(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 216 847 B4** 2023.06.01

(12) # Patentschrift

(21) Aktenzeichen: **10 2013 216 847.0**
(22) Anmeldetag: **23.08.2013**
(43) Offenlegungstag: **26.02.2015**
(45) Veröffentlichungstag der Patenterteilung: **01.06.2023**

(51) Int Cl.: ***H04L 43/028*** (2022.01)
***H04L 43/00*** (2022.01)
***H04L 67/12*** (2022.01)
***H04L 12/46*** (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

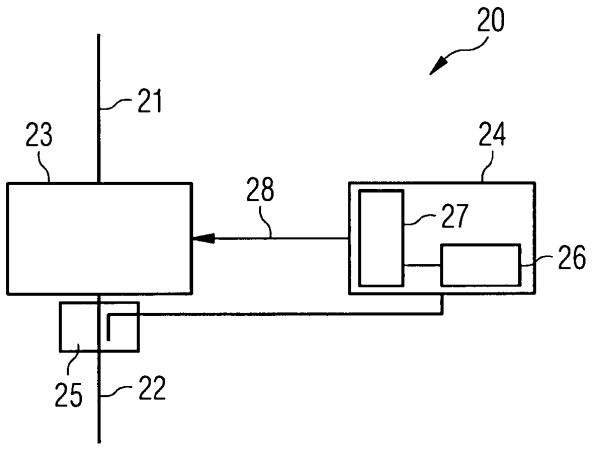
(73) Patentinhaber:
**Siemens Mobility GmbH, 81739 München, DE**

(72) Erfinder:
**Falk, Rainer, 85586 Poing, DE; Oheimb, David von, Dr., 82194 Gröbenzell, DE; Blöcher, Uwe, 82178 Puchheim, DE**

(56) Ermittelter Stand der Technik:
**DE** **10 2005 014 830** **A1**

(54) Bezeichnung: **Verfahren, Vorrichtung und System zur Überwachung einer Sicherheits-Netzübergangseinheit**

(57) Hauptanspruch: Verfahren zur Überwachung einer Sicherheits-Netzübergangseinheit (23), die einen Strom von Datenpaketen über eine erste Schnittstelle (21) empfängt, diesen Datenstrom gegenüber Filterregeln überprüft und an eine zweite Schnittstelle (22) ausgibt, mit den Verfahrensschritten:
- Duplizieren und Auskoppeln (11) des Datenstroms an der zweiten Schnittstelle (22),
- Überprüfen (12) des ausgekoppelten Datenstroms auf unzulässigen Datenverkehr,
- Senden (14) einer Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23), wenn unzulässiger Datenverkehr (12) im Datenstrom erkannt wird, und
- Beschränken (15) des Datenstroms durch die Sicherheits-Netzübergangseinheit (23), wenn die Warnnachricht (28) in der Sicherheits-Netzübergangseinheit (23) empfangen wird.



## Beschreibung

**[0001]** Die Erfindung bezieht sich auf ein Verfahren, eine Vorrichtung und ein System sowie ein Computerprogramm und ein Speichermedium zur Überwachung einer Netzübergangseinheit, die einen Strom von Datenpaketen über eine erste Schnittstelle empfängt, diesen Datenstrom gegenüber Filterregeln überprüft und an eine zweite Schnittstelle ausgibt.

**[0002]** Sicherheits-Netzübergangseinheiten, beispielsweise Firewalls, werden an Netzwerkgrenzen installiert, um eine kontrollierte Kopplung unterschiedlich kritischer Netzwerkbereiche zu realisieren. Es erfolgt dabei eine Filterung des Datenverkehrs, sodass nur zulässiger Datenverkehr durchgelassen wird. In industriellen Automatisierungssystemen, wie zum Beispiel einem Stellwerk oder einer Zugsteuerung in der Bahnautomatisierung, in beispielsweise Produktionshallen der Fertigungsautomatisierung, oder beispielsweise in Raffinerien oder Brauereien in der Prozessautomatisierung, werden bezüglich Sicherheit kritische Automatisierungsbereiche mit allgemeinen Netzen, beispielsweise einem Büronetzwerk, gekoppelt. Dazu werden Sicherheitsgateways beziehungsweise Firewalls eingesetzt und so konfiguriert, dass nur zugelassener Datenverkehr passieren kann.

