

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und ein System zur Sicherstellung von maximalen Reaktionszeiten in einem Datenverarbeitungssystem, insbesondere zwischen einem sicheren Eingangssignal und korrespondierendem sicheren Ausgangssignal.

[0002] Die DE 199 09 091 A1 offenbart ein Bussystem mit einem Master und mehreren Slaves, welche durch eine Busleitung miteinander verbunden sind, und betrifft die Überwachung einer Reaktionszeit zwischen einem Aussenden eines Master-Aufrufs und einem Empfang einer Slave-Antwort, wobei weder dem Master-Aufruf noch der Slave-Antwort irgendein Aktualitätsparameter zugeordnet wird.

[0003] Die Veröffentlichung von Kopetz, H. u. Grunsteidl, G. in Computer, IEEE Service Center, Los Alamitos, CA, US 1994, Vol. 27, 1, S. 14–23, ISSN 0018-9162 unter dem Titel "TTP – A PROTOCOL FOR FAULT-TOLERANT REAL-TIME SYSTEMS" ist auf eine zeitgesteuerte Echtzeitsysteme gerichtet, die auf TDMA-Basis arbeiten (TDMA: Time Domain Multiple Access), wobei zur Fehlererkennung CRC (Cyclic Redundancy Check) eingesetzt wird. Die Daten werden im Zeitmultiplex und nicht etwa synchron eingelesen, wobei kein Aktualitätsparameter, der den eingelesenen Daten in Bezug auf wenigstens einen Datenzyklus zugeordnet ist offenbart wird.

[0004] In kommunizierenden Datenverarbeitungssystem bzw. -anlagen, sind daher Daten einer Nachricht in der Regel nur zu einer bestimmten Zeit oder für eine bestimmte Zeit gültig, da, insbesondere im Falle sicherheitsrelevanter Ein-/Ausgangssignale, festgelegte Reaktionszeiten einzuhalten sind.

[0005] Gemäß Stand der Technik wird hierfür üblicherweise eine Laufzeitüberwachung zwischen Sender und Empfänger durchgeführt. Für eine empfangsseitige Laufzeitüberwachung, hängt der Sender eine entsprechende Zeitinformation an die Daten an, wobei sowohl der Sender als auch der Empfänger die Zeit verfolgen müssen. Für eine senderseitige Überwachung wird der Empfang der Daten durch Rücksenden eines Quittungssignals an den Sender bestätigt, wobei dieses zusätzlich eine Überwachung der richtigen Datenfolge ermöglicht.

[0006] Unter der Annahme, dass sich die Datenübertragung aus fortlaufenden und zeitfolgerichtig übertragenen Signalen zusammensetzt, offenbart die deutsche Patentschrift DE-101 02 435-C2 ferner ein Verfahren, welches zum Einen die Prüfung einer sicheren Datenübertragung als auch eine maximal mögliche oder vertretbare Verzögerung des Sendens eines Nachfolgesignals gewährleistet. Hierzu ist im Einzelnen vorgeschlagen, zur Datenübertragung zwischen miteinander kommunizierenden Datenver-

arbeitungseinheiten, das Absenden eines nachfolgenden Signals erst unter Ansprechen auf den Ablauf einer Mindestzeit zwischen zwei aufeinanderfolgenden Signalen sowie auf das senderseitige Empfangen eines Quittungssignals der Empfangseinheit auszulösen.

[0007] Aufgabe der Erfindung ist es einen gegenüber dem bekannten Stand der Technik neuen und wesentlich verbesserten Weg zur flexiblen und vielseitig anwendbaren Ermittlung, Prüfung und/oder Einhaltung von maximalen Reaktionszeiten in Datenverarbeitungssystemen, einschließlich komplexen oder verteilten, sicheren und/oder nicht sicheren Systemen, insbesondere zwischen einem sicheren Eingangssignal und korrespondierendem sicheren Ausgangssignal, bereitzustellen und insbesondere zur Sicherstellung von maximalen Reaktionszeiten in einem Datenverarbeitungssystem die Aktualität der Eingangs- und/oder Ausgangsdaten zu überwachen.

[0008] Die erfindungsgemäße Lösung der Aufgabe ist auf höchst überraschende Weise bereits durch die Gegenstände mit den Merkmalen der anhängenden unabhängigen Patentansprüche gegeben.

[0009] Vorteilhafte und/oder bevorzugte Ausführungsformen bzw. Weiterbildungen sind Gegenstand der jeweiligen abhängigen Ansprüche.

[0010] Basierend auf dem erfindungsgemäß vorgeschlagenen Verfahren, eingangsseitig an im System eingebundenen Teilnehmern anliegende Eingangs- und/oder Ausgangsdaten während jedes Datenzyklus synchron einzulesen, eingelesene Eingangs- und/oder Ausgangsdaten in Bezug auf wenigstens einen Datenzyklus basierten, den eingelesenen Eingangs- und/oder Ausgangsdaten zugeordneten oder zuzuordnenden Aktualitätsparameter zu überprüfen, unter Ansprechen auf das Erreichen einer definierten Abweichung wenigstens eines Aktualitätsparameters gegenüber einer definierten Aktualitätsschwelle auf einen Fehler zu erkennen und unter Ansprechen auf eine Fehlererkennung eine definierte Funktion, insbesondere eine sicherheitsgerichtete Funktion, auszulösen, ist folglich erstmals eine unmittelbare Überwachung einer Systemspezifisch fortlaufenden und/oder zeitfolgerichtigen Ein-/Ausgangs-Informationsbearbeitung und eine hierauf basierte Sicherstellung von maximalen Reaktionszeiten selbsttätig von Teilnehmern durchführbar.

[0011] Die Erfindung findet somit insbesondere bei Systemen Anwendung, bei denen es wichtig ist sicherzustellen, dass bestimmte Ausgänge einen definierten Zustand einnehmen, wenn keine korrespondierenden aktuellen Eingangsinformationen vorliegen, beispielsweise bei der Zeitkritischen Überwachung eines sicheren Eingangssignals für die Reak-

tion eines korrespondierenden sicheren Ausgangssignals.

[0012] In bevorzugter Ausbildung ist vorgesehen, eine Überprüfung eingelesener Ein- und/oder Ausgangsdaten während jedes Datenzyklus durchzuführen, um auf besonders effektive Weise Reaktionszeiten gemäß anwendungsspezifischem Transport von Daten, insbesondere in festen bzw. bestimmbar Intervallen, Abständen und/oder Zeiten, auch über Grenzen von Systemen, intelligenten Einheiten und/oder innerhalb von Netzwerken, flexibel sicherzustellen.

