(19) österreichisches patentamt

(10) **AT 509 700 A1 2011-10-15**

(12) # Österreichische Patentanmeldung

(21) Anmeldenummer: A 557/2010
(22) Anmeldetag: 07.04.2010
(43) Veröffentlicht am: 15.10.2011

(51) Int. Cl. : ***H04L 12/58*** (2006.01)
G06F 11/20 (2006.01)
H04L 12/40 (2006.01)

(56) Entgegenhaltungen:
US 2003065974 A1
US 6639895 B1
WO 2003028258 A1

(73) Patentanmelder:
FTS - COMPUTERTECHNIK GMBH
A-1040 WIEN (AT)

(72) Erfinder:
BAUER GÜNTHER
WIEN (AT)
POLEDNA STEFAN
KLOSTERNEUBURG (AT)
STEINER WILFRIED
ZISTERSDORF (AT)

(54) **VERFAHREN UND APPARAT ZUR FEHLERTOLERANTEN ZEITGESTEUERTEN ECHTZEITKOMMUNIKATION**

(57) Die vorliegende Erfindung hat zum Ziel in einem fehlertoleranten Kommunikationssystem eines verteilten Echtzeitsystems eine fehlertolerante globale Zeit aufzubauen. Zu diesem Zweck wird eine fehlertolerante Nachrichtenvermittlungseinheit (200) vorgestellt, die aus vier unabhängigen Vermittlungseinheiten (211, 212, 213, 214) besteht. Diese vier unabhängigen Vermittlungseinheiten (211, 212, 213, 214) bauen gemeinsam eine fehlertolerante Zeit auf. Die Endsysteme (221, 222) werden über zwei unabhängige fail-silent Kommunikationskanäle (251, 252, 253, 254) an eine fehlertolerante Nachrichtenvermittlungseinheit 200 angebunden, so dass selbst bei Ausfall eines Teils der fehlertoleranten Vermittlungseinheit (200) oder eines Kommunikationskanals die Uhrensynchronisation und die Netzwerkverbindungen aufrecht bleiben.

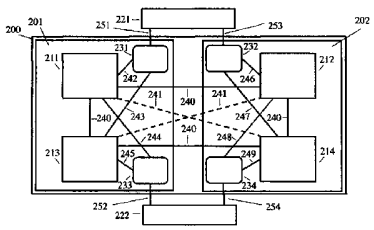

FIG. 2

AT 509 700 A1 2011-10-15

ZUSAMMENFASSUNG

Die vorliegende Erfindung hat zum Ziel in einem fehlertoleranten Kommunikationssystem eines verteilten Echtzeitsystems eine fehlertolerante globale Zeit aufzubauen. Zu diesem Zweck wird eine *fehlertolerante Nachrichtenvermittlungseinheit* vorgestellt, die aus vier unabhängigen Vermittlungseinheiten besteht. Diese vier unabhängigen Vermittlungseinheiten bauen gemeinsam eine fehlertolerante Zeit auf. Die Endsysteme werden über zwei unabhängige *fail-silent* Kommunikationskanäle an eine fehlertolerante Nachrichtenvermittlungseinheit angebunden, so dass selbst bei Ausfall eines Teils der fehlertoleranten Vermittlungseinheit oder eines Kommunikationskanals die Uhrensynchronisation und die Netzwerkverbindungen aufrecht bleiben..

Einreichkopie, 7. April, 2010

Verfahren und Apparat zur fehlertoleranten zeitgesteuerten Echtzeitkommunikation

Zitierte Patente

[1] EP 1 512 254 vom 10.5.2005: Zeitgesteuertes (Time-Triggered (TT)) Ethernet.

[2] EP 2 145 431 vom 07.04.2008: Kommunikationsverfahren und Apparat zur effizienten und sicheren Übertragung von TT-Ethernet Nachrichten.

[3] US 7,334,014 vom 19.02.2008: Consistent time service for fault-tolerant distributed systems.

[4] US 7,649,912 vom 19.01.2010: Time synchronization, deterministic data delivery and redundancy for cascaded nodes on full duplex Ethernet networks

Sonstige Literatur:

[5] Kopetz, H. (1997). *Real-Time Systems, Design Principles for Distributed Embedded Applications; ISBN: 0-7923-9894-7*. Boston. Kluwer Academic Publishers.

TECHNISCHES UMFELD

Diese Erfindung betrifft ein Verfahren und einen Apparat zur fehlertoleranten zeitgesteuerten Kommunikation und zum Aufbau einer fehlertoleranten globalen Zeit von bekannter Präzision im Kommunikationssystem eines verteilten Echtzeitcomputersystems.

HINTERGRUND DIESER ERFINDUNG

Ein verteiltes Echtzeitsystem besteht aus einer Anzahl von Rechnerknoten, den *Endsystemen*, in denen die Applikationssoftware abläuft und einem generischen Kommunikationssystem, über das die Nachrichten der Endsysteme untereinander ausgetauscht werden. In verteilten Echtzeitsystemen muss eine globale fehlertolerante Zeitbasis von guter Präzision aufgebaut werden, damit die Endsysteme die zeitliche Gültigkeit der Echtzeitinformation überprüfen können und synchronisierte verteilte Aktionen ausführen können. Der Aufbau einer fehlertoleranten globalen Zeitbasis erfordert die Ausführung aufwendige Synchronisationsalgorithmen. Um die Endsysteme von diesen Synchronisationsaufgaben zu entlasten, wird erfindungsgemäß die verteilte fehlertolerante Uhrensynchronisation im generischen Kommunikationssystem vorgenommen, so dass die Endsysteme über eine einfache fehlertolerante *Master-*

Slave Synchronisation (siehe Lehrbuch [5], Kapitel 3) mit der globalen Zeit versorgt werden können.