**[0003]** Dabei wird der Datenstrom gemäß konfigurierbaren Filterregeln gefiltert. Bedingt durch Fehler in einer Implementierung der Sicherheits-Netzübergangseinheit oder durch Fehler in ihrer Konfiguration, insbesondere ihrer Filterregeln, oder auch durch eine Kompromittieren der Sicherheits-Netzübergangseinheit durch einen Angriff auf diese Einheit selbst besteht die Möglichkeit, dass eine Sicherheits-Netzübergangseinheit fehlerhaft arbeitet und eigentlich nicht zulässige Datenpakete durchlässt.

**[0004]** Bislang werden mögliche Unzulänglichkeiten einer Sicherheits-Netzübergangseinheit dadurch abgemildert, dass mehrere Sicherheits-Netzübergangseinheiten, beispielsweise mehrere Firewalls, hintereinander geschaltet werden. Dabei werden insbesondere Netzübergangseinheiten unterschiedlicher Hersteller verwendet. Dies hat jedoch den Nachteil, dass durch längere Bearbeitungszeiten die Verzögerung beziehungsweise der Jitter zunehmen und somit die Anforderungen für Echtzeitkommunikation nicht erfüllt werden.

**[0005]** Andererseits müssen die Filterregeln in einer Sicherheits-Netzübergangseinheit kontinuierlich aktualisiert werden, um einen Schutz insbesondere gegen neue Angriffe, beispielsweise durch Viren oder Würmer, abwehren zu können. In manchen Industrieautomatisierungsumgebungen gelten hohe Anforderungen an die Integrität, sodass Sicherheits-Netzübergangseinheiten beziehungsweise die darin implementierten Filterregeln zugelassen werden müssen und eine Änderung bzw. Aktualisierung der Konfiguration der Sicherheits-Netzübergangseinheiten oder der Filterregeln bzw. der Anti-Viren-Software nicht zulässig ist. Zudem muss sichergestellt werden, dass der Datenstrom durch eine Sicherheits-Netzübergangseinheit in das Automatisierungsnetz nicht verändert wird, insbesondere dass keine zusätzlichen Datenpakete durch die Netzübergangseinheit in das Automatisierungsnetz eingespeist werden.

**[0006]** Aus der DE 10 2005 014 830 A1 ist beispielsweise ein Verfahren zur elektronischen Nachrichtenübermittlung bekannt, wobei eine elektronische Nachricht eines Senders nicht an einen Empfänger zugestellt wird, wenn ein Zusatz einer Adresse nicht existent ist.

**[0007]** In der DE 10 2011 007 387 A1 ist beispielsweise eine Selbstüberwachung einer Sicherheits-Netzübergangseinheit bekannt. Dabei wird überprüft, ob zu einem ausgehenden Datenpaket ein korrespondierendes eingehendes Datenpaket empfangen wurde. Dadurch kann sichergestellt werden, dass eine Netzübergangseinheit nicht bei einer Fehlfunktion selbst Datenpakete erzeugt. Es ist somit die Aufgabe der vorliegenden Erfindung ein Verfahren, eine Vorrichtung und ein System zu schaffen, das einen unzulässigen Datenverkehr beim Übergang in ein sicherheitsrelevantes Datennetzwerk zuverlässig filtert und auch bei fehlerhafter Sicherheits-Netzübergangseinheit eine Daten-Integrität im sicherheitsrelevanten Datennetzwerk gewährleistet. Dabei soll eine Rückwirkungsfreiheit der Sicherheits-Netzübergangseinheit sichergestellt sein, d.h. es dürfen keine zusätzlichen Datenpakete durch die Sicherheits-Netzübergangseinheit in das Sicherheitsnetz eingebracht werden.

**[0008]** Die Aufgabe wird durch die in den unabhängigen Ansprüchen beschriebenen Maßnahmen gelöst. In den Unteransprüchen sind vorteilhafte Weiterbildungen der Erfindung dargestellt.

**[0009]** Das erfindungsgemäße Verfahren zur Überwachung einer Sicherheits-Netzübergangseinheit, beispielsweise einer Firewall, die einen Strom von Datenpaketen über eine erste Schnittstelle empfängt, diesen Datenstrom gegenüber Filterregeln überprüft und an eine zweite Schnittstelle ausgibt, umfasst die Verfahrensschritte des Duplizierens und Auskoppelns des Datenstroms an der zweiten Schnittstelle, des Überprüfens des ausgekoppelten Datenstroms auf unzulässigen Datenverkehr, des Sendens einer Warnnachricht an die Sicherheits-Netzübergangseinheit, wenn unzulässiger Datenverkehr im Datenstrom erkannt wird, und des Beschränkens des Datenstroms durch die Sicherheits-Netz-

übergangseinheit, wenn die Warnnachricht in der Sicherheits-Netzübergangseinheit (23) empfangen wird.