[0013] Zur Synchronisation des Einlesens sieht die Erfindung bevorzugt das zumindest zeitweise Übertragen eines Broadcast- und/oder Latchsignals an alle Teilnehmer vor. Zur dauerhaften Gewährleistung einer in festen Grenzen und/oder zu einem Zeitpunkt definierten Transport-Beziehung auf dem Datenweg in Sende- und/oder Empfangs-Richtung mit allen im insbesondere sicheren Datenstrom liegenden beeinflussenden Einheiten ermöglicht die Erfindung für die praktische Umsetzung somit in vorteilhafter Weise den Einsatz von systemspezifischen Mechanismen, die sicherstellen können, dass alle Teilnehmer zum gleichen Zeitpunkt einen TAKT/IMPULS erhalten.

[0014] Bei einer Weiterbildung der Erfindung, erfolgt die Synchronisation bei einem (Bus-)Start und/oder nach einem Fehler durch einen bestimmten Teilnehmer, in bevorzugter Ausführung durch den Master.

[0015] Wird die synchrone Datenübernahme gemäß bevorzugter Ausführungsformen unter Verwendung eines Ringschieberegisters durchgeführt, erhält somit, insbesondere unter Ausnutzung der Eigenschaften des Interbus, in zweckmäßiger Weise jeder Teilnehmer nach dem Schieben der Daten synchron zu allen Teilnehmern einen TAKT/IMPULS, dass der Teilnehmer die Ausgabe-Daten übernehmen kann und die Eingabe-Daten eingelesen werden.

[0016] Um auf besonders einfache und für das Übertragungsprotokoll in Bit-sparender Weise eine Aktualitätsverifizierung eingelesener Eingangs- und/oder Ausgangsdaten durchzuführen, ist wenigstens eine intelligente Einheit mit treiberartigen Mitteln vorgesehen, die den einzulesenden Daten eindeutige und/oder festen Zeit- und/oder Zyklusstrukturen zuordenbare Aktualitätsparameter zuweist.

[0017] Eine bevorzugte Weiterbildung sieht hierbei vor, in jedem Datenzyklus mit von einem bestimmten Teilnehmer, z. B. dem Master, ausgehenden Aktualitätsparameter, beispielsweise Zyklus basierte Werte, wie eine wiederkehrend laufende Nummer, an alle einlesenden Teilnehmer, z. B. den Slaves, zu übertragen, welche der Master in einem folgenden Daten-

zyklus wieder von den Slaves nach Bearbeitung der eingelesenen Daten zur Verifikation zurück erhält.

[0018] Gemäß einer weiteren bevorzugten Weiterbildung zählt jeder Teilnehmer die (gültigen) Datenzyklen bezogen auf die Zeit des Einlesens mit. Ein wesentlicher Vorteil hierbei ist, dass eine Weitergabe von auf eingelesenen Eingangs- und/oder Ausgangsdaten basierten Daten auf einfache Weise nur bis zu einer definierten Anzahl von gezählten Datenzyklen erfolgt und andernfalls auf Fehler erkannt wird. Hierbei ist bevorzugt vorgesehen, dass jeder Teilnehmer, der Daten wieder weitergibt, seine eigene (Datenzyklus-)Zeit des Einlesens auf eine über den Aktualitätsparameter bereits erhaltene Einlesezeit addiert.

[0019] Die Erfindung umfasst somit bevorzugt Ausführungsformen, bei welchen ein Wert oder Datum als Aktualitätsparameter nach einer Teilnehmerspezifischen Datenverarbeitung und/oder -weiterleitung an den Wert oder Datum erzeugenden Teilnehmer rückübersandt wird oder eine Aktualitätsauswertung durch den einlesenden Teilnehmer, insbesondere einen Ausgangsteilnehmer, selbst durchgeführt wird.

[0020] Da die Aktualitätsauswertung somit insbesondere auf die für eine Bearbeitung von eingelesenen Daten benötigte Zeit bezogen ist, wird auf äußerst effizient Weise eine Überprüfung ermöglicht, ob eine Teilnehmerspezifische Datenverarbeitung und/oder -weiterleitung innerhalb einer vorgegebenen/vorgebbaren maximalen Zeit erfolgt, einschließlich einer Verarbeitung von Eingabe-Daten in Ausgabe-Daten durch den Master.

[0021] Applikationsspezifisch ist somit ferner bevorzugt vorgesehen, dass das Einleiten einer definierten Maßnahme, insbesondere einer Sicherheitsmaßnahme, unter Ansprechen auf eine erkannte maximale Reaktionsschwellzeit entsprechend durch den Aktualitätsparameter erzeugenden Teilnehmer und/oder durch den jeweils einlesenden Teilnehmer, insbesondere durch einen Ausgangsteilnehmer oder einen Teilnehmer mit zugeordnetem Ausgangsmodell, erfolgt.

[0022] Ist beispielsweise bei der Durchführung der Erfindung sichergestellt, dass eine Verarbeitung von Eingabedaten in Ausgabedaten durch einen ausgewählten Teilnehmer, bevorzugt durch den Master innerhalb einer vorgegebenen/vorgebbaren maximalen Zeit erfolgt, ermöglicht dies aufgrund der synchronen Übernahme von Informationen einem Ausgangsteilnehmer selbstständig eine Bestimmung und/oder Überwachung der maximalen zulässigen Alterungszeit einer eingelesenen Eingangsinformation durchführen.

[0023] Folglich kann ein Teilnehmer, der weiß, dass seine eingelesenen Daten, die er mit einem be-

stimmten Zyklus erhalten hat, aus Eingangsdaten, die aus dem vorhergehenden Datenzyklus stammen, berechnet wurden, eine dem Teilnehmer zugeordnete Watchdog auf die Zeit des letzten Datenzyklus zurücksetzen.

[0024] Da die Teilnehmer Eingangsteilnehmer und Ausgangsteilnehmer und/oder Master und Slaves umfassen können, ist die Erfindung folglich für im Wesentlichen jedes Datenverarbeitungssystem einsetzbar, wobei Masterfunktionen auch z. B. ähnlich einem Tokenring-System weitergegeben werden können.

[0025] Zur Durchführung der Erfindung weist folglich zumindest ein Teilnehmer eine Auswerteeinheit und Reaktions-Vergleichseinrichtung auf, in bevorzugter Ausführung der oder die Teilnehmer mit Aktualitätsparameter erzeugenden Treiber-artigen Mitteln.

[0026] Umfasst ein erfindungsgemäß adaptiertes Datenverarbeitungssystem auch Systemkoppler, werden dem Systemkoppler zugeordnete Watchdogzeiten aufgeteilt, da dieser sowohl die Funktion des Masters eines unterlagerten Systems als auch eines Slaves des überlagerten Systems wahrnimmt.

[0027] Die Erfindung ist somit aufgrund der äußerst flexiblen Variationsmöglichkeiten bevorzugt bei Datenverarbeitungssystemen einsetzbar, bei welchen die Kommunikation zur Weiterleitung der Daten von einem Slave zu einem anderen und/oder zur Veränderung der Daten über einen Master erfolgt oder ohne einen Master direkt zwischen zwei Slaves erfolgt.

