(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 199 40 874 B4** 2007.05.03

(12) **Patentschrift**

(21) Aktenzeichen: **199 40 874.2**
(22) Anmeldetag: **27.08.1999**
(43) Offenlegungstag: **08.03.2001**
(45) Veröffentlichungstag
der Patenterteilung: **03.05.2007**

(51) Int Cl.[8]: ***H04L 12/40*** (2006.01)
G06F 11/00 (2006.01)
G05B 9/02 (2006.01)

(66) Innere Priorität:
199 39 919.0 23.08.1999

(73) Patentinhaber:
Pilz GmbH & Co. KG, 73760 Ostfildern, DE

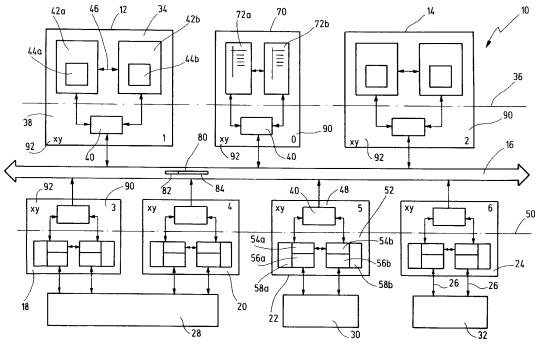
(74) Vertreter:
Witte, Weller & Partner, 70178 Stuttgart

(72) Erfinder:
Rupp, Roland, 73110 Hattenhofen, DE; Wohnhaas, Klaus, 70736 Fellbach, DE; Schwenkel, Hans, 70192 Stuttgart, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 197 13 240 C2
DE 197 42 716 A1
DE 197 33 906 A1
US 56 89 675 A

(54) Bezeichnung: **Verfahren zum Konfigurieren eines sicheren Busteilnehmers und sicheres Steuerungssystem mit einem solchen**

(57) Hauptanspruch: Verfahren zum Konfigurieren eines sicheren Busteilnehmers (12, 14, 18–24) beim Anschließen an einen Feldbus (16) in einem sicheren Steuerungssystem (10), wobei dem sicheren Busteilnehmer (12, 14, 18–24) eine definierte Teilnehmeradresse (90) zugeordnet wird, mit den Schritten:
– Versenden eines ersten Anmeldetelegramms (114) von dem sicheren Busteilnehmer (12, 14, 18–24) zu einer an den Feldbus (16) angeschlossenen Verwaltungseinheit (70), wobei das erste Anmeldetelegramm (114) eine festgelegte Universaladresse (92) beinhaltet,
– Versenden eines Adreßvergabetelegramms (118) von der Verwaltungseinheit (70) an den sicheren Busteilnehmer (12, 14, 18–24), wobei das Adreßvergabetelegramm (118) die definierte Teilnehmeradresse (90) beinhaltet und
– Abspeichern der definierten Teilnehmeradresse (90) in einem Speicher (58; 120) des sicheren Busteilnehmers,
– wobei die Anwesenheit aller aktiv an den Feldbus (16) angeschlossenen Busteilnehmer (12, 14, 18–24) anhand einer Sollkonfiguration von Busteilnehmern (12, 14, 18–24) sowie anhand von Antworttelegrammen (104) der Busteilnehmer (12, 14, 18–24) überprüft wird,...



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Konfigurieren eines sicheren Busteilnehmers beim Anschließen an einen Feldbus in einem sicheren Steuerungssystem, wobei dem sicheren Busteilnehmer eine definierte Teilnehmeradresse zugeordnet wird.

[0002] Die Erfindung betrifft darüber hinaus auch ein Steuerungssystem zum sicheren Steuern von sicherheitskritischen Prozessen, mit zumindest einem sicheren Busteilnehmer, der an einen Feldbus angeschlossen ist, wobei der sichere Busteilnehmer erste Mittel zum Aufnehmen und Auswerten eines Bustelegramms sowie einen Speicher zum Speichern einer dem Busteilnehmer zugeordneten Teilnehmeradresse aufweist.

[0003] Bei einem Feldbus handelt es sich um ein System zur Datenkommunikation, bei dem die angeschlossenen Busteilnehmer über eine Sammelleitung miteinander verbunden sind. Daher können zwei an den Feldbus angeschlossene Busteilnehmer miteinander kommunizieren, ohne individuell direkt miteinander verkabelt zu sein. Beispiele für bekannte Feldbusse sind der sogenannte CAN-Bus, der sogenannte Profibus und der sogenannte Interbus.

[0004] Im Bereich der Steuer- und Automatisierungstechnik ist die Verwendung von Feldbussen bereits seit längerem hinreichend bekannt. Dies gilt jedoch nicht für die Steuerung von sicherheitskritischen Prozessen, bei denen in der Praxis bis in die jüngste Vergangenheit hinein die an der Steuerung beteiligten Einheiten individuell miteinander verkabelt wurden. Grund hierfür ist, daß die bekannten Feldbusse die zur Steuerung von sicherheitskritischen Prozessen erforderliche Fehlersicherheit (Fehlerwahrscheinlichkeit kleiner als 10^{-11}) nicht gewährleisten konnten. Zwar besitzen alle bekannten Feldbusse Maßnahmen zur Fehlersicherung bei der Datenübertragung, diese Maßnahmen sind jedoch nicht ausreichend, um die geforderte Fehlersicherheit zu gewährleisten. Hinzu kommt, daß Feldbusse offene Systeme sind, an die grundsätzlich beliebige Einheiten angeschlossen werden können. Dabei besteht die Gefahr, daß eine Einheit, die mit einem zu steuernden sicherheitskritischen Prozeß gar nichts zu tun hat, diesen ungewollt beeinflußt.

[0005] Unter einem sicherheitskritischen Prozeß wird hier ein Prozeß verstanden, von dem bei Auftreten eines Fehlers eine nicht akzeptable Gefahr für Menschen oder materielle Güter ausgeht. Bei einem sicherheitskritischen Prozeß muß daher mit im Idealfall 100%iger Sicherheit gewährleistet sein, daß der Prozeß bei Auftreten eines Fehlers in einen sicheren Zustand überführt wird. Dies kann bei einer Maschinenanlage beinhalten, daß die Anlage abgeschaltet wird. Bei einem chemischen Produktionsprozeß könnte ein Abschalten jedoch unter Umständen eine unkontrollierte Reaktion hervorrufen, so daß in einem solchen Fall der Prozeß besser in einen unkritischen Parameterbereich gefahren wird.

[0006] Sicherheitskritische Prozesse können auch Teilprozesse von größeren, übergeordneten Gesamtprozessen sein. Bei einer hydraulischen Presse kann bspw. die Materialzuführung ein nicht-sicherheitskritischer Teilprozeß, das Inbetriebnehmen des Preßwerkzeugs dagegen ein sicherheitskritischer Teilprozeß sein. Weitere Beispiele für sicherheitskritische (Teil-)Prozesse sind die Überwachung von Schutzgittern, Schutztüren oder Lichtschranken, die Steuerung von Zwei-Hand-Schaltern oder die Überwachung und Auswertung eines Not-Aus-Schalters.

[0007] Die an der Steuerung eines sicherheitskritischen Prozesses beteiligten Einheiten müssen über ihre eigentliche Funktion hinausgehende, sicherheitsbezogene Einrichtungen aufweisen, um von den zuständigen Aufsichtsbehörden für sicherheitskritische Aufgaben zugelassen zu werden. Diese Einrichtungen dienen vor allem der Fehler- und Funktionsüberwachung. In der Regel sind die beteiligten Einheiten redundant aufgebaut, um eine sichere Funktion auch bei Auftreten eines Fehlers zu gewährleisten. Einheiten mit derartigen sicherheitsbezogenen Einrichtungen werden nachfolgend im Unterschied zu "normalen" Einheiten als sicher bezeichnet.

[0008] Die an den Feldbus angeschlossenen Einheiten werden nachfolgend allgemein als Busteilnehmer bezeichnet. Bei einem Steuerungssystem zum sicheren Steuern von sicherheitskritischen Prozessen handelt es sich bei den Busteilnehmern üblicherweise entweder um Steuerungseinheiten oder um Signaleinheiten. Als Steuerungseinheit wird dabei ein Busteilnehmer bezeichnet, der eine gewisse Intelligenz zur Steuerung eines Prozesses besitzt. In der Fachterminologie werden derartige Busteilnehmer üblicherweise als Clients bezeichnet. Sie erhalten Daten und/oder Signale, die Zustandsgrößen der gesteuerten Prozesse repräsentieren, und aktivieren in Abhängigkeit von diesen Informationen Aktoren, die den zu steuernden Prozeß beeinflussen. Üblicherweise ist die Intelligenz in Form eines veränderbaren Anwenderprogramms in einem Speicher der Steuerungseinheiten abgelegt. In der Regel werden als Steuerungseinheiten sogenannte SPS (Speicher Programmierbare Steuerungen) verwendet.

[0009] Eine Signaleinheit ist demgegenüber ein Busteilnehmer, der im wesentlichen Ein- und Ausgangskanäle (E/A-Kanäle) bereitstellt, an die einerseits Sensoren zur Aufnahme von Prozeßgrößen und andererseits Aktoren angeschlossen werden können. Die Signaleinheiten besitzen in der Regel keine

Intelligenz in Form eines veränderbaren Anwenderprogramms. Sie werden in der Fachterminologie üblicherweise als Server bezeichnet.

