Rechner 1 bekommt eine externe Information i_1, aus der er in eine ersten Verfahrensschritt (a) das anzuzeigende Bild B aufbaut, das an ein X-Terminal 3 ausgegeben wird. Das angezeigte Bild B ist im Grundzustand nicht sicher. Der zweite Rechner 2 bekommt eine externe Information i_2, aus der er in einem zweiten Verfahrensschritt (b) ein Prozessabbild für die Sicherheitsprüfung bildet. Die Verfahrensschritte (a) und (b) können simultan durchgeführt werden. In einem dritten Verfahrensschritt (c) verarbeitet der Rechner 1 Befehle 4, die von einer Maus oder der Tastatur eingeleitet werden.

In einem vierten Verfahrensschritt (d) überprüft der Rechner 2 den Zustand aller Elemente, die einen Einfluss auf die Zulässigkeit eines kritischen Befehls haben könnten, mit seinem eigenen Prozessabbild Z. Für alle Elemente, die einen Zustand einnehmen, der zu einer gefährlichen Handlung des Fahrdienstleiters führen könnte, generiert der Rechner 2 eine Rückfrage R in Textform und verlangt eine Quittierung Q. Der Befehl F, der an das Stellwerk übertragen wird, besteht bei kritischen Bedienungen aus zwei Teilbefehlen F1 und F2. Die zwei Teilbefehle F1 und F2 werden von beiden Rechnern 1 bzw. 2 nur abgesetzt, wenn der Fahrdienstleiter die Rückfragen R vom Rechner 2 positiv quittiert (Q). Bei nichtkritischen Bedienungen genügt ein Teilbefehl, das heisst, F kann dann gleich F1 oder F2 sein. Die Quittierung Q kann über die X-Terminal-Tastatur und/oder Zeigegerät (Maus) oder über eine separate, direkt am Rechner 2 angeschlossene Kommandofreigabe-Taste erfolgen.

Beispiel

Eine Einfahrt kann wegen einer Stellwerkstörung nicht gestellt werden. Wird nun das Hilfssignal verwendet, so muss sich der Fahrdienstleiter auf gewisse Informationen auf der Anzeige verlassen können.

Hilfssignalfahrten müssten mit Start- und Ziel-Angabe eingestellt werden. So ist es dem Rechner 2 möglich, festzustellen, dass der Zug z.B. über eine falsch gestellte Weiche oder eine belegte Isolierung fahren soll. Rechner 2 fragt auch in diesem Fall zurück und verlangt eine Quittierung. Solche Hilfssignale entsprechen im wesentlichen den in anderen Systemen verwendeten sogenannten Ersatzsignalen.

Dieses Verfahren könnte die Sicherheit generell verbessern und evtl. auch mit einer in die Benützerführung des Leitsystems integrierten Verwendung von Checklisten kombiniert werden. Für sich alleine eingesetzt stellt sich bei diese Verfahren das grundsätzliche Problem, dass das System immer darüber informiert sein muss, wenn der Fahrdienstleiter eine Entscheidung gestützt auf die Anzeige trifft, welche bei fehlerhafter Anzeige eine Gefährdung bewirken kann, weil keine Überprüfung durch die Stellwerklogik möglich ist.

In weiterer Ausgestaltung dieses Verfahrens wird die Sicherheit durch ein Rücklesen des Bildes zyklisch oder in vorbestimmten Zeitpunkten gewährleistet. Ein erster Rechner 1 (Fig. 2) bekommt eine externe Information i_1, aus der er in einem ersten Verfahrensschritt (a) das anzuzeigende Bild B aufbaut, das an ein X-Terminal 3 ausgegeben wird. Ein zweiter Rechner 2 bekommt ebenfalls eine externe Information i_2, aus der er in einem zweiten Verfahrensschritt (b) das entsprechende Prozessabbild Z aufbaut. In einem dritten Verfahrensschritt (c) fragt der Rechner 2 zyklisch und zusätzlich in bestimmten Situationen, z.B. bei einer Aenderung der entsprechenden Prozessinformationen im Prozessabbild des zweiten Rechners das Bild im X-Terminal ab, indem im Rechner 2 verglichen wird, ob die Informationen im Bild B mit dem Prozessabbild Z übereinstimmen, wobei bei korrekter Anzeige ein Meldezeichen M angezeigt wird. Eine Aenderung der entsprechenden Prozessinformationen kann beispielsweise durch eine lokale Bedienung einer fernbedienbaren Station stattfinden.