[0028] Als weitere bevorzugte Ausführungsformen umfasst die Erfindung insbesondere Applikationen, bei denen der Master eine sichere Steuerung ist und/oder die Slaves sichere digitale/analoge Eingänge und/oder sichere digitale/analoge Ausgänge besitzen und/oder welche eine Mischung von sicheren und/oder normalen Teilnehmer mit und/oder ohne Zeitinformation auch am gleichen Bus aufweisen.

[0029] Die Erfindung wird nachfolgend anhand bevorzugter Ausführungsformen unter Bezugnahme auf die beigefügten Zeichnungen beispielhaft beschrieben. In den Zeichnungen zeigen:

[0030] [Fig. 1](#) zur Darstellung einer ersten bevorzugten Ausführungsform der Erfindung eine stark vereinfachte Prinzipskizze eines Systems zum Betreiben einer Automatisierungsanlage, umfassend mehrere erfindungsgemäße Teilnehmerkomponenten, die jeweils eine zugeordnete intelligente Einheit aufweisen,

[0031] [Fig. 2](#) ein stark schematisiertes Master-Slave-System zur Darstellung weiterer bevorzugter Ausführungsformen der Erfindung,

[0032] [Fig. 3](#) ein vereinfachtes Ablaufschema von Datenzyklen gemäß einer erfindungsgemäßen Master-Slave-basierten Ausbildungsform.

[0033] Nachfolgend wird zunächst auf [Fig. 1](#) Bezug genommen, welches für die Erfindung wesentliche Elemente eines Standardnetzwerksystems zum Betreiben einer Automatisierungsanlage in stark vereinfachter Weise dargestellt.

[0034] Basierend auf einem derartigen Datenverarbeitungssystem werden bevorzugt von wenigstens einem Eingangsteilnehmer oder einem, einem Teilnehmer zugeordneten Eingangsmodul, Eingangsdaten eingelesen. Diese Daten werden nach Verarbeitung von einem Ausgangsteilnehmer oder einem, einem Teilnehmer zugeordneten Ausgangsmodul, als Ausgangsdaten ausgegeben. Eine Verarbeitung kann im gleichen Teilnehmer erfolgen oder nach Weitergabe der Eingangsdaten durch einen anderen, der nach Verarbeitung der Eingangsdaten zu Ausgangsdaten diese ausgibt oder einem anderen Teilnehmer zur Ausgabe übergibt.

[0035] Im Einzelnen zeigt [Fig. 1](#) eine Anzahl von im Standardnetzwerksystem eingebundenen Teilnehmern **11**, **12**, **13**, **14** und **15**, die jeweils über eine intelligente Einheit **1**, **2**, **3**, **4** bzw. **5** verfügen, welche für definierte Applikationen und/oder an definierten Positionen des Netzwerkes vorgesehen sind.

[0036] Die den Teilnehmern **11**, **12**, **13**, **14** und **15** zugeordneten intelligenten Einheiten **1**, **2**, **3**, **4** und **5** umfassen somit bevorzugt anlagenspezifische Anlagenkomponenten, wie beispielsweise Sensoren und/oder Aktoren, und weisen ferner eine zugeordnete, nicht näher dargestellte Logik zum entsprechenden teilnehmerspezifischen Verarbeiten von Daten auf.

[0037] Bei der in [Fig. 1](#) beispielhaft dargestellten Applikation umfasst zumindest die dem Teilnehmer **12** zugeordnete intelligente Einheit **2** Treiber-artige Mittel **122**, welche wechselnde Werte **123** erzeugen, die eindeutig und in festen Zeitrastern über einen längeren Zeitraum zur Verfügung stehen.

[0038] Zur Überwachung und/oder Feststellung von Reaktionszeiten zwischen sicheren Eingangsdaten und korrespondierenden sicheren Ausgangsdaten übermittelt der Teilnehmer **12** die Werte **123**, wie mit den Pfeilen A gekennzeichnet, synchron an alle intelligenten Einheiten, welche sichere Daten weiterleiten und/oder verarbeiten, im vorliegenden Beispiel an die intelligenten Einheiten **1**, **3**, und **4**.

[0039] Die übermittelten Werte **123** werden daraufhin von den zur Bearbeitung sicherer Daten vorgesehenen Teilnehmer **11**, **13**, und **14** zusammen mit aktuell im entsprechenden Datenzyklus anliegenden sicheren Eingabe- und/oder Ausgabedaten eingele-

sen. Nach Weiterverarbeitung und/oder Weiterleitung dieser eingelesenen Daten durch die jeweiligen intelligenten Einheiten **1**, **3** und **4** wird der entsprechend zuvor zugeordnete Wert **123** an den Wert-Erzeugenden-Teilnehmer **11** zurückgemeldet, wie mit den Pfeilen B gekennzeichnet. Mittels einer Auswerteeinheit **124** der intelligenten Einheit **2** wertet der Teilnehmer **11** die jeweils zurück gesandten Werte **123** zur Ermittlung der jeweiligen Reaktionszeit betreffend Bearbeitung der eingelesenen sicheren Daten in korrespondierende ausgegebene sichere Daten aus.

[0040] Je nach ermittelter Reaktionszeit kann der Teilnehmer **12** eine entsprechende Maßnahmen einleiten. Insbesondere wird nach Überschreiten einer vorgegebenen oder vorgebbaren maximal zulässigen Reaktionszeit das Auslösen einer sicherheitsgerichteten Maßnahme eingeleitet.

[0041] Zusätzlich ist bevorzugt vorgesehen, dass der Teilnehmer **12** Fehler erkennt, sofern zumindest einer der übermittelten Werte **123** nach der maximal zulässigen Reaktionszeit noch nicht zurück übertragen worden ist.

[0042] Die erfindungsgemäßen Mechanismen des gemäß [Fig. 1](#) bereitgestellte Netzwerksystems, mittels denen die, insbesondere Datenzyklus und/oder Bearbeitungszyklus basierten, Werte **123** generiert und übermittelt werden, stellen hierbei folglich ein synchronisierendes Broadcast-Verhalten sicher, mit welchem hinsichtlich allen im sicheren Datenstrom liegenden beeinflussenden Teilnehmern eine in festen Grenzen und/oder zu einem bestimmten Zeitpunkt definierte Transport-Beziehung auf dem Datenweg in Sende- und/oder Empfangsrichtung gewährleistet wird.