[0010] Bei vielen Feldbussen, wie etwa dem CAN-Bus, ist es bekannt, den einzelnen Busteilnehmern eine individuelle Teilnehmeradresse zuzuordnen. Die Teilnehmeradresse dient dazu, Bustelegramme mit zu übertragenden Nachrichten gezielt von dem sendenden Busteilnehmer zu dem empfangenden Busteilnehmer zu übermitteln. Beim Aufbau eines Steuerungssystems zum Steuern von sicherheitskritischen Prozessen stellt die Vergabe der Teilnehmeradressen an die Busteilnehmer eine sicherheitskritische Maßnahme dar. Wenn nämlich bspw. zwei verschiedene Signaleinheiten die Zustandsdaten von zwei verschiedenen Schutzgittern aufnehmen und an die Steuerungseinheit weitergeben, kann eine falsche Adreßzuordnung der beiden Signaleinheiten dazu führen, daß die Steuerungseinheit die Bewegung einer abzusichernden Maschine nicht abschaltet, obwohl das entsprechende Schutzgitter geöffnet wurde.

[0011] Bei den bisher bekannten, gattungsgemäßen Steuerungssystemen bzw. den entsprechenden Verfahren zum Konfigurieren der sicheren Busteilnehmer werden die Teilnehmeradressen direkt am Busteilnehmer eingestellt. Hierzu weist jeder Busteilnehmer entweder einen mechanischen Codierschalter, insbesondere einen Drehschalter, oder eine serielle Programmierschnittstelle auf. Ein Nachteil dieser Lösung ist, daß das Einstellen der Teilnehmeradressen hier direkt am Ort des einzelnen Busteilnehmers erfolgen muß. Bei komplexen Prozeßsteuerungen im industriellen Bereich können die einzelnen an den Feldbus angeschlossenen Busteilnehmer jedoch bis zu mehreren hundert Metern auseinanderliegen. Beim Aufbau eines sicheren Steuerungssystems sind in diesem Fall daher große Laufwege erforderlich, die das Einrichten und Konfigurieren umständlich machen.

[0012] Hinzu kommt, daß es aufgrund der großen Laufwege in diesem Fall leicht möglich ist, den Überblick zu verlieren, was zu fehlerhaften Adreßzuordnungen führen kann. Ein weiterer wesentlicher Nachteil der bekannten Lösungen ist, daß beim Austausch eines defekten Busteilnehmers dessen Teilnehmeradresse bekannt sein muß, damit diese anschließend dem Austausch-Busteilnehmer zugeordnet werden kann. Bei industriellen Anlagen, die häufig rund um die Uhr betrieben werden, bedeutet dies, daß immer entsprechend fachkundiges Personal verfügbar sein muß, um den Austausch eines defekten Busteilnehmers vorzunehmen. In dem Fall, daß dem Busteilnehmer die Teilnehmeradresse mit Hilfe eines Programmiergerätes über die serielle Schnittstelle zugeordnet wird, ist auch stets das entsprechende Programmiergerät erforderlich.

[0013] Bei der Zuordnung einer Teilnehmeradresse über eine Programmierschnittstelle besteht darüber hinaus der Nachteil, daß die dem Busteilnehmer zugeordnete Teilnehmeradresse von außen nicht zu erkennen ist. Hierdurch besteht die Gefahr, daß ein Busteilnehmer, der früher einmal mit einer anderen Teilnehmeradresse verwendet wurde, bei seiner Verwendung in einer neuen Umgebung versehentlich mit seiner alten Teilnehmeradresse betrieben wird. Dieses Risiko ist besonders groß, wenn ein schon einmal verwendeter Busteilnehmer im Rahmen einer Wartung in ein anderes Steuerungssystem integriert werden soll.

Stand der Technik

[0014] Aus DE 197 13 240 C2 ist ein Verfahren zur automatischen Adreßvergabe in einem CAN-Bussystem bekannt. Um die Einstellung von Teilnehmeradressen mit Hilfe von Hardwareschaltern zu vermeiden, wird vorgeschlagen, bei jedem Busteilnehmer, der noch keine zugeordnete Adresse besitzt, eine vorläufige Adresse mit Hilfe eines Zufallsgenerators zu erzeugen. Der entsprechende Busteilnehmer kann sich dann mit dieser vorläufigen, zufällig erzeugten Adresse bei einer steuernden Station anmelden. Bei einer Adreßkollision wird eine neue Zufallszahl bestimmt. Andernfalls wird die vorläufige Adresse als zugeteilte Adresse weiterverwendet.

[0015] Aus DE 197 33 906 A1 ist ein Verfahren zur automatischen Adreßvergabe bekannt, bei dem jeweils der am weitesten von einer Mastereinheit entfernt angeschlossene Busteilnehmer, der noch keine zugewiesene Adresse besitzt, seine Teilnehmeradresse vom Master erhält. Der Master sendet hierzu ein sog. Tauftelegramm an den Busteilnehmer. Die jeweils näher zum Master hin angeordneten, ungetauften Busteilnehmer ignorieren die Adreßvergabe, wobei sie ihre jeweilige Position durch Mithören des Telegrammverkehrs auf dem Feldbus bestimmen können.

[0016] US 5,689,675 offenbart ein Verfahren zur Adreßvergabe, bei dem Nummern verwendet werden, die in den einzelnen Busteilnehmern vorhanden sind. Diese Nummern können entweder bei der Herstellung einprogrammiert sein, wie etwa Seriennummern, oder sie können mittels eines Zufallsgenerators erzeugt werden.

[0017] Die drei bekannten Verfahren beziehen sich nicht auf die Vergabe einer Teilnehmeradresse an einen sicheren Busteilnehmer in einem sicheren Steuerungssystem. Sie sind in der jeweils beschriebenen Ausführung auch nicht für eine Adreßvergabe an einen sicheren Busteilnehmer in einem sicheren Steuerungssystem geeignet.

[0018] Ein sicheres Steuerungssystem mit sicheren

Busteilnehmern ist aus DE 197 42 716 A1 bekannt. Eine Adreßvergabe an einen sicheren Busteilnehmer ist hier jedoch nicht beschrieben.

Aufgabenstellung

[0019] Es ist daher Aufgabe der vorliegenden Erfindung, ein Verfahren der eingangs genannten Art anzugeben, mit dem einem sicheren Busteilnehmer von einer zentralen Stelle aus auf einfache und gleichzeitig fehlersichere Art und Weise eine Teilnehmeradresse zugeordnet werden kann. Es ist darüber hinaus Aufgabe der Erfindung, ein entsprechendes Steuerungssystem anzugeben.

[0020] Diese Aufgabe wird durch ein Verfahren der eingangs genannten Art gelöst, das folgende Schritte aufweist:

– Versenden eines ersten Anmeldetelegramms von dem sicheren Busteilnehmer zu einer an den Feldbus angeschlossenen Verwaltungseinheit, wobei das erste Anmeldetelegramm eine festgelegte Universaladresse beinhaltet,
– Versenden eines Adreßvergabetelegramms von der Verwaltungseinheit an den sicheren Busteilnehmer, wobei das Adreßvergabetelegramm die definierte Teilnehmeradresse beinhaltet und
– Abspeichern der definierten Teilnehmeradresse in einem Speicher des sicheren Busteilnehmers,
– wobei die Anwesenheit aller aktiv an den Feldbus angeschlossenen Busteilnehmer anhand einer Sollkonfiguration von Busteilnehmern sowie anhand von Antworttelegrammen der Busteilnehmer überprüft wird, und
– wobei die Teilnehmeradresse eines als nicht mehr aktiv erkannten Busteilnehmers als definierte Teilnehmeradresse versendet wird.

[0021] Die Aufgabe wird des weiteren durch ein Steuerungssystem gelöst, mit einer Verwaltungseinheit und mit zumindest einem sicheren Busteilnehmer, die an einen Feldbus angeschlossenen sind, wobei der sichere Busteilnehmer erste Mittel zum Aufnehmen und Auswerten eines Bustelegramms sowie einen Speicher zum Speichern einer dem Busteilnehmer zugeordneten Teilnehmeradresse aufweist, wobei der Busteilnehmer zweite Mittel aufweist, um sich unter einer festgelegten Universaladresse bei der Verwaltungseinheit anzumelden, sowie dritte Mittel, um ein Adreßvergabetelegramm mit der Teilnehmeradresse aufzunehmen und auszuwerten, wobei die Verwaltungseinheit dazu ausgebildet ist, die Anwesenheit aller aktiv an den Feldbus angeschlossenen Busteilnehmer anhand einer Sollkonfiguration von Busteilnehmern sowie anhand von Antworttelegrammen der Busteilnehmer zu überprüfen und die Teilnehmeradresse eines als nicht mehr aktiv erkannten Busteilnehmers als definierte Teilnehmeradresse an den zumindest einen Busteilnehmer zu versenden.