Bei dieser Variante sind folgende Einschränkungen zu beachten:

Das Abfragen vollgrafischer Bilder belastet die Datenverarbeitungsanlage stark und kann daher abhängig von der Anzahl der Arbeitsplätze nicht beliebig durchgeführt werden.

Je nach Ausstattung des X-Terminals wird das Bild direkt aus dem Bildspeicher oder aus einem dem Bildspeicher vorgelagerten Speicher zurückgelesen. Das Verhalten muss entsprechend berücksichtigt werden.

Das Zurücklesen des Fensterinhaltes aus dem Bildspeicher stellt dann gewisse Probleme für den Bildvergleich, wenn das entsprechende Fenster ganz oder teilweise überdeckt ist. In diesem Fall kann der Bildvergleich nur für die sichtbaren Ausschnitte durchgeführt werden.

Im Hinblick auf die praktische Ausführung des Verfahrens zur Gewährleistung der logischen Zweikanaligkeit auf einem Bedien- und Anzeigesystem ohne diversitäre Hard- und Software kann noch bemerkt werden, dass die Informationen über die beiden logischen Kanäle auf einem Anzeigesystem unterschiedich dargestellt werden können, z.B. über einen logischen Kanal grafisch und über den zweiten logischen Kanal in Textform, wobei der Bediener Unterschiede zwischen der Anzeige der Informationen und dem tatsächlichen Prozesszustand durch den Vergleich der über zwei logische Kanäle angezeigten Informationen feststellen und nach entsprechender Prüfung dieser Unterschiede durch Bedienungshandlungen "quittieren" kann. Die Datenverarbeitungsanlage kann aufgrund der eingeleiteten Bedienungshandlung feststellen, welchen Prozesszustand die für die Bedienungshandlung relevanten Prozessinformationen haben sollten, um auf dem zweiten logischen Kanal nur davon abweichende Prozessinformationen anzuzeigen, wobei es auch möglich ist, auf dem zweiten logischen Kanal lediglich die Prozessinformationen betreffend die eingeleitete Bedienungshandlung anzuzeigen.

Im Hinblick auf die praktische Ausführung des Verfahrens für Handlungen ohne Bedienung am Bediensystem werden die benötigten Informationen auf der Anzeige des einen logischen Kanals nicht spontan, sondern nur aufgrund der Aenderung einer entsprechenden Prozessinformation im zweiten Prozessabbild geprüft.

Bei einem Prozessabbild, das die logische Abbildung von Zuständen der Anlage darstellt, können die Zustände sowohl Weichenstellungen, Signalbegriffe, Gleisbelegungen oder andere reelle Zustände als auch rein logische interne Zustände, wie Sperrzustände oder Fahrstrassen, sein.

Dabei kann die Kontrolle von Informationen auf der Anzeige durchgeführt werden durch gezieltes Rücklesen von Bildspeicherteilen oder generelles Rücklesen des ganzen Bildspeichers und anschliessenden Vergleich der Informationen mit einem zweiten Prozessabbild.

Anstelle des Rücklesens des Bildspeichers ist auch ein Rücklesen eines dem Bildspeicher vorgelagerten Speichers mit Vergleich und anschliessendem Kopieren des dem Bildspeicher vorgelagerten Speichers in den Bildspeicher möglich unter der Bedingung, dass das korrekte Kopieren des dem Bildspeicher vorgelagerten Speichers in den Bildspeicher auf der Anzeige kontrolliert werden kann.