[0043] Wie nachfolgend in alternativer Ausführung ferner anhand der [Fig. 2](#) und [Fig. 3](#) beschrieben, ist der erfindungsgemäße Ansatz somit zur Überprüfung, Feststellung und/oder Einhaltung von Reaktionszeiten an eine Vielzahl von unterschiedlichen Datenverarbeitungsnetzwerken und/oder Systemen applikationsspezifisch anpassbar bzw. entsprechend der jeweiligen sicheren und/oder nicht sicheren Struktur mit zentraler Ausbildung, beispielsweise innerhalb von Rechnersystemen und deren Aufbau, dezentraler Ausbildung, beispielsweise bei Bussystemen, oder dezentral gekoppelter Ausbildung, beispielsweise mittels Systemkoppler, Übertrager und/oder Router über Systemgrenzen hinweg, adaptierbar.

[0044] [Fig. 2](#) skizziert einen Master-Slave-Ringschiebebus mit einem als Master fungierenden Teilnehmer **21** und zwei Teilnehmern **22** und **23** als Slaves. Der Teilnehmer **22** ist hierbei ein Eingangsteilnehmer, der Eingangs- oder Eingabedaten aus der Peripherie, wie mit dem Pfeil IN angezeigt, ein-

liest und an den Master **21** entsprechende Eingabe- bzw. IN-Daten zur sicheren und/oder nicht sicheren Verarbeitung in Ausgabe- bzw. OUT-Daten weiterleitet. Nach Verarbeitung der IN-Daten in OUT-Daten durch den Master **21** werden diese an die Slave **22** und **23** gesendet, woraufhin der Ausgangsteilnehmer **23** nach Einlesen der OUT-Daten korrespondierende Daten an die entsprechende Peripherie, wie mit dem Pfeil OUT angezeigt, ausgibt.

[0045] An alle zur Datenverarbeitung im System eingebundenen Teilnehmer **21**, **22** und **23** werden die zu verarbeitenden Daten unter Verwendung eines Ringschieberegisters R in einem Datenzyklus übergeben, wobei Netzwerk- und/oder Systemspezifisch alle Teilnehmer **21**, **22**, **23** zur synchronen Datenübernahme angewiesen werden.

[0046] Die Synchronisation kann Netzwerkspezifisch auch auf andere Weise erfolgen. So kann beispielsweise unter Verwendung eines ETHERNET basierten Systems ein Broadcastsignal als eine Art Latchsignal oder TAKT/IMPULS zur Anweisung der Datenübernahme eingesetzt werden.

[0047] Unter der Annahme, dass bei fehlerfreiem Betrieb jeweilige Datenbearbeitungen, d. h. im Wesentlichen Teilnehmer spezifische Datenverarbeitungen und/oder Datenweiterleitungen, innerhalb einer vorgegebenen/vorgebbaren maximalen Zeit, also insbesondere auch die Verarbeitung der IN-Daten in OUT-Daten durch den Master **21** innerhalb einer vorgegebenen/vorgebbaren maximalen Zeit erfolgt, ermöglicht die Erfindung somit, dass grundsätzlich durch jeden Teilnehmer **21**, **22** und **23**, in bevorzugter Weise insbesondere durch den Ausgangsteilnehmer **23** eine Bestimmung der maximalen Zeit des Alters eingelesener Information und folglich eine Überwachung deren Aktualität durchführbar ist. Die Reaktionszeit bildet somit bereits einen unmittelbaren zeitlichen Bezug der OUT-Daten und zu den IN-Daten ohne, dass zusätzliche Information im Übertragungsprotokoll übertragen werden muss.

[0048] Werden zusätzliche Informationen, beispielsweise zur Applikationsspezifischen Überwachung einzelner Teilnehmer, der Übertragung über Systemgrenzen, von einzelnen Busstörungen und/oder von Fehlsynchronisationen benötigt, kann es notwendig sein, ein oder mehrere Bits hierfür im Übertragungsprotokoll bereitzustellen.

[0049] Erkennt der Teilnehmer somit, dass eingelesene Daten, beispielsweise basierend auf einer Unterbrechung eines Buskabels, nicht mehr gültig sind, also ein Ablauf der maximalen Zeit hinsichtlich der Datenaktualität vorliegt, wird ein bestimmter Ausgang in den sicheren Zustand geschaltet. Das Einleiten spezifischer, insbesondere sicherheitsgerichteter

Maßnahmen innerhalb vorgegebener Reaktionszeit ist folglich sichergestellt.

[0050] Bei einer ersten hierauf basierten bevorzugten Ausführungsform zählt jeder Teilnehmer **21**, **22** und **23** die (gültigen) Datenzyklen mit. Bei einem (Bus-)Start und/oder nach einem Fehler erfolgt die Synchronisation durch einen bestimmten Teilnehmer, wie z. B. durch den Master **21** bevorzugt durch ein entsprechendes Signal. Jeder Teilnehmer **21**, **22** und **23** gibt die Zeit des Lesens der eingehenden Daten bezogen auf den vorangegangenen (gültigen) Datenzyklus an, wodurch im Wesentlichen ein relativer Zeitbezug eingestellt wird. Zweckmäßiger Weise werden für die Lesezeiten Zeitdimensionen verwendet, die der Länge zwischen den vergangenen Datenzyklen entsprechen.

[0051] Stammt z. B. das Eingangsdatum eines Teilnehmers aus dem vorhergehendem Datenzyklus, so gibt er eine 1 zurück, stammen die Daten aus dem vor-vorhergehendem Datenzyklus eine 2. Dies ist jedoch nur bis zu einer maximalen Größe zulässig, so dass ab einer vorgegebenen bzw. vorgebbaren Größe eines Eingangsdatum dieses als zu alt erkannt wird.

[0052] Wird gemäß einer bevorzugten Ausbildung z. B. bei einem Aktualitätswert von 7 automatisch davon ausgegangen, dass die Daten zu alt sind, rechnen 3 Bits für die Zeitinformation aus und jeder Teilnehmer **21**, **22** und **23** kann genau berechnen, wie alt die Daten sind bzw. ob die Daten noch ausreichend aktuell sind. Hieraus folgt, dass maximal 6 Datenzyklen alte Daten weitergereicht werden, wobei jeder Teilnehmer, der Daten wieder weitergibt, z. B. der Master **21**, der die Eingangsdaten zu Ausgangsdaten verarbeitet, seine eigene Verarbeitungszeit auf die über den Aktualitätswert erhaltene Lesezeit addiert und daraus einen entsprechend neuen Aktualitätswert weitergibt.

[0053] Bei einer zweiten auf [Fig. 2](#) basierten bevorzugten Ausführungsform überträgt der Master **21** mit jedem Satz von OUT-Daten einen Aktualitätswert an die Slaves **22** und **23** mit. Im gleichen Zyklus erhält der Master **21** von den Slaves **22** und **23** Eingangsinformationen mit Angabe des Aktualitätswertes. Bei fehlerfreiem Betrieb müssen demnach die von den Slaves **22** und **23** mit diesen Eingangsinformationen übertragenen Aktualitätswerte identisch mit dem Aktualitätswert sein, den der Master im vorherigen Zyklus an die Slaves **22** und **23** übertragen hat.