**[0010]** Da der Datenstrom an der zweiten Schnittstelle abgegriffen wird, die hinter der Sicherheits-Netzübergangseinheit und innerhalb des sicherheitsrelevanten Datennetzes liegt, kann eine Fehlfunktion der Sicherheits-Netzübergangseinheit durch ein Überprüfen dieses gefilterten Datenstroms erkannt werden. Ein weiterer Vorteil ist, dass bei einem solchen Verdacht, die Sicherheits-Netzübergangseinheit darüber informiert wird und somit sehr zeitnah Maßnahmen zur Beschränkung des Datenstroms veranlassen kann. Ein Einbringen von Nachrichten in das sicherheitsrelevante Datennetz selbst, das heißt in die zweite Schnittstelle, wird dabei verhindert, da lediglich eine Beschränkung des Datenstroms durch die Sicherheits-Netzübergangseinheit, insbesondere Firewall, als Konsequenz aus dem Melden des Verdachts erfolgt. Somit kann beispielsweise eine zulassungspflichtige oder zertifizierte Sicherheits-Netzübergangseinheit durch aktualisierte Filtersoftware in einer Überwachungseinheit überwacht werden, ohne die Konfiguration beziehungsweise den Softwarestand der Netzübergangseinheit selbst anpassen und damit neu zulassen oder zertifizieren zu müssen. Bei einem Hinweis auf unzulässigen Datenverkehr wird der Datenverkehr durch die Sicherheits-Netzübergangseinheit eingeschränkt. Die Sicherheits-Netzübergangseinheit kann, eventuell durch Zusatzinformationen, in der Warnnachricht geeignete Maßnahmen abhängig von der Zusatzinformation ergreifen.

**[0011]** In einer vorteilhaften Ausführungsform umfasst das erfindungsgemäße Verfahren die zusätzlichen Verfahrensschritte des Duplizierens und Auskoppelns des Datenstroms an der ersten Schnittstelle, ein Vergleichen des Datenstroms an der ersten Schnittstelle mit dem Datenstrom an der zweiten Schnittstelle und eines Sendens einer Warnnachricht an die Sicherheits-Netzübergangseinheit, wenn sich der Datenstrom der zweiten Schnittstelle von dem Datenstrom der ersten Schnittstelle unterscheidet.

**[0012]** Dies hat den Vorteil, dass durch die auch Sicherheits-Netzübergangseinheit erfolgreich abgewehrter unzulässiger Datenverkehr erkannt wird. Es kann hierbei, abhängig von getroffenen Vorgaben, konfiguriert werden, dass ein Wechsel in eine restriktive Betriebsart der Sicherheits-Netzübergangseinheit, beispielsweise einer Firewall, erfolgt. Es wird dadurch auch erkannt, wenn neue Datenpakete, die nicht auf der ersten Schnittstelle vorhanden waren, in das sicherheitsrelevante Datennetz eingebracht werden und der Datenstrom durch die Sicherheits-Netzübergangseinheit sofort beschränkt werden.

**[0013]** In einer vorteilhaften Ausführungsform erfolgt das Beschränken des Datenstroms durch eine Aktivierung von Ersatz-Filterregeln der Sicherheits-Netzübergangseinheit. Somit können abgestimmte und beispielsweise zugelassene Filterregeln bzw. restriktive Filterregeln für einen eingeschränkten Betrieb im Voraus definiert werden und beim Verdacht eines unzulässigen Dateneintritts in das Sicherheitsrelevante Datennetz diese Regeln sofort aktiviert werden.

**[0014]** Somit ist eine schnelle Abwendung der Gefahr bei möglichst geringer Ausfallzeit des Netzübergangs durchführbar.

**[0015]** In einer vorteilhaften Ausführungsform erfolgt das Beschränken des Datenstroms durch einen Neustart der Sicherheits-Netzübergangseinheit mit einer geschützten Start-Software oder durch einen Neustart der Sicherheits-Netzübergangseinheit mit einer Ersatz-Firmware oder durch einen Wechsel von einer aktiven virtuellen Maschine zu einer Ersatz-virtuellen Maschine in einer Firewall.