Da bei vollgrafischen Anzeigen fehlerhafte Anzeigen von Informationen bestehend aus einer grösseren Anzahl von Bildpunkten, welche der Benutzer nicht als fehlerhaft erkennen kann, sehr unwahrscheinlich sind, ist für die Informationskontrolle beim Rücklesen einer Information nicht notwendig, sämtliche betroffenen Bildpunkte zu berücksichtigen, sondern es genügt eine systematisch oder zufällig gebildete Auswahl davon.

Aufgrund der verwendeten unterschiedlichen Funktionen, und zwar auch bei Verwendung von Standard-Hardware und Software ohne Anspruch auf signaltechnische Sicherheit, kann für die Sicherungsmassnahmen bei den über die beiden Kanäle ausgeführten Operationen eine funktionale Softwarediversität angenommen werden.

Patentansprüche

1. Verfahren zur Gewährleistung der signaltechnischen Sicherheit der Benutzeroberfläche einer Datenverarbeitungsanlage mit Hilfe von zwei eigenständigen Rechnern der Datenverarbeitungsanlage, wobei ein Prozessabbild auf der Benutzeroberfläche über ein Anzeigesystem dargestellt wird und wobei Benutzerbefehle zur Einflussnahme auf den Prozess über eine Bedienungseinrichtung eingebbar sind, **dadurch gekennzeichnet**, dass

   a) dem ersten Rechner (1) eine erste externe Information (i_1) zugeführt wird, aus der dieser ein dem Zustand des Prozesses entsprechendes Bild (B) erzeugt und auf dem Anzeigesystem (3) darstellt,

   b) dem zweiten Rechner (2) eine zweite externe Information (i_2) zugeführt wird, aus der dieser ein für eine Sicherheitsprüfung relevantes zweites Prozessabbild (Z) erzeugt,

   c) der zweite Rechner (2) bei Eingabe von Benutzerbefehlen diese durch Vergleich mit dem für die Sicherheitsprüfung relevanten zweiten Prozessabbild (Z) auf ihre Zulässigkeit prüft, und dass

   d) der zweite Rechner (2) dann, wenn keine Benutzerbefehle vorliegen, das vom ersten Rechner (1) auf dem Anzeigesystem (3) dargestellte, dem Prozess entsprechende Bild (B) mit dem zweiten Prozessabbild (Z) in vorbestimmten Zeitabständen vergleicht und verifiziert.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die vorbestimmten Zeitabstände zyklisch oder nach einer Änderung der entsprechenden Prozessinformationen im Prozessabbild (Z) des zweiten

Rechners (2) gewählt werden.

3. Verfahren nach Anspruch 1, zur Gewährleistung der logischen Zweikanaligkeit auf einem Bedien- und Anzeigesystem (3) ohne diversitäre Hard- und Software, **dadurch gekennzeichnet**, dass die Informationen über zwei logische Kanäle auf einem Anzeigesystem (3) unterschiedlich dargestellt werden.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet**, dass auf dem zweiten logischen Kanal lediglich die Prozessinformationen betreffend eine eingeleitete Bedienungshandlung angezeigt werden.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, dass die Datenverarbeitungsanlage aufgrund der eingeleiteten Bedienungshandlung feststellt, welchen Prozesszustand die für die Bedienungshandlung relevanten Prozessinformationen haben sollten, und dass auf dem zweiten logischen Kanal nur davon abweichende Prozessinformationen angezeigt werden.

