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

(10) **DE 699 35 452 T2** 2007.11.15

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 142 259 B1**
(21) Deutsches Aktenzeichen: **699 35 452.8**
(86) PCT-Aktenzeichen: **PCT/GB99/02125**
(96) Europäisches Aktenzeichen: **99 929 556.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/002345**
(86) PCT-Anmeldetag: **02.07.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **13.01.2000**
(97) Erstveröffentlichung durch das EPA: **10.10.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **07.03.2007**
(47) Veröffentlichungstag im Patentblatt: **15.11.2007**

(51) Int Cl.[8]: ***H04L 29/06*** (2006.01)
H04L 12/28 (2006.01)
H04L 29/08 (2006.01)

(30) Unionspriorität:
91665 P **02.07.1998** **US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Amino Holdings Ltd., Willingham, Cambridge, GB

(74) Vertreter:
Patent- und Rechtsanwälte Böck - Tappe - v.d. Steinen - Weigand, 80538 München

(72) Erfinder:
GILBERT, Martyn, Longstanton Cambridge CB4 5BZ, GB

(54) Bezeichnung: **ELEKTRONISCHE SYSTEMARCHITEKTUR**

Beschreibung

[0001] Diese Erfindung betrifft eine elektronische Systemarchitektur und insbesondere eine elektronische Systemarchitektur für ein verteiltes elektronisches Heimsystem mit einer Verbindung zu einem größeren Netzwerk, wie zum Beispiel ein verteiltes Heimcomputersystem, das mit dem Internet verbunden ist.

[0002] Die Nutzung großer elektronischer Datenübertragungsnetze nimmt stetig zu. Das bedeutendste und am häufigsten genutzte Netzwerk ist allgemein das Internet, insbesondere für Privatnutzer und Kleingewerbetreibende. Es gibt aber auch andere Netzwerke, wie zum Beispiel Firmen- oder Regierungsnetzwerke und Nahbereichsnetze, die Nutzer an einem einzelnen Standort oder in einem einzelnen Bürogebäude verbinden. Solche Privat- oder Nahbereichsnetze sind oft selbst mit Verbindungen zum Internet versehen.

[0003] Derzeit werden eine zunehmende Zahl von Diensten über das Internet und andere Netzwerke erbracht oder zur Erbringung angeboten. Des Weiteren kommen zahlreiche Geräte auf den Markt, die dafür gedacht sind, über ein Netzwerk gesteuert zu werden oder über ein Netzwerk zu berichten und zu kommunizieren, häufig im Zusammenhang mit Schutz- und Sicherheitsaufgaben. Beispiele sind die Übermittlung von Musik- oder Fernsehsignalen zum Ermöglichen von "Video auf Abruf' (Video-on-Demand) als Alternative zum Fernsehfunk sowie Geräte wie zum Beispiel Überwachungskameras oder Rauchmelder.

[0004] Im Prinzip können solche Dienste über jedes beliebige Netzwerk erbracht werden, und solche Geräte können an jedes beliebige Netzwerk angeschlossen werden, sofern – das versteht sich – die Netzwerkkapazität ausreicht, um die Mindestanforderungen eines Dienstes oder eines Gerätes zu erfüllen. Netzwerkdienste können über eine Satellitenverbindung wie zum Beispiel DVB oder DBS erbracht werden. In der Praxis arbeiten jedoch die meisten Heimanwender mit terrestrischen Telekommunikations- oder Kabelfernsehverbindungen, und das ist auch die normale Wahl für die meisten Organisationen. Es wird davon ausgegangen, dass das Internet die häufigste Netzwerkwahl ist.

[0005] Da die Kosten für Hardware zur Ermöglichung des Zugangs zum Internet allgemein sowie für räumlich abgesetzte Geräte wie zum Beispiel Überwachungskameras und Rauchmelder sinken, und da die Zahl der über das Internet angebotenen Dienste zunimmt, gibt es eine steigende Tendenz, über mehrere Internetzugangsgeräte im Haushalt zu verfügen, und es wird davon ausgegangen, dass sich diese Tendenz in der absehbaren Zukunft fortsetzt. Zum Beispiel könnte ein einzelner Haushalt über einen oder mehrere digitale Fernsehapparate verfügen, die Video-on-Demand-Bilder anzeigen können, die über ein Fernbereichsnetz, wie zum Beispiel das Internet, oder über einen Kabelfernsehanbieter oder über eine ADSL-Verbindung (Asymmetric Digital Subscriber Line) von der örtlichen Telefongesellschaft oder über ein sonstiges Netzwerk mit genügend Datenkapazität abgerufen werden. Ein solcher Haushalt kann auch über einen oder mehrere Personalcomputer verfügen, die in der Lage sind, sich mit dem Internet zu verbinden, und eventuell auch eine oder mehrere eigenständige Spielekonsolen, die in der Lage sind, Spiele-Software aus dem Internet oder einem anderen Netzwerk herunterzuladen und sich optional über das Internet zu verbinden, um Mehrspieler-Spiele zu ermöglichen, und einen oder mehrere Rauch- oder Einbruchmelder und/oder räumlich abgesetzte Überwachungskameras.

[0006] Des Weiteren bieten viele Hersteller von Haushaltsgeräten an, Internetzugangseinrichtungen nicht nur in Musik- und Video- oder Fernsehsysteme zu integrieren, sondern auch in "weiße Ware", wie zum Beispiel Herde, Kühlschränke und Gefriertruhen, um einen ferngesteuerten Betrieb, Online-Störungsbeseitigung und automatische Nachbestellungsfunktionen zu ermöglichen. Obgleich diese Vorschläge heute noch überaus spekulativ sind, erscheint es doch wahrscheinlich, dass sie im Lauf der Zeit Standard oder zumindest üblich werden.

[0007] Die meisten Privatnutzer zu Hause haben nur einen einzigen Internetanschluss, im Allgemeinen in Verbindung mit dem Haustelefonanschluss. Das kann zu Problemen mit Konflikten im Hinblick auf den Bedarf an einem Internetzugang durch verschiedene Geräte und durch einen Konflikt zwischen auf das Internet zugreifenden Geräten und telefonierenden Nutzern führen. Eine logische Lösung für dieses Problem ist, den Haushalt mit einem separaten oder mit mehreren separaten Internetanschlüssen über verschiedene Telefonleitungen auszustatten. Jedoch hat diese Brechstangenlösung des Problems eine Reihe von Nachteilen. Vor allem schrecken die Mehrkosten für mehrere Telefonanschlüsse in einem einzelnen Haushalt die Verbraucher von einer solchen Lösung ab. Es ist vielmehr wahrscheinlicher, dass mehrere Dienste und mehrere Clients durch eine oder mehrere Breitbandverbindungen bereitgestellt werden, von denen jeder viele praktisch gleichzeitige Dienste handhaben kann. Selbst wenn nur ein einziger Telefonanschluss zur Verfügung steht, gestattet die Verwendung des Internet Protocol (IP), dass mehrere Dienste mit niedriger Datenrate gleichzeitig angeboten werden.

[0008] Obgleich es sich nicht unmittelbar auf den einzelnen Verbraucher auswirkt, gibt es des Weiteren ein allgemeines Problem bei der Befürwortung von Technologie, die eine zunehmende Zahl von Telefo-

nanschlüssen je Haushalt erfordert, weil die Zahl der verfügbaren Telefonleitungen begrenzt ist. Es besteht bereits ein Problem in einigen Industrieländern, zum Beispiel Großbritannien, dass die zunehmende Nachfrage nach Telefonanschlüssen infolge des raschen Anstiegs beim Gebrauch von Faxgeräten, Modems und Mobiltelefonen dazu führt, dass dem Telekommunikationssystem die Rufnummern ausgehen, so dass regelmäßig kostspielige und umständliche Änderungen bei den Rufnummerformaten und Vorwahlnummern erforderlich sind.

[0009] Dementsprechend ist es notwendig, elektronische Systeme, einschließlich beispielsweise Kleincomputersysteme und Netzwerke, bereitzustellen, die in der Lage sind, mehrere Systeme innerhalb eines einzelnen Gebäudes oder Haushalts miteinander zu verbinden und sie mit Zugang zu einer oder mehreren Verbindungen zum Internet oder einem sonstigen größeren Netzwerk zu akzeptablen Kosten auszustatten.

[0010] Ein Verfahren, dies zu realisieren, ist, alle Geräte, die einen Internetzugang benötigen, miteinander und mit einem Server zu einem Nahbereichsnetz (Local Area Network – LAN) zu verbinden. Der Server kann dann für alle Geräte als ein Gateway zum Internet fungieren und kann den Internetzugang steuern und verwalten.

[0011] Herkömmlicherweise würden die elektronischen Geräte in einem solchen LAN einen Datenbus in ihrem Aufbau aufweisen und würden in der Regel auf den Gebrauch eines einzigen Mediums, wie zum Beispiel verdrillte Doppelleitungen, beschränkt sein, um den Server und die Geräte untereinander zu verbinden. Dieser Lösungsansatz ist aber mit einer Reihe von Problemen behaftet.

[0012] Erstens gibt es innerhalb der elektronischen Geräte, zu denen einschließlich beispielsweise Computer gehören können, Probleme aufgrund der globalen Eigenart eines Datenbusses. Eine elektrische Störung an einer beliebigen Stelle entlang des Busses kann die Datenausbreitung zwischen zwei oder mehreren Kommunikationselementen unterbrechen, was möglicherweise zu einem vollständigen Produkt- oder Netzwerkausfall führt.

[0013] Des Weiteren ist in busgestützten Systemen keine Skalierbarkeit möglich. Das heißt, es ist nicht möglich, zusätzliche Leistungskapazität in Reaktion auf eine gewünschte Arbeitslast mit einer linearen Beziehung zwischen Kapazität und Arbeitslast hinzuzufügen.

[0014] Des Weiteren können andere Parteien, die nicht die vorgesehenen Informationsempfänger sind, auf jegliche Kommunikation zwischen zwei Parteien an einem Bus zugreifen. Folglich ist das einzig verfügbare Verfahren zur Datenabsicherung die Verschlüsselung. Selbst dann ist es nicht möglich zu verhindern, dass Geräte, die keine vorgesehenen Datenempfänger sind, auf die Daten zugreifen, wenn auch eventuell nur in verschlüsselter Form.

[0015] Dieser Mangel an Sicherheit in busgestützten Systemen mag in einem Einzelhaushaltssystem nicht unbedingt als Problem empfunden werden. Es ergibt sich jedoch eine große Zahl an Betrügereien durch unrechtmäßige Nutzung von Kreditkarten oder Geldautomatenkarten durch Familienangehörige, und das Risiko des Missbrauchs von Finanzdaten innerhalb eines Haushalts ist ein Problem bei Datenbusnetzen. Ein weiteres Problem ist die Bereitstellung von Datendiensten wie zum Beispiel Video-on-Demand. Die Anbieter solcher Daten versenden praktisch verschlüsselte Videodaten, und Nutzer bezahlen für die Erlaubnis, sie zu entschlüsseln. Infolge dessen hat der Datenanbieter keine Einwände gegen das Versenden der verschlüsselten Videodaten über ein lokales Netzwerk, aber er hätte Einwände gegen das Versenden der entschlüsselten Videodaten über einen Datenbus, weil das unbefugte Kopieren zu einfach wäre. Folglich besteht ein großer kommerzieller Bedarf an Produkten, die von sich aus wertvolle Daten von jeglichen Mitteln, mit denen sie kopiert werden könnten, fernhalten.

[0016] Des Weiteren ist der mögliche Verlust an Vertraulichkeit infolge dieses Mangels an Datensicherheit ein Problem – selbst innerhalb eines Haushalts.

[0017] Und schließlich bedeutet die Verfügbarkeit aller Daten an allen Punkten eines Datenbusses innerhalb entweder eines elektronischen Produkts oder des Netzwerks oder der Netzwerke, mit dem oder mit denen es verbunden ist, dass, sobald sich ein unbefugter Nutzer Zugang zu Daten für ein Gerät in dem Netzwerk verschafft hat, am wahrscheinlichsten durch Fernzugriff auf den Server über das Internet oder ein anderes öffentliches Netzwerk, möglicherweise auch andere Daten gefährdet sind.

[0018] Diese Sicherheitsprobleme sind natürlich schwerwiegender, wenn das Netzwerk von einem Kleinunternehmen oder von mehr als einem einzigen Haushalt, zum Beispiel in einer Wohngemeinschaft, verwendet wird.

[0019] Ein weiteres Problem bei einem busgestützten System ist die Zuverlässigkeit. Im Allgemeinen setzt eine Störung am Datenbus das gesamte Netzwerk außer Betrieb.

[0020] Des Weiteren ist bei datenbusgestützten Systemen die Gesamtleistung des Systems durch die Geschwindigkeit des langsamsten Gerätes begrenzt. Das liegt daran, dass die Datenübertragungs-

rate oder Taktrate des Busses nicht höher sein kann als die Datenübertragungsrate des langsamsten an ihn angeschlossenen Gerätes, weil sonst keine zuverlässige Kommunikation erfolgen kann. Infolge dessen können Verbesserungen bei der Datenübertragungsrate des Netzwerks nur erreicht werden, indem man alle Geräte austauscht oder modernisiert.

[0021] Außerdem erzeugen Datenbusse erhebliche Mengen an elektromagnetischen Störungen (EMS).

[0022] Und schließlich sind datenbusgestützte Netzwerke relativ teuer, und breite Busse wirken sich durch entsprechenden Mehraufwand nachteilig auf die Leiterplatte, die Herstellung und die Produktgröße aus und verursachen infolge dessen höhere Kosten für die zu vernetzenden Geräte.

[0023] Eine bekannte Netzwerkanordnung ist in EP-A-0537408 beschrieben. Darin wird ein Datennetz beschrieben, bei dem Geräte zu mehreren Nahbereichsnetzen (Local Area Networks – LAN) gruppiert sind, die durch bidirektionale Kommunikationsverbindungen über Brückenelemente miteinander verbunden sind.

[0024] Die vorliegende Erfindung hat die Aufgabe, elektronische Systemarchitekturen, Komponenten, Geräte und Netzwerke bereitzustellen, die diese Probleme wenigstens teilweise überwinden.

[0025] Gemäß einem ersten Aspekt stellt die Erfindung eine Vorrichtung mit wenigstens zwei Kommunikationsabschnitten bereit, die dafür geeignet sind, über verschiedene bidirektionale Kommunikationsverbindungen mit ähnlichen Vorrichtungen verbunden zu werden, dadurch gekennzeichnet, dass die Vorrichtung einen ersten Kommunikationsabschnitt aufweist, der dafür konfiguriert ist, auf den Empfang eines Taktübergangs über eine erste Kommunikationsverbindung mit dem Übertragen eines Taktübergangs, der die gleiche Polarität aufweist, zurück über die erste Kommunikationsverbindung zu reagieren, und einen zweiten Kommunikationsabschnitt aufweist, der dafür konfiguriert ist, auf den Empfang eines Taktübergangs über eine zweite Kommunikationsverbindung mit dem Übertragen eines Taktübergangs, der die entgegengesetzte Polarität aufweist, zurück über die zweite Kommunikationsverbindung zu reagieren.

[0026] Gemäß einem zweiten Aspekt stellt die Erfindung ein elektronisches Kommunikationsnetz bereit, das wenigstens zwei Vorrichtungen umfasst, die über mindestens eine bidirektionale Kommunikationsverbindung verbunden sind, und dadurch gekennzeichnet, dass durch die erste Vorrichtung, die einen Taktübergang über die Kommunikationsverbindung empfängt und einen Taktübergang, der die gleiche Polarität aufweist, zurück über die Kommunikationsverbindung sendet, und die zweite Vorrichtung, die einen Taktübergang über die Kommunikationsverbindung empfängt und einen Taktübergang, der die entgegengesetzte Polarität aufweist, zurück über die Kommunikationsverbindung sendet, eine Schleife gebildet wird und die erste und die zweite Vorrichtung dafür geeignet sind, die Taktübergänge, die sich in der Schleife entlang bewegen, zur Erzeugung eines Taktsignals zu verwenden, um die Datenübertragung über die Kommunikationsverbindung zu steuern.

[0027] Es werden nun Ausführungsformen der Erfindung lediglich beispielhaft anhand der begleitenden schaubildhaften Figuren beschrieben, in denen Folgendes dargestellt ist:

[0028] Fig. 1 zeigt eine Netzwerkstruktur gemäß einem ersten Aspekt der Erfindung.

[0029] Fig. 2 zeigt Details der Vorrichtungen, aus denen das Netzwerk von Fig. 1 besteht.

[0030] Fig. 3 zeigt Details eines Schalters, der in den Vorrichtungen von Fig. 2 verwendet wird.

[0031] **Fig.** 4 zeigt einen Empfängerabschnitt, der in dem Schalter von Fig. 3 verwendet wird.

[0032] Fig. 4B zeigt einen Senderabschnitt, der in dem Schalter von Fig. 3 verwendet wird.

[0033] Fig. 5A und Fig. 5B sind erläuternde Zeitablaufdiagramme, welche die Nachrichtenausbreitung in dem Netzwerk gemäß Fig. 1 zeigen.

[0034] Fig. 6 zeigt ein Verschlüsselungssystem, das zur Verwendung in dem Netzwerk geeignet ist.

[0035] Fig. 7 zeigt ein verbessertes Verschlüsselungssystem zur Verwendung in dem Netzwerk.

[0036] Fig. 8 zeigt ein weiteres verbessertes Verschlüsselungssystem zur Verwendung in dem Netzwerk.

[0037] Fig. 9A bis Fig. 9C zeigen Nachrichtenformate und -codes, die zur Verwendung in dem Netzwerk geeignet sind.

[0038] Fig. 10 ist ein erläuterndes Schaubild, das zeigt, wie Taktimpulsschaltkreise automatisch zwischen den Vorrichtungen des Netzwerks erzeugt werden.

[0039] Fig. 11 zeigt Beispiele von Taktdaten und Framesignalen in dem Netzwerk.

[0040] Fig. 12 zeigt eine Vorrichtungsarchitektur gemäß der Erfindung.

[0041] Fig. 13 zeigt eine alternative Vorrichtungsarchitektur gemäß der Erfindung.

[0042] Fig. 14 ist ein erläuterndes Schaubild, das Sicherheitsmerkmale der Vorrichtungsarchitekturen zeigt.

[0043] Fig. 15 zeigt eine Prozessoranordnung zur Verwendung in den Vorrichtungen.

[0044] Fig. 16 zeigt ein alternatives Nachrichtenformat zur Verwendung in dem Netzwerk oder in den Vorrichtungen.

[0045] Ein elektronisches Netzwerk gemäß einem ersten Aspekt der Erfindung ist in Fig. 1 gezeigt. Dieses Netzwerk kann aus beliebigen Kommunikations-, Computer- oder sonstigen elektronischen Geräten und Produkten bestehen. Obgleich dieses Beispiel anhand eines Heim-, d. h. Einzelhaushaltsanschlusses an das Internet beschrieben wird, was vermutlich die häufigste und kommerziell bedeutsamste Nutzung der Erfindung sein wird, versteht es sich, dass die erfindungsgemäße Architektur gleichermaßen auf den kommerziellen Einsatz oder den Anschluss an ein sonstiges digitales Kommunikationsnetz anwendbar ist.

[0046] In Fig. 1 ist ein Server **1** mit dem elektronischen System oder der elektronischen Architektur verbunden, die mehrere Client-Vorrichtungen **2** umfasst, die in einer hierarchischen Struktur über eine Anzahl lokaler Netzwerkanschlüsse zu einem Nahbereichsnetz angeordnet sind.