Viele der bekannten Verfahren der Uhrensynchronisation, wie z.B. die in den zitierten Patenten [1]-[4] veröffentlichen Verfahren, verwenden die Uhren der Endsysteme, um eine globale Zeit aufzubauen. Um dies zu erreichen, müssen in den Endsystemen aufwendige Synchronisationsalgorithmen ausgeführt werden. Entsprechend der vorliegenden Erfindung wird eine fehlertolerante Zeit nicht in den Endsystemen, sondern innerhalb des Kommunikationssystems aufgebaut. Zu diesem Zweck wird eine fehlertoleranter Vermittlungseinheit (*fehlertoleranter Switch*) vorgestellt, die vier unabhängige Vermittlungseinheiten enthält, wobei jede Vermittlungseinheit eine autonome Fehlereindämmungseinheit (*Fault-Containment Unit—FCU*) bildet. Diese vier Vermittlungseinheiten bauen gemeinsam durch den Austausch von Nachrichten eine fehlertolerante Zeitbasis auf. Jeweils zwei der vier Vermittlungseinheiten bilden ein *Switchpaar*, so dass in der fehlertoleranten Vermittlungseinheit zwei Switchpaare enthalten sind. Jede der beiden Vermittlungseinheiten eines Switchpaares sendet periodisch je eine Synchronisationsnachricht an einen Vergleicher, der eine Synchronisationsnachricht nur dann an ein Endsystem weiterleitet, wenn beide empfangene Synchronisationsnachrichten nahezu gleichzeitig eintreffen und inhaltlich identisch sind. Da sich in der fehlertoleranten Vermittlungseinheit zwei Switchpaare befinden, wird durch dieses Verfahren ein beliebiger Fehler in einem Switchpaar tolerieret.

Der genaue Ablauf des neuen Verfahrens zur fehlertoleranten Kommunikation und fehlertoleranten Uhrensynchronisation wird im folgenden Abschnitt anhand der Abbildungen genau beschrieben.

ZUSAMMENFASSUNG

Die vorliegende Erfindung hat zum Ziel in einem fehlertoleranten Kommunikationssystem eines verteilten Echtzeitsystems eine fehlertolerante globale Zeit aufzubauen. Zu diesem Zweck wird eine *fehlertolerante Nachrichtenvermittlungseinheit* vorgestellt, die aus vier unabhängigen Vermittlungseinheiten besteht. Diese vier unabhängigen Vermittlungseinheiten bauen gemeinsam eine fehlertolerante Zeit auf. Die Endsysteme werden über zwei unabhängige *fail-silent* Kommunikationskanäle an eine fehlertolerante Nachrichtenvermittlungseinheit angebunden, so dass selbst bei Ausfall eines Teils der fehlertoleranten Vermittlungseinheit oder eines Kommunikationskanals die Uhrensynchronisation und die Netzwerkverbindungen aufrecht bleiben.

KURZE BESCHREIBUNG DER ABBILDUNGEN

Das vorab beschriebene Ziel und andere neue Eigenschaften der vorliegenden Erfindung werden an Hand der angeführten Abbildungen erläutert.

Fig. 1 zeigt ein Beispiel für die Struktur fehlertoleranten Kommunikationssystems, das aus mehreren fehlertoleranten Vermittlungseinheiten besteht.

Fig. 2 zeigt den inneren Aufbau einer fehlertoleranten Vermittlungseinheit.

BESCHREIBUNG EINER REALISIERUNG

Im folgenden Abschnitt wird eine mögliche Realisierung des neuen Verfahrens an einem Beispiel mit drei Switches und einer Anzahl von Endsystemen gezeigt. Dieses Beispiel zeigt eine konkrete von vielen möglichen Realisierungen des in den Patentansprüchen beschriebenen Verfahrens.

Fig. 1 zeigt eine Konfiguration mit drei fehlertoleranten Vermittlungseinheiten **101**,**102** und **103**—im folgenden *Switches* genannt—und acht Endsystemen **111** bis **118**. Ein *Endsystem* ist ein *Knotenrecher*, in dem ein Teil einer verteilten Echtzeitapplikation abläuft. Die drei Switches **101**, **102** und **103** sind untereinander mittels jeweils zwei Kommunikationskanäle **121** und **122** verbunden, da der Ausfall eines Kommunikationskanals toleriert werden muss. Jeder Switch, z.B., der Switch **101** beinhaltet zwei Switchpaare, **151** und **152**, wobei jedes Switchpaar aus zwei Switches besteht. Jeder Switch bildet eine autonome Fehlereindämmungseinheit (*Fault-Containment Unit—FCU*). Das Endsystem **111** ist über den Kommunikationskanal **121** mit dem linken Switchpaar **151** und über den Kommunikationskanal **122** mit dem rechten Switchpaar **152** des fehlertoleranten Switches **101** verbunden. Analog sind die anderen Endsysteme **112** bis **118** über jeweils einen Kommunikationskanal mit dem einen Switchpaar und mit dem anderen Kommunikationskanal mit dem anderen Switchpaar eines fehlertoleranten Switches verbunden.

Fig. 2 zeigt den inneren Aufbau eines fehlertoleranten Switches. Die Anzahl n der Endsysteme, die an einem Switch angeschlossen werden können, wird durch diese Erfindung nicht fest gelegt und hängt von dem konkreten Aufbau des fehlertoleranten Switches ab. Typischerweise liegt n zwischen 8 und 16. Zum Beispiel lassen sich im fehlertoleranten Switch **101** auf der oberen und unteren Seite jeweils vier Endsysteme anschließen. Um die Fig. 2 zu vereinfachen sind im fehlertoleranten Switch **200** nur zwei Endsysteme, das Endsystem **221** und das Endsystem **222** angeführt.