[0022] Mit dem genannten Verfahren ist es möglich, den zu konfigurierenden Busteilnehmer zunächst ohne Zuordnung der individuellen Teilnehmeradresse an den Feldbus anzuschließen. Aufgrund der festgelegten Universaladresse kann sich dieser Busteilnehmer anschließend bei der genannten Verwaltungseinheit anmelden. Die Verwaltungseinheit ist bevorzugt eine zentrale Verwaltungseinheit für das gesamte Steuerungssystem. Im nächsten Schritt wird dem zu konfigurierenden Busteilnehmer von der Verwaltungseinheit die individuelle Teilnehmeradresse übermittelt. Dies geschieht mit Hilfe eines speziellen Adreßvergabetelegramms, das die Verwaltungseinheit an den zu konfigurierenden Busteilnehmer versendet. Der angesprochene Busteilnehmer wertet das empfangene Adreßvergabetelegramm aus, indem er die übermittelte Teilnehmeradresse extrahiert und anschließend in einem Speicher abspeichert. Bevorzugt speichert er die Teilnehmeradresse dabei in einem nicht-flüchtigen Speicher, wie bspw. einem EEPROM.

[0023] Mit Hilfe dieses Verfahrens ist es möglich, dem sicheren Busteilnehmer von einer zentralen Stelle aus, nämlich der Verwaltungseinheit, die definierte Teilnehmeradresse zuzuordnen. Bei einem räumlich ausgedehnten Steuerungssystem entfallen daher die bisher erforderlichen, langen Laufwege. Darüber hinaus wird durch die Möglichkeit, sämtliche Busteilnehmer von einer zentralen Stelle aus zu konfigurieren, der Überblick erleichtert und so das Fehlerrisiko einer versehentlich falschen Adreßvergabe verringert. Da zudem sowohl der sichere Busteilnehmer als auch die Verwaltungseinheit sicherheitsbezogene Einrichtungen aufweisen, kann die Übertragung der definierten Teilnehmeradresse trotz der an sich bestehenden Fehlermöglichkeiten des Bussystems auf fehlersichere Weise erfolgen.

[0024] Die Erfindung ist besonders vorteilhaft im Hinblick auf Wartungsarbeiten an einem bereits eingerichteten, sicheren Steuerungssystem. Mit der Erfindung ist es nämlich auf einfache Weise möglich, einen defekten Busteilnehmer durch einen neuen Busteilnehmer auszutauschen, ohne daß dem neuen Busteilnehmer hierbei bewußt eine Teilnehmeradresse zugeordnet werden muß. Die Verwaltungseinheit prüft nämlich, ob alle bei ihr angemeldeten Busteilnehmer aktiv am Feldbus angeschlossen sind. Fehlt ein einzelner Busteilnehmer, so deutet dies auf einen Defekt oder darauf hin, daß dieser Busteilnehmer bereits vom Feldbus abgetrennt wurde. Aufgrund der bekannten Sollkonfiguration kann die Verwaltungseinheit die Teilnehmeradresse dieses fehlenden Busteilnehmers identifizieren. Sobald sich bei der Verwaltungseinheit dann ein neuer Busteilnehmer unter der festgelegten Universaladresse anmeldet, wird diesem die Teilnehmeradresse des fehlenden Busteilnehmers zugeordnet. Auf diese Weise ist der Austausch eines defekten Busteilnehmers möglich, ohne

daß dem neuen Busteilnehmer die alte Teilnehmeradresse von Hand zugeordnet werden muß.

[0025] Besonders bevorzugt ist es dabei, wenn das definierte Wartungstelegramm nur nach Aktivieren eines besonderen Wartungsmodus der Verwaltungseinheit versendet wird. In dieser Kombination ist nämlich einerseits eine sehr große Sicherheit bezüglich der Zuordnung einer Teilnehmeradresse gegeben, während andererseits ein defekter Busteilnehmer sehr einfach und ohne Fachkenntnisse ausgetauscht werden kann. Dies ist besonders vorteilhaft im Hinblick auf Produktionsanlagen, die rund um die Uhr betrieben werden.

[0026] In einer Ausgestaltung des Verfahrens versendet der sichere Busteilnehmer nach Empfang des Adreßvergabetelegramms ein zweites Anmeldetelegramm an die Verwaltungseinheit, wobei das zweite Anmeldetelegramm die definierte Teilnehmeradresse beinhaltet.

[0027] Diese Maßnahme besitzt den Vorteil, daß die Verwaltungseinheit überprüfen kann, ob der sichere Busteilnehmer die zugeordnete Teilnehmeradresse nicht nur fehlerfrei empfangen, sondern auch fehlerfrei verarbeitet hat. Hierdurch wird die Sicherheit der Adreßzuordnung nochmals erhöht. Anschaulich gesprochen bedeutet die genannte Maßnahme, daß sich der sichere Busteilnehmer nach Erhalt der ihm zugeordneten Teilnehmeradresse ein zweites Mal bei der Verwaltungseinheit anmeldet. Die Maßnahme besitzt darüber hinaus den weiteren Vorteil, daß aus Sicht der Verwaltungseinheit die Universaladresse eindeutig wieder freigegeben ist. Somit steht sie einem anderen Busteilnehmer zur Benutzung zur Verfügung, ohne daß es zu Mehrdeutigkeiten hinsichtlich des betroffenen Busteilnehmers kommen kann.

[0028] In einer weiteren Ausgestaltung der Erfindung versendet der sichere Busteilnehmer das erste Anmeldetelegramm erst nach Empfang eines definierten Wartungstelegramms an die Verwaltungseinheit.

[0029] Diese Maßnahme besitzt den Vorteil, daß die Verwaltungseinheit stets die Kontrolle über das Geschehen am Feldbus behält. Es ist hiernach ausgeschlossen, daß sich ein neuer, zu konfigurierender Busteilnehmer von sich aus in das Geschehen am Feldbus einmischt, ohne hierzu von der Verwaltungseinheit eine Freigabe erhalten zu haben. Auch hierdurch wird die Sicherheit des Steuerungssystems verbessert, da eine zentrale Kontrolle gewährleistet ist.

[0030] In einer bevorzugten Ausgestaltung dieser Maßnahme versendet der sichere Busteilnehmer das erste Anmeldetelegramm nur nach dem erstmaligen Empfang des definierten Wartungstelegramms an die Verwaltungseinheit, während er bei einem wiederholten Empfang des definierten Wartungstelegramms das zweite Anmeldetelegramm versendet.

[0031] Diese Maßnahme besitzt den Vorteil, daß das Wartungstelegramm als sogenanntes Broadcast-Telegramm jeweils gleichzeitig an alle an den Feldbus angeschlossenen Busteilnehmer gemeinsam versendet werden kann. Hierdurch vereinfacht sich das erfindungsgemäße Verfahren, da die Anmeldung des neuen, zu konfigurierenden Busteilnehmers nicht von bereits angemeldeten und konfigurierten Busteilnehmern gestört oder verzögert wird. Es ist hierdurch auch möglich, das erfindungsgemäße Verfahren mit wesentlich weniger Verfahrensschritten durchzuführen. Der erstmalige Empfang kann sich je nach der konkreten Realisierung des erfindungsgemäßen Verfahrens auf den erstmaligen Empfang nach jedem Einschalten des Steuerungssystems beziehen. Bevorzugt bezieht er sich jedoch auf den erstmaligen Empfang nach dem Anschluß des Busteilnehmers an den Feldbus.

[0032] In einer weiteren Ausgestaltung der zuvor genannten Maßnahmen wird das definierte Wartungstelegramm nur nach Aktivieren eines besonderen Wartungsmodus der Verwaltungseinheit versendet.

[0033] Die Aktivierung des besonderen Wartungsmodus erfolgt bevorzugt durch die Betätigung eines Schlüsselschalters oder eines Codeschlosses, das mit der Verwaltungseinheit verbunden ist. Der besondere Wartungsmodus der Verwaltungseinheit unterscheidet sich von allen anderen Betriebsmodi der Verwaltungseinheit darin, daß nur in diesem Wartungsmodus das definierte Wartungstelegramm versendet wird. Die Maßnahme besitzt den Vorteil, daß die Zuordnung von Teilnehmeradressen nur nach einem bewußten Eingriff in das sichere Steuerungssystem möglich ist. Hierdurch wird eine versehentliche Vergabe von Teilnehmeradressen verhindert. Infolge dessen ist das Risiko einer falschen Zuordnung von Teilnehmeradressen beträchtlich reduziert.

[0034] In einer weiteren Ausgestaltung der zuvor genannten Maßnahme beendet die Verwaltungseinheit den besonderen Wartungsmodus automatisch nach Empfang des zweiten Anmeldetelegramms.

[0035] Auch diese Maßnahme trägt erheblich dazu bei, das Risiko einer fehlerhaften Adreßzuordnung zu minimieren, da der besondere Wartungsmodus in diesem Fall nur für jeweils eine einzige Adreßzuordnung aktiviert werden kann. Es ist hiernach also für jede Zuordnung einer Teilnehmeradresse der erneute, bewußte Eingriff in das sichere Steuerungssystem notwendig. Die Sicherheit des Systems wird hierdurch nochmals beträchtlich verbessert.

[0036] In einer weiteren Ausgestaltung der Erfin-

dung versendet die Verwaltungseinheit Wartungstelegramme in definierten Zeitabständen an alle an den Feldbus angeschlossenen Busteilnehmer.