[0047] Der Server **1** kann ein einzelner Server oder ein Netzwerk aus separaten Servern sein, die ein Hostnetzwerk bilden, wie zum Beispiel das Internet.

[0048] Die Client-Vorrichtungen **2** sind in einer hierarchischen Baumstruktur angeordnet, die durch Zweige verbunden ist, welche durch die Kommunikationsverbindungen des Nahbereichsnetzes gebildet werden. In der hierarchischen Struktur haben Zweige, die sich weiter unten in der Struktur befinden, eine geringere Bandbreite als die Zweige darüber, das heißt, die Zweige, über die sie mit dem Server **1** verbunden sind. Wo mehrere stromabwärtige Zweige und ein einzelner stromaufwärtiger Zweig mit einem einzelnen Knoten verbunden sind, muss die Summe der Bandbreiten dieser stromabwärtigen Zweige kleiner sein als die Bandbreite des stromaufwärtigen Zweigs. Die Datensicherheit wird im System von unten nach oben gewährleistet, wie weiter unten noch erläutert wird.

[0049] Die Client-Vorrichtungen **2**, welche die Endknoten des Systems bilden, sind Client-Vorrichtungen **2**, die eine interne Verarbeitungsfähigkeit besitzen und dem Nutzer Zugang zu Servereinrichtungen bieten. Die Client-Vorrichtungen **2**, welche die Knoten in der Struktur bilden, die keine Endpunkte sind, steuern die Erbringung von Diensten für die niederen Client-Vorrichtungen **2**. Sie besitzen eine interne Verarbeitungsfähigkeit und können selbst auch Client-Vorrichtungen **2** sein, die dem Nutzer eigenständig Zugang zu Servereinrichtungen bieten und außerdem die Erbringung von Diensten für die Client-Vorrichtungen **2** der unteren Ebenen steuern.

[0050] Die Verringerung der Bandbreite für Zweige, die von dem Server **1** weiter entfernt liegen, ist notwendig, um zu verhindern, dass die Bandbreitenanforderungen für das System geometrisch zunehmen, wenn es größer wird, und um zu gewährleisten, dass keine Client-Vorrichtung **2** einer niederen Ebene eine Client-Vorrichtung **2** einer höheren Ebene überfordert, indem sie eine größere Bandbreite, das heißt eine höhere Datenübertragungsrate, anfordert, als die Client-Vorrichtung **2** der höheren Ebene unterstützen kann.

[0051] Ein Grund für die Verwendung eines Mehrprozessorsystems, das mehrere verschiedene Client-Vorrichtungen umfasst, ist, die Rechen- und Funktionslast so zu verteilen, dass die benötigte Rechenleistung dort platziert wird, wo sie am dringendsten gebraucht wird, und die richtige Elektronik für eine bestimmte Funktion an der wirtschaftlichsten und effektivsten Stelle anzusiedeln, um diese Funktion in einer zuverlässigen und aufrechterhaltbaren Weise bereitzustellen.

[0052] Ein weiterer Grund für die Verwendung eines Mehrprozessorsystems, das mehrere separater Client-Vorrichtungen **2** umfasst, ist, dass die Datensicherheit gewahrt wird. Diese Datensicherheit kann erforderlich sein, um eine befugte Kontrolle, einen finanziell verlässlichen e-Commerce oder einfach die Vertraulichkeit zu gewährleisten. Zum Beispiel kann ein Anwendungsprozessor, auf dem Internet-Softwareanwendungen ablaufen können, für Angriffe von außen anfällig sein. Das Behalten der Kontrolle über eine Smartcard für elektronischen Handel in einer separaten Einheit erhöht darum die Sicherheit der e-Commerce-Funktionen und verbessert die vorhersagbare Servicequalität, die durch das Verwenden der Smartcard möglich ist.

[0053] [0034) Um die gewünschte Datensicherheit zu ermöglichen, unterstützt die erfindungsgemäße elektronische Systemarchitektur hierarchische Datenstrukturen. Der Zugriff auf eine bestimmte Client-Vorrichtung **2** wird allein durch diese Client-Vorrichtung **2** gesteuert. Datennutzer einer höheren Ebene, das heißt der Server **1** und Client-Vorrichtungen **2**, die sich zwischen einer bestimmten Client-Vorrichtung **2** und dem Server **1** befinden, müssen bei den Client-Vorrichtungen **2** der unteren Ebenen ihre Daten anfordern und in der Lage sein, diese

Anforderungen zu authentifizieren. Natürlich können Client-Vorrichtungen **2**, die keine Daten absichern müssen, Anforderungen und Antworten ungehindert durch sich selbst hindurch weit oder auf Anforderungen nach ungeschützten Daten, die sie speichern, antworten, ohne eine Authentifizierung zu verlangen.

[0054] Zugriffsanforderungen von Client-Vorrichtungen **2** einer höheren Ebene an Client-Vorrichtungen **2** einer niederen Ebene können durch Hardware oder Software erfolgen. Wenn eine Client-Vorrichtung **2** einer höheren Ebene in der Lage ist, eine Hardwarezugriffsanforderung für eine Client-Vorrichtung **2** einer niederen Ebene zu stellen, so kann es dieser Hardwarezugriffsanforderung gestattet werden, unverändert durch jegliche Zwischen-Client-Vorrichtungen **2** zu passieren. Wenn die Hardwarezugriffsanforderung gesperrt wird, so versucht die Client-Vorrichtung **2** der Zwischenebene, den Zugriff im Namen der Client-Vorrichtung **2** der höheren Ebene auszuführen, sofern es gestattet ist. Um es dem System zu ermöglichen, transparent zu sein, so dass der Ursprungs-Client-Vorrichtung **2** Hardware- und Softwarezugriffsanforderungen gleich erscheinen, muss die Zwischen-Client-Vorrichtung **2** mit Ausnahmehandhabungseinrichtungen ausgestattet sein, das heißt mit der Einrichtung, die ein zu verwendendes Software-Protokoll veranlasst, eine Zugriffsanforderung anstelle einer abgebrochenen Hardwarezugriffsanforderung auszuführen. Es ist aufgrund der resultierenden höheren Kosten nicht wünschenswert, die Verwendung von Ausnahmeverarbeitungselementen auf allen Ebenen in dem Computersystem zu verlangen. Jedoch muss jede Client-Vorrichtung **2**, die keine Ausnahmeverarbeitung unterstützt, entweder ein Endpunkt in dem hierarchischen System sein oder eine Client-Vorrichtung **2** sein, die niemals Hardwarezugriffsanforderungen an Client-Vorrichtungen **2** niederer Ebenen stellt oder weiterleitet.

[0055] Ein Beispiel für diese Anforderung wäre eine Set-Top-Box, die in der Lage ist, digitale Videosignale aus dem Internet abzurufen, um sie auf einem digitalen Fernsehgerät anzuzeigen. Die Set-Top-Box ist selbst eine Client-Vorrichtung **2**, die mit dem Internet in Form eines Internet-Servers **1** über eine oder mehrere andere Client-Vorrichtungen **2** verbunden ist, und wird mittels einer Infrarotfernbedienung gesteuert, die mit einer integrierten Smartcard-Schnittstelle versehen ist. Um die Fernbedienung bedienen zu können, muss die den Nutzer identifizierende Smartcard eingesteckt werden. Wenn die Smartcard eingesteckt ist, so kann die Fernbedienung die Set-Top-Box anweisen, Pay-per-View- (Bezahlfernsehen), Video-on-Demand- oder ähnliche mit einer Zugangsbeschränkung versehene Videosignale zur Anzeige auf dem Fernsehschirm zuzulassen.

[0056] Obgleich die Set-Top-Box und die Fernbedienung beides Client-Vorrichtungen **2** sind, kann die Set-Top-Box freilich keinen Hardwarezugriff auf die Smartcard vornehmen und muss sich auf ein Software-Protokoll über die Infrarotverbindung stützen. Infolge dessen braucht der Prozessor in der Set-Top-Box keine Ausnahmeverarbeitung zu unterstützen, auch wenn die Fernbedienung eine Vorrichtung ist, die sich im Netzwerk auf einer niedrigeren Ebene als die Set-Top-Box befindet.

[0057] Jede Client-Vorrichtung **2**, die einen Knoten in dem elektronischen Netzwerk gemäß dem ersten Aspekt der Erfindung bildet, ist eine aktive Informationsverarbeitungsvorrichtung, die in der Lage ist, Daten, die durch sie hindurchfließen, zu handhaben. Oder präziser ausgedrückt: Jede Client-Vorrichtung **2** kann die Daten, die sie empfängt, handhaben, und kann diese Daten selektiv wiederversenden. Ein Mindestbetrag an Verarbeitung wäre null, das heißt, was in einen Knoten hineingelangt, geht auch wieder hinaus. Alternativ kann auch sehr wenig der ursprünglichen Informationen, die durch eine Client-Vorrichtung **2**, welche den Knoten bildet, empfangen werden, weitergereicht werden. In einem Extremfall kann eine bestimmte Client-Vorrichtung **2** auch gar keine der empfangenen Daten weitersenden. Statt dessen kann sie auf die empfangenen Daten in der Weise reagieren, dass sie eine andere Nachricht weitersendet, die andere Daten enthält, die allerdings zu den empfangenen Daten in Bezug stehen oder aus den empfangenen Daten abgeleitet sind.

[0058] Die höchstgelegene stromaufwärtige Client-Vorrichtung **2**, die dem Server **1** am nächsten liegt, bildet einen Gateway zu dem Server und steuert und verwaltet den Serverzugang für das gesamte Netzwerk. Diese Gateway-Client-Vorrichtung **2** muss normalerweise unterschiedliche Kommunikationsprotokolle in dem Netzwerk und zur Kommunikation mit dem Server unterstützen, obgleich die Protokolle dieselben sein könnten.

[0059] Das Passieren von Daten durch die Client-Vorrichtungen **2**, die Knoten in dem Netzwerk bilden, ermöglicht das Implementieren einer hierarchischen Sicherheit durch Client-Vorrichtungen **2** an Knoten auf höherer Ebene in dem Netzwerk, welche die Erbringung von Diensten an weiter unten befindliche Komponenten steuern, während Client-Vorrichtungen, die Knoten weiter unten im Netzwerk bilden, eine Endnutzerauthentifizierung steuern. Somit ermöglichen im Wesentlichen die höheren Knoten eine serverseitige Sicherheit, während die weiter unten befindlichen Knoten eine clientseitige Sicherheit ermöglichen.

[0060] Weil die einzelnen Kommunikationsverbindungen zwischen Knotenpaaren physisch getrennt sein können und Client-Vorrichtungen **2**, welche die Knoten bilden, empfangene Daten selektiv zum nächsten Knoten weitereichen oder sie sperren kön-

nen, kann die Datensicherheit im Netzwerk deutlich verbessert werden, weil Daten nur Client-Vorrichtungen **2**, welche die Daten benötigen, und jenen Client-Vorrichtungen **2**, die einen Teil des Datenpfades bilden, über den die Daten fließen, verfügbar gemacht werden. Somit kann das Sicherheitsmerkmal von Daten, auf die nur physisch an bestimmten Punkten in dem Netzwerk zugegriffen werden kann, dafür genutzt werden, einen zusätzlichen Grad an Sicherheit über denjenigen hinaus zu schaffen, der durch Verschlüsselung allein geschaffen wird. Weil des Weiteren die Daten, die zwischen verschiedenen Paaren von Client-Vorrichtungen **2** und verschiedenen Knoten ausgeführt werden, nicht nur logisch, sondern auch physisch unterscheidbar gemacht werden können, führt ein Ausfall einer einzelnen Kommunikationsverbindung oder Client-Vorrichtung **2** nicht unbedingt zu einem Ausfall des gesamten Systems. Der Umfang, in dem das System nach einem Ausfall weiter funktionstüchtig ist, richtet sich natürlich nach der Größe, der Struktur und der Funktion des Netzwerks, der Funktion der einzelnen Client-Vorrichtungen **2**, aus denen es besteht, und der Art und dem Ort des Ausfalls. Darum kann nicht garantiert werden, dass in der Praxis alle Systeme in der Lage wären, im Anschluss an alle möglichen Ausfälle teilweise weiter zu funktionieren. Jedoch besteht die Möglichkeit eines teilweisen Funktionierens nach einem Ausfall in Netzwerken gemäß der Erfindung zu einem Grad, der in datenbusgestützten Netzwerken nicht möglich ist.

[0061] Eine generische Client-Vorrichtung **2** ist in Fig. 2 gezeigt. Es versteht sich, dass diese Illustration nur als erläuterndes Schaubild gedacht ist, um die Funktionen einer generischen Client-Vorrichtung **2** zu erklären, und keine spezielle Komponentenanordnung oder physische Struktur implizieren soll.

[0062] Zur Veranschaulichung sind eine Reihe von Client-Vorrichtungen **2** gezeigt, die in einem Netzwerk angeordnet sind, das einen obersten Knoten M und einen untersten Knoten 0 aufweist. Die Client-Vorrichtung **2**, die den Zwischenknoten N+1 bildet, ist im Detail gezeigt. Die Netzwerkstruktur aus einer linearen Kette aus Knoten ist ein einfaches Beispiel, das aus Gründen der besseren Übersichtlichkeit gewählt wurde, und es versteht sich, dass auch andere Netzwerkstrukturen möglich sind.

[0063] Die Client-Vorrichtung **2** umfasst drei Hauptkomponenten: einen lokalen Schalter **3**, einen lokalen Verarbeitungsabschnitt **4** und einen lokalen Dateneingabe- und -ausgabeabschnitt **5**.

[0064] Während des Betriebes werden Daten zwischen den Client-Vorrichtungen **2**, die sich an der Kette aus Knoten befinden, aus denen das Netzwerk besteht, auf und ab gereicht. An jedem Knoten werden Informationen durch den lokalen Schalter **3** der Client-Vorrichtung **2** in der Kette auf oder ab gesendet oder empfangen. In jeder Client-Vorrichtung **2** arbeitet der Schalter **3** allein unter der Kontrolle der Client-Vorrichtung **2**. Daten, die durch das Netzwerk geleitet werden, sind an einen bestimmten Zielort gerichtet, und dieser Zielort kann logisch oder physisch definiert sein. Alle Client-Vorrichtungen **2**, aus denen alle Knoten bestehen, sind in der Lage, Daten zu empfangen, und jene Client-Vorrichtungen **2**, die keine Endpunkte des Netzwerks sind, sind in der Lage, Daten weiterzureichen. Im Prinzip können die Client-Vorrichtungen **2** an jedem Knoten eine Informationstransaktion einleiten, indem sie Daten an eine andere Client-Vorrichtung **2** an einem anderen Knoten senden. Es ist jedoch möglich, dass einige Client-Vorrichtungen dies in der Praxis nicht tun, weil ihre Funktion von ihnen nur verlangt, Daten zu empfangen und keine Informationstransaktion einzuleiten.

[0065] Der Schalter **3** in jeder Client-Vorrichtung **2** kann so komplex sein, wie es die konkrete Anwendung verlangt. Jedoch besteht die Mindestfunktionalität des Schalters **3** darin, dass er alle empfangenen Nachrichten, die für seine lokale Client-Vorrichtung **2** bestimmt sind, aus dem ankommenden Datenstrom entfernen muss und in derselben Richtung entlang der Netzwerkkette empfangene Nachrichten weiterleiten muss, die für andere Client-Vorrichtungen **2** als die lokale Client-Vorrichtung **2** bestimmt sind.

[0066] Es mag den Anschein haben, dass diese Funktionalität im Widerspruch zu den obigen Anmerkungen steht, dass eine bestimmte Client-Vorrichtung möglicherweise Daten nicht in der empfangenen Form weiterleitet, sondern statt dessen in Reaktion auf dem Empfang der Originaldaten möglicherweise vollkommen neue Daten weitersendet. Im Hinblick auf die oben beschriebene Schalterfunktionalität würden die Originaldaten als eine Nachricht betrachtet werden, die für den lokalen Knoten bestimmt sind, der dann das Versenden der neuen Nachricht, welche die neuen Daten enthält, einleiten würde.

[0067] Wie oben erläutert, leitet der Schalter **3** Nachrichten, die für andere Client-Vorrichtungen **2** bestimmt sind, entlang der Kette weiter und extrahiert die empfangene Nachricht, die für die lokale Client-Vorrichtung **2** bestimmt sind, aus dem Nachrichtenstrom, der durch das Netzwerk fließt. Diese Nachrichten, die für die lokalen Client-Vorrichtungen **2** bestimmt sind, werden an den lokalen Verarbeitungsabschnitt **4** weitergeleitet.

[0068] Der lokale Verarbeitungsabschnitt **4** verarbeitet die empfangenen Daten bedarfsgemäß. Erforderlichenfalls leitet der lokale Verarbeitungsabschnitt **4** Daten oder Anweisungen an einen lokalen Eingabe/Ausgabe-Abschnitt **5** weiter, bei dem es sich um eine Datenanzeigevorrichtung oder um ein Gerät,

das unter der Kontrolle des lokalen Verarbeitungsabschnitts **4** steht oder an den lokalen Verarbeitungsabschnitt **4** berichtet, oder um eine Schnittstelle zu einem externen Gerät, das unter der Kontrolle der Client-Vorrichtung **2** steht oder an die Client-Vorrichtung **2** berichtet, handeln kann. Gleichermaßen kann der lokale Eingabe/Ausgabe-Abschnitt **5** Daten nach Bedarf an den lokalen Verarbeitungsabschnitt **4** senden. Der lokale Verarbeitungsabschnitt **4** verarbeitet diese Daten, und gemäß Vorgabe durch Daten, die vom Schalter **3** und dem lokalen Eingabe/Ausgabe-Abschnitt **5** kommend empfangen wurden, und durch sonstige weitere Faktoren, wie zum Beispiel die aktuelle Zeit, erstellt der lokale Verarbeitungsabschnitt **4** Nachrichten an andere Client-Vorrichtungen **2** und sendet sie an den Schalter **3**, um an das Netzwerk hinausgesendet zu werden.

[0069] Im Prinzip wäre eine Client-Vorrichtung möglich, die nur einen Schalter **3** und einen lokalen Verarbeitungsabschnitt **4** oder nur einen Schalter **3** und einen lokalen Verarbeitungsabschnitt **5** umfasst, auch wenn es in der Praxis nur sehr wenige Situationen gibt, in denen eine Client-Vorrichtung nützlich wäre, die nur in der Lage ist, Daten im Netzwerk zu empfangen, zu verarbeiten und zu senden, ohne über eine lokale Eingabe- und Ausgabefunktion zu verfügen. Und auch wenn gleichermaßen eine Client-Vorrichtung möglich wäre, die in der Lage ist, lokal erzeugte Daten direkt in das Netzwerk einzuspeisen oder Daten aus dem Netzwerk direkt auszugeben, ist es in der Praxis normalerweise der Fall, dass wenigstens eine Mindestmenge an lokaler Verarbeitung innerhalb der Client-Vorrichtung **2** erforderlich ist.

[0070] Obgleich der Abschnitt **5** als der lokale Dateneingabe- und -ausgabeabschnitt **5** beschrieben ist, könnte er in der Praxis in einigen Anwendungen nur ein Datenausgang oder nur ein Dateneingang sein. Der Schalter **3** ist normalerweise in der Lage, einen Vollduplexbetrieb zu unterstützen.