Der fehlertolerante Switch **200** besteht aus den beiden Switchpaaren **201** und **202**. Das Switchpaar **201** besteht aus den beiden (nicht fehlertoleranten) Switches **211** und **213** sowie den Vergleichern **231** und **233**. Das Switchpaar **202** besteht aus den beiden (nicht fehlertoleranten) Switches **212** und **214** sowie den Vergleichern **232** und **234**. Jedem Endsystem sind somit zwei Vergleicher zugeordnet, einer vom rechten und

einer vom linken Switchpaar. Erfindungsgemäß können die Vergleicher auch *multiplexed* werden, so dass sich je ein Vergleicher mit ***n*** Ein/Ausgängen **251** bzw. **252** zu ***n*** Endsystemen **221** bzw. **222** in einem Switchpaar befindet. Jeder der vier Switches **211**, **212**, **213**, und **214** bildet eine autonome Fehlereindämmungseinheit (*Fault Containment Unit*). Die vier Switches **211**, **212**, **213**, und **214** sind über die Kommunikationskanäle **240** und **241** miteinander verbunden. Über diese Kommunikationskanäle **240** und **241** werden periodisch interne Synchronisationsnachrichten ausgetauscht, um eine interne globale fehlertolerante Zeit mit der bekannten Präzision ***P*** aufzubauen. Dies geschieht mittels eines fehlertoleranten nachrichtenbasierten Uhrensynchronisationsalgorithmus für die interne Uhrensynchronisation, wie er z.B. in Kapitel 3 des Lehrbuchs [5] erklärt ist. Wenn die internen Synchronisationsnachrichten mit einer elektronischen Unterschrift des Senders ausgestattet werden, so sind erfindungsgemäß die beiden Verbindungen **241** nicht erforderlich. In sicherheitskritischen Applikation ist es vorteilhaft die beiden Switchpaare **201** und **202**, die einen fehlertoleranten Switch bilden, räumlich entfernt anzuordnen, damit Fehler die an einem Ort im Raum auftreten (*spatial proximity faults*) toleriert werden können. In einem solchen Fall ist es vorteilhaft, wenn die Anzahl der Verbindungsleitungen zwischen den Switchpaaren auf die beiden Kanäle **240** reduziert wird.

Ein ausgewählter Switch, z.B., Switch **103** in Fig. 1, oder ein Endsystem das mit einer Zeitquelle, z.B. einen GPS Zeitempfänger ausgerüstet ist, kann an die angeschlossenen Switches eine externe Zeitbasis vorgeben. Dies geschieht über *externe Synchronisationsnachrichten*, die die externe Zeit enthalten. Nach dem Empfang einer solchen externen Synchronisationsnachricht muss der empfangende fehlertolerante Switch seine interne Uhrensynchronisation an die extern vorgegebene Zeit anpassen. Wenn die externe Zeitquelle ausfällt, so hält der fehlertolerante interne Synchronisationsalgorithmus die globale Zeit aufrecht. Die externe Zeitquelle kann auch benutzt werden, um den Uhrengang der Switches **211**, **212**, **213**, und **214** dynamisch an den Gang der externen Zeit anzupassen.

Wenn das Endsystem **221** eine Nachricht an das Endsystem **222** zu senden beabsichtigt, so wird diese Nachrichte parallel über den Kommunikationskanal **251** an den Vergleicher **231** im Switchpaar **201** und über den Kommunikationskanal **253** an den Vergleicher **232** im Switchpaar **202** gesendet. Das Format dieser Nachricht kann einem gegeben Standard entsprechen, z.B. dem weit verbreiteten Ethernet Standard oder dem AFDX Standard, aber auch jedem anderen Standard der vorgibt, dass die Adressinformation im *Header* der Nachricht enthalten sein muss damit die Nachrichten von den Switches **211**, **212**, **213**, und **214** im schnellen *cut-through* Verfahren vermittelt werden können.

Die Nachrichten können vom Endsystem **221** zeitgesteuert, bandbreitenbegrenzt oder ereignisgesteuert gesendet werden. Bei zeitgesteuerten Nachrichten können die Switches **211**, **212**, **213**, und **214** *a priori* mit *Planungsinformationen* versorgt werden, die die erlaubten Zeitpunkte des Sendens einer zeitgesteuerten Nachricht von einem Endsystem vorgeben. Eine zu einem falschen Zeitpunkt vom Endsystem **221** gesendete zeitgesteuerte Nachricht kann dann von den Switches **211**, **212**, **213**, und **214** erkannt und verworfen werden. Bei bandbreitenbegrenzten Nachrichten können die Switches **211**, **212**, **213**, und **214** *a priori* mit Planungsinformationen versorgt werden, die die erlaubte Bandbreite des Sendens von bandbreitenbegrenzten Nachrichten vorgeben. Wenn die vom Endsystem **221** gesendete

bandbreitenbegrenzten Nachrichten über die erlaubte Bandbreite hinausgehen, können die Switches **211**, **212**, **213**, und **214** die Annahme von weiteren Nachrichten verweigern.

Die *a priori Planungsinformationen*, die an die Switches **211**, **212**, **213**, und **214** vor der Durchführung einer Nachrichtenübertragung von einem Entwurfssystem zur gesendet werden, können mit einer elektronischen Unterschrift versehen werden, so dass die Switches **211**, **212**, **213**, und **214** überprüfen können, ob diese Informationen von einem autorisierten Entwurfssystem stammen. Alternativ können die Planungsinformationen verschlüsselt gesendet werden. Die a priori Planungsinformationen können während des Betriebs durch das Senden einer neuen Nachricht mit den neuen Planungsinformationen und dem Zeitpunkt, ab wann diese neue Planungsinformationen anzuwenden sind, dynamisch geändert werden.