**[0016]** Durch einen Neustart der Sicherheits-Netzübergangseinheit kann in vielen Fällen eine Manipulation an der Software der Netzübergangseinheit rückgängig gemacht werden, da bei einem Neustart die Software wieder in einen initialen Ausgangszustand versetzt wird. Bei eingebetteten Systemen, sogenannten Embedded Systems, kann ein Neustart mit einer Ersatz-Firmware, die entweder dem Ausgangszustand der ursprünglichen Netzübergangseinheit entspricht oder strengere Filterregeln umfasst, zurückgesetzt werden. Die Ersatz-Firmware kann dabei in einen Nurlesespeicher (Read Only Memory) oder in einen Flash-Speicher abgelegt sein, die im regulären Betrieb der Firewall nicht modifizierbar sind. Bei der Implementierung einer Sicherheits-Netzübergangseinheit als virtuelle Maschine, kann ein entsprechender Effekt durch einen Wechsel von einer aktiven virtuellen Maschine in eine Ersatzvirtuelle Maschine erzielt werden. Dabei sind die Ausfallzeiten während des Wechsels besonders gering. Der Datenverkehr in das Sicherheitsrelevante Datennetz wird somit nur sehr kurz unterbrochen.

**[0017]** In einer weiteren vorteilhaften Ausführungsform erfolgt das Beschränken des Datenstroms durch Deaktivierung der zweiten und/oder durch Deaktivierung der ersten Schnittstelle der Firewall.

**[0018]** Wird die zweite Schnittstelle deaktiviert, wird definitiv sichergestellt, dass keine weiteren Daten in das Sicherheitsnetz eindringen können. Durch ein Deaktivieren der ersten Schnittstelle der Netzübergangseinheit wird ein Überlaufen der Filter beziehungsweise ein Schädigen der Sicherheits-Netz-

übergangseinheit durch den eintreffenden Datenstrom vermieden.

**[0019]** In einer weiteren vorteilhaften Ausführungsform erfolgt das Beschränken des Datenstroms durch Deaktivieren einer Stromversorgung der Sicherheits-Netzübergangseinheit.

**[0020]** Somit ist eine physikalische Unterbrechung des Datenstroms über die Netzwerkgrenze hinweg sichergestellt. Diese Maßnahme hat den Vorteil, dass sie für jegliche Sicherheits-Netzübergangseinheit einsetzbar ist, ungeachtet eventuell vorhandender beziehungsweise nicht vorhandener Möglichkeiten zur Datenbegrenzung an der Netzübergangseinheit. Dadurch wird mit sehr hoher Zuverlässigkeit sichergestellt, dass keine Datenkommunikation über die Sicherheits-Netzübergangseinheit erfolgt. Auch kann dadurch erreicht werden, dass ggf. auf der Sicherheits-Netzübergangseinheit dauerhaft gespeicherte Logdaten und der Softwarestand für eine spätere Auswertung verfügbar sind, d.h. nicht überschrieben oder gelöscht werden.

**[0021]** In einer Ausführungsform bleibt die Beschränkung der Sicherheits-Netzübergangseinheit solange aktiv, wie die Warnnachricht an der Firewall empfangen wird.

**[0022]** Dies hat den Vorteil, dass nach Behebung der Sicherheitslücke die Datenkommunikation über die Netzwerkgrenze hinweg sofort wieder aktiv geschalten werden kann. Ausfallzeiten werden somit minimiert.

**[0023]** In einer weiteren Ausführungsform bleibt die Beschränkung der Netzübergangseinheit solange aktiv, bis ein explizites Signal zur Aufhebung der Beschränkung, bevorzugt durch eine Handlung von Administrationspersonal, an der Sicherheits-Netzübergangseinheit empfangen wird.

**[0024]** Dies hat den Vorteil, dass erst nach Sicherstellung der Behebung des Mangels beziehungsweise nach Durchführung aller gewünschter Maßnahmen die Netzübergangseinheit wieder in Betrieb geht. In einer Variante ist dazu eine lokale Eingabeschnittstelle an der Sicherheits-Netzübergangseinheit vorgesehen, die in Form eines Tasters oder Schlüsselschalters realisiert ist.

**[0025]** Die erfindungsgemäße Vorrichtung zur Überwachung einer Sicherheits-Netzübergangseinheit, die einen Strom von Datenpaketen über eine erste Schnittstelle empfängt, diesen Datenstrom gegenüber Filterregeln überprüft und an eine zweite Schnittstelle ausgibt, umfasst eine Auskoppeleinheit, die ausgebildet ist, um den Datenstrom an der zweiten Schnittstelle zu duplizieren und in eine Leitung auszukoppeln, eine Überprüfungseinheit, die ausgebildet ist um den ausgekoppelten Datenstrom auf unzulässigen Datenverkehr zu überprüfen und eine Kommunikationseinheit, die ausgebildet ist, um eine Warnnachricht an die Sicherheits-Netzübergangseinheit zu senden, wenn unzulässiger Datenverkehr im Datenstrom erkannt wird.