[0071] Ein Schalter **3** ist in Fig. 3 im Detail gezeigt. Der Schalter **3** umfasst zwei separate Schaltblöcke **6a** und **6b**. Der Schaltblock **6a** handhabt stromabwärtigen Verkehr, das heißt, der Schaltblock **6a** empfängt Nachrichten von dem nächsten Knoten stromaufwärts und überträgt Nachrichten zum nächsten Knoten stromabwärts, während der Schaltblock **6b** stromaufwärtigen Verkehr handhabt, das heißt, der Schaltblock **6b** empfängt Daten von dem nächsten Knoten stromabwärts und sendet Daten zum nächsten Knoten stromaufwärts.

[0072] Die Schaltblöcke **6** sind durch eine Verbindung **7** miteinander verbunden, um einen Datenpfad für Bestätigungen empfangener Nachrichten bereitzustellen, und jeder Datenblock **6** ist so angeschlossen, dass er Daten, die er von dem lokalen Prozessor **4** empfangen hat, über Leitungen **8** hinaussenden kann.

[0073] Außer der Verbindung **7** zum Ermöglichen einer automatischen Erzeugung von Bestätigungen empfangener Nachrichten und einer Empfangsmitteilung oder -bestätigung gibt es keine weitere direkte Verbindung zwischen dem stromaufwärtigen und dem stromabwärtigen Schaltblock **6a** bzw. **6b**.

[0074] Jeder Schaltblock **6** enthält einen Empfänger- (Eingabe-) Abschnitt **9** und einen Sender- (Ausgabe-) Abschnitt **10**, die unter der Kontrolle eines synchronisierenden endlichen Automaten arbeiten, der einen Teil des Schaltblocks **6** bilden.

[0075] Geeignete Beispiele für Empfänger- und Senderstrukturen sind in den Fig. 4a und Fig. 4b gezeigt, wobei Fig. 4a die Empfängerstruktur zeigt, während Fig. 4b die Senderstruktur zeigt.

[0076] Der Empfängerabschnitt **9** empfängt Nachrichten nur von dem Senderabschnitt **10** eines Schaltblocks **6** einer Client-Vorrichtung **2**, die einen benachbarten Knoten bildet, obgleich die eigentlichen Daten, die von der Nachricht transportiert werden, ihren Ursprung an jeder beliebigen Stelle in dem Netzwerk haben können.

[0077] Jede Nachricht enthält einen Nachrichtentyp- und -routinginformationsabschitt, der die Ursprungs-Client-Vorrichtung **2** und die Ziel-Client-Vorrichtung **2**, den Typ der Nachricht und die Menge an transportierten Daten identifiziert, und in der Regel einen Nutzdatenabschnitt, der aus den Daten besteht, die durch die Nachricht transportiert werden. Jedoch können einige Nachrichtentypen, insbesondere Bestätigungen für den Empfang früherer Nachrichten, einfach als solche anhand des Nachrichtentyp- und -routinginformationsabschitts identifiziert werden und keine Nutzdaten transportieren.

[0078] Jede Nachricht wird über den Eingangsdatenpfad durch ein Synchronisiererelement **11** empfangen und dann zu einem Nachrichtentyp- und -routingelement **12** weitergeleitet, das die von der Nachricht transportierten Nachrichtentypdaten untersucht, um festzustellen, um welchen Nachrichtentyp es sich handelt. Wenn die Nachricht eine Bestätigung ist, dass eine Nachricht empfangen wurde, so werden diese Informationen an einen endlichen Automaten **17** weitergeleitet, der den anderen Schaltblock **6** des lokalen Schalters **3** darüber in Kenntnis setzt, dass die Benachrichtigung über die Verbindung **7** empfangen wurde, so dass der andere Schaltblock **6** weiß, dass sein gegenüberliegender Eingangsabschnitt zum Empfang der nächsten Nachricht bereit ist. Der Eingangsabschnitt **9** erwartet dann die nächste Nachricht.

[0079] Wenn die Nachricht durch das Nachrichtentyp- und -routingelement **12** nicht als eine Bestätigung identifiziert wird, so extrahiert das Nachrichtentyp- und -routingelement **12** die von der Nachricht transportierten Routenidentifikationsinformationen, das heißt die lokale Schaltkreisnummer der Client-Vorrichtung **2**, für die die Nachricht gedacht ist, und leitet sie an einen Routenkomparator **13** weiter. Der Routenkomparator **13** vergleicht die aus der Nachricht extrahierte Zielschaltkreisnummer mit der lokalen Schaltkreisnummer, die in dem Lokale-Schaltkreisnummern-Speicher **14** gespeichert ist. Wenn der Routenkomparator **13** die Schaltkreisnummern als identisch identifiziert, so leitet das Nachrichtentyp- und -routingelement **12** die relevanten Teile der Nachrichtentyp- und -routinginformationen an das Host-Schnittstellenelement **16** weiter, und das Nachrichtennutzdatenelement **15** leitet den Dateninhalt der Nachricht an das Host-Schnittstellenelement **16** weiter. Das Host-Schnittstellenelement **16** sendet diese Daten an die anderen Teile der Client-Vorrichtung **2**. Das heißt, diese Daten werden an die lokale Verarbeitungsstation **4** und/oder an den lokalen Eingabe/Ausgabe-Abschnitt **5** gesendet.

[0080] Wenn die zwei Routeninformationsteile nicht identisch sind, so wird alternativ die Nachricht an den Senderabschnitt **10** weitergeleitet.

[0081] In jedem Fall instruiert, nachdem die Nachricht entweder an den Senderabschnitt **10** oder an die anderen Teile der lokalen Client-Vorrichtung **2** gesendet wurde, der endliche Automat **17** des Empfängerabschnitts **9** den anderen Schaltblock **6** des lokalen Schalters **3**, eine Empfangsbestätigungsantwort in seinem Namen an die Client-Vorrichtung **2** an dem benachbarten Knoten, von wo die Nachricht erhalten wurde, zurückzusenden. Diese Bestätigung informiert die sendende Client-Vorrichtung **2** darüber, dass der Empfängerabschnitt **9** zum Empfang der nächsten Nachricht bereit ist.

[0082] Der Senderabschnitt **10** kann Nachrichten zum Versenden sowohl von dem Empfängerabschnitt **9**, der einen Teil desselben Schaltblocks **6** bildet, als auch von anderen Teilen der lokalen Client-Vorrichtung **2** empfangen und kann angewiesen werden, Empfangsbestätigungsnachrichten durch den Empfängerabschnitt **9** des anderen Schaltblocks **6** des lokalen Schalters zu versenden. Da der Senderabschnitt **10** nur eine einzelne Nachricht auf einmal versenden kann, muss der endliche Automat zwischen drei Nachrichtenquellen arbitrieren, und es muss ein Mittel zum vorübergehenden Speichern oder Puffern von Nachrichten zum Versenden bereitgestellt werden. Weil des Weiteren der Betrieb des Empfängerabschnitts **9** und des Senderabschnitts **10** eines einzelnen Schaltblocks **6** nicht synchronisiert ist und beide mit unterschiedlichen Taktraten betrieben werden können, das heißt, weil die Rate, mit der Daten an einem einzelnen Schaltblock **6** empfangen werden und von einem einzelnen Schaltblock **6** gesendet werden, verschieden sein kann, und weil die Länge der empfangenen und gesendeten oder aufeinanderfolgenden Nachrichten ebenfalls unterschiedlich sein kann, würde man in jedem Fall einen Puffer zwischen dem Empfängerabschnitt **9** und dem Senderabschnitt **10** benötigen. Die erforderlichen Puffer können nach Bedarf lokal in den Empfängerabschnitt **9**, den Senderabschnitt **10** oder an anderer Stelle integriert werden. In diesem Beispiel enthält der Sendehost-Schnittstellenabschnitt **17**, der Daten von anderen Teilen der lokalen Client-Vorrichtung **2** empfängt, einen Sendepuffer, und ein weiterer Puffer befindet sich innerhalb des Schaltblocks **6** zwischen dem Empfängerabschnitt **9** und dem Senderabschnitt **10**, was aber in den Figuren nicht gezeigt ist.

[0083] Wenn eine Nachricht versendet werden soll, so werden die zu transportierenden Daten von dem Puffer oder der Host-Schnittstelle **17** zu einem Nutzdatenspeicher **18** verbracht. Die Daten werden dann zu einem Nachrichtentyp- und -routinggenerator **19** geleitet, der den entsprechenden Nachrichtentyp- und -routinginformationsteil der Nachricht auf der Grundlage von Daten erzeugt, die von der Host-Schnittstelle **17** übermittelt wurden, oder einfach die Nachrichtentyp- und -routinginformationen prüft und wiederholt, die bereits in der empfangenen Nachricht enthalten sind. Wenn die Nachricht ihren Ursprung in der lokalen Client-Maschine **2** hat, so wird die lokale Schaltkreisnummer, welche die Ursprungs-Client-Vorrichtung **2** identifiziert, durch einen Lokale-Schaltkreisnummern-Speicher **20** in den Nachrichtentyp- und -routinggenerator **19** eingespeist.

[0084] In Reaktion auf eine Anweisung von dem Empfängerabschnitt **9** des anderen Schaltblocks **6** des lokalen Schalters **3**, eine Empfangsbestätigungsnachricht zu senden, erzeugt der Nachrichtentyp- und -routinggenerator **19** einen Nachrichtentyp- und -routinginformationsteil der Nachricht, der sie als eine Bestätigung identifiziert. Eine solche Nachricht hat keine Nutzdaten zu transportieren.

[0085] Wenn schließlich der Bereitschaftsstatus des entsprechenden Empfängerabschnitts **9** der Client-Maschine **2** an dem benachbarten Knoten bestätigt wird, so wird die assemblierte Nachricht über die Kommunikationsverbindung zu dieser Client-Maschine **2** durch einen Sendesynchronisator **21** gesendet.

[0086] In der obigen Besprechung sind der Empfängerabschnitt **9** und der Senderabschnitt **10** beide so dargestellt, dass sie durch einen synchronisierenden endlichen Automaten gesteuert werden. Es kann ein separater steuernder endlicher Automat für den Senderabschnitt **9** und den Empfängerabschnit **10** vorhanden sein, oder es kann ein einzelner synchroni-

sierender endlicher Automat vorhanden sein, der den gesamten Schaltblock **6** steuert. Gleichermaßen sind separate Lokale-Schaltkreisnummern-Speicher **14** und **20** für den Empfängerabschnitt **9** und den Senderabschnitt **10** gezeigt. Natürlich könnten diese durch einen einzelnen gemeinsamen Lokale-Schaltkreisnummern-Speicher ersetzt werden.

[0087] Wie oben erläutert, kann der Senderabschnitt **10** Nachrichten sowohl von dem Empfängerabschnitt **9** desselben Schaltblocks **6** als auch von anderen Teilen der lokalen Client-Vorrichtung **2** oder Bestätigungen übertragen, so wie es durch den Empfängerabschnitt **9** des anderen Schaltblocks **6** des lokalen Schalters **3** angewiesen wird, doch er kann nur eine einzige Nachricht auf einmal versenden, so dass der endliche Automat zwischen den drei Nachrichtenquellen arbitrieren muss. Um zu vermeiden, dass die wahrgenommene Bandbreite und Latenz des Netzwerks verschlechtert werden, erhalten Bestätigungen Priorität, gefolgt von Nachrichten, die von dem Empfängerabschnitt **9** desselben Schaltblocks **6** an den Senderabschnitt **10** weitergeleitet werden.

[0088] Zum besseren Verständnis wurde bei der obigen Beschreibung angenommen, dass jeder lokalen Client-Vorrichtung **2** eine einzelne lokale Schaltkreisnummer zugeordnet wurde. Es wäre natürlich auch möglich, dass einer lokalen Client-Vorrichtung **2** mehrere lokale Schaltkreisnummern zugewiesen werden.

[0089] In herkömmlichen busgestützten Systemen wird ein über den Bus gesandtes Signal von allen Vorrichtungen, die an den Bus angeschlossen sind, praktisch gleichzeitig empfangen. Das heißt, Bussysteme arbeiten auf der Grundlage der Annahme, dass in den Bus eingespeiste Systeme zu allen Punkten am Bus augenblicklich ausgebreitet werden, obgleich es in Wirklichkeit eine sehr geringe Differenz von einem Punkt zum anderen entlang des Busses gibt, weil es eine Zeit dauert, bis sich die elektrischen Signale physikalisch entlang des Busses ausgebreitet haben. Dementsprechend können Busse allgemein als synchrone Systeme angesehen werden, weil Signale überall im System gleichzeitig zur Verfügung stehen.

[0090] Im Gegensatz dazu ist das elektronische Netzwerk gemäß der Erfindung ein asynchrones System, in dem Nachrichten an verschiedenen Punkten im System zu unterschiedlichen Zeiten empfangen werden, wobei es sich bei der Zeitverzögerung um Mehrfache der Zeit handelt, die es dauert, um die Nachricht von einer Client-Vorrichtung **2** zur nächsten Client-Vorrichtung **2** am benachbarten Knoten zu senden.

[0091] Ein veranschaulichendes Beispiel ist in den Fig. 5a und Fig. 5b gezeigt, welche die gleiche einfache lineare Gruppe aus Knoten zeigen, die in Fig. 2 gezeigt ist.

[0092] In **Fig.** 5 ist der zeitliche Ablauf einer Nachricht veranschaulicht, die sich vom Knoten N+1 zum Knoten N bewegt. Am Zeitpunkt t=0 wird eine Nachricht vom Knoten N+1 zum Knoten N gesandt. Dann wird am Zeitpunkt t=1 eine Bestätigung vom Knoten N an den Knoten N+1 zurückgesendet. Dies bestätigt, dass die Nachricht wohlbehalten empfangen wurde und dass die Client-Vorrichtung **2** und der Knoten N nun frei sind, um eine andere Nachricht zu empfangen.

[0093] Ein komplexeres Beispiel ist in Fig. 5b gezeigt, wobei eine Nachricht vom Knoten M ganz oben im Netzwerk zum Knoten 0 ganz unten im Netzwerk gesendet werden soll. Am Zeitpunkt t=0 wird die Nachricht vom Knoten M zum Knoten N+1 gesandt. Dann bestätigt am Zeitpunkt t=1 der Knoten N+1 den Empfang der Nachricht an den Knoten N, und am Zeitpunkt t=2 sendet der Knoten N+1 die ursprüngliche Nachricht an den Knoten N weiter. Es ist zu beachten, dass, obgleich das erneute Senden der Nachricht und das Senden der Bestätigung als zu den Zeitpunkten t=1 bzw. t=2 stattfindend identifiziert werden, um zu zeigen, dass sie nicht synchron sind und zu unterschiedlichen Zeiten stattfinden können, es möglich ist, dass sie gleichzeitig versendet werden können oder dass die Nachricht an den Knoten N weitergesendet werden kann, bevor die Bestätigung an den Knoten M zurückgesendet wird. Das liegt daran, dass das Senden von Nachrichten in entgegengesetzte Richtungen durch die zwei Schaltblöcke **6a** und **6b** in jedem Schalter **3** unabhängig und nicht-synchronisiert stattfindet und beide warten müssen, bis das Versenden von Nachrichten beendet ist, die bereits durch ihre jeweiligen Senderabschnitte **10** gesendet werden. Dann wird, wenn die Nachricht am Knoten N empfangen wurde, am Zeitpunkt t=3 eine Bestätigung durch den Knoten N zum Knoten N+1 zurückgesendet, und zum Zeitpunkt t=4 wird die Nachricht in den Knoten 0 kopiert. Schließlich sendet am Zeitpunkt t=5 der Knoten 0 eine Bestätigung des Empfangs der Nachricht an den Knoten N.

[0094] Es wird keine Bestätigung, dass die Nachricht erfolgreich am Knoten 0 empfangen wurde, an den Knoten M geleitet. Nur der erfolgreiche Empfang am nächsten Knoten wird auf jeder Stufe des Nachrichtentransports bestätigt. Um den Betrag der genutzten Systembandbreite zu minimieren, ist die Bestätigung eine einfache Letzte-Nachricht-erhalten-Bestätigung, die keinerlei Daten, welche die ursprüngliche Nachricht oder ihren Inhalt identifizieren, oder Originalnachricht-Routingdaten enthält. Die Bestätigung ist immer eine Bestätigung des Empfangs der letzten Nachricht, die in der entgegengesetzten Richtung versandt wurde, so dass es nicht erforderlich ist, diese Daten in die Bestätigungsnachricht auf-

zunehmen.

[0095] Die oben beschriebene Schaltblockarchitektur ist eine Minimalimplementierung, die nur einen einzigen Puffer zwischen dem Sende- und dem Empfangsabschnitt aufweist. Sobald eine empfangene Nachricht von dem Empfängerabschnitt **9** zu dem Senderabschnitt **10** weitergeleitet wurde, kann der Empfängerabschnitt **9** beginnen, eine zweite Nachricht zu empfangen, so dass der Schaltblock **6** als Ganzes praktisch doppelt gepuffert ist.

[0096] Ein Nachteil dieser minimalistischen Schaltblockarchitektur ist, dass, wenn eine Reihe von Nachrichten durch den Knoten geleitet werden sollen, die Rate, mit der ankommende Nachrichten empfangen werden können, auf die Rate begrenzt ist, mit der abgehende Nachrichten gesendet werden können, weil eine empfangene Nachricht erst dann in den Puffer übertragen werden kann, um den Empfang der nächsten Nachricht zu ermöglichen, wenn die Nachricht, die zuvor in den Puffer übertragen wurde, gesendet wurde. Dieses Problem kann durch Verwenden einer komplexeren Architektur überwunden werden, indem der Puffer vergrößert wird, um das Speichern mehrerer Nachrichten zu ermöglichen, wodurch der Schaltblock **6** als ein Geschwindigkeitsanpassungselement fungieren kann. Ein solcher vergrößerter Puffer, der mehrere Nachrichten speichern kann, muss ein Speicher vom FIFO-Typ (First in First out) sein, um die Reihenfolge der Nachrichten, die den Knoten passieren, konstant zu halten, aber es gibt keine Grenze dafür, wie viele Nachrichten der FIFO-Puffer speichern kann; das heißt, der FIFO-Puffer kann beliebig tief sein, so wie es erforderlich ist, um einen reibungslosen Datenfluss zu ermöglichen, und ist nur durch die Kosten begrenzt.

[0097] Die oben beschriebene Netzwerkarchitektur bietet ein Grundniveau an Datensicherheit innerhalb des Systems, weil Nachrichten, die an eine Client-Vorrichtung **2** an einem bestimmten Knoten gesendet werden, durch den lokalen Schalter **3** aus dem Signalstrom entlang des Netzwerks extrahiert werden und dadurch für Client-Vorrichtungen **2** an Knoten weiter unten im Netzwerk weder verfügbar noch zugänglich sind. Des Weiteren werden Nachrichten, die durch eine Client-Vorrichtung **2** an einem bestimmten Knoten zu einer Client-Vorrichtung an einem anderen Knoten gesendet werden, nur durch den lokalen Schalter **3** der Zwischen-Client-Vorrichtung **2** geleitet und werden nicht in den lokalen Verarbeitungsabschnitt **4** der Zwischen-Client-Vorrichtung **2** eingespeist.

[0098] Dieses Grundniveau an Sicherheit ist natürlich angreifbar. Normalerweise wäre es einem Nutzer einer Client-Vorrichtung möglich, den lokalen Verarbeitungsabschnitt **4** zu benutzen, um sich Zugriff auf Nachrichten zu verschaffen, die durch den lokalen Schalter **3** zu anderen Client-Vorrichtungen **2** passieren, aber ein gelegentliches unerlaubtes Mithören würde verhindert werden. Ebenso könnte jeder mit physischem Zugang zum System Instrumente wie zum Beispiel einen Logikzustandsanalysator verwenden, um Transaktionen auf einem Datenpfad aufzuzeichnen, und ein unbefugter Knoten könnte dann in den Datenpfad eingefügt werden, um zulässige Nachrichten abzufangen und Nachrichten einzuspeisen, um die eine oder andere Form eines Angriffs auf die Datenintegrität des Netzwerks zu führen. Ein solcher Angriff hängt allerdings vom physischen Zugang zum System ab.