[0054] Bei einer weiteren bevorzugten Ausführungsform, insbesondere unter Ausnutzung der Eigenschaften des Interbus, erhält jeder Slave **22** und **23** nach dem Schieben der Daten ein Signal, dass die Teilnehmer **22** und **23** die Out-Daten übernehmen können und die IN-Daten vom Master **21** eingelesen werden. Dieses Signal erhalten alle Teilnehmer syn-

chron, also in Form eines Ziel unabhängigen Signals (TIC-Target Independent Code).

[0055] Unter zusätzlicher Bezugnahme auf das in [Fig. 3](#) skizzierte Ablaufschema von aufeinanderfolgenden Datenzyklen sendet der Master M im ersten Datenzyklus D1 und/oder nach einem Identitäts-(ID)-Zyklus an alle Slave-Teilnehmer TN1 und TN2 eine Null. Diese Null dient der Synchronisation. Die Slaves TN1 und TN2 senden in diesem Datenzyklus D1 eine Null bzw. ihren letzten Zählerstand, wenn es sich bei dem Datenzyklus D1 um ein Zyklus nach einem ID-Zyklus im laufenden Busbetrieb handelt.

[0056] Im nächsten Datenzyklus D2, also nachdem die Slaves TN1 und TN2 von dem Master M die Null erhalten haben, senden die Slaves TN1 und TN2 die Null zurück. Der Master M sendet in D2 den ersten Zeitwert 01.

[0057] Die DATA Werte in dem Telegramm mit dem der Zeitwert oder -stempel Null übertragen wird sind Statusinformationen und keine Werte, die zu den Peripherie-Ein- und/oder Ausgängen der Slaves TN1 und TN2 gehören. Folglich ist es möglich, bei jeder Fehlsynchronisation bzw. nach einem Fehler Fehlerinformationen mit zu übertragen.

[0058] Im nächsten Datenzyklus D3, also nachdem die Slaves TN1 und TN2 von dem Master M den ersten Zeitwert 01 erhalten haben, senden auch die Slaves TN1 und TN2 diesen ersten Zeitwert 01 mit gültigen Daten (gD) zurück. Der Master M sendet in D3 den zweiten Zeitwert 02 für jeden Slave TN1 bzw. TN2. Ferner werden in diesem Zyklus D3 von den sicheren Slaves TN1 und TN2 deren zu diesem Zeitpunkt gültigen Eingangsinformationen mit übertragen. Folglich merkt sich jeder Teilnehmer, also alle Slaves TN1 und TN2 und der Master M im Bus diese Zeit.

[0059] Bis zum nächsten Zyklus D4 hat der Master M alle Ausgangsinformationen aus den letzten Eingangsinformationen gewonnen. Im nächsten Zyklus D4 werden dann somit diese Ausgangsinformationen mit der nächsten Zeitinformation 03 zu jedem Slave TN1 und TN2 gesendet. Da der Slave TN1 bzw. TN2 im Bus weiß, dass seine eingelesene Ausgangsinformation, die er mit diesem Zyklus D4 erhalten hat, aus Eingangsinformationen, die aus dem letzten Datenzyklus D3 stammen, berechnet wurden, kann er seine Watchdog WD auf die Zeit des letzten Datenzyklus D3 zurücksetzen.

[0060] Gehen zwischendurch Zyklen defekt oder reagiert ein Teilnehmer nicht rechtzeitig, so sendet wenigstens ein Slave oder der Master eine Null oder ein FF oder einen anderen definierbaren Wert, damit erst wieder eine Synchronisation gefahren wird, und alle Teilnehmer M, TN1 und TN2 in Folge wissen, dass ih-

re Ausgangsinformationen aus veralteten Eingangsinformationen stammen. Werden diese Ausgangsinformationen älter als für einen Ausgangsteilnehmer bzw. dessen zugeordnetes -modul erlaubt ist, schaltet dieser selbstständig sicher ab oder führt eine sicherheitsgerichtete Funktion durch.

[0061] Jeder Teilnehmer M, TN1 und TN2 erhält also seine eigene Watchdogzeit. Diese müssen nicht von dem Master M zentral überwacht werden. Auch ist es nicht notwendig, eine Zeit im Protokoll mit zu versenden.

[0062] In Abwandlung zu vorstehend beschriebenen Beispiel zählt gemäß einer weiteren bevorzugten Ausführung jeder TN1 und TN2 für sich.

[0063] Insbesondere ist hierzu vorgeschlagen, dass nach der Überprüfung der Initialisierung jeder Slave TN1 und TN2 mit 1 als Aktualitätsparameter TIME anfängt und dieser pro Zyklus hoch zählt, wohingegen der Master M erst mit 1 anfängt, nachdem er die ersten Daten von den Slaves TN1 und TN2 verarbeitet hat, also einen Zyklus nachdem die Slaves die 1 gesendet haben. Jeder Teilnehmer M, TN1 und TN2 lässt somit einen Versatz von 1 zu.

[0064] TIME = 0 bedeutet somit, dass die anderen Daten im Telegramm nicht für IN-Daten oder OUT-Daten verwendet werden dürfen, wohingegen TIME <> 0 bedeutet, dass die anderen Daten im Telegramm als IN-Daten oder OUT-Daten zu interpretieren sind.

[0065] Werden hierbei wiederum bevorzugt die Eigenschaften des Interbus genutzt, erhält somit jeder Teilnehmer M, TN1 und TN2 nach dem Schieben der Daten ein Signal, dass der Teilnehmer jetzt die OUT-Daten übernehmen kann und/oder die IN-Daten eingelesen werden.

[0066] Im ersten Datenzyklus nach einem ID-Zyklus sendet der Master M somit die für die Slaves TN1 und TN2 gültigen Aktualitätsparameter, welche jeweils einem wiederholt auftretendem Zählerstand entsprechen. Die Slaves TN1 und TN2 senden im ersten Datenzyklus nach dem ID-Zyklus ihre jeweils gültigen Zählerstände als Aktualitätsparameter.

[0067] Nach einem (erneuten) Einschalten des Systems, d. h. insbesondere nach dem Einschalten (POWER ON) oder einem Neustart (RESET) des Masters M, sendet der Master M an alle Slaves TN1, TN2 eine 0 zur Synchronisation. Die Slaves senden ebenfalls im ersten Datenzyklus nach dem Einschalten, im Falle eines Einschaltens (POWER ON) oder eines Neustarts (RESET) der Slaves TN1, TN2 eine Null. Haben die Slaves TN1, TN2 keine Einschalt- oder Neustartanweisung erhalten, senden sie ihren letzten Zählerstand als Aktualitätsparameter.