**[0026]** Diese Vorrichtung kann vorteilhafterweise eine Sicherheits-Netzübergangseinheit mit beispielsweise fest vorgegebenen und nur schwer anpassbaren Filterregeln durch Überprüfen des von der Netzübergangseinheit ausgegebenen Datenstroms mit einer mit den neuesten Sicherheitsregeln ausgestatteten Vorrichtung zu überprüfen und somit auch neue Angriffsmethoden, beziehungsweise unzulässige Daten, zu erkennen. Da die Vorrichtung keinen Einfluss auf den Datenstrom auf der zweiten Schnittstelle hat, wirkt die Vorrichtung rückwirkungsfrei, also ohne einen Eingriff in das Sicherheitsrelevante Datennetzwerk, in das die Daten übergeben werden. Dennoch ist eine schnelle Reaktion zur Beschränkung des Datenstroms auf der zweiten Schnittstelle gegeben. Dies ist insbesondere von Vorteil, wenn die eigentliche Sicherheits-Netzübergangseinheit nicht oder nur eingeschränkt aktualisiert werden kann, das heißt Filterregeln aktualisiert oder gepatcht werden können, zum Beispiel wegen einer geforderten Zertifizierung oder Zulassung, die bei einer Aktualisierung wiederholt werden muss. Die Vorrichtung, im Weiteren auch Überwachungsvorrichtung genannt, kann dagegen, da sie rückwirkungsfrei auf die zulässige Kommunikation ist, flexibel aktualisiert werden. Solange dabei die „aktive“ Sicherheits-Netzübergangseinheit hinreichend gut ist, kann eine nicht aktualisierte Sicherheits-Netzübergangseinheit in Betrieb bleiben. Sobald aber das Auftreten von unzulässigem Datenverkehr beobachtet wird, wird die Konnektivität von außen eingeschränkt.

**[0027]** In einer vorteilhaften Ausführungsform umfasst die Vorrichtung eine zusätzliche Auskoppeleinheit, die ausgebildet ist, um den Datenstrom auf der ersten Schnittstelle zu duplizieren und auszukoppeln und eine Vergleichseinheit, die ausgebildet ist, um den ausgekoppelten Datenstrom der ersten Schnittstelle mit dem Datenstrom der zweiten Schnittstelle zu vergleichen und bei Erkennen von Unterschieden zwischen dem Datenstrom der zweiten Schnittstelle und dem Datenstrom der ersten Schnittstelle die Kommunikationseinheit zu veranlassen, eine Warnnachricht an die Sicherheits-Netzübergangseinheit zu senden.

**[0028]** Vorteilhafterweise wird dadurch erkannt, dass die Netzübergangseinheit erfolgreich unzulässigen Datenverkehr abwehrt und andererseits wird erkannt, wenn die Netzübergangseinheit selbst fehlerhaft, beispielsweise durch Manipulation verändert, arbeitet und beispielsweise zusätzliche Datenpa-

kete, die nicht über die erste Schnittstelle empfangen wurde, an die zweite Schnittstelle ausgibt.

**[0029]** Das vorteilhafte System zur Überwachung einer Sicherheits-Netzübergangseinheit umfasst eine Sicherheits-Netzübergangseinheit, die derart ausgebildet ist, um einen Strom von Datenpaketen über eine erste Schnittstelle zu empfangen, diese Daten gegenüber Filterregeln zu überprüfen und an eine zweite Schnittstelle auszugeben und eine Überwachungseinheit mit einer Auskoppeleinheit, die ausgebildet ist zum Duplizieren und Auskoppeln des Datenstroms an der zweiten Schnittstelle, mit einer Überprüfungseinheit zum Überprüfen des ausgekoppelten Datenstroms auf unzulässigen Datenverkehr, und einer Kommunikationseinheit, die ausgebildet ist zum Senden einer Warnnachricht an die Sicherheits-Netzübergangseinheit, wenn unzulässiger Datenverkehr im Datenstrom erkannt wird, woraufhin die Sicherheits-Netzübergangseinheit eingerichtet ist, den Datenstrom zu beschränken.

**[0030]** Die Warnnachricht kann in einer Variante als elektrisches Schaltsignal bereitgestellt werden.

**[0031]** In einer vorteilhaften Ausführungsform des erfindungsgemäßen Systems umfasst die Überwachungseinheit zusätzlich eine Auskoppeleinheit, die ausgebildet ist, um den Datenstrom auf der ersten Schnittstelle zu duplizieren und auszukoppeln und eine Vergleichseinheit, die ausgebildet ist, um den ausgekoppelten Datenstrom der ersten Schnittstelle mit dem Datenstrom der zweiten Schnittstelle zu vergleichen und bei Erkennen von Unterschieden zwischen dem Datenstrom der zweiten Schnittstelle und dem Datenstrom der ersten Schnittstelle die Kommunikationseinheit zu veranlassen, eine Warnnachricht an die Sicherheits-Netzübergangseinheit zu senden.