[0099] Eine bessere Datensicherheit kann man durch Verschlüsseln der Nachrichten erhalten, die über die einzelnen Datenverbindungen zwischen Paaren verbundener Knoten gesendet werden.

[0100] Ein erstes Verfahren, dies zu bewerkstelligen, ist in Fig. 6 gezeigt, wobei jeder der Empfänger **9** und Sender **10**, aus denen die Schaltblöcke **6** eines lokalen Schalters **3** bestehen, mit einem programmierbaren Exklusiv-ODER-Element **33** versehen ist, das nach dem Empfang durch den Empfängerabschnitt **9** oder vor dem Senden durch den Senderabschnitt **10** eine logische Exklusiv-ODER-Funktion auf jede Nachricht anwendet.

[0101] Die Exklusiv-ODER-Funktion, die durch die programmierbaren Exklusiv-ODER-Elemente **33** in jedem lokalen Schalter **3** angewendet wird, hat die Form einer Exklusiv-ODER-Maske, die durch den lokalen Verarbeitungsabschnitt **4** gesteuert wird.

[0102] Die Exklusiv-ODER-Maske codiert die gesamte gesendete Nachricht so, dass neben den eigentlichen Daten, die durch die Nachricht transportiert werden, auch der Nachrichtenkopf und die Routinginformationen, wie zum Beispiel die Virtuelle-Schaltkreis-Identifikation des Empfängers, der Datentyp und die Datengröße, allesamt codiert werden.

[0103] Die Exklusiv-ODER-Maske, die durch die Exklusiv-ODER-Elemente **33** angewendet wird, kann periodisch modifiziert werden, indem Nachrichten an alle Client-Vorrichtungen **2** in dem System gesendet werden, mit denen sie angewiesen werden, die Exklusiv-ODER-Maske zu ändern.

[0104] Ein solches System macht Angriffe auf das System mit Hilfe eines Logikzustandsanalysators wertlos, weil es nicht möglich ist zu identifizieren, was Nachrichten bedeuten, und selbst wenn versucht wird, die benutzte Exklusiv-ODER-Maske zu schlussfolgern, dürfte dies durch die periodischen Änderungen zunichte gemacht werden.

[0105] Das Ändern der Exklusiv-ODER-Masken kann entweder in der Weise geschehen, dass alle

Client-Vorrichtungen **2** angewiesen werden, zu einem bestimmten künftigen Zeitpunkt zu der neuen Exklusiv-ODER-Maske zu wechseln, oder indem eine Maskenwechselnachricht so durch das Netzwerk hindurch ausgebreitet wird, dass jede Client-Maschine **2** der Reihe nach die Maskenwechselnachricht erhält, die ihr sagt, die neue Exklusiv-ODER-Maske auf alle künftigen Nachrichten anzuwenden und die Maskenwechselnachricht an die nächste Client-Vorrichtung **2** am nächsten Knoten weiterzusenden. Jeder der beiden Wege dürfte effektiv sein, obgleich die Asynchronität des Systems und die Tatsache, dass die Schaltblöcke **6**, die in demselben Schalter **3** in entgegengesetzten Richtungen arbeiten, und der Empfangs- und der Sendeabschnitt **9** bzw. **10** jedes Schaltblocks **6** nicht synchron sind, die Anwendung eines Protokolls erfordern, um Nachrichten zu handhaben, die gesendet oder empfangen werden, wenn Anweisungen zum Ändern der Exklusiv-ODER-Maske empfangen werden oder zur Ausführung anstehen.

[0106] Die Nachrichten, die durch die Exklusiv-ODER-Maske verschlüsselt werden, sind in ihrer Größe identisch mit den Originalnachrichten vor der Verschlüsselung, weshalb dieses Verschlüsselungsverfahren nicht die Systemleistung wegen zusätzlichen Bandbreitenbedarfs schmälert.

[0107] Durch Einbinden eines zusätzlichen Sicherheitsprozessors in jeden lokalen Schalter **3** kann die Sicherheit erhöht werden.

[0108] In Fig. 7 ist ein lokaler Schalterabschnitt **3** gezeigt, der zwei Schaltblöcke **6a** und **6b** umfasst, die auf dem stromabwärtigen bzw. dem stromaufwärtigen Datenpfad arbeiten, die durch den Schalter **3** hindurch verlaufen. Der lokale Schalter **3** enthält ebenfalls einen zusätzlichen Sicherheitsprozessor **34**.

[0109] Der zusätzliche Sicherheitsprozessor **34** setzt die Exklusiv-ODER-Masken, die durch die Exklusiv-ODER-Elemente **33** angewendet werden. Das heißt, die Exklusiv-ODER-Masken werden nicht durch den lokalen Verarbeitungsabschnitt **4** gesetzt, wie es in dem oben beschriebenen System ohne den zusätzlichen Sicherheitsprozessor **34** der Fall ist.

[0110] Während des Betriebes kommunizieren die zusätzlichen Sicherheitsprozessoren **34** in den gegenüberliegenden lokalen Schaltern **3** in den Client-Vorrichtungen **2** in benachbarten Knoten miteinander und tauschen öffentliche Verschlüsselungsschlüssel aus. Die zusätzlichen Sicherheitsprozessoren **34** verwenden dann diese öffentlichen Schlüssel zum Verschlüsseln und gegenseitigen Ausgeben von Exklusiv-ODER-Masken, die auf die zwischen ihnen versendeten Nachrichten angewendet werden.

[0111] Diese Kommunikation und dieser Austausch von öffentlichen Schlüsseln erfolgen durch Einspeisen zusätzlicher Nachrichten in den Nachrichtenstrom in der Kommunikationsverbindung zwischen den beiden Knoten. Dies erfordert zusätzliches Routen und Verarbeiten von empfangenen Nachrichten und Arbitrieren von zu versendenden Nachrichten durch die Empfängerabschnitte **9** und Senderabschnitte **10**, da das System nun Nachrichten zu und von dem zusätzlichen Sicherheitsprozessor **34** an jedem lokalen Schalter **3** sowie Nachrichten zu und von den lokalen Verarbeitungsabschnitten **4** und Nachrichten, die über das Netzwerk zu anderen Knoten weiterzuleiten sind, und Bestätigungen transportiert.

[0112] Der Austausch von öffentlichen Schlüsseln und das Setzen von Exklusiv-ODER-Masken erfolgt separat durch jeden zusätzlichen Sicherheitsprozessor **34** für Nachrichten zu und von dem nächsten Knoten stromaufwärts und zu und von dem nächsten Knoten stromabwärts, so dass die stromaufwärtigen Nachrichten und die stromabwärtigen Nachrichten mittels verschiedener Exklusiv-ODER-Masken verschlüsselt und entschlüsselt werden.

[0113] In Intervallen stellt jeder zusätzliche Sicherheitsprozessor **34** die Kommunikation zu den zusätzlichen Sicherheitsprozessoren **34** in benachbarten Knoten wieder her, und in synchronisierter Form wechseln sie die Exklusiv-ODER-Masken. Wird dieses System verwendet, so ist es lediglich erforderlich, dass die Exklusiv-ODER-Masken zur gleichen Zeit an beiden Enden jeder Kommunikationsverbindung zwischen Knoten gewechselt werden. Es ist nicht notwendig, dass alle Exklusiv-ODER-Masken in dem Netzwerk gleichzeitig gewechselt werden. Das heißt, ebenso, wie die Intervalle, in denen die Exklusiv-ODER-Masken gewechselt werden, zeitbasiert sind, könnten sie auch unabhängig auf der Grundlage der Anzahl von Nachrichten gewechselt werden, die über jede Kommunikationsverbindung ausgetauscht werden, oder auf der Grundlage einer Kombination dieser zwei Kriterien.

[0114] Es ist in der Regel zweckmäßig, die gleiche Exklusiv-ODER-Maske in beiden Richtungen über jede Kommunikationsverbindung zwischen Knoten zu verwenden. Darauf kommt es aber nicht an. Es kommt nur darauf an, dass die gleiche Exklusiv-ODER-Maske verwendet wird; um Nachrichten in einer Richtung über jede Kommunikationsverbindung zu verschlüsseln und zu entschlüsseln. Die Exklusiv-ODER-Maske, die in dem Empfängerabschnitt **9** des stromabwärtigen Schaltblocks **6a** verwendet wird, und die Exklusiv-ODER-Maske, die in dem Senderabschnitt **10** des stromaufwärtigen Schaltblocks **6b** in einem bestimmten lokalen Schalter **3** verwendet wird, brauchen nicht die gleichen zu sein. Gleichermaßen könnten die Intervalle, in denen diese Exklusiv-ODER-Masken gewechselt werden, verschie-

den sein. Jedoch verdoppelt das Verwenden verschiedener Masken in jeder Richtung auf derselben Kommunikationsverbindung praktisch den Verarbeitungsaufwand, der von jedem zusätzlichen Sicherheitsprozessor **34** erbracht werden muss, und verdoppelt die Anzahl der Nachrichten, die zum Steuern der Verschlüsselung versendet werden müssen. Dementsprechend kann die Verwendung der gleichen Masken in jeder Richtung in der Kommunikationsverbindung bevorzugt sein.

[0115] Die Verwendung der gleichen oder unterschiedlicher Verschlüsselungsmasken in jeder Richtung in jeder Kommunikationsverbindung ist gleichermaßen valid, und was verwendet wird, hängt von der Entscheidung der Konstrukteure oder der Nutzer ab.

[0116] Ein Vorteil dieses Systems ist, dass der Verschlüsselungsprozess vollständig durch die zusätzlichen Sicherheitsprozessoren **34** ausgeführt wird, die in jedem lokalen Schalter **3** enthalten sind, so dass die lokalen Verarbeitungsabschnitte **4** und jegliche zugehörigen Anwendungen weder die Kontrolle über den Maskenerzeugungs- und Verschlüsselungsprozess noch einen Zugriff auf den Maskenerzeugungs- und Verschlüsselungsprozess haben. Dadurch wird die Sicherheit der Verschlüsselung erhöht, weil ein Nutzer nicht von einer Anwendung in einer Client-Vorrichtung **2** aus auf Daten bezüglich der verwendeten Verschlüsselungsmasken zugreifen kann. Des Weiteren geht selbst dann, wenn auf den lokalen Schalter **3** einer Client-Vorrichtung **2** physisch zugegriffen wird, nur bei denjenigen Verschlüsselungsmasken die Sicherheit verloren, die für Nachrichten verwendet werden, die zu oder von diesem lokalen Schalter **3** transportiert werden, und diese Nachrichten stehen an dem lokalen Schalter **3** sowieso zur Verfügung.

[0117] Ein weiterer Vorteil ist, dass die eigentliche Maskenerzeugung und verschlüsselung durch den zusätzlichen Sicherheitsprozessor **34** nicht in Echtzeit zu erfolgen braucht. Das heißt, die Maskenerzeugung und -verschlüsselung kann durch den zusätzlichen Sicherheitsprozessor **34** außerhalb des Bandes ausgeführt werden, während der Rest des lokalen Schalters **3** Nachrichten unter Verwendung der bereits gesetzten Exklusiv-ODER-Masken versendet und empfängt. Infolge dessen ist die Zeit, die für die Ausführung des Maskenerzeugung und -verschlüsselungsprozesses benötigt wird, nicht maßgeblich, so dass der zusätzliche Sicherheitsprozessor **34** aus einfachen, kleinen und billigen Mikroprozessoren bestehen kann, wodurch sie in die lokalen Schalterelemente **3** mit nur marginalen Kostenauswirkungen integriert werden können. Der zusätzliche Sicherheitsprozessor **34** könnte in Makrozellen innerhalb der lokalen Schalterelemente **3** eingebettet werden.

[0118] In den obigen Beispielen sind die zusätzlichen Sicherheitsprozessoren **34** als eine einzelne Einheit gezeigt, die mit beiden Schaltblöcken **6a** und **6b** eines lokalen Schalters **3** verbunden sind. Es wäre natürlich möglich, separate zusätzliche Sicherheitsprozessoren innerhalb jedes Sicherheitsblocks **6a** und **6b** zu verwenden, aber die zwei zusätzlichen Sicherheitsprozessoren müssen miteinander in Kontakt stehen, um den Verschlüsselungsprozess richtig steuern zu können.

[0119] Diese Anordnung gewährleistet, dass jeder Versuch, die Sicherheit des Systems zu beeinträchtigen und Daten herauszuziehen, nur Zugriff auf einen Teil der Daten, die über das Netzwerk transportiert werden, über einen relativ kurzen Zeitraum verschaffen würde.

[0120] Wenn das Netz zu Beginn eingeschaltet wird, oder nach einer netzwerkweiten Rücksetzung, tauschen die zusätzlichen Sicherheitsprozessoren **34** öffentliche Schlüssel aus und setzen die Exklusiv-ODER-Verschlüsselungsmasken, bevor sie das Versenden anderer Nachrichten gestatten.

[0121] Ein Verfahren, die Sicherheit, die durch die zusätzlichen Sicherheitsprozessoren **34** geboten wird, weiter zu erhöhen, ist, eine Smartcard-Nutzerauthentifizierung in die lokalen Schalter **3** zu integrieren.

[0122] Ein Beispiel ist in Fig. 8 gezeigt, wo eine Smartcard-Einschubschlitz **35**, der mit dem zusätzlichen Sicherheitsprozessor **34** verbunden ist, in den lokalen Schalter **3** integriert ist.

[0123] Der Einschub der Smartcard in den Schlitz **35** fungiert als Nutzerauthentifizierung und ermöglicht es dem zusätzlichen Sicherheitsprozessor **34**, den Betrieb aufzunehmen. Des Weiteren stellt die Smartcard einen Ausgangspunkt oder Ausgangspunkte für die verwendeten Exklusiv-ODER-Verschlüsselungsmasken bereit.

[0124] Wenn sich keine Smartcard in dem Smartcard-Einschubschlitz **35** befindet, so ist der lokale Schalter **3** nicht funktionsfähig, weil der zusätzliche Sicherheitsprozessor **34** nicht die Exklusiv-ODER-Masken setzt und nicht den Betrieb der Schaltblöcke **6a** und **6b** ermöglicht. Natürlich kann es in der Praxis zweckmäßig sein, auch Verbindungen von dem Smartcard-Einschubschlitz **35** zu anderen Teilen des lokalen Schalters **3** zu integrieren, um weitere Teile des lokalen Schalters **3** zu deaktivieren, wenn sich keine Smartcard in dem Schlitz **35** befindet.

[0125] Des Weiteren ist selbst dann, wenn eine physisch kompatible Smartcard in den Smartcard-Einschubschlitz **35** eingesteckt wird, aber diese Smartcard keine korrekte Smartcard ist, wenn sie zum Bei-

spiel nur bis zu einem bestimmten Datum gültig ist, das bereits abgelaufen ist, diese Smartcard nicht in der Lage, für den zusätzlichen Sicherheitsprozessor **34** einen Ausgangspunkt für eine Exklusiv-ODER-Maske bereitzustellen, der mit den Netzwerkanforderungen kompatibel ist. Infolge dessen ist der zusätzliche Sicherheitsprozessor **34** nicht in der Lage, wirksame Exklusiv-ODER-Verschlüsselungsmasken zu setzen, die zu denen passen, die in Schaltern **3** an benachbarten Knoten verwendet werden, und der lokale Schalter **3** ist auch hier funktionsunfähig.

[0126] Wie oben erläutert, bietet die Funktionsweise der Netzwerkarchitektur gemäß der Erfindung selbst ohne die Verwendung eines zusätzlichen Sicherheitsprozessors **34** einen gewissen Grad an Sicherheit. Ob die oben beschriebenen verbesserten verschlüsselungsgestützten Sicherheitsoptionen verwendet werden oder nicht, ist wie bei den meisten Sicherheitsentscheidungen ein Kompromiss zwischen der Bedeutung, die der Sicherheit beigemessen wird, und den Kosten.

[0127] Wenn nutzerauthentifizierende Smartcards verwendet werden sollen, so können sie je nach dem gewünschten Sicherheitsgrad für einen einzigen, mehrere oder alle lokalen Schalter **3** in dem Netzwerk verwendet werden. Bei einigen Anwendungen mit extrem hohem Sicherheitsbedarf kann es angebracht sein, Smartcards zur Nutzerauthentifizierung an allen lokalen Schaltern **3** einzusetzen, während es in weniger sicherheitskritischen Anwendungen genügen kann, eine Smartcard-Nutzerauthentifizierung nur in der Gateway-Client-Vorrichtung **2**, die sich mit dem Internet verbindet, oder in der Gateway-Client-Vorrichtung **2**, welche die sicherheitskritischsten Daten enthält und erzeugt, zu verwenden.

[0128] Es versteht sich, dass die oben beschriebenen Sicherheitsmerkmale von der Netzwerk-Hardware und -Software selbst abhängen und vollkommen unabhängig von Anwendungen – und vollständig transparent für Anwendungen – sind, die das Netzwerk nutzen und über das Netzwerk tätig sind. Jegliche anwendungsbasierten Sicherheitsmerkmale wie zum Beispiel Datenverschlüsselung durch die Anwendungen sind vollkommen von den oben beschriebenen Sicherheitsmerkmalen unabhängig.

[0129] Die Verwendung von Exklusiv-ODER-Masken ist vorteilhaft, weil sie das Senden und Empfangen von Nachrichten nur geringfügig zusätzlich verzögern, weil sie nicht die Nachrichten vergrößern und weil sie einfach und kostengünstig implementiert werden können. Es könnten aber auch alternative Verschlüsselungsmasken oder -anordnungen verwendet werden.

[0130] Es wird nun ein Beispiel für ein Nachrichtenformat und für Codes beschrieben, die sich zur Verwendung in einem System dieses Typs eignen.

[0131] Wie in Fig. 9a gezeigt, hat das Nachrichtenformat einen Nachrichtentyp- und -routingabschnitt, der einen 2-Bit-Nachrichtentypcode, einen 2-Bit-Datengrößencode und 6-Bit-Zielort- und -Quellenidentifikatoren umfasst. Das Nachrichtenformat kann auch einen Datenabschnitt aufweisen, der 32- oder 128-Bit-Nutzdaten umfasst.

[0132] Diese Anordnung vereinfacht die Logik, die in den endlichen Automaten der Schaltblöcke **6** verwendet wird, da der Bitzähler und der Frühabbruch des folgendes Feldes verarbeitet werden können.

[0133] Die Verwendung des 6-Bit-Quellen- und -Zielortcodes in dem Beispiel würde das Netzwerk auf 64 Client-Vorrichtungen an 64 Knoten beschränken. Das wird für die meisten Heimsysteme als ausreichend angesehen. Das ist aber ein reines Beispiel, und es könnten bei Bedarf auch mehr Zielort- und Quellenidentifikatorbits verfügbar gemacht werden.

[0134] Die Nachrichtentypcodes sind in Fig. 9B gezeigt, und diese identifizieren die Nachricht als eine Bestätigung der letzten gesendeten Nachricht oder die Sicherheitsstufe der Nachricht. In diesem Beispiel sind Stufe-1-Nachrichten nicht-sichere Nachrichten zwischen Verarbeitungselementen an den Knoten. Jeder Knoten darf nur Datenanforderungsnachrichten oder Antworten an frühere Anforderungen in diesem Format senden und darf nur Datenanforderungen oder Rücklaufinformationen als Antwort auf eine frühere Anforderung empfangen. Eine Nachrichtenweitergabe dieses Typs wird normalerweise dafür verwendet, Interrupt-Anforderungen zu berichten und Netzwerkprotokolle zu transportieren.