Im folgenden wird die Nachrichtenbearbeitung im Switchpaar **201** genau beschrieben. Eine vom Kommunikationskanal **251** im Vergleicher **231** eintreffende Nachricht wird vom Vergleicher **231** über den Kommunikationskanal **242** an den Switch **211** und über den Kommunikationskanal **243** an den Switches **213** zur Vermittlung weitergeleitet. Aufgrund der im *Header* einer Nachricht enthaltenen Adressinformation wird die Nachricht vom Switch **211** über den Kommunikationskanal **244** und vom Switch **213** über den Kommunikationskanal **245** an den adressierten Vergleicher—im Beispiel an den Vergleicher **233**—weitergeleitet. Sobald die zeitlich erste an den Vergleicher **233** adressierte Nachricht von einem der beiden Switches **211** oder **213** beim Vergleicher **233** eintrifft, eröffnet der Vergleicher **233** ein Zeitfenster von der *a priori* vorgegebenen Dauer ***D***. Wenn innerhalb dieses Zeitfensters ***D*** die zeitlich zweite Nachricht vom anderen Switch des Switchpaares **201** nicht eintrifft, verwirft der Vergleicher die erste Nachricht und in der Folge auch die zweite Nachricht (falls sie jemals eintrifft). Wenn innerhalb dieses Zeitfensters ***D*** die zweite Nachricht vom anderen Switch des Switchpaares **201** eintrifft, dann vergleicht der Vergleicher **233** die beiden Nachrichten bitweise und leitet sie umgehend über den Kommunikationskanal **252** an das adressierte Endsystem **222** weiter. Dieser Vergleich der beiden Nachrichten kann im *error-free-cut-through* Verfahren erfolgen, d.h. die eintreffenden Bitströme werden im Vergleicher **233** nur kurz verzögert, laufend verglichen und sofort weitergeleitet falls der Bitvergleich richtig ist. Im Fehlerfall wird der Bitstrom zum Endsystem **222** abgebrochen. Da jede Nachricht ein CRC Feld enthält, kann das Endsystem **222** eine abgebrochene Nachricht erkennen und verwerfen.

Die Dauer der notwendigen Verzögerung einer Nachricht im Vergleicher **233** hängt von der Präzision ***P*** der Uhrensynchronisation ab, die im wesentlichen von der Dauer der Synchronisationsperiode und der Qualität der verwendeten Oszillatoren bestimmt wird. Die Anzahl der Bits, die im Vergleicher gespeichert werden müssen, hängt von der Präzision ***P*** und der Bandbreite der Datenübertragung ab.

Die Vergleicher **231**, **232**, **233**, und **234** sind so ausgelegt, dass keine vollständige Nachricht in einem Vergleicher gespeichert werden kann und kein Vergleicher über die Informationen verfügt, wie ein korrektes CRC Feld einer Nachricht zu bilden ist. Es ist somit äußerst unwahrscheinlich, dass ein fehlerhafter Vergleicher eine *syntaktische korrekte aber inhaltlich falsche Nachricht* erzeugen kann oder eine *syntaktische korrekte aber inhaltlich falsche Nachricht* zu einem anderen als vom Switch **211** oder **212** produzierten Zeitpunkt senden kann. Vom Switchpaar **201** wird somit nur dann eine syntaktisch korrekte Nachricht an das Endsystem **222** über den

Kommunikationskanal **252** weitergeleitet, wenn alle vier Subsysteme **231**, **211**, **213** und **233** fehlerfrei funktionieren und der Nachrichtentransport über die Kanäle **251**, **242**, **243**, **244**, **245**, und **252** fehlerfrei abläuft. Das Switchpaar **201** realisiert somit am Kommunikationskanal **252** die *fail-silent Abstrakion*: es produziert entweder Nachrichten die im Wertebereich und im Zeitbereich richtig sind oder es produziert keine Nachrichten. Das Switchpaar **202** funktioniert analog zum Switchpaar **201**.

Zusätzlich zu den von den Endsystemen empfangen Nachrichten sendet der fehlertolerante Switch **200** periodisch zwei intern generierte Synchronisationsnachrichten an alle angeschlossenen Endsystemen, wobei nahezu gleichzeitig eine Synchronisationsnachricht vom linken Switchpaar **201** über den Kommunikationskanal **251** und **252** und eine zweite Synchronisationsnachricht vom rechten Switchpaar über den Kommunikationskanal **253** und **254** gesendet wird. Der Zeitpunkt des Eintreffens einer Synchronisationsnachricht bei einem Endsystem entspricht jenem Zeitpunkt, der im Datenfeld der Synchronisationsnachricht enthalten ist. Da die Signallaufzeiten auf den Kommunikationskanälen **251**, **252**, **253** und **254** aufgrund der unterschiedlichen Länge diese Signallaufzeiten auf den Kommunikationskanäle unterschiedlich sind, kann eine Korrektur des Eintreffenszeitpunkts eine Synchronisationsnachricht beim Endsystem erforderlich werden. Diese Korrektur kann entweder im Endsystem oder in den Switchpaaren **201** und **202** erfolgen.

Im fehlerfreien Fall erhält das Endsystem **222** somit zwei richtige Synchronisationsnachrichten, eine über den Kommunikationskanal **252** und die andere über den Kommunikationskanal **254**, deren Eintreffenszeitpunkte sich maximal um die Präzision ***P*** unterscheiden. Wenn in einem Switchpaar ein Fehler auftritt, so erhält das Endsystem **222** noch immer eine richtige Synchronisationsnachricht.

WIRTSCHAFTLICHE VORTEILE

Die vorliegende Erfindung ermöglicht es mit Standardkomponenten, d.h., Komponenten die nicht die *self-checking* Eigenschaft besitzen, eine fehlertolerante Zeitbasis und einen fehlertoleranten Switch aufzubauen, der ***einen beliebigen Fehler*** in einer Fehlereindämmungseinheit (*Fault-Containment Unit—FCU*) toleriert. In Fig. 2 sind folgende Subsysteme *Fehlereindämmungseinheiten*: die vier Switches **211**, **212**, **213**, und **214** und die vier Vergleicher **231**, **232**, **233** und **234**. Besonderes Augenmerk verdient das letzte Subsystem, der Vergleicher, der vor der Ausgabe einer Nachricht an das Endsystem angeordnet ist. Durch die beschriebenen Konstruktionsmaßnahmen kann ausgeschlossen werden, dass ein fehlerhafter Vergleicher eine syntaktisch korrekte aber inhaltlich falsche Nachricht produziert, obwohl der Vergleicher selbst nicht als *self-checking Checker* ausgeführt werden muss.