[0068] Nachdem die Slaves TN1, TN2 die Null von dem Master M erhalten haben, senden die Slaves TN1, TN2 im nächsten Datenzyklus die Null zurück.

[0069] Sind vom Master M oder einem Slave TN1, TN2 eine Null gesendet worden, befinden sich beide solange in einer Initialisierungsphase, bis diese von beiden als gültig abgeschlossen wurde.

[0070] Der Master M sendet in diesem Zyklus den ersten Aktualitätsparameter an jeden Slave TN1 und TN2. Die DATA-Werte in dem Telegramm, in dem der Zeitstempel Null übertragen wird, sind Statusinformationen und keine Werte für die Peripherieeingänge oder -ausgänge. Somit ist es wiederum möglich bei jedem Fehler oder bei einer Fehlsynchronisation Fehlerinformationen mit zu übertragen.

[0071] In dem nächsten Datenzyklus werden dann von den Slaves TN1 und TN2 die ersten Aktualitätsparameter, die sie vorher von dem Master M erhalten haben, an diesen zurückgesendet. Der Master M sendet danach entsprechend den zweiten Aktualitätsparameter für jeden Slave TN1 und TN2. Von dem Slave TN1 bzw. TN2 werden in diesem Zyklus seine zu diesem Zeitpunkt gültigen Eingangsinformationen mit übertragen.

[0072] Deshalb merkt sich jeder Slave TN1 und TN2 im Bus den zum Aktualitätsparameter zugehörigen Zeitpunkt.

[0073] Bis zum nächsten Zyklus hat der Master M wiederum alle Ausgangsinformationen aus den letzten Eingangsinformationen gewonnen. Im nächsten Datenzyklus werden dann diese Ausgangsinformationen mit dem nächsten Aktualitätsparameter zu jedem Slave TN1 und TN2 gesendet. Da der Slave TN1, TN2 weiß, dass seine Ausgangsinformation, die er mit diesem Zyklus erhalten hat, aus den Eingangsinformationen, die aus dem letzten Datenzyklus stammen, berechnet wurden, kann er seine Watchdog auf den Zeitpunkt des letzten Datenzyklus zurücksetzen.

[0074] Gehen zwischendurch Zyklen defekt oder reagiert ein Teilnehmer nicht rechtzeitig, so sendet der entsprechende Slave oder der Master als Aktualitätsparameter beispielsweise eine Null oder ein FF oder einen anderen definierbaren Wert, damit erst wieder eine Synchronisation gefahren wird, und alle Teilnehmer in Folge wissen, dass ihre Ausgangsinformationen aus veralteten Eingangsinformationen stammen. Werden diese Ausgangsinformationen älter als für einen Ausgangsteilnehmer bzw. dessen zugeordnetes -modul erlaubt, schaltet dieser selbstständig sicher ab oder führt eine sicherheitsgerichtete Funktion durch.

[0075] Jeder Slave TN1 und TN2 erhält also seine eigene Watchdogzeit. Diese muss nicht von der sicheren Steuerung überwacht werden. Auch ist es nicht notwendig, eine absolute Zeitinformation im Protokoll mit zu versenden.

[0076] Ein fehlerfreier Betrieb ist somit bei beiden vorstehend beschriebenen Applikationen grundsätzlich gewährleistet, dass, solange der Master M das Protokoll für den nächsten Zyklus synchron abarbeitet, die neuen Ausgangsinformationen im nächsten Zyklus zur Verfügung stehen und alle Eingangsteilnehmer bzw. -module ihre Eingangsinformation synchron zur Verfügung stellen.

[0077] Wie aus [Fig. 3](#) ersichtlich ist, findet die Erfindung auch Anwendung bei Gesamtsystemen, bei denen der Master M eine sichere Steuerung ist und/oder ein Systemkoppler eingesetzt ist, wobei die Watchdogzeit in diesem Fall aufgeteilt wird, da der Systemkoppler in diesem Fall sowohl Master M eines unterlagerten Systems als auch Slave des überlagerten Systems ist.

[0078] Der Systemkoppler erhält folglich je eine Watchdogzeit für die Ausgänge des unterlagerten Systems und eine Watchdogzeit für die Eingänge des unterlagerten Systems. Die Watchdogzeiten auf den Ausgangsteilnehmern bzw. deren Ausgangsmodulen des unterlagerten Systems müssen dann entsprechend verkleinert werden. Dies ist jedoch von der Zeit her im Wesentlichen unkritisch, da sichere Eingänge aus überlagerten oder unterlagerten Systemen herkömmlicher Weise immer langsamer sind, als direkt am Bus angeschlossene Eingänge.

[0079] Auch wenn die vorstehende Beschreibung der Erfindung auf einigen bevorzugten Ausführungsformen basiert, ist es für einen Fachmann ersichtlich, dass Modifikationen innerhalb des durch die anhängenden Ansprüche definierten Schutzbereichs erfasst sind.

[0080] So deckt die Erfindung insbesondere ferner Weiterbildungen ab, bei denen sichere und/oder normale Teilnehmer mit und/oder ohne Zeitinformation am gleichen Bus gemischt vorliegen, eine Verarbeitung der Daten im Master und/oder in einem oder mehreren Slaves erfolgt und/oder es sich nicht um ein Master-Slave-System sondern um ein System, bei dem z. B. die Masterfunktion ähnlich einem Tokenring-Ansatz weitergegeben wird.

[0081] Ferner ist es nicht zwingend, dass die Kommunikation immer über einen Master erfolgt. Alternativ kann für die Anwendung der Erfindung die Kommunikation auch ohne Master direkt zwischen Slaves und/oder über einen Master erfolgen, der die Daten lediglich von einem Slave zu einem anderen weiterleitet, ohne diese zu verändern. Ferner können Sla-

ves für die Anwendung der Erfindung sichere digitale/ analoge Eingänge und/oder sichere digitale/ analoge Ausgänge besitzen.

[0082] Die Erfindung ist somit im Wesentlichen bei allen Datenverarbeitungssystemen einsetzbar, bei denen gewährleistet ist, dass alle Teilnehmer zum gleichen Zeitpunkt einen Art "Takt" oder "Impuls" erhalten und insbesondere, bei denen es wichtig ist sicherzustellen, dass die Ausgänge einen definierten Zustand einnehmen, wenn keine aktuellen Eingangsinformationen vorliegen.