[0135] Nachrichten, die Daten enthalten, die zu und von den Anwendungen der Client-Vorrichtungen **2** anstatt von und zu den Schaltern **3** selbst gesendet werden, werden ebenfalls als Stufe-1-Nachrichten betrachtet.

[0136] Stufe-2-Nachrichten sind vorcodierte Nachrichten zwischen Anwendungsprozessoren zum Aufstellen von Verschlüsselungsmasken zwischen den Knoten und sind im Wesentlichen einem speziellen Zweck dienende Stufe-1-Nachrichten.

[0137] Stufe-3- und -4-Nachrichten dienen der Kommunikation zwischen den zusätzlichen Sicherheitsprozessoren **34** an verschiedenen Knoten.

[0138] Bestätigungsnachrichten enthalten keine Nutzdaten und sind durch den Nachrichtentypcode ausdrücklich als solche identifiziert.

[0139] In Fig. 9c sind die Datengößencodes ge-

zeigt, und diese zeigen an, ob die Nachricht null Daten, ein einzelnes Wort (32 Bits) oder Daten aus vier Wörtern (**128** Bits) an Daten als Nutzdaten enthält. Normalerweise haben nur Bestätigungen einen Datengehalt von null.

[0140] Wie in den Fig. 4a und Fig. 4b angedeutet, transportiert die Kommunikationsverbindung zwischen benachbarten Knoten Daten-, Takt- und Framesignale.

[0141] Das Datensignal stellt natürlich die eigentlichen Daten dar, aus denen die Nachrichten bestehen, die über das Netzwerk transportiert werden, wie oben erläutert.

[0142] Das Taktsignal wird benötigt, um zu gewährleisten, dass die gegenüberliegenden Sender- und Empfängerabschnitte **9** und **10** in den Schaltern **3** an jedem Ende jeder Kommunikationsverbindung in dem System Daten mit der gleichen Rate senden bzw. empfangen, um eine zuverlässige Datenübertragung gestatten.

[0143] Herkömmlicherweise arbeiten Netzwerke mit einem gemeinsamen Taktsignal im gesamten Netzwerk, wobei jegliche Differenzen allein die Folge von Ausbreitungsverzögerungen sind, und in der Tat ist eine solchen Anordnung mit Taktgleichheit in einem System vom Datenbustyp obligatorisch.

[0144] In der erfindungsgemäßen elektronischen Netzwerkarchitektur sind die gegenüberliegenden Sender- und Empfängerpaare **9** und **10** in den Schaltern **3** benachbarter Knoten so verbunden, dass eine asynchrone Logikschleife gebildet wird, die ein Taktsignal erzeugt, das zum Synchronisieren der Sender und Empfänger und der Datenverbindung zwischen ihnen verwendet wird. Diese Logikschleife ist schaubildhaft in Fig. 10 gezeigt.

[0145] Ein Taktstatuswechsel wird in dem Sendeabschnitt **9** des stromaufwärtigen lokalen Schalters **3a** an dem stromaufwärtigen Knoten erzeugt und über den Kommunikationspfad zu dem Empfangsabschnitt **10** des lokalen Schalters **3b** an dem stromabwärtigen Knoten gesendet. Der Taktübergang wird dann durch einen Inverter **36** invertiert, um einen Taktübergang mit entgegengesetzter Polarität zu erzeugen, und wird durch den Sendeabschnitt **10** des stromabwärtigen lokalen Schalters **3b** zurück zu dem Empfangsabschnitt **9** des stromaufwärtigen lokalen Schalters **3a** wiederversendet, wo es zu dem Sendeabschnitt **9** zurückgeleitet und wiederversendet wird.

[0146] Das erzeugt eine Schleife mit einer Verstärkung von –1.

[0147] Wenn die Gesamtverzögerung um die Schleife herum als δTu plus δTd angesehen wird, wobei δTu die Verzögerung ist, die den stromaufwärtigen lokalen Schalter **3a** passiert, und δTd die Verzögerung ist, die den stromabwärtigen lokalen Schalter **3b** passiert, so kommt die Taktimpulsschleife bei einer Frequenz in Resonanz, die eine Periode von ungefähr 2 (δTu + δTd) hat.

[0148] In dem System ist es erforderlich, dass die Verzögerung in jedem Knoten, das heißt δTu und δTd, ausreicht, damit ein Senderabschnitt ein Bit aus seinem Ausgangsregister senden kann oder damit ein Empfänger ein ankommendes Bit korrekt empfangen und speichern kann.

[0149] In der Schleife verleiht der Inverter eine Phasenverschiebung von 180°, und der Rest der Phasenverschiebung bei der Schleifenresonanzfrequenz wird durch die verschiedenen Verzögerungen an das Signal, das die Schleife durchquert, erzeugt.

[0150] Dadurch wird es möglich, dass das Taktsignal, das in jeder Datenverbindung in dem Netzwerk verwendet wird, automatisch auf den optimalen Wert für die schnellste Datenübertragung gesetzt wird, die durch die Elektronik in den gegenüberliegenden lokalen Schaltern **3**, die Länge der Kommunikationsverbindung und die Umgebungstemperatur zugelassen wird.

[0151] Die Schalter **3** sind so konfiguriert, dass, wenn ihre stromaufwärtigen oder stromabwärtigen Abschnitte nicht über eine Kommunikationsverbindung mit einem anderen Schalter **3** verbunden sind, ein nicht-verbundener stromabwärtiger Sendeport auf einem logischen Taktpegel von Eins gehalten wird, während ein nicht-verbundener stromaufwärtiger Empfangsabschnitt auf einem logischen Taktpegel von Null gehalten wird.

[0152] Wenn die nicht-verbundenen stromaufwärtigen und stromabwärtigen Abschnitte von zwei mit Strom versorgten Schaltern durch eine Kommunikationsverbindung entgegengesetzt verbunden werden, so setzt die logische Eins, die durch den stromabwärtigen Sendeabschnitt des stromaufwärtigen Schalters **3** erzeugt wird, die logische Null in dem stromaufwärtigen Empfangsabschnitt des stromabwärtigen Schalters **3** außer Kraft. Diese Änderung erscheint dem stromabwärtigen Schalter als ein Taktstatusübergang, so dass die Schleife zu oszillieren beginnt, wie oben dargelegt.

[0153] Das verschafft den Vorteil, dass neue Client-Vorrichtungen während des Betriebes an das System angeschlossen werden können und dass automatisch ein Taktsignal erzeugt wird, dass eine Kommunikation mit der neuen Client-Vorrichtung ermöglicht. Wenn des Weiteren keine Client-Vorrichtung angeschlossen ist, so werden die nicht-verbundenen Ports auf einem konstanten Spannungspegel

ohne Wechselstromaktivität gehalten und erzeugen so keinerlei elektromagnetische Störungen.

[0154] Systeme, die ein automatisches Anschließen neuer Elemente an ein in Betrieb befindliches System ermöglichen – ein sogenanntes "Hot Plugging" –, gibt es zwar, aber bekannte Systeme dieses Typs erfordern die kontinuierliche Übertragung alternierender Signale, wie zum Beispiel Taktsignale, an den ungenutzten Verbindern, damit das Anschließen einer neuen Vorrichtung detektiert werden kann. Infolge dessen erzeugen solche bekannten Systeme sehr viele elektromagnetische Störungen.

[0155] Des Weiteren erfordern bekannte Systeme dieses Typs komplexe Hardware und Software, um das Integrieren neu angeschlossener Vorrichtungen in ein System zu ermöglichen.

[0156] Es versteht sich, dass die obige Beschreibung rein veranschaulichend ist. Die logischen Taktpegel, die an den verschiedenen nicht-verbundenen Ports gehalten werden, können in vielen Kombinationen variiert werden, sofern ein offensichtlicher Taktimpulsstatusübergang beim Anschließen erzeugt wird.

[0157] Die Verwendung einer einzelnen Inversion in der Schleife ist nicht wesentlich. Das wesentliche Kriterium ist, eine ungerade Zahl an Inversionen zu haben. Die genaue Position der oder jeder Inversion ist unwichtig, und der Inverter **36** kann sich in jedem der Schalter **3** befinden.

[0158] Es ist bevorzugt, dass die Schleifen durch einen initialen Taktimpuls von dem stromaufwärtigen Schalter **3** angesteuert werden.

[0159] Wenn einer der lokalen Schalter **3** durch ein neues Modell ersetzt wird, das in der Lage ist, schneller zu arbeiten, so bewirkt die verringerte Verzögerung in der Schleife automatisch, dass die Taktsignale für die Kommunikationsverbindungen, die der Schalter verwendet, vermehrt werden. Gleichermaßen werden Änderungen bei den Verzögerungszeiten in den Datenverbindungen, zum Beispiel aufgrund eines Austauschs eines Kabels gegen ein anderes mit anderer Länge, automatisch durch eine Änderung der Taktrate kompensiert, wie auch im Fall von Änderungen bei der Betriebsgeschwindigkeit der Schalter **3** infolge von Temperaturveränderungen.

[0160] Es versteht sich, dass die Taktrate für jede Kommunikationsverbindung in dem Netzwerk eine andere sein kann, und in der Praxis wird sie wahrscheinlich wenigstens geringfügig verschieden sein. Und obgleich die internen Taktraten, die von den Schaltern **3** verwendet werden, und die Taktraten, die zum Übertragen von Daten über die Datenverbindungen verwendet werden, zueinander in Beziehung stehen, weil eine Erhöhung der Schaltertaktrate das Unterstützen einer erhöhten Datenübertragungstaktrate in seinen Datenverbindungen gestattet, sind sie nicht die gleichen.

[0161] Obgleich die oben beschriebene Technik zum Einstellen von Taktraten in Datenverbindungen als überaus vorteilhaft angesehen wird, ist sie nicht von wesentlicher Bedeutung und in einigen Situationen unpraktisch. Um diese Technik des automatischen Einstellens von Taktraten verwenden zu können, muss eine Zweiweg-Datenverbindung zwischen den Schaltern an zwei benachbarten Knoten bestehen. Wo nur eine Einweg-Datenverbindung besteht, zum Beispiel, wenn nur eine Einweg-Infrarotdatenverbindung vorhanden ist, muss ein herkömmliches Verfahren zum Einstellen und Synchronisieren von Taktraten verwendet werden.

[0162] Ein Beispiel für die Takt-, Daten- und Framesignale in einer Richtung über eine einzelne Kommunikationsverbindung ist in Fig. 11 gezeigt.

[0163] Die Verwendung einer Bit-synchronen Zeitsteuerung ist bevorzugt, damit die Datenrate zwischen benachbarten Knoten so groß wie möglich sein kann, ohne Bandbreite infolge von Synchronisationspräambeln zu verlieren. Das lässt sich auch einfach implementieren.

[0164] Nachrichten können partiell in eine Pipeline gesetzt werden. Wenn ein Pipelining inmitten einer Nachricht verwendet werden soll, so müssen die lokalen Schalter **3** auf der Pipeline-Datenroute so zusammenarbeiten, dass sie alle die gleiche Taktrate auf allen Kommunikationsverbindungen verwenden. Die gemeinsame Taktgeschwindigkeit muss die langsamste auf der Datenroute sein. Dementsprechend sollte das Einstellen einer gemeinsamen Taktrate durch die lokalen Verarbeitungsabschnitte **4** der Client-Vorrichtungen **2** ausgeführt werden, die ein Nachrichten-Pipelining erfordern, wobei die benötigten Schalter **3** angewiesen werden, dies nur zu tun, wenn in eine Pipeline gesetzte Nachrichten zu versenden sind, wobei die oben beschriebenen lokal eingestellten Taktraten anderweitig genutzt werden.

[0165] In jedem Netzwerk ist ein Knoten der am weitesten stromaufwärts befindliche, und einer ist der am weitesten stromabwärts befindliche. Der am weitesten stromaufwärts befindliche Knoten gilt als der Netzwerk-Master für Positionsauflösungszwecke und für das Zuweisen logischer oder Virtueller-Schaltkreis-Nummern. Wenn ein Knoten der oberste Knoten ist, so hat er bei Inbetriebnahme oder Rücksetzung kein ankommendes Taktsignal an seinem zum Ausgang (nach stromaufwärts) weisenden Empfänger. Bei Inbetriebnahme oder einer Systemrücksetzung senden alle Schalter **3** Taktsignale stromabwärts, und das Vorhandensein oder Sonstiges eines

empfangenen Taktsignals von stromaufwärts dient dem Bestimmen, ob ein Knoten ein Master ist oder nicht. Nachdem Taktsignale über einen voreingestellten Zeitraum empfangen wurden oder nicht empfangen wurden, wird der Umstand, dass sich ein Schalter **3** an einem Master-Knoten befindet oder nicht an einem Master-Knoten befindet, in einem Statusregister angezeigt, und dann wird der Rücksetzungsstatus deaktiviert.

[0166] Nach der Rücksetzung werden alle Schalter **3** mit einer zugewiesenen Adresse von null konfiguriert. Der zugewiesene Schaltkreis wird dann vom Master-Knoten ausgehend nach außen ermittelt, indem der Schalter **3** am Master-Knoten der logische Schaltkreis Null ist und eine Nachricht stromabwärts zum Knoten 1 gesendet wird, welche die logische Schaltkreisnummer **1** vergibt. Der Schalter **3** am Knoten 1 erfasst diese Nachricht und weist sich selbst die empfangene Schaltkreisnummer zu und verwendet dabei das Ergebnis als seine eigene Knotenadresse. Der Schalter **3** am Knoten 1 inkrementiert dann die empfangene Schaltkreisnummer und sendet sie stromabwärts zum Knoten 2. Dieser Prozess setzt sich fort, wobei die Virtuellen-Schaltkreis-Nummern Knoten für Knoten zugewiesen werden. Erforderlichenfalls können einem bestimmten Knoten mehrere Schaltkreisnummern zugewiesen werden. Diese Adresszuweisungsfunktionen können durch Hardware oder Software in den Schaltern **3** oder durch eine lokale Verarbeitung in der Client-Vorrichtung **2** ausgeführt werden.

[0167] Diese automatische Zuweisung von Knotennummern anstatt einer dauerhaften anfänglichen Zuweisung von Knotennummern ist erforderlich, um die Möglichkeit zu berücksichtigen, dass im Lauf der Zeit Schalter einem Netzwerk hinzugefügt oder aus einem Netzwerk entfernt oder in einem Netzwerk von einer Stelle an eine andere gesetzt werden könnten, was eine Neuzuweisung von Nummern erforderlich macht. Des Weiteren kann ein Rücksetzen, gefolgt von einer Zuweisung neuer Identifikationsnummern, zweckmäßig oder erforderlich sein, um es einem Teilnetzwerk, das durch einen Komponentenausfall von einem größeren Netzwerk getrennt wird, zu ermöglichen, unabhängig weiter zu funktionieren.

[0168] Es ist möglich, dass die Geräte an jedem Knoten nicht die gleichen technischen Fähigkeiten haben. Die Möglichkeit, dass verschiedene Knoten in der Lage sein können, unterschiedliche Taktraten zu unterstützen, wird durch das oben beschriebene Verfahren zur automatischen Taktrateneinstellung berücksichtigt.

[0169] Die Geräte aller Knoten müssen in der Lage sein, asynchrone Bit-breite und synchrone Bit-breite Übertragungen zu unterstützen, aber alle anderen Merkmale sind optional. Beim Systemstart oder einer Systemrücksetzung muss durch lokale Verarbeitung festgestellt werden, welche Einrichtungen an jedem Knoten in dem Netzwerk zur Verfügung stehen.

[0170] Zum Beispiel muss ein lokaler Prozessor, der in der Lage ist, 128-Bit-Nachrichten zu senden und zu empfangen, nicht nur prüfen, dass der Empfängerknoten einer Nachricht in der Lage ist, 128-Bit-Nachrichten zu senden und zu empfangen, sondern auch, dass alle Zwischenknoten dazu befähigt sind, wenn 128-Bit-Nachrichten zu versenden sind. Andernfalls muss die Nachricht in eine Anzahl kleinerer Nachrichten aufgeschlüsselt werden, die von den Zwischenknoten gehandhabt werden können.

[0171] Die obigen Beschreibungen des Betriebes der Computernetzwerkarchitektur und der netzwerkfunktionsspezifischen Teile der Client-Vorrichtungen **2** wurden lediglich anhand eines sehr einfachen linearen Netzwerks besprochen. Es sind jedoch auch, wie in Fig. 1 gezeigt, komplexere Netzwerkstrukturen möglich, in denen Knoten mehrere Verbindungen zu mehreren stromabwärtigen Knoten aufweisen. Um die mehreren stromabwärtigen Kommunikationsverbindungen zu bedienen, erfordern diese mehrfach verbundenen Knoten lokale Schalter **3**, die mit stromaufwärtigen und stromabwärtigen Schaltblöcken **6a** und **6b** arbeiten, die mehrere stromabwärts weisende Empfängerabschnitte **9** und Senderabschnite **10** aufweisen.

[0172] In dem stromabwärtigen Schaltblock **6a** ist die einzige zusätzliche Anforderung Hardware oder eine Logikschaltung, die es ermöglicht, dass anhand der Nachrichtenzielortadresse der entsprechende der Sendeabschnitte ausgewählt wird.

[0173] Der stromaufwärtige Schaltblock **6b** erfordert zusätzliche Pufferung und Nachrichtenarbitrierung, um die Möglichkeit zu berücksichtigen, dass mehrere Nachrichten gleichzeitig an den verschiedenen stromabwärts zeitgesteuerten Empfangsabschnitten empfangen werden, und um zu arbitrieren, welche empfangene Nachricht als nächstes gesendet werden soll.

[0174] Die Verwendung separater Sendeabschnitte zu jeder Kommunikationsverbindung ist nicht unbedingt wesentlich. Es könnte auch ein einzelner Sendeabschnitt zusammen mit einem Schalten stromabwärts des Sendeabschnitts verwendet werden, um den Zielknoten auszuwählen. Jedoch ist die Verwendung separater Sendeabschnitte für jede Kommunikationsverbindung bevorzugt, weil dies die volle Nutzung der Technik zur automatischen Taktrateneinstellung und der weiterentwickelten Sicherheitstechniken, die oben beschrieben wurden, ermöglicht.

[0175] Die beschriebene Netzwerkarchitektur kann auch als eine Architektur innerhalb der einzelnen Cli-

ent-Vorrichtungen **2** verwendet werden, um den lokalen Verarbeitungsabschnitt **4** bereitzustellen.

[0176] Obgleich eine solche Herangehensweise an die Gerätearchitektur für eine Einzelprozessorvorrichtung übermäßig komplex ist, sind in der Praxis die meisten Vorrichtungen Mehrprozessorgeräte, die von dieser Herangehensweise an die Architektur profitieren können.

[0177] Ein typischer Mikroprozessor- und Lokalverarbeitungsabschnitt **4** ist in Fig. 12 gezeigt.

[0178] Der Verarbeitungsabschnitt **4** wird durch mehrere Prozessoren **40**, in diesem Beispiel sechs Prozessoren **40a** bis **40f**, gebildet, die durch eine Reihe von Ein/Aus-Bussen oder Datenübertragungsverbindungen **41a** bis **41e**, die jeweils ein Paar Prozessoren **40** verbinden, zu einer Kette verknüpft sind.