Durch den erfindungsgemäßen Aufbau eines fehlertoleranten Switches, der eine fehlertolerante Uhrensynchronisation beinhaltet, ergeben sich folgende weitere wesentliche wirtschaftliche Vorteile:

- Es wird verhindert, dass im Fehlerfall falsche Ergebnisse produziert werden. Diese Eigenschaft ist in sicherheitskritischen Systemen von besonderer Wichtigkeit.
- Durch die Tolerierung eines Fehlers wird die Zuverlässigkeit eines fehlertoleranten Switches im Vergleich mit einem nicht-fehlertoleranten Switch wesentlich verbessert.
- Der Uhrensynchronisationsalgorithmus muss nur einmal entwickelt, getestet und zertifiziert und kann in einer Vielzahl von Anwendungen eingesetzt werden.
- Durch die Verlagerung der fehlertoleranten Uhrensynchronisation von den Endsystemen in das Kommunikationssystem werden die Endsysteme wesentlich einfacher und kostengünstiger.
- Eine generische Lösung der Uhrensynchronisation im Kommunikationssystem kann in einem VLSI Chip sehr kostengünstig implementiert werden.

PATENTANSPRÜCHE

(1) Verfahren zur fehlertoleranten Uhrensynchronisation und zur fehlertoleranten zeitgesteuerten Echtzeitkommunikation unter Verwendung einer Anzahl von Endsystemen und einem oder mehreren fehlertoleranten Switches die je über mindesten zwei Kommunikationskanäle verbunden sind **dadurch gekennzeichnet dass** jeder fehlertoleranten Switch **200** zwei Switchpaare **201** und **202** enthält und wo das Switchpaar **201** die Switches **211** und **213** enthält und wo das Switchpaar **202** die Switches **212** und **214** enthält, und wo jeder der vier Switches **211, 212, 213** und **214** über die Kommunikationskanäle **240** und **241** mit den anderen drei Switches verbunden ist, und wo die vier Switches über einen bekannten nachrichtenbasierten internen fehlertoleranten Synchronisationsalgorithmus über die Kommunikationskanäle **240** und **241** eine interne globale fehlertolerante Zeitbasis mit bekannter Präzision ***P*** aufbauen, und wo eine Vielzahl von Endsystemen jeweils über einen einem Endsystem zugeordnete Vergleicher an die beiden Switchpaare **201** und **202** angeschlossen werden kann, und wo ein Endsystem **221** jeweils eine Kopie einer an ein Endsystem zu sendenden Nachricht über den Kommunikationskanal **251** an das Switchpaar **201** und über den Kommunikationskanal **253** an das Switchpaar **202** sendet und wo der Vergleicher **231** die eintreffende Nachricht über den Kommunikationskanal **242** an den Switch **211** und über den Kommunikationskanal **243** an den Switch **213** sendet und wo der Vergleicher **232** die eintreffende Nachricht über den Kommunikationskanal **246** an den Switch **212** und über den Kommunikationskanal **247** an den Switch **214** sendet und wo die vier Switches die eintreffenden Nachrichten vermitteln und falls eine Nachricht an das Endsystem **222** adressiert ist die Switches **211** und **213** je eine Kopie der Nachricht über die Kommunikationskanäle **244** und **245** an den dem Endsystem **222** zugeordneten Vergleicher **233** senden und wo der Vergleicher **233** unmittelbar nach Eintreffen der zeitlich ersten Nachricht ein Zeitfenster von der Dauer ***D*** öffnet und falls in diesem Intervall ***D*** keine zweite Kopie dieser Nachricht beim Vergleicher **233** eintrifft der Vergleicher **233** die Nachricht verwirft und falls in diesem Intervall ***D*** eine zweite Kopie der Nachricht eintrifft der Vergleicher **233** die beiden Nachrichten bitweise vergleicht und falls der Vergleich einen Bitfehler offenbart die Nachrichtenübertragung unterbricht und die Nachricht verwirft und falls alle Bits dieser Nachricht identisch sind, die vollständige Nachricht über den Kommunikationskanal **252** an das Endsystem **222** sendet und wo das Switchpaar **202** analog vorgeht und somit im fehlerfreien Fall beim Endsystem zwei überprüfte Kopien einer Nachricht eintreffen und falls eines der beiden Switchpaare **201** oder **202** fehlerhaft ist oder einen Fehler erkennt und die Nachricht verwirft noch immer eine korrekte Nachricht beim Endsystem **222** eintrifft und wo der fehlertolerante Switch **200** zusätzlich zu den von den Endsystemen empfangen Nachrichten periodisch zwei im Switch **200** generierte Synchronisationsnachrichten an alle angeschlossenen Endsysteme sendet, wobei eine Synchronisationsnachricht vom Switchpaar **201** gesendet wird und die andere Synchronisationsnachricht vom Switchpaar **202** gesendet

wird, und wo der Zeitpunkt des Eintreffens einer Synchronisationsnachricht bei einem Endsystem dem Zeitpunkt entspricht, der im Datenfeld der Synchronisationsnachricht enthalten ist.

(2) Verfahren nach Anspruch (1) **dadurch gekennzeichnet dass** die beiden Switchpaare **201** und **202** räumlich getrennt voneinander angeordnet sind.

(3) Verfahren nach einem oder mehreren der Ansprüche (1) bis (2) **dadurch gekennzeichnet dass** im Rahmen der Uhrensynchronisation signierte Nachrichten verwendet werden und daher auf die beiden Kommunikationskanäle **241** verzichtet werden kann.

(4) Verfahren nach einem oder mehreren der Ansprüche (1) bis (3) **dadurch gekennzeichnet dass** im ein fehlertoleranter Switch nach dem Empfang einer externen Synchronisationsnachricht seine interne synchronisierte Zeit an die durch die externe Synchronisationsnachricht vorgegebene Zeit anpasst.

(5) Verfahren nach einem oder mehreren der Ansprüche (1) bis (4) **dadurch gekennzeichnet dass** die Switches **211, 212, 213** und **214** die Nachrichten nur um einige Bitlängen verzögern und im *cut-through* Verfahren an die Vergleicher **231, 232, 233,** und **234** übermitteln.