6. Verfahren nach Anspruch 2, **dadurch gekennzeichnet**, dass die für Handlungen ohne Bedienung am Bediensystem benötigten Informationen auf der Anzeige eines logischen Kanals dann gezielt von der Datenverarbeitungsanlage automatisch kontrolliert werden, wenn sich die entsprechende Prozessinformation im zweiten Prozessabbild (Z) ändert.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet**, dass die Kontrolle von Informationen auf der Anzeige durch gezieltes Rücklesen von Bildspeicherteilen oder generelles Rücklesen des ganzen Bildspeichers und anschliessenden Vergleich der Informationen mit einem zweiten Prozessabbild (Z) oder durch Rücklesen eines dem Bildspeicher vorgelagerten Speichers mit Vergleich und anschliessendem Kopieren des dem Bildspeicher vorgelagerten Speichers in den Bildspeicher durchgeführt wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet**, dass für die Informationskontrolle beim Rücklesen einer Information nur eine systematisch oder zufällig gebildete Auswahl der betroffenen Bildpunkte verwendet wird und nicht sämtliche betroffenen Bildpunkte berücksichtigt werden.

Hiezu 1 Blatt Zeichnungen

ÖSTERREICHISCHES PATENTAMT
Ausgegeben 25. 9.1997
Blatt 1

Patentschrift Nr. AT 402 909 B
Int. Cl.[6] : B61L 25/08
G06F 11/00

Fig.1

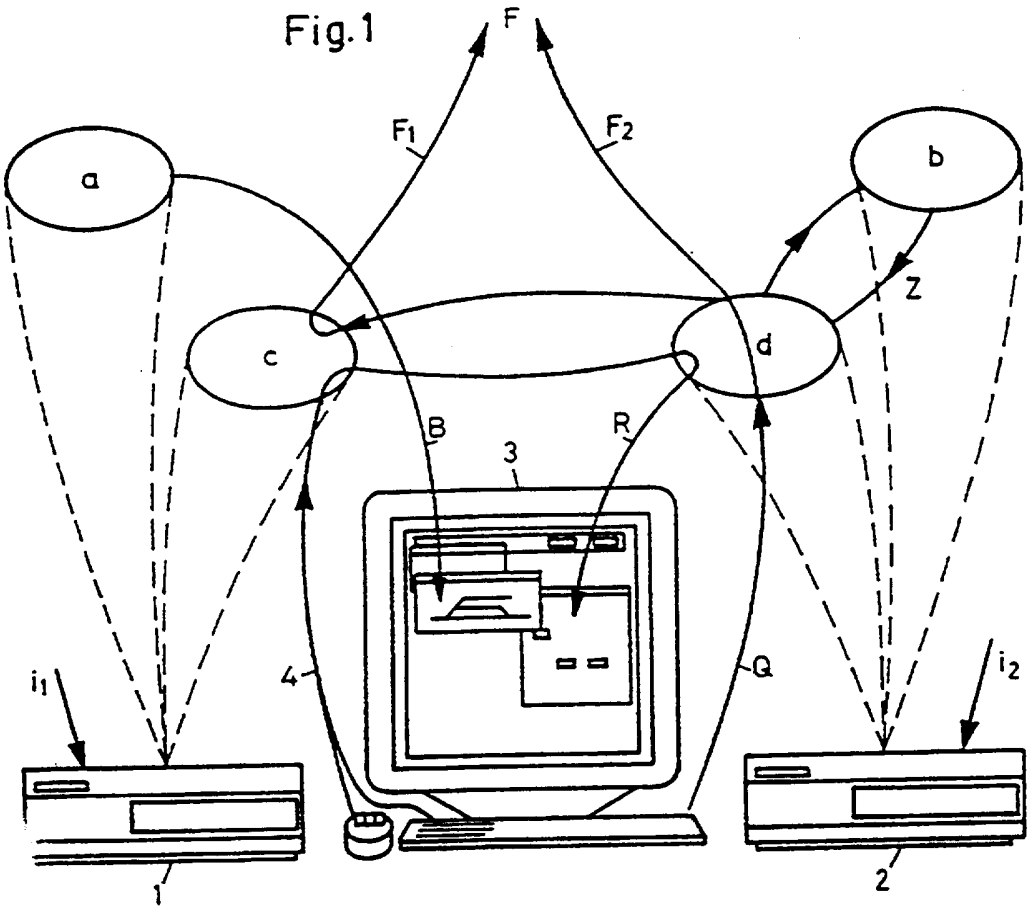


Fig. 2