[0179] Daten werden durch einen Ein/Aus-Bus oder eine Ein/Aus-Verbindung **42**, der bzw. die zu anderen Elementen wie zum Beispiel dem lokalen Schalter **3** und zum lokalen Eingabe- und Ausgabeabschnitt **5** führt, in den Verarbeitungsabschnitt **4** hinein- und aus dem Verarbeitungsabschnitt **4** heraustransportiert. Obgleich die Verbindungen **41a** bis **41e** Busse sein können, verbinden solche Busse lediglich zwei aufeinanderfolgende Prozessoren **40** in der Kette, und nicht alle Prozessoren **40**, wie es in einer herkömmlichen busgestützten Mehrprozessorvorrichtung.

[0180] Es sind separate Videoeingabe- und -ausgabebusse **43a** und **43b**, die alle Prozessoren **40** verbinden, vorhanden, um zu verhindern, dass Videogeräte die Verbindungen **41** zwischen den Prozessoren mit sehr großen Mengen an Videodaten überfordern.

[0181] Der Verarbeitungsabschnitt **4** arbeitet ähnlich wie das oben beschriebene lineare Netzwerk, wobei der Prozessor **40** als der am höchsten stromaufwärts befindliche Prozessor angesehen wird, der den externen Zugriff zu und von dem Verarbeitungsabschnitt **4** steuert.

[0182] Es versteht sich, dass alle Datenübertragungen zu und von den stromabwärtigen Prozessoren **40** möglicherweise durch die stromaufwärtigen Prozessoren **40** gegattert und gesteuert werden, wodurch Sicherheit geschaffen wird. Jedoch kann – ähnlich dem Netzwerk – ein Prozessor **40**, der keine Sicherheitskontrollen auf die übertragenen Daten anwenden will, die Daten einfach unverändert passieren lassen.

[0183] Die Prozessoren brauchen nicht ausschließlich arithmetisch zu sein. Sie könnten auch Audio- oder Videoprozessoren sein, die ihre eigenen Eingänge und Ausgänge haben.

[0184] Eine einfache Veranschaulichung dieses Prinzips ist in Fig. 14 gezeigt. Die Vorrichtung in Fig. 14 ist extrem einfach und hat nur drei Knoten, wobei der erste Netzwerkknoten **30** mit einem zweiten Smartcard-Knoten **31** verbunden ist, der seinerseits mit einem dritten Anwendungsprozessorknoten **32** verbunden ist. Der Netzwerkknoten **30** wird durch einen Prozessor gebildet, der eine Verbindung zu dem lokalen Schalter **3** bildet. Der Smartcard-Knoten **31** enthält einen Smartcard-Schlitz. Daten, die aus dem Netzwerk zu und von der Smartcard gesendet werden, können nicht durch den Anwendungsprozessor an dem Anwendungsprozessorknoten **32** interpretiert werden, weil die Daten, die zu und von der Smartcard gesendet werden und zu denen e-Commerce- und biometrische Daten gehören können, einfach nicht physisch an ihn gesendet werden.

[0185] Dieser Grad an Basissicherheit ist nur für eingebettete Anwendungen in einer Client-Vorrichtung **2** zuverlässig, die nur Software-Upgrades durch einen geschützten Dienst empfängt, in diesem Fall durch eine Smartcard. Andernfalls könnte die Software innerhalb des Smartcard-Knoten **31** so von einem räumlich abgesetzten Ort aus geändert werden, dass die Nachrichten, welche die sensiblen Daten enthalten, in den Prozessor an dem Anwendungsprozessorknoten **32** kopiert werden würden.

[0186] Ähnlich der oben beschriebenen Netzwerksicherheit ist dieser Grad an Sicherheit durch jeden angreifbar, der physischen Zugang zu der Vorrichtung hat, weil ein Logikzustandsanalysator benutzt werden könnte, um Transaktionen auf einem Datenpfad aufzuzeichnen und dann das Einfügen eines unbefugten Knotens zu ermöglichen. Jedoch ist ein solcher Angriff davon abhängig, dass ein physischer Zugang zu der Vorrichtung besteht, und das ist zum Beispiel eventuell nicht möglich, wenn es sich bei der Vorrichtung um einen Geldautomaten handelt oder wenn sich die Vorrichtung in einer medizinischen Apparatur befindet.

[0187] Eine alternative Struktur ist schaubildhaft in Fig. 13 gezeigt, wo eine Vorrichtung **4** mit fünf Prozessoren **40a** bis **40e** eine zusätzliche Kommunikationsverbindung **41f** aufweist, die zwischen dem am weitesten stromaufwärts befindlichen Prozessor **40a** und dem am weitesten stromauwärts befindlichen Prozessor **40f** angeschlossen ist, so dass die Prozessoren in einem Ring miteinander verknüpft sind. Diese Struktur unterstützt doppelt-gesteuerte Rotationsschleifen-Kommunikationsverbindungen. In dieser Veranschaulichung sind die möglichen separaten Videoeingangs- und -ausgangsbusse zur besseren Verständlichkeit nicht gezeigt.

[0188] Diese Ringstruktur weist eine Reihe von Vorteilen auf. Der erste ist eine erhöhte Redundanz und eine höhere Systemintegrität. Wenn der Ring auf-

grund eines Ausfalls einer Kommunikationsverbindung **41** oder eines Prozessors **40** an irgend einer Stelle unterbrochen wird, so kann die Kommunikation zwischen den übrigen Teilen der Vorrichtung trotzdem gewahrt werden, indem man Nachrichten entlang der Schleife in derjenigen Richtung routet, welche die Unterbrechung umgeht.

[0189] Im Fall eines mutmaßlichen Ausfalls kann jeder Prozessor **40** die Integrität der Schleife testen, indem er versucht, Nachrichten in beiden Richtungen entlang der Schleife an sich selbst zu schicken, und wenn eine oder beide dieser Nachrichten blockiert werden, Nachrichten der Reihe nach an die anderen Prozessoren **40** sendet, bis die Ausfallstelle ermittelt werden kann.

[0190] Obgleich in der Vergangenheit in FDDI-basierten Systemen (FDDI = Fibre Distributed Data Interface) gegenläufig rotierende Schleifen verwendet wurden, wurden sie bisher noch nie in Architekturen auf Geräteebene verwendet. Die Verwendung einer gegenläufig rotierenden Doppelschleife verleiht einen Grad an Systembetriebssicherheit, der mit herkömmlichen parallelbusbasierten Architekturen nicht erreichbar war.

[0191] Des Weiteren wird die Kommunikationsbandbreite innerhalb der Vorrichtung effektiv vergrößert, da jeder Quellenprozessor **40** Daten in beiden Richtungen an denselben Zielprozessor **40** senden kann. Durch zweckmäßige Positionierung der Prozessoren **40** entlang der Schleife kann es jedem einzelnen Prozessor ermöglicht werden, die doppelte Bandbreite in das System hinein bereitzustellen, als er es mittels einer linearen Anordnung bei ansonsten identischer Hardware könnte.

[0192] Man könnte meinen, dass, weil Daten entlang der Schleife in beiden Richtungen gesendet werden, einige der Sicherheitsvorteile, die oben in Bezug auf die Netzwerkarchitektur besprochen wurden, bei der Schleifengerätearchitektur verloren gehen. Das ist jedoch nicht unbedingt der Fall. Die Sicherheitsvorteile, die durch die Nichtverfügbarkeit von Nachrichten an einigen Knoten in dem System realisiert werden, können immer noch in der Schleifengerätearchitektur für Prozessoren realisiert werden, die während des Normalbetriebes Nachrichten in nur einer Richtung entlang der Schleife senden.

[0193] Dies würde es immer noch ermöglichen, ein höheres Maß an Sicherheit zu realisieren, wenn die Vorrichtung normal arbeitet, und die Sicherheit würde nur beeinträchtigt werden, wenn ein Ausfall eine Änderung der Richtung, in der die Nachricht gesendet wird, erzwingen würde. Wenn die Schleifenstruktur dafür verwendet wird, die Bandbreite von einem bestimmten Prozessor zu vergrößern, so gibt es einen Kompromiss zwischen Sicherheit und verfügbarer Bandbreite.

[0194] Eine geeignete Prozessorstruktur zur Verwendung innerhalb der Gerätestruktur, die in den Fig. 12 und Fig. 13 gezeigt ist, ist in Fig. 15 dargestellt.

[0195] Analog zu der Netzwerkarchitektur enthält in der Gerätearchitektur jeder Prozessor **40** ein Schaltelement **43** sowie den eigentlichen Anwendungsprozessor **44**. Dementsprechend verläuft ein virtueller Schaltkreis durch den Schalter **43** zu einem bestimmten Port am Prozessor **44**. Eine Software-gesteuerte Sicherheit wird implementiert, indem der Schalter **43** so programmiert wird, dass er die ausgewählten virtuellen Schaltkreise, das heißt ausgewählte Zieladressen, in den lokalen Prozessor **44** routet. Die Bedingungen, unter denen die akzeptierten Daten wieder in den Schalter eingespeist werden, um an den nächsten Prozessor **40** in der Reihenfolge weitergeleitet zu werden, ist dann eine Angelegenheit implementierungsspezifischer Sicherheitsregeln. Es ist bevorzugt, ATM zum Transportieren von Daten innerhalb der Vorrichtung zu verwenden. Wenn ATM verwendet wird, so ist es im Gegensatz zu einem herkömmlichen ATM-Schalter bevorzugt, dass die wieder eingespeisten Daten den gleichen Virtuellen-Schaltkreis-Kopf bekommen wie die ankommenden Daten, um zu vermeiden, dass das Empfängergerät auf einen anderen virtuellen Schaltkreis, als der ankommende es ist, umprogrammiert werden muss. Dadurch bleibt der Schalter aus der Sicht der geräteinternen Transparenz transparent.

[0196] Bei niedrigen Datenraten können alle ankommenden Daten unter Softwaresteuerung inspiziert, gefiltert und geroutet werden, doch bei höheren Datenraten ist die Verwendung von Hardwareschaltung wünschenswert.

[0197] Wie oben erläutert, bleibt die Sicherheit, die in dem Netzwerk dadurch geschaffen wird, dass Nachrichten nicht in dem gesamten System verfügbar sind, auch in einer einzelnen Vorrichtung gewahrt. Das ist innerhalb einer Vorrichtung bedeutsamer als in einem Netzwerk, weil die physische Sicherheit der internen Teile einer einzelnen Vorrichtung in der Regel viel größer ist als die physische Sicherheit des Netzwerks.

[0198] Die beschriebene Prozessorstruktur gestattet die Verwendung eines sehr einfachen Schalters **43** an jedem Prozessor, weil nur jene virtuellen Schaltkreise, die dafür bestimmt sind, an diesem Geräteknoten zur Verwendung durch den Anwendungsprozessor **44** behalten zu werden, in dem Schalter **43** registriert zu werden brauchen. Nachrichten für alle anderen Virtuellen-Schaltkreis-Zielorte werden einfach unverändert durchgelassen.

[0199] Das in Fig. 15 veranschaulichte Beispiel erfordert eine gewisse Verarbeitungskapazität an jedem Geräteknoten. Wenn es gewünscht wird, herkömmliche Peripheriegeräte mit der Vorrichtung zu verbinden, ohne einer Verarbeitungsunterstützung von der Vorrichtung zu bedürfen, so könnte ein einfacher unintelligenter Knoten verwendet werden, in dem die Peripheriekomponenten nicht in der Lage sind, den Schalter **43** zu steuern.

[0200] In Fig. 15 ist nur die Kommunikation eines einzelnen Nachrichtenstroms in einer einzigen Richtung gezeigt. Es ist außerdem erforderlich, Nachrichten in der Gegenrichtung zu senden, und das kann dadurch ausgeführt werden, dass der Schalter **43** eine Duplexfähigkeit besitzt und in der Lage ist, Nachrichten in beiden Richtungen zu senden oder zu empfangen, so dass der Schalter **43** analog zu dem lokalen Schalter **3** ist, der mit Bezug auf das Netzwerk beschrieben wurde, oder dadurch, dass zwei separate Schalter **43** vorgesehen werden, und zwar einer für jede Richtung des Nachrichtenstroms, so dass der Schalter **43** analog zu dem Schaltblock **6** ist, der mit Bezug auf das Netzwerk beschrieben wurde.

[0201] Der Grad an Datensicherheit, der innerhalb der Vorrichtungen bereitgestellt wird, kann ähnlich wie die Datensicherheit erhöht werden, die in dem Netzwerk geschaffen wird, indem Exklusiv-ODER-Masken oder sonstige Verschlüsselungseinrichtungen bereitgestellt werden, um es zu ermöglichen, dass die Nachrichten zwischen den Prozessoren **40** an verschiedenen Knoten der zu verschlüsselnden Vorrichtung transportiert werden können.

[0202] Solche Verschlüsselungsschemata sind analog zu den oben beschriebenen Schemata zur Verschlüsselung auf Netzwerkebene und werden darum hier nicht im Einzelnen beschrieben. Eine solche Verschlüsselung kann mit Exklusiv-ODER-Masken arbeiten, die unter der Kontrolle des Anwendungsprozessors **44** gesetzt werden oder autonom durch einen zusätzlichen Sicherheitsprozessor gesetzt werden, der in den Prozessor **40** integriert ist und die Exklusiv-ODER-Masken, die durch den oder die Schalter **43** verwendet werden, in einer ähnlichen Weise steuert wie der zusätzliche Sicherheitsprozessor, der mit Bezug auf die Netzwerksicherheit beschrieben wurde.

[0203] Ähnlich wie die netzwerkbasierten zusätzlichen Sicherheitsprozessoren können auch die zusätzlichen Sicherheitsprozessoren, die einen Teil der einzelnen Prozessoren **40** innerhalb einer Vorrichtung bilden, durch eine Smartcard gesteuert und mit Maskenausgangspunkten versehen werden.

[0204] Die Sicherheitsvorteile, die durch diese Anordnung auf Geräteebene realisiert werden, ähneln denen, die auf Netzwerkebene realisiert werden.

[0205] Die oben beschriebenen Gerätearchitekturen sind rein lineare Ketten von Prozessoren **40** oder Schleifen von Prozessoren **40**, und es wird erwartet, dass diese Architekturen normalerweise die zweckmäßigsten für echte Geräte sein würden. Jedoch wären auch alternative Anordnungen ähnlich denen möglich, die für das Netzwerk vorgeschlagen wurden.

[0206] Die Taktrate, die zwischen separaten Prozessoren einer einzelnen Vorrichtung verwendet wird, und die zu verwendende Nachrichtengröße können in ähnlicher Weise eingestellt werden wie bei den Techniken, die oben zur Verwendung in dem Netzwerk beschrieben wurden.

[0207] Die Verwendung der oben beschriebenen Architekturen sowohl für ein Netzwerk als Ganzes als auch für die darin befindlichen einzelnen Vorrichtungen ist aufgrund der Vorteile bevorzugt, die wie oben erläutert realisiert werden. Dies ist jedoch nicht wesentlich, und die beschriebene Architektur ist dafür vorgesehen, für Netzwerke unabhängig von der Architektur, die innerhalb der einzelnen Vorrichtungen, aus denen das Netzwerk besteht, verwendet wird, und für Vorrichtungen unabhängig von der Architektur des Netzwerks, an das sie angeschlossen sind, und sogar unabhängig davon, ob sie überhaupt an ein Netzwerk angeschlossen sind, verwendet werden zu können.

[0208] Sowohl in der Netzwerkarchitektur als auch in der Nicht-Schleifen-Gerätearchitektur ist es möglich, zusätzliche Vorrichtungen oder Prozessoren weiter stromabwärts anzuschließen, ohne den Betrieb der stromaufwärtigen Teile des Netzwerks oder der Vorrichtung zu beeinträchtigen. Dies gestattet ein "Hot Plugging", d. h. ein Anschließen während des Betriebes, sowohl neuer Vorrichtungen an ein Netzwerk als auch neuer Prozessoren an eine Vorrichtung, ohne den Betrieb des Restes des Netzwerks oder der Vorrichtung zu unterbrechen. Das ist in Konsumgütern oder -produkten normalerweise nicht möglich und ist allgemein bei datenbusgestützten Architekturen nicht möglich.

[0209] Um ein solches "Hot Plugging" zu ermöglichen, müssen die Verbinder für Vorrichtungen an das Netzwerk oder für Prozessoren innerhalb einer Vorrichtung so konfiguriert sein, dass zuerst Strom und Erdung verbunden werden und es dann ermöglicht wird, dass das neu hinzugefügte Element mit dem Empfang des Taktsignals von der Vorrichtung beginnt, von dem aus es stromabwärts angeschlossen wude. Das neu hinzugefügte Element kann sich dann in das Netzwerk oder in die Vorrichtung integrieren. Dieser Prozess ist am einfachsten, wo das Netzwerk oder die Vorrichtung eine rein lineare Anordnung ist, weil das neu hinzugefügte Element dann einfach eine Adresse oder eine logische Schaltkreisnummer zu-

gewiesen bekommen kann, indem einfach die Nummer oder die Nummern inkrementiert werden, die in der stromaufwärtigen Vorrichtung gespeichert sind. Wo eine komplexere Netzwerk- oder Gerätestruktur mit Abzweigungen verwendet wird, ist es erforderlich, dem neuen Element eine oder mehrere verfügbare eindeutige Nummern zuzuweisen, indem entweder das Netzwerk oder die Vorrichtung abgefragt wird, um herauszufinden, welche Nummern in Gebrauch sind, oder indem die Vorrichtungen oder Prozessoren, die bereits in das Netzwerk oder in die Vorrichtung integriert sind, eine Aufzeichnung zum aktuellen Status des Netzwerks oder der Vorrichtung führen, in der alle Nummern angeführt sind, die momentan in Gebrauch sind.

[0210] Ein solches Einfügen des neuen Prozessors während des Betriebes kann nicht so ohne Weiteres in einer Vorrichtung ausgeführt werden, die als eine Schleife konfiguriert ist, sofern nicht normalerweise Nachrichten entlang der Schleife nur in einer einzigen Richtung gesendet werden, so dass die zusätzliche Verbindung **40F** normalerweise nicht in Gebrauch ist, wobei in diesem Fall ihre Verbindung unterbrochen und dergestalt neu hergestellt werden könnte, dass ein weiterer Prozessor eingebunden ist, ohne dass der Betrieb des Rests der Vorrichtung gestört wird.

[0211] In der obigen Beschreibung sowohl der Netzwerk- und der Gerätearchitektur als auch der darin verwendeten Vorrichtungen und Prozessoren sind die beschriebenen generischen Vorrichtungen und Prozessoren in der Lage, Nachrichten stromaufwärts und stromabwärts sowohl zu senden als auch zu empfangen.

[0212] Es versteht sich natürlich, dass das am meisten stromaufwärts befindliche oder Gateway-Element Nachrichten stromaufwärts aus der Vorrichtung oder dem Netzwerk heraus sendet und empfängt, während die am meisten stromabwärts befindlichen Elemente an keine weitere stromabwärtige Position angeschlossen sind. Dementsprechend brauchen diese Elemente an den äußersten Positionen der Vorrichtung oder des Netzwerks nicht in der Lage zu sein, Nachrichten sowohl stromaufwärts und stromabwärts zu senden. Jedoch ist es in der Praxis normalerweise bevorzugt, die uneingeschränkte Fähigkeit zum stromaufwärtigen und stromabwärtigen Senden und Empfangen von Nachrichten in allen Elementen beizubehalten, um eine bessere Wirtschaftlichkeit durch Massenproduktion bei der Komponentenherstellung zu ermöglichen und um maximale Flexibilität bei der Umordnung von Elementen innerhalb eines Netzwerks oder einer Vorrichtung zu gestatten, selbst wenn dies beinhaltet, dass die Elemente an den äußersten Positionen des Netzwerks oder der Vorrichtung redundante Komponenten und Fähigkeiten aufweisen.