Patentansprüche

1. Verfahren zur Sicherstellung der Einhaltung von vorgegebenen oder vorgebbaren maximalen Reaktionszeiten in einem Datenverarbeitungssystem mit im System eingebundenen Teilnehmern, wobei während jedem Datenzyklus eingangsseitig an im System eingebundenen Teilnehmern (**11**, **13**, **14**, **21**, **22**, **23**, M, TN1, TN2) anliegende Daten synchron eingelesen werden,

wobei zur Synchronisation des Einlesens zumindest zeitweise ein Synchronisierungssignal an alle Teilnehmer gesendet wird,

wobei von einem ersten Teilnehmer ausgegebene und von einem zweiten Teilnehmer während eines Datenzyklus eingelesene Daten (IN, OUT) zusammen mit einem ausgehenden zugeordneten Aktualitätsparameter (**123**) übertragen werden,

wobei eine Überprüfung erfolgt, ob eine teilnehmerspezifische Datenverarbeitung und/oder -weiterleitung innerhalb einer vorgegebenen oder vorgebbaren maximalen Zeit erfolgt, indem der zweite Teilnehmer den den eingelesenen Daten zugeordneten Aktualitätsparameter (**123**) überprüft und bei Erreichen einer definierten Abweichung gegenüber einer definierten Aktualitätsschwelle einen Fehler erkennt, und wobei unter Ansprechen auf die Fehlererkennung eine definierte Funktion ausgelöst wird.

2. Verfahren nach vorstehendem Anspruch, ferner gekennzeichnet dadurch, dass der Schritt der Überprüfung während jedes Datenzyklus durchgeführt wird.

3. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass das Synchronisierungssignal durch einen ausgewählten Teilnehmer an alle Teilnehmer, insbesondere durch einen Master an alle Slaves, gesendet wird.

4. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass das Synchronisierungssignal bei einem Systemstart und/oder nach einem System- und/oder Teilnehmer basierten Fehler gesendet wird.

5. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass zur Synchronisation des Einlesens mit jedem Datenzyklus ein Broadcast- oder Latchsignal an alle Teilnehmer gesendet wird.

6. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass eine Datenweitergabe unter Verwendung von Ringschieberegistern (R) erfolgt.

7. Verfahren nach vorstehendem Anspruch, ferner gekennzeichnet dadurch, dass jeder Teilnehmer die (gültigen) Datenzyklen mitzählt und/oder ein ausgewählter Teilnehmer zusammen mit einzulesenen Daten Aktualitätsparameter überträgt.

8. Verfahren nach vorstehendem Anspruch, ferner gekennzeichnet dadurch, dass jeder Teilnehmer, der Daten weitergibt, zur Erkennung von Fehlern seine eigene Zeit des Einlesens auf eine über den Aktualitätsparameter erhaltene Zeit des Einlesens addiert.

9. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass der Aktualitätsparameter erzeugende Teilnehmer oder ein Ausgangsteilnehmer eine Auswertung des Aktualitätsparameters durchführt, insbesondere zur Bestimmung und/oder Überwachung der maximalen Zeit einer Eingangsinformation und/oder in Bezug einer auf der Eingangsinformation basierten Reaktionszeit.

10. Verfahren nach einem der vorstehenden Ansprüche, wobei Eingangsdaten in Ausgangsdaten innerhalb einer vorgegebenen/vorgebbaren maximalen Zeit von einem ausgewähltem Teilnehmer verarbeitet werden.

11. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass ein von einem Teilnehmer zuzuordnender Aktualitätsparameter, insbesondere ein Zähler und/oder eine Watchdogzeit, unter Ansprechen auf das Einlesen einer Ausgangsinformation, die auf einer zeitfolgerichtigen Eingangsinformation basiert, zurückgesetzt wird.

12. Verfahren nach einem der vorstehenden Ansprüche, ferner gekennzeichnet dadurch, dass die Überwachung von Aktualitätsparametern, zentral oder dezentral erfolgt.

13. Datenverarbeitungssystem, welches zur Durchführung eines Verfahrens nach einem der vorstehenden Ansprüche angepasst ist.

14. Datenverarbeitungssystem nach vorstehendem Anspruch 13, wobei die Teilnehmer sichere und/oder nicht sichere Eingangsteilnehmer, Ausgangsteilnehmer, Teilnehmer mit zugeordneten Ein- und/

oder Ausgangsmodulen umfassen und sichere digitale/analoge Eingänge und/oder sichere digitale/analoge Ausgänge besitzen.

15. Datenverarbeitungssystem nach einem der vorstehenden Ansprüche 13 bis 14, wobei die Teilnehmer wenigstens einen Master und Slaves umfassen, zur Verarbeitung von Eingangs- zu Ausgangsdaten eine Kommunikation zwischen zwei Slaves direkt oder über einen Master erfolgt und/oder Daten ohne Veränderung über einen Master von einem Slave zu einem anderen Weiterleitbar sind und/oder eine Masterfunktion übergebbar ist.

16. Datenverarbeitungssystem nach vorstehendem Anspruch 15, wobei ein Master eine sichere Steuerung und/oder Teil eines Systemkopplers ist.

17. Datenverarbeitungssystem nach einem der vorstehenden Ansprüche 13 bis 16, ferner gekennzeichnet dadurch, dass jeder Teilnehmer wenigstens eine Watchdogzeit erhält.

18. Datenverarbeitungssystem nach einem der vorstehenden Ansprüche 13 bis 17, wobei Teilnehmer mit und ohne Zeitinformation am gleichen Bus, insbesondere einem Ringbus, gemischt vorliegen.

19. Datenverarbeitungssystem nach einem der vorstehenden Ansprüche 13 bis 18, wobei wenigstens einem Teilnehmer eine intelligente Einheit mit Treiber-artigen Mitteln zur Erzeugung wechselnder Aktualitätsparameter zugeordnet ist, die eindeutig und/oder in festen Zeit- und/oder Zyklusstrukturen über einen definierbaren Zeitraum zur Verfügung stehen.

20. Datenverarbeitungssystem nach einem der vorstehenden Ansprüche 13 bis 19, wobei zumindest ein Aktualitätsparameter erzeugender Teilnehmer und/oder Ausgangsteilnehmer eine den Aktualitätsparameter auswertende Einheit aufweist.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