**[0032]** Zusätzlich wird ein Computerprogramm mit Programmbefehlen zur Durchführung des Verfahrens sowie ein Datenträger, der das Computerprogramm speichert, beansprucht.

**[0033]** Ausführungsbeispiele des erfindungsgemäßen Verfahrens, der erfindungsgemäßen Vorrichtung und des erfindungsgemäßen Systems sind in den Zeichnungen beispielhaft dargestellt und werden anhand der nachfolgenden Beschreibung näher erläutert. Es zeigen:

**Fig. 1a** eine erste beispielhafte Ausführungsform des erfindungsgemäßen Verfahrens als Ablaufdiagramm;

**Fig. 1b** eine zweite beispielhafte Ausführungsform des erfindungsgemäßen Verfahrens als Ablaufdiagramm;

**Fig. 1c** eine dritte beispielhafte Ausführungsform des erfindungsgemäßen Verfahrens als Ablaufdiagramm;

**Fig. 2** ein erstes Ausführungsbeispiel eines erfindungsgemäßen Systems mit einer Auskopplung des Datenstroms lediglich auf einer zweiten Schnittstelle, in schematischer Darstellung; und

**Fig. 3** ein zweites Ausführungsbeispiel eines erfindungsgemäßen Systems mit einer Auskopplung des Datenstroms an einer ersten und an einer zweiten Schnittstelle in schematischer Darstellung.

**[0034]** Einander entsprechende Teile sind in allen Figuren mit den gleichen Bezugszeichen versehen. Im Weiteren wird die Sicherheits-Netzübergangseinheit auch lediglich mit Netzübergangseinheit bezeichnet.

**[0035]** **Fig. 1a** zeigt das vorgeschlagene Verfahren um die korrekte Funktion einer Netzübergangseinheit rückwirkungsfrei zu überwachen. Dabei bedeutet Rückwirkungsfreiheit, dass das Datennetzwerk, in das der Datenverkehr übergegeben wird, durch die Netzübergangseinheit nicht beeinflusst wird. Insbesondere werden keine zusätzlichen Datenpakete an ein solches beispielsweise sicherheitsrelevantes Automatisierungsnetz durch die Netzübergangseinheit erzeugt und ausgegeben.

**[0036]** Im Zustand 10 des Verfahrens empfängt die Sicherheits-Netzübergangseinheit auf einer ersten Schnittstelle einen Datenstrom von einem ersten Datennetz und gibt den Datenstrom nach einer Überprüfung auf eine zweite Schnittstelle in ein zweites Datennetz, beispielsweise ein sicherheitsrelevantes Automatisierungsnetzwerk, aus.

**[0037]** Im ersten Verfahrensschritt 11 wird der Datenstrom an der zweiten Schnittstelle, das heißt bereits innerhalb des zweiten Datennetzwerks, der Datenstrom dupliziert und beispielsweise in eine separate Leitung ausgekoppelt. Dabei muss sichergestellt sein, dass der Datenstrom innerhalb des sicherheitsrelevanten Netzes und vor Komponenten, die den Datenstrom verändern, ausgekoppelt wird. Daraufhin wird im Verfahrensschritt 12 der ausgekoppelte Datenstrom auf unzulässigen Datenverkehr überprüft. Die Überprüfung 12 kann beispielsweise durch Filterregeln entsprechend den aktiven Filterregeln der Netzübergangseinheit stattfinden. Vorzugsweise wird der ausgekoppelte Datenstrom aber durch erweiterte, beispielsweise mit den neuesten Anti-Virus-Patchen aktualisierte Filterregeln überprüft. Typischerweise werden dabei eine IP-Adresse der Datenpakete und/oder die Portnummern im Datenpaket oder die Nutzdateninhalte im Datenpaket überprüft oder es wird nach gezielten Angriffs-

mustern über mehrere Datenpakete hinweg der Datenstrom untersucht.

**[0038]** Das Überprüfen 12 findet vollkommen entkoppelt von der Überprüfung des Datenstroms in der Netzübergangseinheit statt. Der Datenstrom auf der zweiten Schnittstelle wird weder zeitlich verzögert noch inhaltlich verändert. Somit bleibt die Überprüfung 12 des ausgekoppelten Datenstroms völlig unsichtbar und somit rückwirkungsfrei für das den Datenstrom empfangende Netzwerk. Wird der Datenstrom als zulässiger Datenverkehr erkannt, werden die Datenpakete an die zweite Schnittstelle ausgegeben und das Verfahren ist beendet, siehe Verfahrensschritt 13.