[0213] Die Verwendung des asynchronen Transfermodus' (ATM) als ein Netzwerktransportprotokoll wird als besonders vorteilhaft im Hinblick auf die Netzwerkleistung erachtet. Derzeit steht jedoch die notwendige Hardware zum Implementieren von ATM zu akzeptabel niedrigen Kosten für ein Heimnetzwerk nicht zur Verfügung.

[0214] Die Datenverbindungen zwischen Knoten in dem Netzwerk können durch Netzträgermodem, verdrillte Doppelleitungen der Kategorie 5, 75 Ω-Koaxialkabel, drahtlos oder über Verbraucher-Infrarot hergestellt werden. Dies ist eine Aufzählung brauchbarer Beispiele, die nicht erschöpfend sein sollen.

[0215] Ein alternatives Nachrichtenformat zu dem, das in Fig. 9A gezeigt ist, ist in Fig. 16 dargestellt.

[0216] In diesem alternativen Nachrichtenformat hat die Nachricht eine feste Größe mit einer Nutzdatenmenge von nur 32 Bits. Dementsprechend besteht keine Notwendigkeit für einen Datengrößencode. Der 6-Bit-Quellenidentifikator wird durch einen 8-Bit-Virtuelle-Schaltkreis-Nummer ersetzt, die zum Identifizieren der Quelle verwendet wird.

[0217] Die genannten Nachrichtenformate sind reine Beispiele. Als weitere Alternativen wäre es möglich, Nachrichtentyp und -größe in einen einzelnen Code aufzunehmen, wenn eine variable Nachrichtengröße erforderlich wäre, anstatt separate Nachrichtentyp- und Nachrichtengrößencodes zu haben.

[0218] Die oben beschriebenen Beispiele sind rein beispielhaft, und der Fachmann erkennt, dass zahlreiche Änderungen und Ersetzungen innerhalb des Geltungsbereichs der Erfindung vorgenommen werden können, der durch die angehängten Ansprüche definiert wird.

Patentansprüche

1. Vorrichtung (**3**) mit mindestens zwei Kommunikationsabschnitten (**9**, **10**), die für die Verbindung zu ähnlichen Vorrichtungen über verschiedene bidirektionale Kommunikationsverbindungen geeignet sind, gekennzeichnet dadurch, dass die Vorrichtung einen ersten Kommunikationsabschnitt hat, der angeordnet ist, auf Empfang eines Taktwechsels über eine erste Kommunikationsverbindung durch Übertragung eines Taktwechsels, der die gleiche Polarität hat, zurück über die erste Kommunikationsverbindung zu reagieren, und einen zweiten Kommunikationsabschnitt, der angeordnet ist, auf Empfang eines Taktwechsels über eine zweite Kommunikationsverbindung durch Übertragung eines Taktwechsels, der die entgegengesetzte Polarität hat, zurück über die zweite Kommunikationsverbindung zu reagieren.

2. Vorrichtung nach Anspruch 1, in der, wenn der

erste Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines ersten Taktzustands als einen Ausgang, und wenn der zweite Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines zweiten Taktzustands, der eine zum ersten entgegengesetzte Polarität hat, als einen Eingang.

3. Vorrichtung nach Anspruch 1, in der , wenn der zweite Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines ersten Taktzustands als einen Ausgang, und wenn der erste Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines zweiten Taktzustands, der eine zum ersten entgegengesetzte Polarität hat, als einen Ausgang.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, in der, wenn der erste Kommunikationsabschnitt mit dem zweiten Kommunikationsabschnitt einer anderen Vorrichtung oder umgekehrt durch eine bidirektionale Kommunikationsverbindung verbunden ist, die verbundenen Kommunikationsabschnitte angeordnet sind zum Bilden einer Schleife und die Vorrichtung ein Oszillationssignal von der Schleife als ein Taktsignal für Kommunikation über die Kommunikationsverbindung verwendet.

5. Vorrichtung nach Anspruch 4, in der, wenn der erste Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines ersten Taktzustands als einen Ausgang, und wenn der zweite Kommunikationsabschnitt nicht mit einer andern Vorrichtung verbunden ist, er angeordnet ist zum Halten eines zweiten Taktzustands, der eine zum ersten entgegengesetzte Polarität hat, als einen Eingang, wenn die Kommunikationsabschnitte zuerst verbunden werden, und
wenn der zweite Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines ersten Taktzustands als einen Ausgang, und wenn der erste Kommunikationsabschnitt nicht mit einer anderen Vorrichtung verbunden ist, er angeordnet ist zum Halten eines zweiten Taktzustands, der eine zum ersten entgegengesetzte Polarität hat, als einen Ausgang, und wenn der
erste Kommunikationsabschnitt mit dem zweiten Kommunikationsabschnitt einer anderen Vorrichtung oder umgekehrt durch eine bidirektionale Kommunikationsverbindung verbunden ist, die verbundenen Kommunikationsabschnitte angeordnet sind zum Bilden einer Schleife, und wenn die Kommunikationsabschnitte zuerst verbunden werden, die Differenz zwischen ihren gehaltenen Eingangs- und Ausgangs-Taktzuständen bewirkt, dass ein Oszillationssignal um die Schleife läuft.

6. Elektronisches Kommunikationsnetz, umfassend mindestens zwei Vorrichtungen (**3**), die über mindestens eine bidirektionale Kommunikationsverbindung verbunden sind, und dadurch gekennzeichnet, dass eine Schleife gebildet wir durch die erste Vorrichtung (**3A**), die einen Taktwechsel über die Kommunikationsverbindung empfängt und einen Taktwechsel, der dieselbe Polarität hat, zurück über die Kommunikationsverbindung sendet, und die zweite Vorrichtung (**3B**), die einen Taktwechsel über die Kommunikationsverbindung empfängt und einen Taktwechsel, der die entgegengesetzte Polarität hat, zurück über die Kommunikationsverbindung sendet, und die erste und zweite Vorrichtung angeordnet sind, zur Verwendung der Taktwechsel, die um die Schleife laufen, um ein Taktsignal zum Steuern von Datenübertragung über die Kommunikationsverbindung bereitzustellen.

7. Netz nach Anspruch 6, in dem die Taktwechsel, die um die Schleife laufen, als das Taktsignal verwendet werden.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

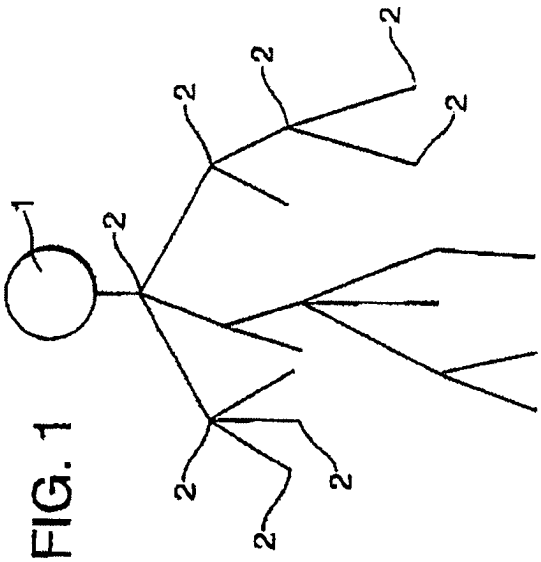


FIG. 2

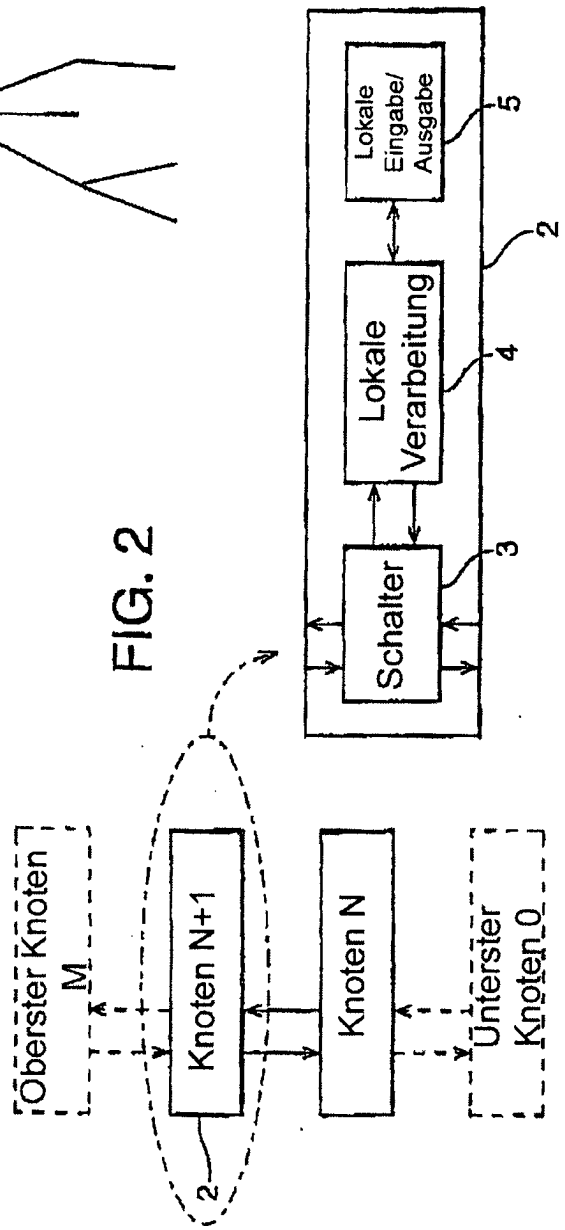
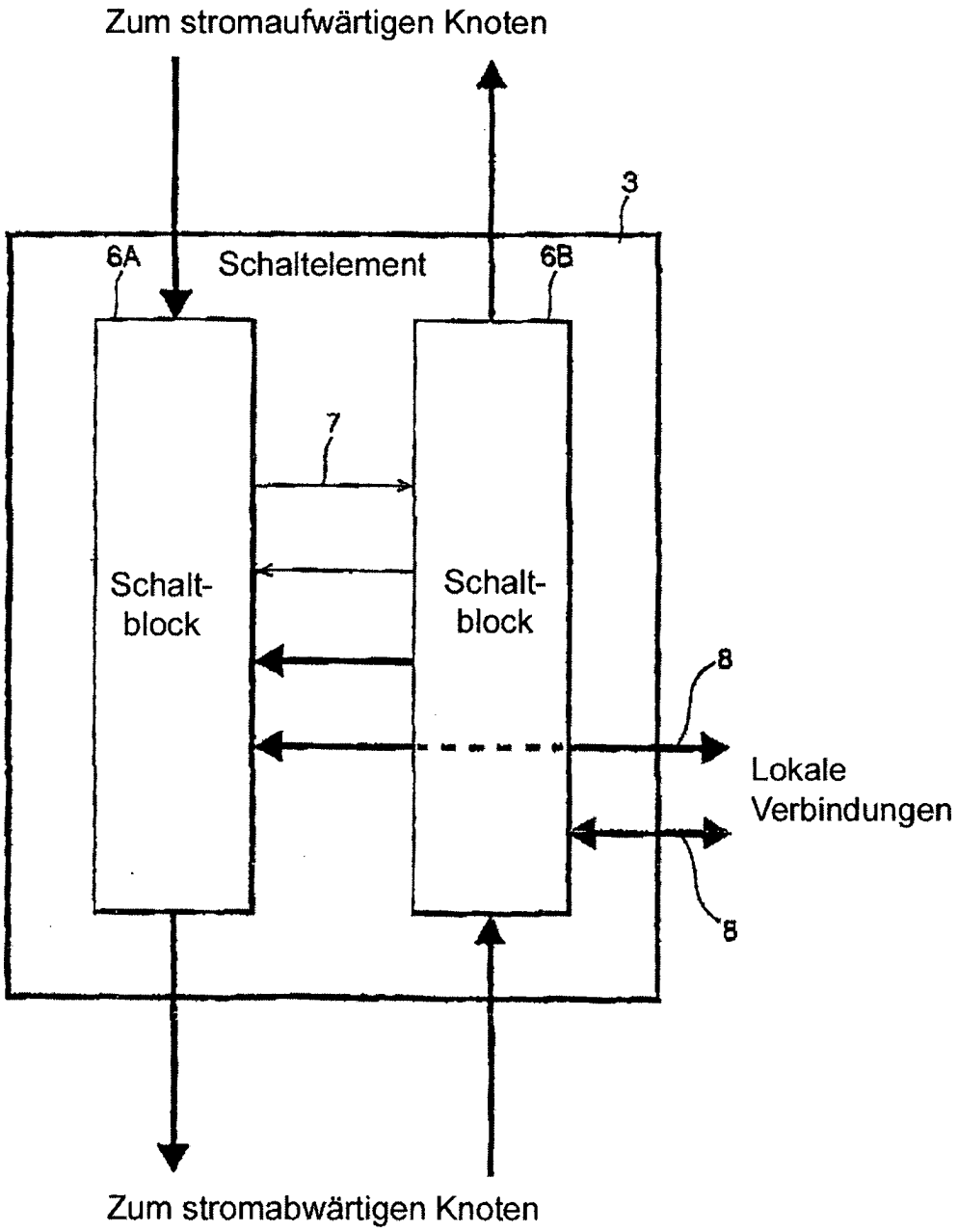


FIG. 3


Zum stromaufwärtigen Knoten
3
6A
Schaltelement
6B
7
Schalt-
block
Schalt-
block
8
Lokale
Verbindungen
8
Zum stromabwärtigen Knoten

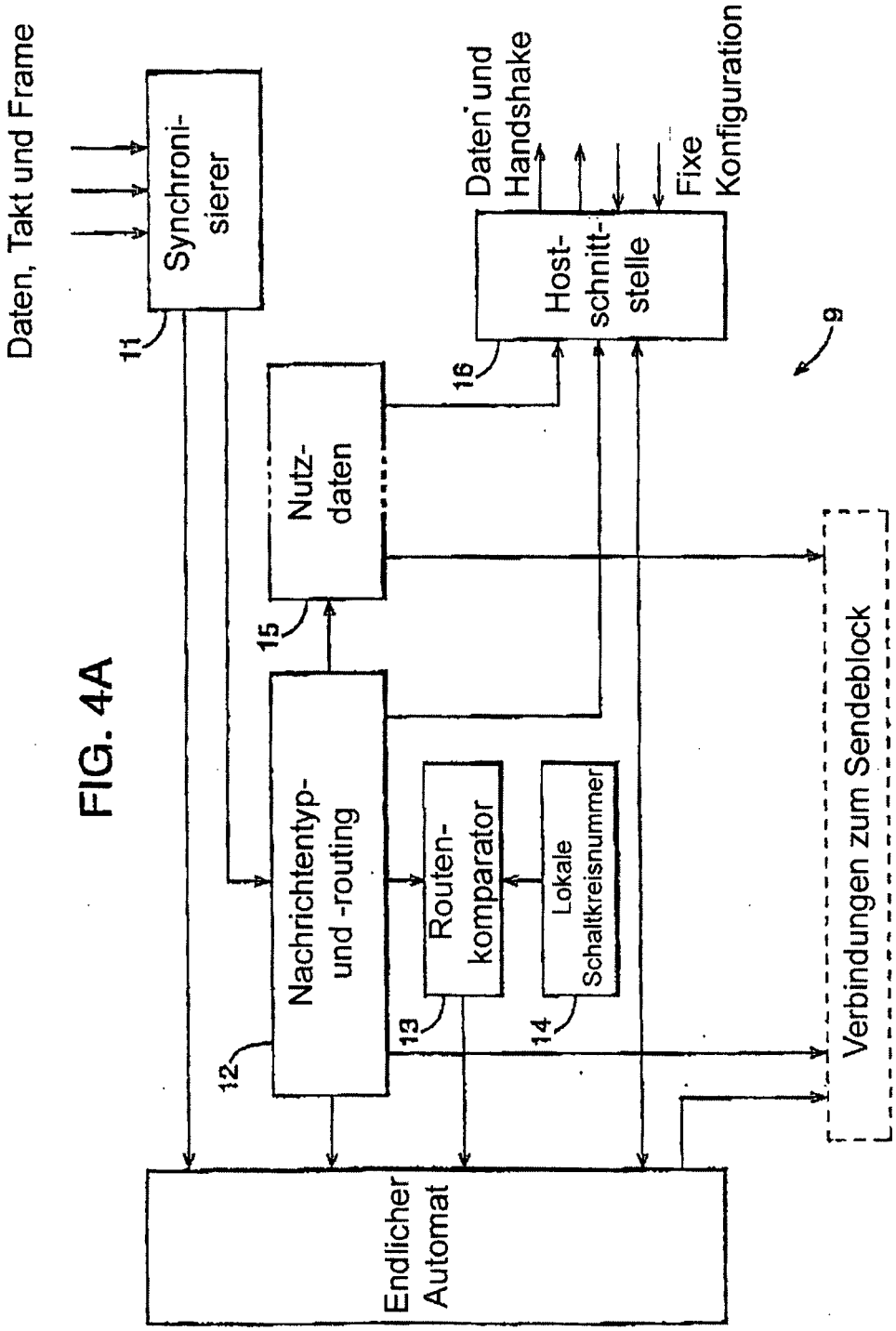

Daten, Takt und Frame
Synchroni-sierer
11
Daten und Handshake
Fixe Konfiguration
Host-schnitt-stelle
16
9
Nutz-daten
15
Nachrichtentyp- und -routing
12
Routen-komparator
13
Lokale Schaltkreisnummer
14
Verbindungen zum Sendeblock
Endlicher Automat