(6) Verfahren nach einem oder mehreren der Ansprüche (1) bis (5) **dadurch gekennzeichnet dass** die Vergleicher **231, 232, 233** und **234** die Nachrichten nur um einige Bitlängen verzögern und im *error-free-cut-through* Verfahren an das Endsystem übermitteln.

(7) Verfahren nach einem oder mehreren der Ansprüche (1) bis (6) **dadurch gekennzeichnet dass** die an einen fehlertoleranten Switch angeschlossenen Endsysteme eine Mischung von ereignisgesteuerten, bandbreitenbegrenzten, oder zeitgesteuerten Nachrichten senden.

(8) Verfahren nach einem oder mehreren der Ansprüche (1) bis (7) **dadurch gekennzeichnet dass** in die Switches **211, 212, 213** und **214** *a priori* Planungsinformationen über das erlaubte zeitliche Verhalten der Endsysteme geladen werden, so dass ein Switch ein fehlerhaftes zeitliches Verhalten eines Endsystems erkennen kann.

(9) Verfahren nach einem oder mehreren der Ansprüche (1) bis (8) **dadurch gekennzeichnet dass** die in Anspruch (8) angeführten a priori Planungsinformationen an den Switch mit einer elektronischen Unterschrift des Senders versehen werden.

(10) Verfahren nach einem oder mehreren der Ansprüche (1) bis (9) **dadurch gekennzeichnet dass** die in Anspruch (8) angeführten a priori Planungsinformationen an den Switch verschlüsselt werden.

(11) Verfahren nach einem oder mehreren der Ansprüche (1) bis (10) **dadurch gekennzeichnet dass** die in Anspruch (7) angeführten a priori Planungsinformationen dynamisch während des Betriebes geändert werden können.

(12) Verfahren nach einem oder mehreren der Ansprüche (1) bis (11) **dadurch gekennzeichnet dass** die Vergleicher **231, 232, 233,** und **234** im Multiplex-Verfahren betrieben werden.

(13) Verfahren nach einem oder mehreren der Ansprüche (1) bis (12) **dadurch gekennzeichnet dass** die unterschiedlichen Signallaufzeiten auf den Kommunikationskanälen **251, 252, 253** und **254** von den Switchpaaren **201** und **202** kompensiert werden.

(14) Verfahren nach einem oder mehreren der Ansprüche (1) bis (13) **dadurch gekennzeichnet dass** die von den Endsystemen produzierten und konsumierten Nachrichten dem Ethernet Standard entsprechen.

(15) Apparat zur fehlertoleranten zeitgesteuerten Echtzeitkommunikation bestehend aus einem oder mehreren fehlertoleranten Switches die je über mindesten zwei Kommunikationskanäle verbunden sind **dadurch gekennzeichnet dass** jeder fehlertoleranten Switch **200** zwei Switchpaare **201** und **202** enthält und wo das Switchpaar **201** die Switches **211** und **213** enthält und wo das Switchpaar **202** die Switches **212** und **214** enthält, und wo jeder der vier Switches **211, 212, 213** und **214** über die Kommunikationskanäle **240** und **241** mit den anderen drei Switches verbunden ist, und wo eine Vielzahl von Endsystemen jeweils über ein dem Endsystem zugeordnetes dediziertes Vergleicher an die beiden Switchpaare **201** und **202** angeschlossen werden kann, und wo in diesem Apparat einer oder mehrere der in Anspruch (1) bis (14) angeführten Verfahrenschritte realisiert werden.

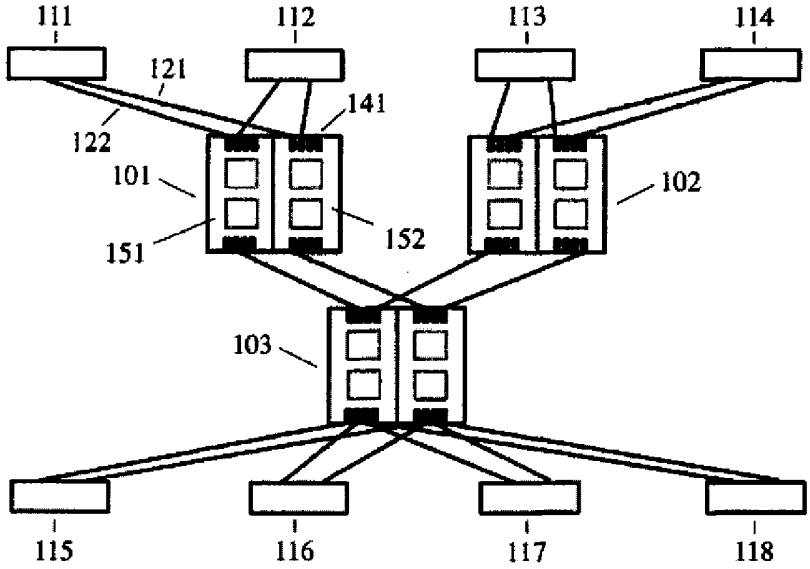
111
112
113
114
121
122
141
101
102
151
152
103
115
116
117
118