**[0039]** Wird im Datenstrom unzulässiger Datenverkehr erkannt, wird im Verfahrensschritt 14 eine Warnnachricht an die Netzübergangseinheit gesendet. Erhält die Netzübergangseinheit die Warnnachricht, so veranlasst sie ein Beschränken des Datenstroms, siehe Verfahrensschritt 15. Das Verfahren ist damit beendet, siehe Verfahrensschritt 13.

**[0040]** In einer Variante des Verfahrens, die in **Fig. 1b** dargestellt ist, erfolgt für ein Datenpaket der zweiten Schnittstelle, das nicht bereits in Schritt 12 als zulässig erkannt wurde, zusätzlich eine Prüfung abhängig von dem an der ersten Schnittstelle empfangenen Datenstrom. Dazu wird ein an der ersten Schnittstelle der Netzübergangseinheit duplizierter und ausgekoppelter Datenstrom erfasst, siehe Verfahrensschritt 16. Im nächsten Verfahrensschritt 17 wird dann der ausgekoppelte Datenstrom der ersten Schnittstelle zur weiteren Prüfung des Datenpakets herangezogen.

**[0041]** Es kann z.B. an der zweiten Schnittstelle eine Statusnachricht, z.B. eine Überlastnachricht oder eine Wartungsmodusnachricht, durch die Netzübergangseinheit ausgesendet werden, was in diesem Beispiel nur dann zulässig ist, wenn an der ersten Schnittstelle des Netzübergangs bestimmte Datenpakete empfangen wurden. Es kann z.B. geprüft werden, ob ein Denial-of-Service-Angriffsmuster an der ersten Schnittstelle der Netzübergangseinheit vorliegt bzw. ob ein Wartungszugang (Remote Service Access) zur Netzübergangseinheit über die erste Schnittstelle der Netzübergangseinheit stattfindet, z.B. über eine HTTPS- oder SSH-Verbindung.

**[0042]** Wird der Datenstrom bei der Überprüfung im Verfahrensschritt 17 als zulässiger Datenverkehr erkannt, werden die Datenpakete an die zweite Schnittstelle ausgegeben und das Verfahren ist beendet, siehe Verfahrensschritt 13. Wird das Paket der zweiten Schnittstelle als unzulässig erkannt, wird auch hier eine Warnnachricht an die Netzübergangseinheit im Verfahrensschritt 14 gesendet, woraufhin die Netzübergangseinheit eine Beschränkung des Datenstroms veranlasst, siehe Verfahrensschritt 15.

**[0043]** In einer weiteren Ausführungsform des Verfahrens wird der in die Sicherheits-Netzübergangseinheit eingehende Datenstrom an der ersten Schnittstelle dupliziert und ausgekoppelt und dann zusätzlich der ausgekoppelte Datenstrom der ersten Schnittstelle mit dem ausgekoppelten Datenstrom der zweiten Schnittstelle verglichen. Diese Überprüfung kann parallel zu der in **Fig. 1a** oder **Fig. 1b** dargestellten Überprüfungen erfolgen.

**[0044]** In der in **Fig. 1c** dargestellten Variante erfolgt diese zusätzliche Überprüfung 18, falls in Schritt 12 der Datenstrom als zulässiger Datenverkehr erkannt wird. Dazu wird ein an der ersten Schnittstelle der Netzübergangseinheit duplizierte und ausgekoppelte Datenstrom erfasst, siehe Verfahrensschritt 16. Im nächsten Verfahrensschritt 18 wird dann der ausgekoppelte Datenstrom der ersten Schnittstelle zur weiteren Prüfung des Datenpakets herangezogen. Für das an der zweiten Schnittstelle empfangenes Datenpaket wird dabei geprüft, ob ein identisches Paket im Datenstrom der ersten Schnittstelle vorlag bzw. in einem bestimmten zurückliegenden Zeitfenster im Datenstrom der ersten Schnittstelle vorlag. Ist dies der Fall, so ist diese Überprüfung abgeschlossen siehe Verfahrensschritt 13. Wird jedoch eine Inkonsistenz in den beiden Datenströmen festgestellt, wird auch hier eine Warnnachricht an die Netzübergangseinheit im Verfahrensschritt 14' gesendet, woraufhin die Netzübergangseinheit eine Beschränkung des Datenstroms veranlasst, siehe Verfahrensschritt 15.