FIG. 4A

FIG. 4B

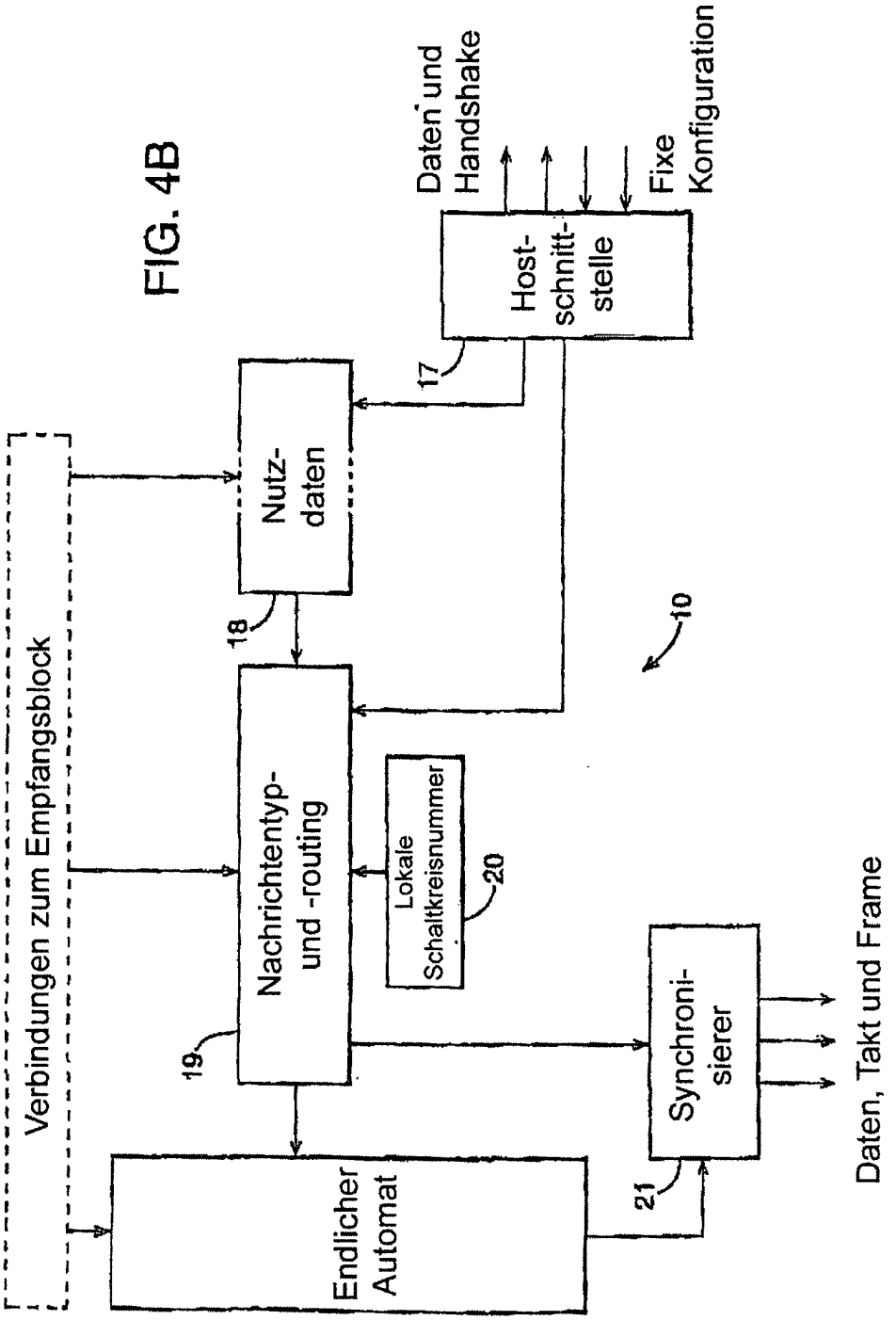

Verbindungen zum Empfangsblock
Endlicher Automat
Nachrichtentyp- und -routing
Lokale Schaltkreisnummer
Nutz- daten
Host- schnitt- stelle
Daten und Handshake
Fixe Konfiguration
Synchroni- sierer
Daten, Takt und Frame
10
17
18
19
20
21

FIG. 5A

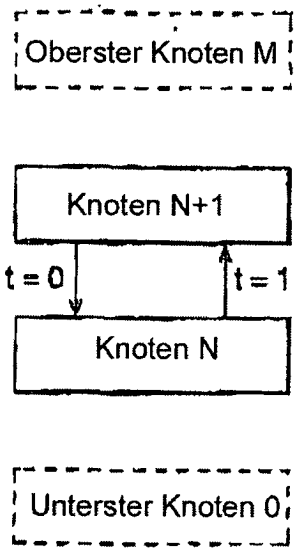


FIG. 5B

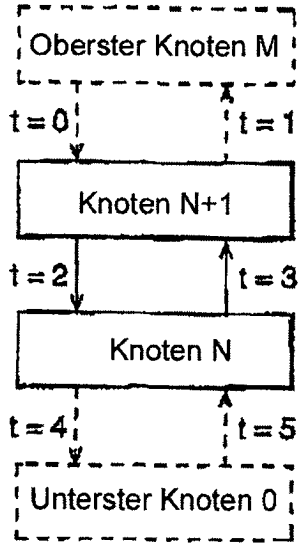


FIG. 6

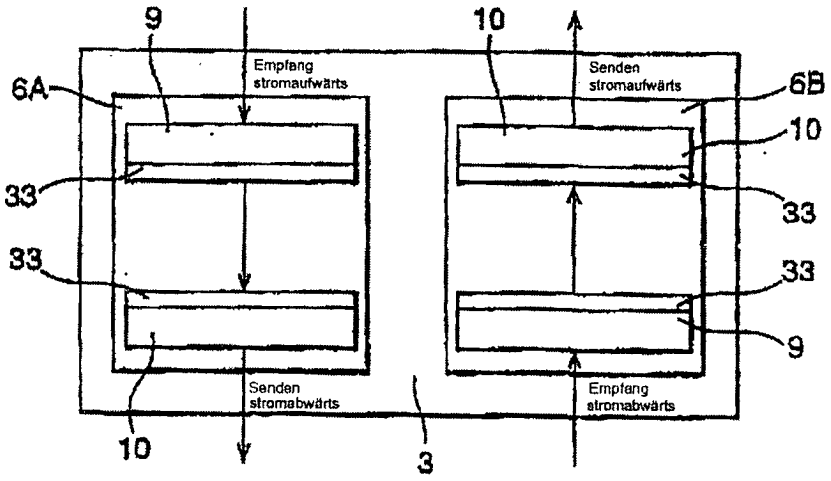


FIG. 7

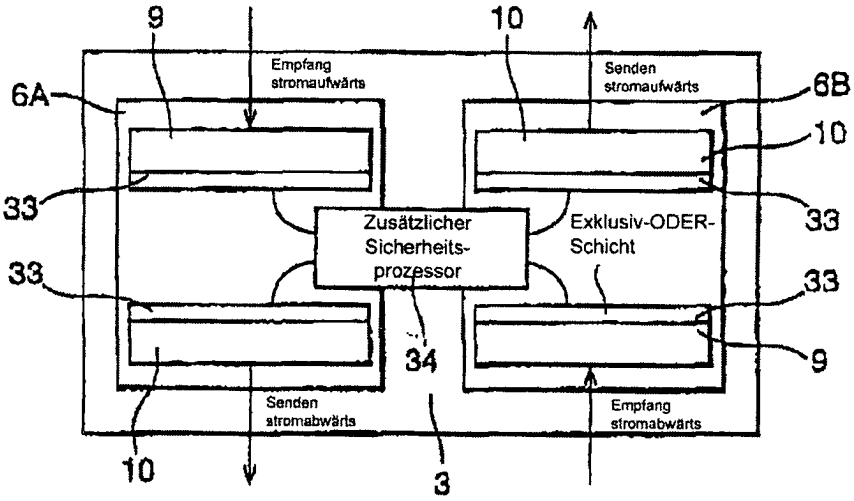

9
10
Empfang stromaufwärts
Senden stromaufwärts
6A
6B
10
33
33
Zusätzlicher Sicherheits-prozessor
Exklusiv-ODER-Schicht
33
33
34
9
Senden stromabwärts
Empfang stromabwärts
10
3

FIG. 8

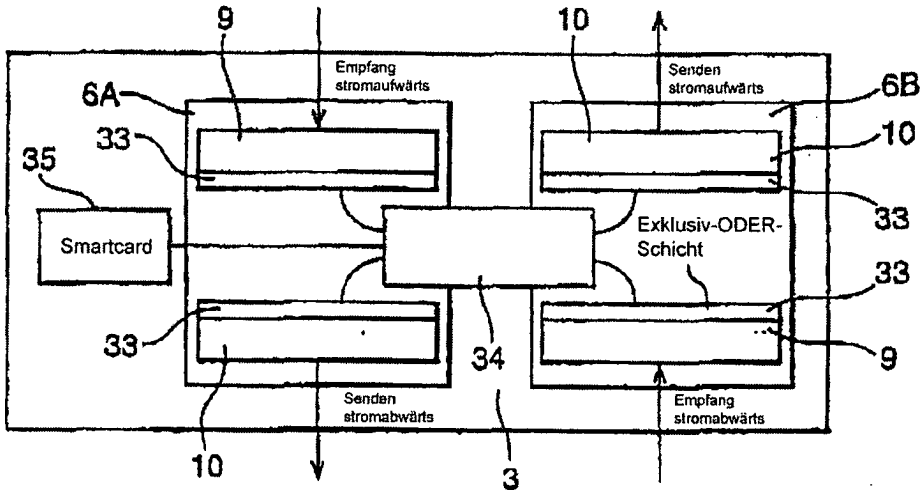
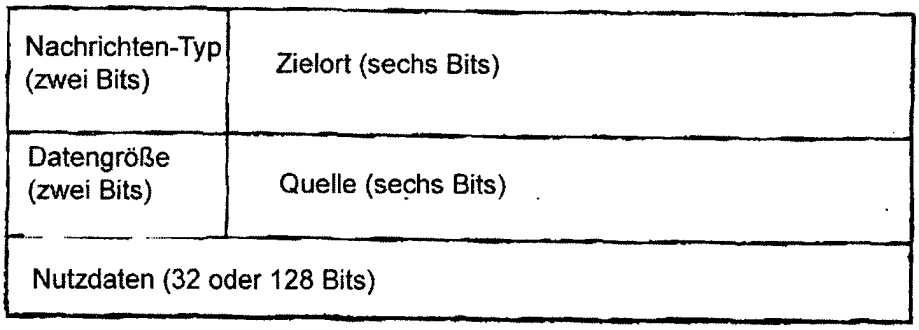

9
10
Empfang stromaufwärts
Senden stromaufwärts
6A
6B
33
10
35
Smartcard
Exklusiv-ODER-Schicht
33
33
33
34
9
Senden stromabwärts
Empfang stromabwärts
10
3

FIG. 9A



Nachrichten-Typ (zwei Bits)	Zielort (sechs Bits)
Datengröße (zwei Bits)	Quelle (sechs Bits)
Nutzdaten (32 oder 128 Bits)	

FIG. 9B

00	Stufe 1
01	Stufe 1
10	Stufe 3 und 4
11	Bestätigung

Nachrichtenformatcodierung

FIG. 9C

00	Null (keine Nutzdaten)
01	Wort (zweiunddreißig Bits)
10	Quad-Wort (128 Bits)
11	(Reserviert)

Datengrößencodierungen

FIG. 10

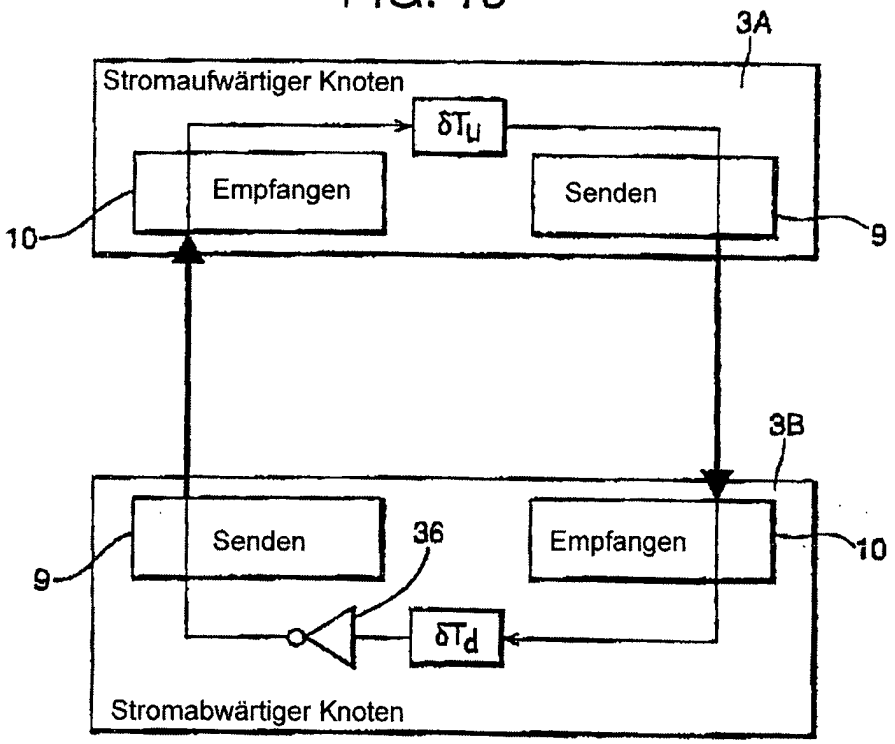

3A
Stromaufwärtiger Knoten
δT_u
Empfangen
Senden
10
9
3B
Senden
36
Empfangen
9
10
δT_d
Stromabwärtiger Knoten

FIG. 11

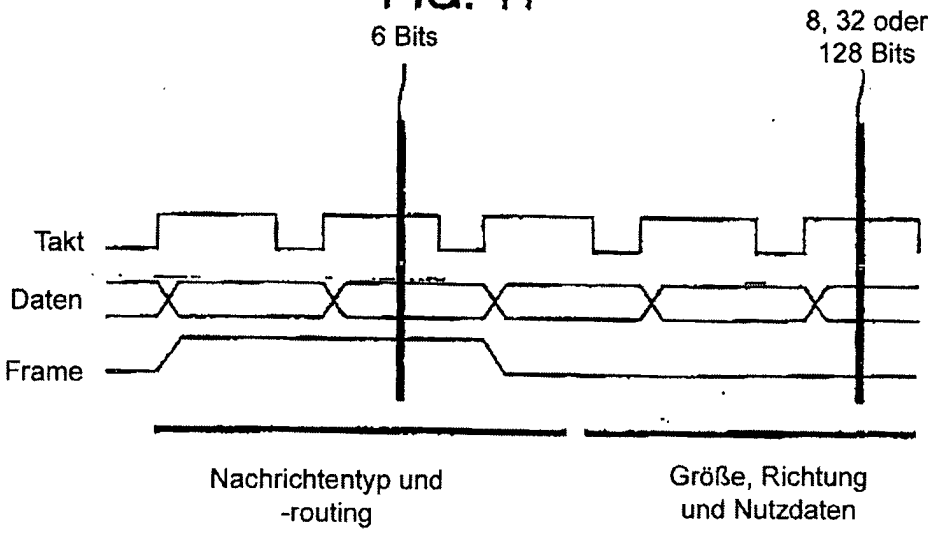

6 Bits
8, 32 oder
128 Bits
Takt
Daten
Frame
Nachrichtentyp und
-routing
Größe, Richtung
und Nutzdaten

FIG. 12

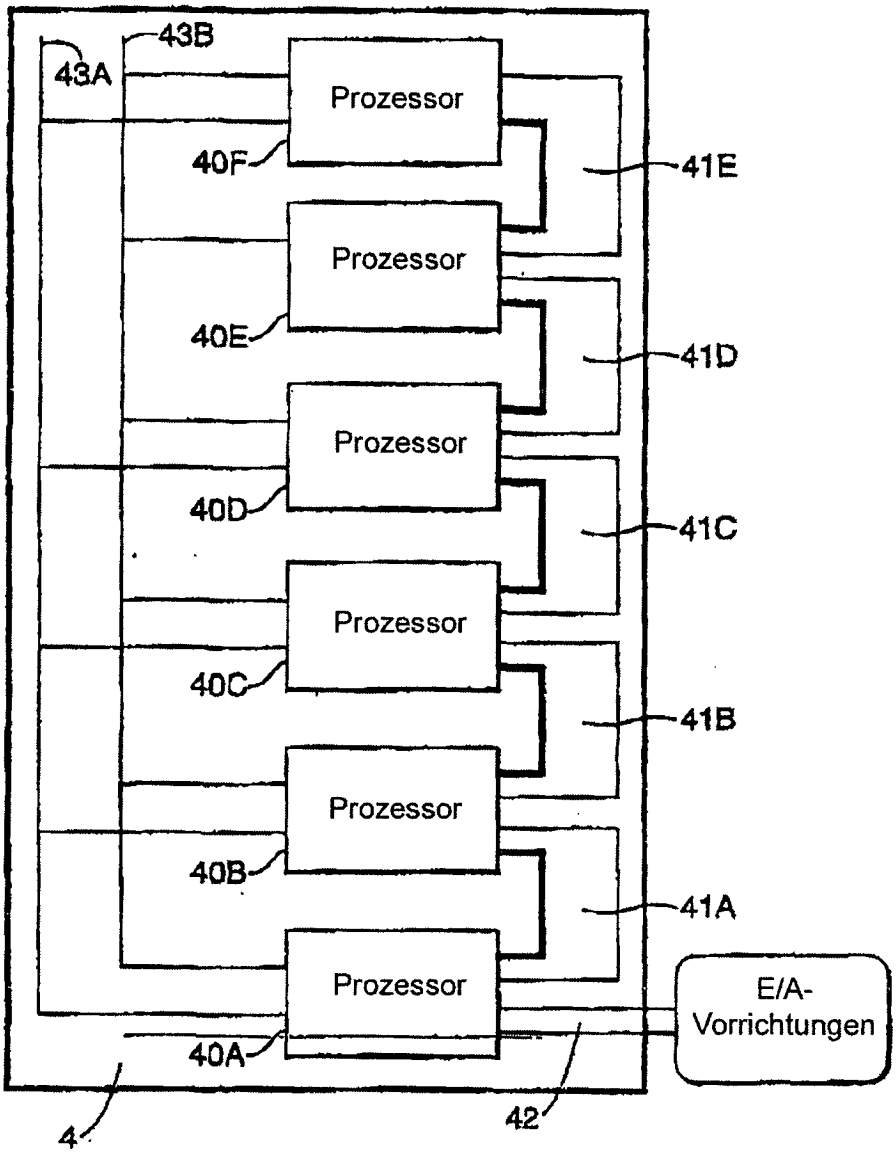

43B
43A
Prozessor
40F
41E
Prozessor
40E
41D
Prozessor
40D
41C
Prozessor
40C
41B
Prozessor
40B
41A
Prozessor
40A
E/A-
Vorrichtungen
4
42

FIG. 13

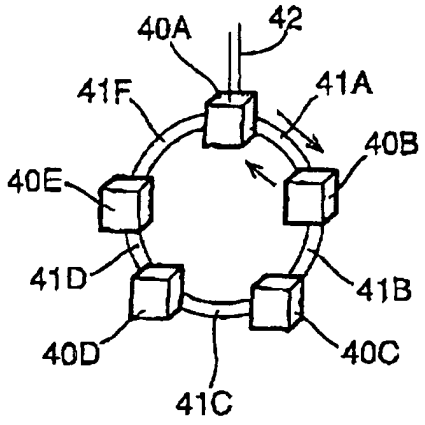


FIG. 14

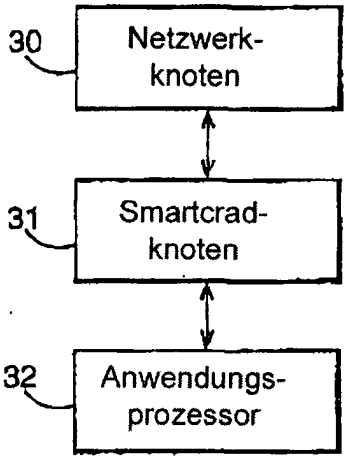


FIG. 15

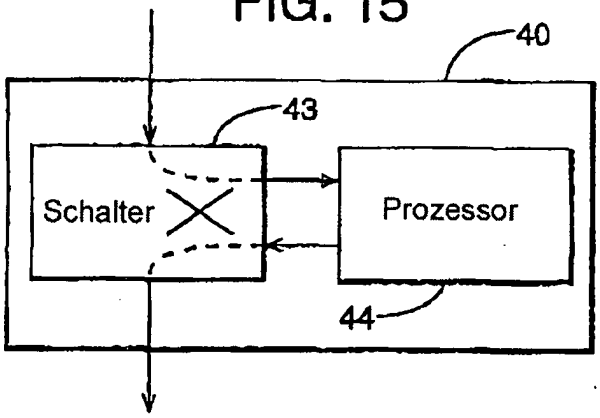


FIG. 16

Nachrichtentyp (zwei Bits)	Zielort (sechs Bits)
Virtuelle-Schaltkreis-Nummer (acht Bits)	
Nutzdaten (zweiunddreißig Bits)	

Nachrichtenformat