[0037] Diese Maßnahme steht im Gegensatz dazu, daß ein Wartungstelegramm jeweils nur nach einer individuellen Aktivierung eines besonderen Wartungsmodus versendet werden kann. Die genannte Maßnahme besitzt demgegenüber den Vorteil, daß der Anschluß eines neuen Busteilnehmers im laufenden Betrieb des Steuerungssystems auf sehr einfache und komfortable Weise möglich ist. Die Teilnehmeradresse kann hierbei entweder von der Verwaltungseinheit automatisch aus einer Liste von möglichen Teilnehmeradressen ausgewählt werden oder sie kann der Verwaltungseinheit vor dem Anschließen des neuen Busteilnehmers übermittelt werden.

[0038] In einer weiteren Ausgestaltung der Erfindung erzeugt die Verwaltungseinheit ein Fehlersignal, wenn mehr als ein Busteilnehmer das erste Anmeldetelegramm versendet.

[0039] Auch diese Maßnahme besitzt den Vorteil, daß die Sicherheit erhöht wird, da in diesem Fall die gleichzeitige Zuordnung einer Teilnehmeradresse an mehrere Busteilnehmer verhindert ist.

[0040] In einer weiteren Ausgestaltung der Erfindung werden zumindest das erste Anmeldetelegramm sowie das Adreßvergabetelegramm mit jeweils einem Quittungstelegramm beantwortet.

[0041] Diese Maßnahme zielt darauf ab, daß der Empfänger der genannten Telegramme unabhängig von deren eigentlicher Verarbeitung ein Quittungstelegramm an den Absender zurückschickt. Hierdurch wird ebenfalls die Sicherheit der Adreßzuordnung beträchtlich erhöht, da der Absender auf diese Weise überprüfen kann, ob der Empfänger das jeweilige Telegramm fehlerfrei erhalten hat.

[0042] Es versteht sich, daß die vorstehend genannten und die nachstehend noch zu erläuternden Merkmale nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der vorliegenden Erfindung zu verlassen.

Ausführungsbeispiel

[0043] Ausführungsbeispiele der Erfindung sind in der Zeichnung dargestellt und werden in der nachfolgenden Beschreibung näher erläutert. Es zeigen:

[0044] Fig. 1 eine schematische Darstellung eines Steuerungssystems zum sicheren Steuern von sicherheitskritischen Prozessen,

[0045] Fig. 2 den Kommunikationsablauf zwischen einer Verwaltungseinheit und zwei Busteilnehmern bei einem ersten Ausführungsbeispiel der Erfindung und

[0046] Fig. 3 den Kommunikationsablauf zwischen der Verwaltungseinheit und den beiden Busteilnehmern bei weiteren Ausführungsbeispielen der Erfindung.

[0047] In Fig. 1 ist ein Steuerungssystem zum sicheren Steuern von sicherheitskritischen Prozessen in seiner Gesamtheit mit der Bezugsziffer **10** bezeichnet.

[0048] Das Steuerungssystem **10** besitzt zwei sichere Steuerungseinheiten **12** und **14**, die über einen Feldbus **16** mit insgesamt vier sicheren Signaleinheiten **18**, **20**, **22** und **24** verbunden sind. Die Steuerungseinheiten **12**, **14** und die Signaleinheiten **18** bis **24** sind Busteilnehmer im Sinne der vorliegenden Erfindung.

[0049] Jede der sicheren Signaleinheiten **18** bis **24** weist mehrere E/A-Kanäle auf, über die sie mit jeweils einem sicherheitskritischen Prozeß **28**, **30**, **32** verbunden ist. Im vorliegenden Fall sind die sicheren Signaleinheiten **18** und **20** mit dem Prozeß **28** verbunden, während die Signaleinheit **22** mit dem Prozeß **30** und die Signaleinheit **24** mit dem Prozeß **32** verbunden ist. Bei dem sicherheitskritischen Prozeß **28** handelt es sich bspw. um die Zwei-Hand-Steuerung einer Maschinenanlage, bei der außerdem auch die Drehzahl einer hier nicht dargestellten Maschinenwelle überwacht wird. Der sicherheitskritische Prozeß **30** ist bspw. die Überwachung eines Not-Aus-Schalters und der sicherheitskritische Prozeß **32** die Überwachung eines Schutzgitters (hier ebenfalls nicht dargestellt).

[0050] Die Signaleinheiten **18** bis **24** lesen über ihre E/A-Kanäle **26** Signale und/oder Datenwerte der sicherheitskritischen Prozesse **28** bis **32** ein. Derartige Signale bzw. Datenwerte sind bspw. die aktuelle Drehzahl der Maschinenwelle und die Schalterstellung des Not-Aus-Schalters. Andererseits können die Signaleinheiten **18** bis **24** über die E/A-Kanäle **26** auf hier nicht dargestellte Aktoren einwirken, mit denen die sicherheitskritischen Prozesse **28** bis **32** beeinflußt werden. So gehört bspw. zu dem sicherheitskritischen Prozeß **30**, bei dem die Schalterstellung des Not-Aus-Schalters überwacht wird, ein Aktor, mit dem die Stromversorgung der gesteuerten und überwachten Maschinenanlage abgeschaltet werden kann.

[0051] Die sicheren Steuerungseinheiten **12** und **14** sind SPS-Steuerungen. Sie sind hier vom Grundsatz her gleich zueinander aufgebaut und unterscheiden sich im wesentlichen durch verschiedenen Anwendungsprogramme, die auf ihnen ausgeführt werden.

[0052] Bei der nachfolgenden Erläuterung der Steuerungseinheiten **12**, **14** bzw. der Signaleinheiten **18** bis **24** sind die jeweils genannten Bezugszeichen in Fig. 1 aus Gründen der Übersichtlichkeit nur einfach aufgeführt.

[0053] Die Steuerungseinheiten **12**, **14** beinhalten jeweils einen sicheren Verarbeitungsteil **34**, der in Fig. 1 oberhalb der strichpunktierten Linie **36** dargestellt ist. Unterhalb der Linie **36** befindet sich ein nicht-sicherer Teil **38**, der im wesentlichen einen als Buscontroller bezeichneten Baustein **40** enthält. Der Buscontroller **40** ist ein Standard-Baustein, in dem das Standard-Protokoll des verwendeten Feldbusses **16** implementiert ist. Der Buscontroller **40** ist in der Lage, das Versenden und Empfangen von Nachrichten in Form von Telegrammen eigenständig abzuwickeln. Die zu versendenden Nachrichten erhält der Buscontroller **40** von dem sicheren Verarbeitungsteil **34**. Umgekehrt stellt der Buscontroller **40** empfangene Nachrichten dem sicheren Verarbeitungsteil **34** zur Verfügung.

[0054] Entsprechend einer bevorzugten Ausführung der Erfindung handelt es sich bei dem Feldbus **16** hier um einen CAN-Bus. Bei diesem Bus werden die zu versendenden Nachrichten innerhalb eines Nutzdatenfeldes übertragen, das für seinen Weg über den Feldbus **16** mit zusätzlichen Steuerungsinformationen ergänzt wird. Das gesamte Paket aus Steuerungsinformationen und Nutzdatenfeld bildet das Bustelegramm. Der Buscontroller **40** ist in der Lage, Nachrichten, die er von dem sicheren Verarbeitungsteil **34** erhält, selbständig in der dem Protokoll entsprechenden Form in die zu versendenden Bustelegramme einzubetten. Umgekehrt kann er bei einem empfangenen Bustelegramme die im Nutzdatenfeld enthaltenen Nachrichten extrahieren.

[0055] Der sichere Verarbeitungsteil **34** jeder Steuerungseinheit **12**, **14** ist zweikanalig-redundant aufgebaut. Jeder der beiden Kanäle enthält im wesentlichen einen Prozessor **42a**, **42b** mit jeweils zugehöriger Peripherie, mit dem ein Anwendungsprogramm **44a**, **44b** ausgeführt wird. In dem Anwendungsprogramm **44a**, **44b** ist die Steuerung der Maschinenanlage und damit die Intelligenz der Steuerungseinheiten **12**, **14** niedergelegt.

[0056] Die beiden Prozessoren **42a**, **42b** führen sicherheitsrelevante Aufgaben redundant zueinander aus. Dabei kontrollieren sie sich gegenseitig, was in Fig. 1 durch einen Pfeil **46** dargestellt ist. Die sicherheitsrelevanten Aufgaben beinhalten bspw. Maßnahmen zur Fehlersicherung von übertragenen bzw. versendeten Nachrichten. Diese Maßnahmen erfolgen zusätzlich und in Ergänzung zu Fehlersicherungsmaßnahmen, die bereits standardmäßig von dem Buscontroller **40** durchgeführt werden. Hierdurch ist es möglich, die Fehlerwahrscheinlichkeit gegenüber dem an sich nicht-sicheren Feldbus **16** beträchtlich zu erhöhen.

[0057] Die Signaleinheiten **18** bis **24** sind über den gleichen Buscontroller **40** an den Feldbus **16** angeschlossen wie die sicheren Steuerungseinheiten **12**, **14**. Dementsprechend ist der Teil **48** oberhalb der Linie **50** in Fig. 1 wiederum nicht-sicher im Sinne der vorliegenden Erfindung. In dem sicheren Verarbeitungsteil unterhalb der Linie **50** ist jede Signaleinheit **18** bis **24** wiederum zweikanalig-redundant aufgebaut. Die beiden redundanten Verarbeitungskanäle sind wiederum in der Lage, eine gegenseitige Fehlerüberwachung durchzuführen.