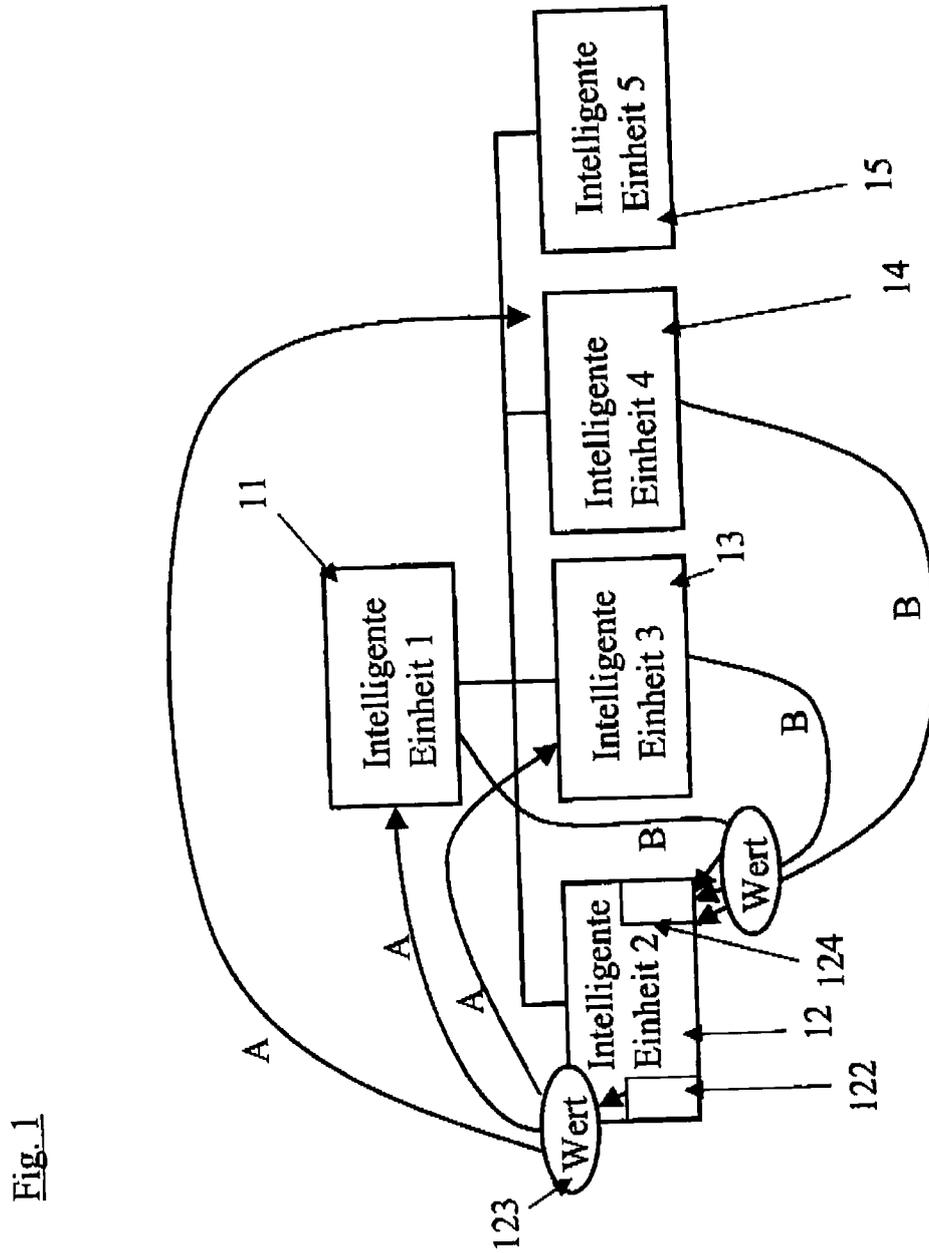


Fig. 1

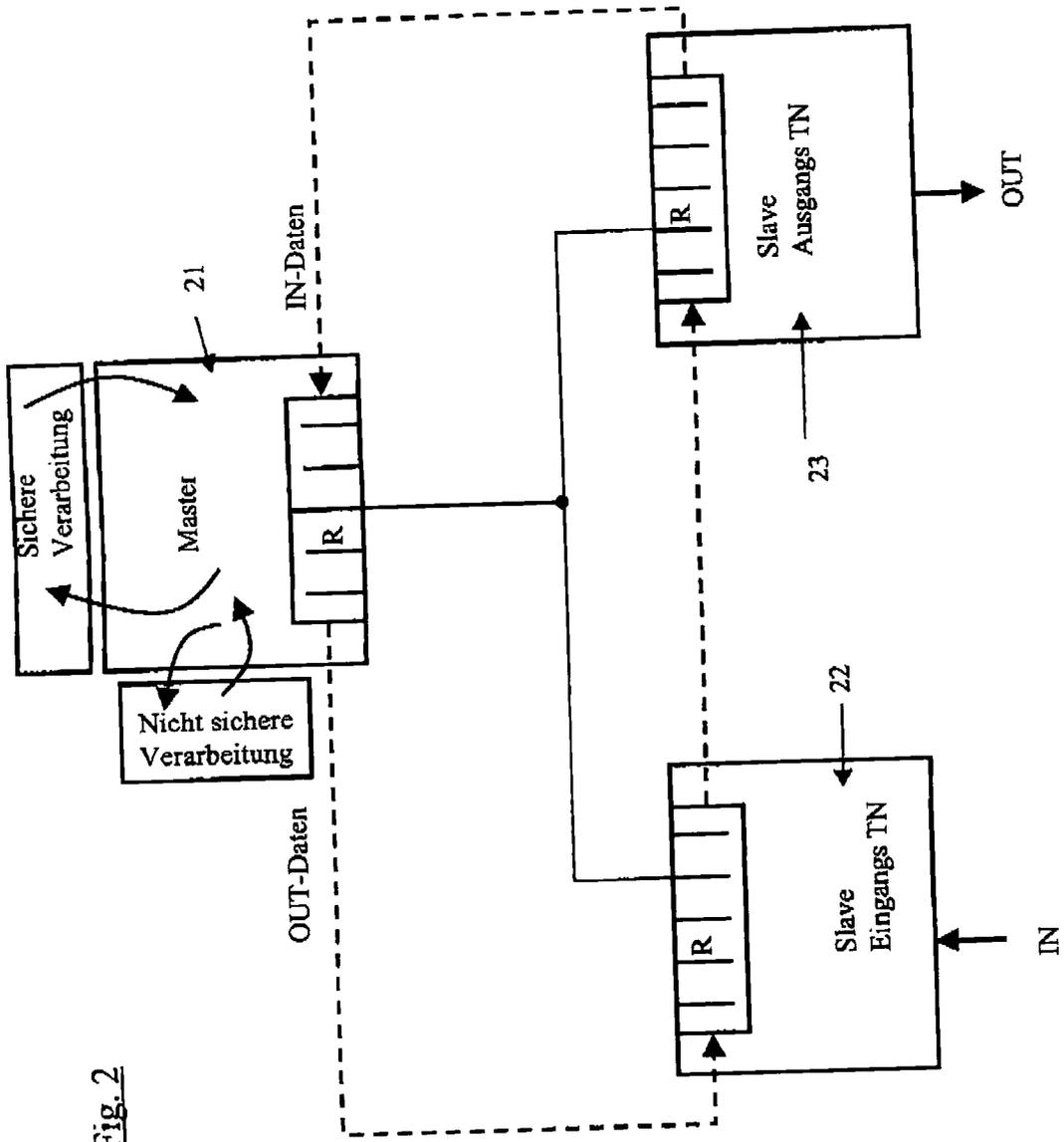


Fig. 2

Fig. 3