FIG. 1

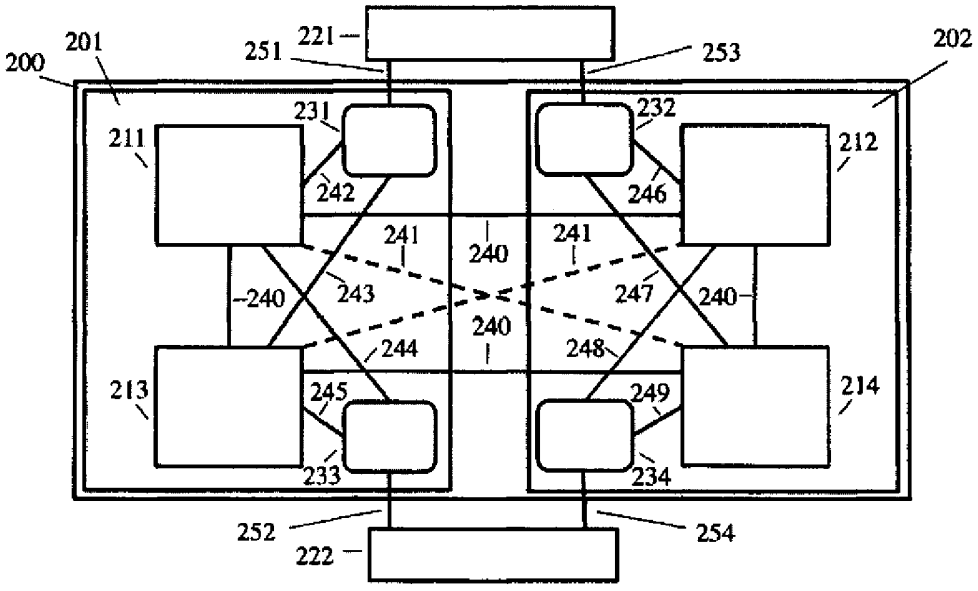
200
201
251
221
253
202
231
232
211
212
242
246
241
240
241
240
243
247
240
240
244
248
213
245
249
214
233
234
252
254
222

FIG. 2

PATENTANSPRÜCHE

(1) Verfahren zur fehlertoleranten Uhrensynchronisation und zur fehlertoleranten zeitgesteuerten Echtzeitkommunikation unter Verwendung einer Anzahl von Endsystemen (221, 222) und einem oder mehreren fehlertoleranten Switches (200) die je über mindesten zwei Kommunikationskanäle verbunden sind, **dadurch gekennzeichnet, dass** jeder fehlertolerante Switch (**200**) ein erstes (201) und ein zweites Switchpaar (**202**) enthält und wo das erste Switchpaar (**201**) einen ersten (211) und einen zweiten Switch (**213**) enthält und wo das zweite Switchpaar (**202**) einen dritten (212) und einen vierten Switch (**214**) enthält, und wo jeder der vier Switches (**211, 212, 213, 214**) über Kommunikationskanäle (**240, 241**) mit den anderen drei Switches verbunden ist, und wo die vier Switches über einen bekannten nachrichtenbasierten internen fehlertoleranten Synchronisationsalgorithmus über die Kommunikationskanäle (**240, 241**) eine interne globale fehlertolerante Zeitbasis mit bekannter Präzision (***P***) aufbauen, und wo eine Vielzahl von Endsystemen (221, 222) jeweils über einen einem Endsystem zugeordneten Vergleicher an die beiden Switchpaare (**201, 202**) angeschlossen werden kann, und wo ein erstes Endsystem (**221**) jeweils eine Kopie einer an ein Endsystem zu sendenden Nachricht über den ersten Kommunikationskanal (**251**) an das erste Switchpaar (**201**) und über den zweiten Kommunikationskanal (**253**) an das zweite Switchpaar (**202**) sendet und wo der erste Vergleicher (**231**) die eintreffende Nachricht über einen Kommunikationskanal (**242**) an den ersten Switch (**211**) und über einen Kommunikationskanal (**243**) an den zweiten Switch (**213**) sendet und wo der dritte Vergleicher (**232**) die eintreffende Nachricht über einen Kommunikationskanal (**246**) an den dritten Switch (**212**) und über einen Kommunikationskanal (**247**) an den vierten Switch (**214**) sendet und wo die vier Switches die eintreffenden Nachrichten vermitteln und falls eine Nachricht an das zweite Endsystem (**222**) adressiert ist die Switches (**211, 213**) je eine Kopie der Nachricht über Kommunikationskanäle (**244, 245**) an den dem zweiten Endsystem (**222**) zugeordneten zweiten Vergleicher (**233**) senden und wo der zweite Vergleicher (**233**) unmittelbar nach Eintreffen der zeitlich ersten Nachricht ein Zeitfenster von der Dauer ***D*** öffnet und falls in diesem Intervall (***D***) keine zweite Kopie dieser Nachricht beim zweiten Vergleicher (**233**) eintrifft der zweite Vergleicher (**233**) die Nachricht verwirft und falls in diesem Intervall (***D***) eine zweite Kopie der Nachricht eintrifft der zweite Vergleicher (**233**) die beiden Nachrichten bitweise vergleicht und falls der Vergleich einen Bitfehler offenbart die Nachrichtenübertragung unterbricht und die Nachricht verwirft und falls alle Bits dieser Nachricht identisch sind, die vollständige Nachricht über den zweiten Kommunikationskanal (**252**) an das zweite Endsystem (**222**) sendet und wo das zweite Switchpaar (**202**) analog vorgeht und somit im fehlerfreien Fall beim Endsystem zwei überprüfte Kopien einer Nachricht eintreffen und falls eines der beiden Switchpaare (**201, 202**) fehlerhaft ist oder einen Fehler erkennt und die Nachricht verwirft noch immer eine korrekte Nachricht beim zweiten Endsystem (**222**) eintrifft und wo der fehlertolerante Switch (**200**) zusätzlich zu den von den

Endsystemen empfangen Nachrichten periodisch zwei im Switch (**200**) generierte Synchronisationsnachrichten an alle angeschlossenen Endsysteme sendet, wobei eine Synchronisationsnachricht vom ersten Switchpaar (**201**) gesendet wird und die andere Synchronisationsnachricht vom zweiten Switchpaar (**202**) gesendet wird, und wo der Zeitpunkt des Eintreffens einer Synchronisationsnachricht bei einem Endsystem dem Zeitpunkt entspricht, der im Datenfeld der Synchronisationsnachricht enthalten ist.

(2) Verfahren nach Anspruch (1) **dadurch gekennzeichnet dass** die beiden Switchpaare (**201**, **202**) räumlich getrennt voneinander angeordnet sind.

(3) Verfahren nach einem oder mehreren der Ansprüche (1) bis (2) **dadurch gekennzeichnet dass** im Rahmen der Uhrensynchronisation signierte Nachrichten verwendet werden und daher auf die beiden Kommunikationskanäle **241** verzichtet werden kann.