[0058] Jeder der Verarbeitungskanäle der Signaleinheiten **18** bis **24** besitzt einen Prozessor **54a**, **54b** sowie ein Schaltmittel **56a**, **56b**.

[0059] Mit den Bezugsziffern **58a**, **58b** ist jeweils ein Speicher bezeichnet, in dem einerseits eine festgelegte Universaladresse abgelegt ist und in dem die Prozessoren **54a**, **54b** andererseits eine zugeordnete Teilnehmeradresse abspeichern können. In Verbindung mit dem Buscontroller **40** ist jede Signaleinheit **18** bis **24** daher in der Lage, sich unter der festgelegten Universaladresse bei einer an dem Feldbus angeschlossenen Verwaltungseinheit anzumelden bzw. umgekehrt ein Adreßvergabetelegramm mit einer zugeordneten Teilnehmeradresse aufzunehmen und auszuwerten. Dieselbe Fähigkeit besitzen auch die sicheren Steuerungseinheiten **12**, **14**, wenngleich dies in Fig. 1 nicht explizit dargestellt ist.

[0060] Die Schaltmittel **56a**, **56b** versetzen die Signaleinheiten **18** bis **24** in die Lage, die hier nicht dargestellten Aktoren zur Beeinflussung der sicherheitskritischen Prozesse **28** bis **32** zu aktivieren. Damit sind die sicheren Signaleinheiten **18** bis **24** in der Lage, die sicherheitskritischen Prozesse **28** bis **32** in einen sicheren Zustand zu überführen, wie bspw. bei einer Betätigung des Not-Aus-Schalters die Maschinenanlage abzuschalten.

[0061] Mit der Bezugsziffer **70** ist in Fig. 1 die bereits erwähnte Verwaltungseinheit bezeichnet, die in der Fachterminologie auch als "Management Device" bezeichnet wird. Die Verwaltungseinheit **70** ist ebenfalls über einen Buscontroller **40** an den Feldbus **16** angeschlossen. Sie kann daher mit den übrigen an den Feldbus **16** angeschlossenen Einheiten kommunizieren. An der Steuerung der sicherheitskritischen Prozesse **28** bis **32** ist sie jedoch nicht unmittelbar beteiligt.

[0062] In ihrem sicheren Verarbeitungsteil besitzt die Verwaltungseinheit **70** im wesentlichen zwei zueinander redundante Speicher **72a**, **72b**, in denen unter anderem die gesamte Konfiguration des Steuerungssystems **10**, insbesondere die Zuordnung der

definierten Teilnehmeradressen an die Busteilnehmer **12**, **14** bzw. **18** bis **24** abgelegt ist. Die Verwaltungseinheit **70** besitzt eine zentrale Verwaltungs- und Überwachungsfunktion, die unabhängig von der Steuerung der Prozesse **28** bis **32** abläuft. Beispielsweise initiiert die Verwaltungseinheit **70** in regelmäßigen Zeitintervallen eine Verbindungsprüfung zwischen den Steuerungseinheiten **12**, **14** und den Signaleinheiten **18** bis **24**. Dabei überprüft die Verwaltungseinheit **70** durch Versenden eines Verbindungsprüftelegramms an die Steuerungseinheiten **12**, **14**, ob die Verbindung zu diesen Steuerungseinheiten fehlerfrei funktioniert. Als Reaktion auf dieses Prüftelegramm versenden die Steuerungseinheiten **12**, **14** ihrerseits Prüftelegramme an die ihnen zugeordneten Signaleinheiten **18** bis **24**. Die Verwaltungseinheit **70** überwacht dabei den gesamten Datenverkehr und erhält hierdurch in regelmäßigen Zeitintervallen eine Information darüber, ob immer noch alle ihr bekannten Busteilnehmer aktiv am Feldbus **16** angeschlossen sind. Bei Ausbleiben eines erwarteten Prüftelegramms oder auch beim Ausbleiben eines erwarteten Antworttelegramms erzeugt die Verwaltungseinheit ein Fehlertelegramm, aufgrund dessen die sicherheitskritischen Prozesse **28** bis **32** in ihren sicheren Zustand überführt werden.

[0063] Alternativ zu dem hier dargestellten Ausführungsbeispiel kann die Verwaltungseinheit **70** auch in einer der Steuerungseinheiten **12**, **14** integriert sein. In diesem Fall stellt die Verwaltungseinheit **70** einen Funktionsblock innerhalb der Steuerungseinheit **12**, **14** dar. In einem weiteren, hier ebenfalls nicht dargestellten Ausführungsbeispiel besitzt das Steuerungssystem **10** nur eine Steuerungseinheit **12**.

[0064] Mit der Bezugsziffer **80** ist beispielhaft ein Bustelegramm bezeichnet, das zwischen zwei Busteilnehmern über den Feldbus **16** übertragen wird. Das Bustelegramm **80** weist dem verwendeten, standardisierten Protokoll entsprechend ein Adreßfeld **82** sowie ein Nutzdatenfeld **84** auf. Zudem können weitere, hier nicht dargestellte Steuerungsinformationen in dem Bustelegramm **80** enthalten sein.

[0065] In der Darstellung in Fig. 1 ist jeder der an den Feldbus **16** angeschlossenen Einheiten eine individuelle, definierte Teilnehmeradresse **90** zugeordnet, die bei der Steuerungseinheit **14** beispielhaft mit "2" angenommen ist. Die Verwaltungseinheit **70** besitzt hiernach die definierte Teilnehmeradresse "0" und die Signaleinheit **18** beispielhaft die Teilnehmeradresse "3". Darüber hinaus ist in jeder Einheit eine festgelegte Universaladresse **92** abgelegt, die in Fig. 1 symbolisch als "xy" dargestellt ist. Es versteht sich, daß sowohl die Teilnehmeradresse **90** als die Universaladresse **92** jeweils als Datenwert in einem Speicher der einzelnen Einheiten abgelegt ist.

[0066] In Fig. 2 ist am Beispiel der Verwaltungseinheit **70**, der sicheren Steuerungseinheit **12** sowie der sicheren Signaleinheit **18** der zeitliche Ablauf der Kommunikation beim Konfigurieren der Signaleinheit **18** dargestellt. Dabei verläuft eine Zeitachse in Richtung des Pfeils **100**. Die einzelnen Telegramme, die zwischen den verschiedenen Einheiten versendet werden, sind anhand von Pfeilen symbolisiert, deren Ausgangspunkt beim Absender mit einem Punkt versehen ist und deren Endpunkt jeweils auf den Empfänger verweist.

[0067] In dem ersten Zeitabschnitt in Fig. 2 ist die sichere Signaleinheit **18** noch nicht am Feldbus **16** angeschlossen. Sie ist daher in diesem Zeitabschnitt nur gestrichelt dargestellt. Die Verwaltungseinheit **70** versendet in regelmäßigen Zeitabständen ein Verbindungsprüfungstelegramm **102** an die Steuerungseinheit **12**. Diese antwortet daraufhin mit einem Antworttelegramm **104**. Der Eingang des Antworttelegramms **104** innerhalb einer vorgegebenen Zeitspanne wird von der Verwaltungseinheit **70** überwacht. Infolge dessen ist die Verwaltungseinheit **70** in der Lage, die tatsächliche Anzahl der aktiv an den Feldbus **16** angeschlossenen Einheiten mit der Sollanzahl gemäß einer Sollkonfiguration zu vergleichen. Nach Ablauf der festgelegten Zeitspanne wiederholt sich der Vorgang, d.h. die Verwaltungseinheit **70** versendet erneut das Verbindungsprüfungstelegramm **102** und empfängt das Antworttelegramm **104**.

[0068] Nun sei angenommen, daß die Signaleinheit **18** neu an den Feldbus **16** angeschlossen werden soll. Dementsprechend muß die Signaleinheit **18** konfiguriert werden, wobei ihr eine definierte Teilnehmeradresse **90** zugeordnet wird. Gemäß dem hier dargestellten Ausführungsbeispiel der Erfindung wird die Verwaltungseinheit **70** zunächst in einen besonderen Wartungsmodus versetzt. Dies geschieht bei dem bevorzugten Ausführungsbeispiel mit Hilfe eines Schlüsselschalters, der an der Verwaltungseinheit **70** angeordnet ist. Die Aktivierung des besonderen Wartungsmodus ist in Fig. 2 anhand der Linie **106** symbolisiert.

[0069] Nach der Aktivierung des besonderen Wartungsmodus wird der Verwaltungseinheit **70** mit Hilfe eines Eingabegerätes **108** die definierte Teilnehmeradresse **90** übermittelt, die der Signaleinheit **18** zugeordnet werden soll. Anschließend versendet die Verwaltungseinheit **70** ein definiertes Wartungstelegramm **110**, das sich von dem Verbindungsprüfungstelegramm **102** im normalen Betriebsmodus der Verwaltungseinheit **70** unterscheidet. Die bereits an den Feldbus **16** angeschlossene Steuerungseinheit **12** antwortet auf den Empfang des Wartungstelegramms **110** mit einem Anmeldetelegramm **112**, das die definierte Teilnehmeradresse der Steuerungseinheit **12**, hier also beispielhaft die Teilnehmeradresse "1", beinhaltet. Das Anmeldetelegramm **112** ist somit das zweite Anmeldetelegramm im Sinne der vorlie-

genden Erfindung. Gemäß einer bevorzugten Ausführung der Erfindung ist das Anmeldetelegramm **112** der Steuerungseinheit **12** mit dem zuvor erwähnten Antworttelegramm **104** identisch. Dies ist jedoch zur Durchführung des Verfahrens nicht unbedingt notwendig.

[0070] Der Versand des Wartungstelegramms **110** bzw. der Empfang des zweiten Anmeldetelegramms **112** wiederholt sich zyklisch. Während dieser Zeit ist es möglich, die sichere Signaleinheit **18** an den Feldbus **16** anzuschließen. Nachdem dies geschehen ist, empfängt die Signaleinheit **18** ebenso wie die Steuerungseinheit **12** das Wartungstelegramm **110**. Während die Steuerungseinheit **12** auf dieses Wartungstelegramm **110**, wie zuvor beschrieben, mit dem zweiten Anmeldetelegramm **112** antwortet, versendet die Signaleinheit **18** als Antwort auf den erstmaligen Empfang des Wartungstelegramms **110** ein erstes Anmeldetelegramm **114**, das die festgelegte Universaladresse "xy" beinhaltet. Die Verwaltungseinheit **70** empfängt das erste Anmeldetelegramm **114** und versendet ein Quittungstelegramm **116** an die Signaleinheit **18**. Anschließend versendet die Verwaltungseinheit **70** ein Adreßvergabetelegramm **118**, in dessen Nutzdatenfeld die definierte Teilnehmeradresse "3" enthalten ist. Die Signaleinheit **18** quittiert den Empfang des Adreßvergabetelegramms **118** mit einem Quittungstelegramm **116**. Anschließend legt die Signaleinheit **18** die definierte Teilnehmeradresse "3" in einem Speicher **120** ab.

[0071] Nachdem die Verwaltungseinheit **70** das Quittungstelegramm **116** von der Signaleinheit **18** empfangen hat, versendet sie erneut das Wartungstelegramm **110**. Daraufhin meldet sich die Steuerungseinheit **12**, wie üblich, mit dem zweiten Anmeldetelegramm **112** bei der Verwaltungseinheit **70** an. Darüber hinaus meldet sich nun jedoch auch die Signaleinheit **18** mit ihrem zweiten Anmeldetelegramm **112** bei der Verwaltungseinheit **70** an. In diesem Fall enthält das zweite Anmeldetelegramm **112** die Teilnehmeradresse "3", die der Signaleinheit **18** zugeordnet wurde. Die Verwaltungseinheit **70** quittiert den Empfang des zweiten Anmeldetelegramms **112** mit einem Quittungstelegramm **116**.

[0072] Nach dem Ablauf des beschriebenen Telegrammverkehrs ist die Signaleinheit **18** im Sinne der vorliegenden Erfindung konfiguriert. Gemäß dem bevorzugten Ausführungsbeispiel der Erfindung beendet die Verwaltungseinheit **70** daher automatisch den besonderen Wartungsmodus, was anhand der Linie **122** angedeutet ist. Sodann findet wiederum der bereits beschriebene, normale Datenverkehr zwischen der Verwaltungseinheit **70** und den an den Feldbus **16** angeschlossenen Einheiten **12**, **18** statt. Hierbei versendet die Verwaltungseinheit **70** in zyklischen Zeitabständen das Verbindungsprüfungstelegramm **102** und empfängt die Antworttelegramme **104**.

[0073] Abweichend von dem hier dargestellten Ablauf beendet die Verwaltungseinheit **70** in einem anderen Ausführungsbeispiel der Erfindung den besonderen Wartungsmodus bereits nach dem Abspeichern der zugeordneten Adresse in der Signaleinheit **18**. In diesem Fall meldet sich die Signaleinheit **18** mit dem zweiten Anmeldetelegramm **112** erst wieder im normalen Betriebsmodus der Verwaltungseinheit **70** bei dieser an.

[0074] Aus Gründen der Übersichtlichkeit wurde der Versand des Quittungstelegramms **116** hier nur in Bezug auf die zu konfigurierende Signaleinheit **18** erwähnt. Abweichend hiervon wird bei dem bevorzugten Ausführungsbeispiel des Steuerungssystems **10** jedoch jedes versendete Telegramm mit einem Quittungstelegramm **116** beantwortet. Das Ausbleiben des Quittungstelegramms **116** führt automatisch zur Erzeugung einer Fehlermeldung.

[0075] Fig. 3 zeigt den Ablauf des erfindungsgemäßen Verfahrens bei einem Austausch der Signaleinheit **18**. Auch hierbei befindet sich die Verwaltungseinheit **70** zunächst in ihrem normalen Betriebsmodus, in dem sie in zyklischen Zeitabständen Verbindungsprüfungstelegramme **102** an sämtliche an den Feldbus **16** angeschlossenen Einheiten versendet. Die angeschlossenen Einheiten, in diesem Fall die Steuerungseinheit **12** und die Signaleinheit **18**, antworten mit entsprechenden Antworttelegrammen **104**. Aufgrund dieser Antworttelegramme ist die Verwaltungseinheit **70** über die Anzahl der aktiv an den Feldbus **16** angeschlossenen Einheiten **12**, **18** informiert.

[0076] Zum Austausch der Signaleinheit **18** wird zunächst die Verwaltungseinheit **70** in den besonderen Wartungsmodus versetzt. Dies ist anhand der Linie **106** dargestellt. Zuvor wurde die auszutauschende Signaleinheit **18** vom Feldbus **16** abgetrennt.

[0077] In dem besonderen Wartungsmodus versendet die Verwaltungseinheit **70**, wie erläutert, ein definiertes Wartungstelegramm **110**, das jedoch die Signaleinheit **18** nicht mehr erreicht. Dies ist in Fig. 3 anhand des gestrichelten Pfeils **123** dargestellt. Die Steuerungseinheit **12** antwortet wie üblich mit dem zweiten Anmeldetelegramm **112** auf den Empfang des Wartungstelegramms **110**. Das zweite Anmeldetelegramm der Signaleinheit **18** bleibt hingegen aus, was durch den gestrichelten Pfeil **124** dargestellt ist. Die Verwaltungseinheit **70** kann daher erkennen, daß die Signaleinheit **18** nicht mehr aktiv an den Feldbus **16** angeschlossen ist. Sie speichert daher die definierte Teilnehmeradresse "3", die der Signaleinheit **18** zugeordnet war, in einem Speicher **126**. Anschließend versendet sie das Wartungstelegramm **110** erneut in zyklischen Zeitabständen. Die Steuerungseinheit **12** antwortet hierauf, wie erläutert, mit dem zweiten Anmeldetelegramm **112**.

[0078] Nun kann die Signaleinheit **18** oder ein entsprechendes Austauschgerät an den Feldbus **16** angeschlossen werden.

[0079] Sobald die neu angeschlossene Signaleinheit **18** das Wartungstelegramm **110** empfängt, versendet sie das erste Anmeldetelegramm **114**, in dem die festgelegte Universaladresse "xy" enthalten ist. Die neue Signaleinheit **18** meldet sich hierdurch bei der Verwaltungseinheit **70** unter der festgelegten Universaladresse "xy" an. Die Verwaltungseinheit **70** quittiert den Empfang des ersten Anmeldetelegramms **114**, wie bereits erläutert, mit einem Quittungstelegramm **116** und versendet anschließend das Adreßvergabetelegramm **118**. Dieses enthält nun die definierte Teilnehmeradresse "3", die die Verwaltungseinheit **70** zuvor in den Speicher **126** abgelegt hat. Die Signaleinheit **18** quittiert den Empfang des Adreßvergabetelegramms **118** mit einem Quittungstelegramm **116** und speichert die zugeordnete Teilnehmeradresse "3" in ihrem Speicher **120** ab. Anschließend versendet die Verwaltungseinheit **70** erneut das Wartungstelegramm **110** und empfängt sowohl von der Steuerungseinheit **12** als auch von der Signaleinheit **18** das zweite Anmeldetelegramm **112**. Sie quittiert den Empfang dieser Anmeldungstelegramme mit dem Quittungstelegramm **116** und beendet den besonderen Wartungsmodus, was wiederum anhand der Linie **122** dargestellt ist.

[0080] Mit diesem beschriebenen Verfahren ist es somit möglich, einen an den Feldbus **16** angeschlossenen Busteilnehmer auszutauschen, ohne daß man dessen definierte Teilnehmeradresse kennen muß.

[0081] In dem nächsten Zeitabschnitt in Fig. 3 ist der Verfahrensablauf dargestellt, der sich ergibt, wenn sich mehrere Busteilnehmer unter der festgelegten Universaladresse "xy" bei der Verwaltungseinheit **70** anmelden. Wie zuvor beschrieben, wurde die Verwaltungseinheit **70** zunächst in den besonderen Wartungsmodus versetzt. Sie versendet daraufhin das Wartungstelegramm **110**. Wenn nun sowohl die Steuerungseinheit **12** als auch die Signaleinheit **18** mit dem ersten Anmeldetelegramm **114** antworten, aktiviert die Verwaltungseinheit **70** eine Fehleranzeige **128** und bricht den besonderen Wartungsmodus ab.