(4) Verfahren nach einem oder mehreren der Ansprüche (1) bis (3) **dadurch gekennzeichnet dass** ein fehlertoleranter Switch (200) nach dem Empfang einer externen Synchronisationsnachricht seine interne synchronisierte Zeit an die durch die externe Synchronisationsnachricht vorgegebene Zeit anpasst.

(5) Verfahren nach einem oder mehreren der Ansprüche (1) bis (4) **dadurch gekennzeichnet dass** die Switches (**211**, **212**, **213**, **214**) die Nachrichten nur um einige Bitlängen verzögern und im *cut-through* Verfahren an die Vergleicher (**231**, **232**, **233**, **234**) übermitteln.

(6) Verfahren nach einem oder mehreren der Ansprüche (1) bis (5) **dadurch gekennzeichnet dass** die Vergleicher (**231**, **232**, **233**, **234**) die Nachrichten nur um einige Bitlängen verzögern und im *error-free-cut-through* Verfahren an das Endsystem übermitteln.

(7) Verfahren nach einem oder mehreren der Ansprüche (1) bis (6) **dadurch gekennzeichnet dass** die an einen fehlertoleranten Switch (200) angeschlossenen Endsysteme (221, 222) eine Mischung von ereignisgesteuerten, bandbreitenbegrenzten, oder zeitgesteuerten Nachrichten senden.

(8) Verfahren nach einem oder mehreren der Ansprüche (1) bis (7) **dadurch gekennzeichnet dass** in die Switches (**211**, **212**, **213**, **214**) *a priori* Planungsinformationen über das erlaubte zeitliche Verhalten der Endsysteme (221, 222) geladen werden, so dass ein Switch ein fehlerhaftes zeitliches Verhalten eines Endsystems erkennen kann.

(9) Verfahren nach Anspruch (8) **dadurch gekennzeichnet dass** die in Anspruch (8) angeführten a priori Planungsinformationen an den Switch mit einer elektronischen Unterschrift des Senders versehen werden.

(10) Verfahren nach Anspruch (8) oder (9) **dadurch gekennzeichnet dass** die in Anspruch (8) angeführten a priori Planungsinformationen an den Switch verschlüsselt werden.

(11) Verfahren nach einem oder mehreren der Ansprüche (8) bis (10) **dadurch gekennzeichnet dass** die in Anspruch (8) angeführten a priori Planungsinformationen dynamisch während des Betriebes geändert werden können.

(12) Verfahren nach einem oder mehreren der Ansprüche (1) bis (11) **dadurch gekennzeichnet dass** die Vergleicher (**231**, **232**, **233**, **234**) im Multiplex-Verfahren betrieben werden.

(13) Verfahren nach einem oder mehreren der Ansprüche (1) bis (12) **dadurch gekennzeichnet dass** die unterschiedlichen Signallaufzeiten auf den Kommunikationskanälen (**251**, **252**, **253**, **254**) von den Switchpaaren (**201**, **202**) kompensiert werden.

(14) Verfahren nach einem oder mehreren der Ansprüche (1) bis (13) **dadurch gekennzeichnet dass** die von den Endsystemen produzierten und konsumierten Nachrichten dem Ethernet Standard entsprechen.

(15) Apparat zur fehlertoleranten zeitgesteuerten Echtzeitkommunikation bestehend aus einem oder mehreren fehlertoleranten Switches die je über mindesten zwei Kommunikationskanäle verbunden sind **dadurch gekennzeichnet dass** jeder fehlertoleranten Switch (**200**) zwei Switchpaare (**201**, **202**) enthält und wo das erste Switchpaar (**201**) einen ersten (211) und einen zweiten Switch (,**213**) enthält und wo das zweite Switchpaar (**202**) einen dritten (212) und einen vierten Switch (,**214**) enthält, und wo jeder der vier Switches (**211**, **212**, **213**, **214**) über die Kommunikationskanäle (**240**, **241**) mit den anderen drei Switches verbunden ist, und wo eine Vielzahl von Endsystemen jeweils über ein dem Endsystem zugeordnetes dediziertes Vergleicher an die beiden Switchpaare (**201**, **202**) angeschlossen werden kann, und wo in diesem Apparat einer oder mehrere der in Anspruch (1) bis (14) angeführten Verfahrenschritte realisiert werden.

Recherchenbericht zu **A 557/2010**

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC: ***H04L 12/58*** (2006.01); ***G06F 11/20*** (2006.01); ***H04L 12/40*** (2006.01)
Klassifikation des Anmeldungsgegenstands gemäß ECLA: H04L 12/58; G06F 11/20C2; H04L 12/40R1A
Recherchierter Prüfstoff (Klassifikation): H04L, G06F
Konsultierte Online-Datenbank: EPODOC, WPI, XPI3E
Dieser Recherchenbericht wurde zu den am 7. April 2010 eingereichten Ansprüchen 1-15 erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
A	US 2003065974 A1 (LAM AN H et al.) 03. April 2003 (03.04.2003) Zusammenfassung; Absatz 25; Ansprüche 1 - 7	1, 15
A	US 6639895 B1 (HELLES MICHAEL A et al.) 28. Oktober 2003 (28.10.2003) Zusammenfassung; Absätze 10 - 12; Ansprüche 1, 9	15
A	WO 2003028258 A1 (SIEMENS AKTIENGESELLSCHAFT) 03. April 2003 (03.04.2003) Zusammenfassung; Seite 3, Zeile 23 - Seite 4, Zeile 26	1

Datum der Beendigung der Recherche:	☐ Fortsetzung siehe Folgeblatt	Prüfer(in): ENGLISCH M.

*) **Kategorien** der angeführten Dokumente:

- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann alleln aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist.
- **A** Veröffentlichung, die den **allgemeinen Stand der Technik** definiert.
- **P** Dokument, das **von Bedeutung** ist (Kategorien **X** oder **Y**), jedoch nach dem **Prioritätstag** der Anmeldung **veröffentlicht** wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein **älteres Recht** hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.