[0082] In dem nächsten Zeitabschnitt ist eine weitere Fehlerquelle dargestellt. Hierbei ist angenommen, daß der Verwaltungseinheit **70** nach dem Aktivieren des besonderen Wartungsmodus über das Eingabegerät **108** eine Teilnehmeradresse übermittelt wird, die bereits einem an den Feldbus **16** angeschlossenen Busteilnehmer zugeordnet ist. Die Verwaltungseinheit **70** erkennt aufgrund der ihr bekannten Sollkonfiguration der aktiven Busteilnehmer die doppelte Adreßvergabe und aktiviert die Fehleranzeige **128**. Außerdem beendet sie wiederum den besonderen Wartungsmodus.

Patentansprüche

1. Verfahren zum Konfigurieren eines sicheren Busteilnehmers (**12**, **14**, **18**–**24**) beim Anschließen an einen Feldbus (**16**) in einem sicheren Steuerungssystem (**10**), wobei dem sicheren Busteilnehmer (**12**, **14**, **18**–**24**) eine definierte Teilnehmeradresse (**90**) zugeordnet wird, mit den Schritten:
– Versenden eines ersten Anmeldetelegramms (**114**) von dem sicheren Busteilnehmer (**12**, **14**, **18**–**24**) zu einer an den Feldbus (**16**) angeschlossenen Verwaltungseinheit (**70**), wobei das erste Anmeldetelegramm (**114**) eine festgelegte Universaladresse (**92**) beinhaltet,
– Versenden eines Adreßvergabetelegramms (**118**) von der Verwaltungseinheit (**70**) an den sicheren Busteilnehmer (**12**, **14**, **18**–**24**), wobei das Adreßvergabetelegramm (**118**) die definierte Teilnehmeradresse (**90**) beinhaltet und
– Abspeichern der definierten Teilnehmeradresse (**90**) in einem Speicher (**58**; **120**) des sicheren Busteilnehmers,
– wobei die Anwesenheit aller aktiv an den Feldbus (**16**) angeschlossenen Busteilnehmer (**12**, **14**, **18**–**24**) anhand einer Sollkonfiguration von Busteilnehmern (**12**, **14**, **18**–**24**) sowie anhand von Antworttelegrammen (**104**) der Busteilnehmer (**12**, **14**, **18**–**24**) überprüft wird, und
– wobei die Teilnehmeradresse (**90**) eines als nicht mehr aktiv erkannten Busteilnehmers (**12**, **14**, **18**–**24**) als definierte Teilnehmeradresse (**90**) versendet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der sichere Busteilnehmer (**12**, **14**, **18**–**24**) nach Empfang des Adreßvergabetelegramms (**118**) ein zweites Anmeldetelegramm (**112**) an die Verwaltungseinheit (**70**) versendet, wobei das zweite Anmeldetelegramm (**112**) die definierte Teilnehmeradresse (**90**) beinhaltet.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der sichere Busteilnehmer (**12**, **14**, **18**–**24**) das erste Anmeldetelegramm (**114**) nach dem Empfang eines definierten Wartungstelegramms (**110**) an die Verwaltungseinheit (**70**) versendet.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß der sichere Busteilnehmer (**12**, **14**, **18**–**24**) das erste Anmeldetelegramm (**114**) nur nach dem erstmaligen Empfang des definierten Wartungstelegramms (**110**) an die Verwaltungseinheit (**70**) versendet, während er bei einem wiederholten Empfang des definierten Wartungstelegramms (**110**) das zweite Anmeldetelegramm (**112**) an die Verwaltungseinheit (**70**) versendet.

5. Verfahren nach Anspruch 3 oder 4, dadurch

gekennzeichnet, das definierte Wartungstelegramm (**110**) nur nach Aktivieren (**106**) eines besonderen Wartungsmodus (**106**) der Verwaltungseinheit (**70**) versendet wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß die Verwaltungseinheit (**70**) den besonderen Wartungsmodus nach Empfang des zweiten Anmeldetelegramms (**112**) automatisch beendet (**122**).

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Verwaltungseinheit (**70**) Wartungstelegramme (**110**) in definierten Zeitabständen an alle an den Feldbus (**16**) angeschlossenen Busteilnehmer (**12**, **14**, **18**–**24**) versendet.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß ein Fehlersignal (**128**) erzeugt wird, wenn mehr als ein Busteilnehmer (**12**, **14**, **18**–**24**) das erste Anmeldetelegramm (**114**) versendet.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß zumindest das erste Anmeldetelegramm (**114**) sowie das Adreßvergabetelegramm (**118**) mit jeweils einem Quittungstelegramm (**116**) beantwortet werden.

10. Steuerungssystem zum sicheren Steuern von sicherheitskritischen Prozessen (**28**–**32**), mit einer Verwaltungseinheit (**70**) und mit zumindest einem sicheren Busteilnehmer (**12**, **14**, **18**–**24**), die an einen Feldbus (**16**) angeschlossen sind, wobei der sichere Busteilnehmer (**12**, **14**, **18**–**24**) erste Mittel (**40**) zum Aufnehmen und Auswerten eines Bustelegramms (**80**) sowie einen Speicher (**58**; **120**) zum Speichern einer dem Busteilnehmer (**12**, **14**, **18**–**24**) zugeordneten Teilnehmeradresse (**90**) aufweist, wobei der Busteilnehmer (**12**, **14**, **18**–**24**) zweite Mittel (**40**, **120**; **40**, **58**) aufweist, um sich unter einer festgelegten Universaladresse (**92**) bei der Verwaltungseinheit (**70**) anzumelden, sowie dritte Mittel (**42**, **54**), um ein Adreßvergabetelegramm (**118**) mit der Teilnehmeradresse (**90**) aufzunehmen und auszuwerten, wobei die Verwaltungseinheit (**70**) dazu ausgebildet ist, die Anwesenheit aller aktiv an den Feldbus (**16**) angeschlossenen Busteilnehmer (**12**, **14 18**–**24**) anhand einer Sollkonfiguration von Busteilnehmern (**12**, **14**, **18**–**24**) sowie anhand von Antworttelegrammen (**104**) der Busteilnehmer (**12**, **14**, **18**–**24**) zu überprüfen und die Teilnehmeradresse (**90**) eines als nicht mehr aktiv erkannten Busteilnehmers (**12**, **14**, **18**–**24**) als definierte Teilnehmeradresse (**90**) an den zumindest einen Busteilnehmer (**12**, **14**, **18**–**24**) zu versenden.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

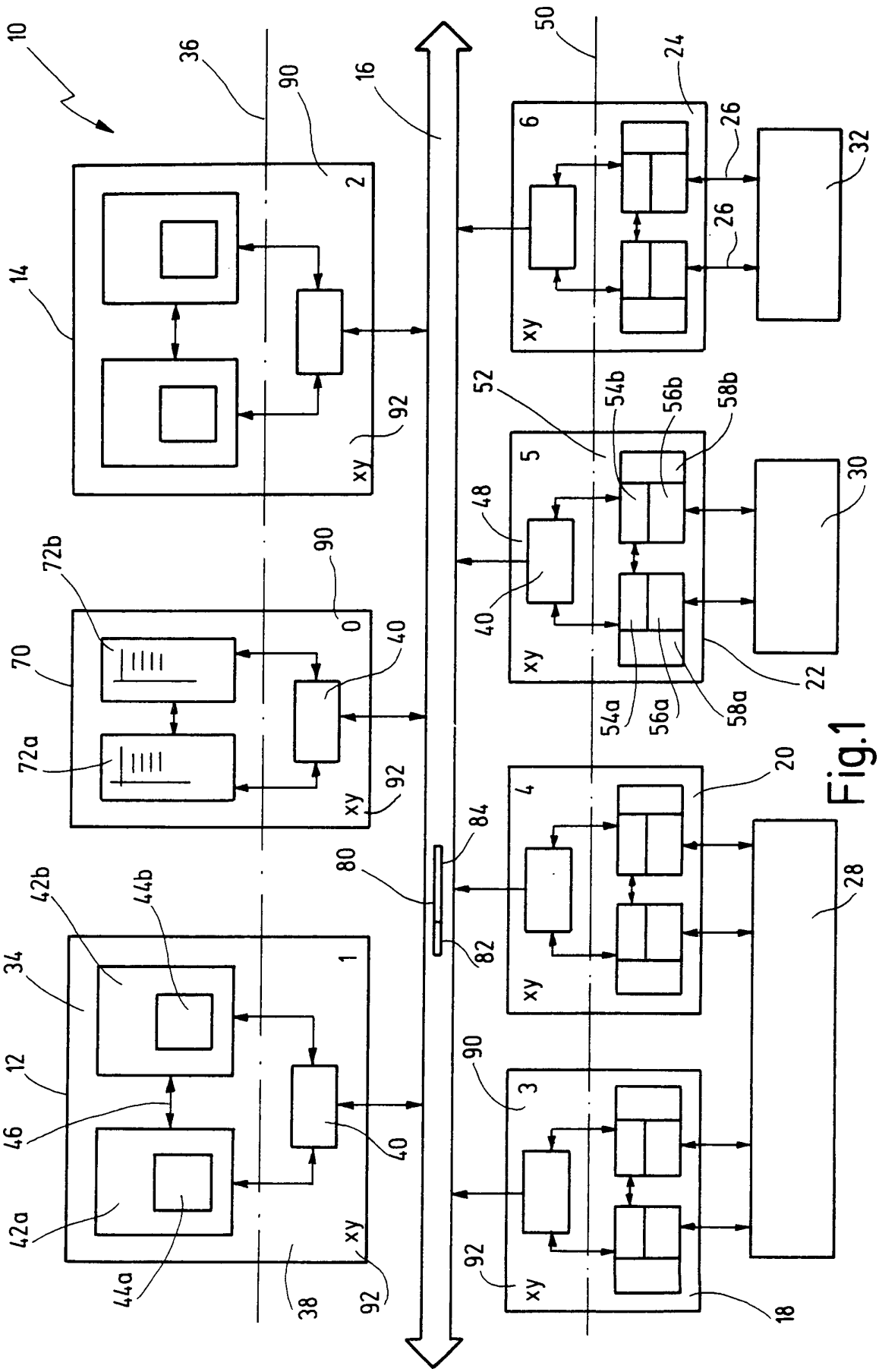


Fig.1

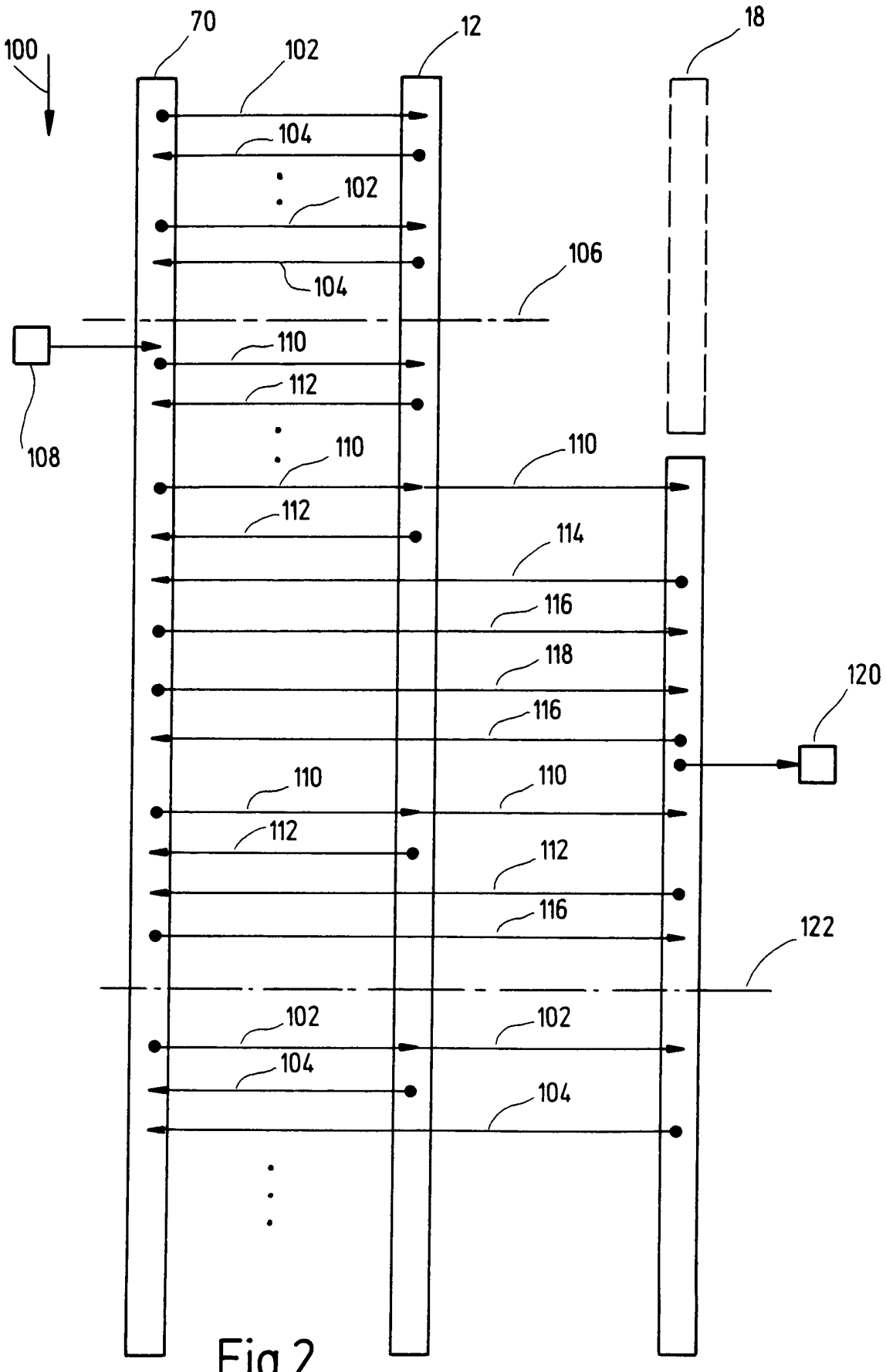

100
70
102
12
18
104
102
106
104
110
112
108
110
110
112
114
116
118
120
116
110
110
112
112
116
122
102
102
104
104

Fig.2

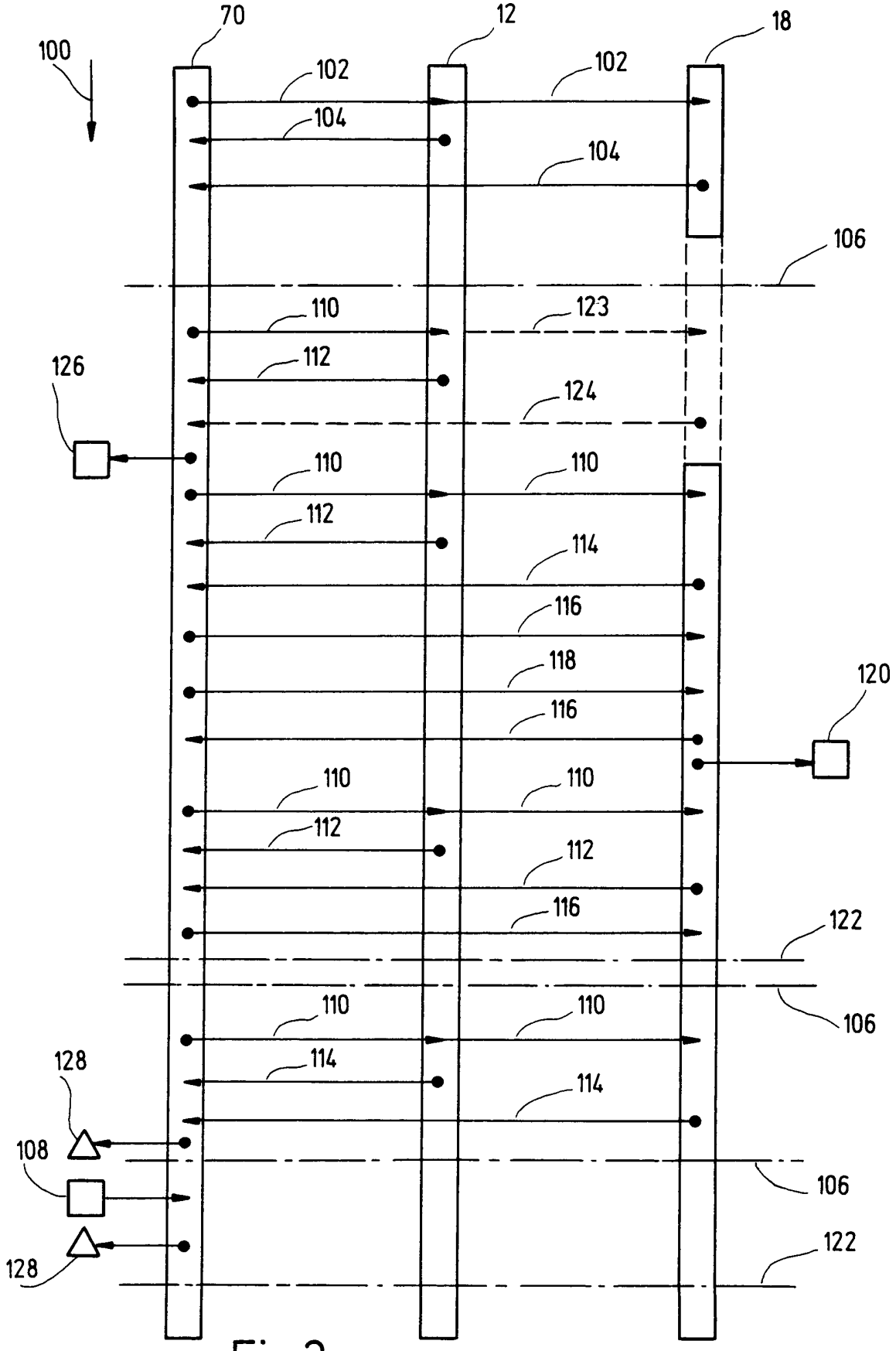

70
12
18
100
102
102
104
104
106
110
123
126
112
124
110
110
112
114
116
118
120
116
110
110
112
112
116
122
106
110
110
128
114
114
108
106
128
122

Fig.3