**[0045]** Diese zusätzliche, in **Fig. 1c** dargestellte Überprüfung, kann auch entsprechend in der in **Fig. 1b** dargestellten Variante ergänzt werden.

**[0046]** Durch den Vergleich des eingehenden Datenstroms mit dem ausgehenden Datenstrom kann einerseits detektiert werden, dass eine Filterung durch die Netzübergangseinheit stattgefunden hat, das heißt wenn unzulässige eingehende Datenpakete nicht im ausgehenden Datenstrom enthalten sind. Werden im ausgehenden Datenstrom auf der zweiten Schnittstelle dagegen Datenpakete detektiert, die nicht auf der ersten Schnittstelle in die Netzübergangseinheit eingegangen sind, so kann ebenfalls auf einen Fehler in der Netzübergangseinheit geschlossen werden. Insbesondere kann dadurch detektiert werden, wenn die Netzübergangseinheit ein Datenpaket nicht entweder blockt oder unverändert weiterleitet, sondern ein modifiziertes Datenpaket oder ein zusätzliches Datenpaket aussendet. Es kann dabei also erkannt werden, wenn die Netzübergangseinheit ein Datenpaket aussendet, das sie nicht vorher auch tatsächlich empfangen hat.

**[0047]** Durch die Warnnachricht wird die Netzübergangseinheit beispielsweise dazu veranlasst auf einen restriktiven Filterungsmodus, beispielsweise durch Aktivierung von Ersatz-Filterregeln, zu wechseln. Durch die Warnnachricht kann in einer Variante die Netzübergangseinheit zu einem Neustart veranlasst werden, der vorzugsweise mit einem unveränderten, gestützten Software-Stand, beziehungsweise Boot-Image, ausgeführt wird, sodass wieder eine fest hinterlegte, zulässige Default-Konfiguration beziehungsweise Recovery-Konfiguration aktiviert wird. Ist die Netzübergangseinheit als ein eingebettetes System ausgebildet, wird der Arbeitsspeicher bei einem Neustart in einen initialen Zustand zurückgesetzt. Somit kann eine fehlerhafte oder manipulierte Software-Version deaktiviert werden.

**[0048]** Alternativ kann ein Neustart der Netzübergangseinrichtung mit einem Ersatz-Firmware-Abbild vorgesehen sein. Es können zum Beispiel zwei Dateisystem-Partitionen mit unterschiedlichen Implementierungen der Netzübergangseinheit vorgesehen sein. Beim Empfang einer Warnnachricht in der Netzübergangseinrichtung erfolgt ein Neustart, wobei die Dateisystem-Partition mit der restriktiven Implementierung gestartet wird.

**[0049]** Ist die Netzübergangseinheit als virtuelle Maschine mit einem Hypervisor beziehungsweise Microvisor implementiert, so liegen mehrere logische Partitionen separiert als virtuelle Maschinen oder auch Partitionen vor. Eine Datenpaketfilterung erfolgt dabei in einer virtuellen Maschine. Bei Anlegen der Warnnachricht wird eine erste virtuelle Maschine deaktiviert und eine Ersatz-virtuelle Maschine mit restriktiven Filterregelungen und/oder einer alternativen Filterrealisierung aktiviert. Ein solcher Wechsel ist in weniger als einer Sekunde, insbesondere im Bereich von Millisekunden möglich und erlaubt somit ein nahezu unterbrechungsfreien Betrieb der Netzübergangseinrichtung.

**[0050]** In einer Variante ist hierbei die Überwachungseinheit als separate physische Komponente realisiert. In einer anderen Variante ist die Überwachungseinheit als virtuelle Maschine realisiert, die durch denselben Hypervisor bzw. Microvisor wie die Netzübergangseinheit ausgeführt wird.

**[0051]** Des Weiteren kann bei Anlegen beziehungsweise bei Empfang der Warnnachricht eine oder beide Schnittstellen deaktiviert werden. Bevorzugt wird die zweite Schnittstelle deaktiviert, sodass keine Datenpakete an die zweite Schnittstelle ausgegeben werden. Ebenfalls von Vorteil ist es die erste Schnittstelle zu deaktivieren um ein Überlaufen der Speicher in der Netzübergangseinheit zu vermeiden. Ebenso kann ein Deaktivieren der ersten Schnittstelle einen Abbruch des Datenverkehrs in das Sicherheitsrelevante Datennetz bewirken.

**[0052]** Eine sehr universell anwendbare Variante zur Beschränkung des Datenverkehrs ist es, die Stromversorgung der Netzübergangseinheit zu deaktivieren, das heißt stromlos zu schalten. Dies ist mit sehr geringem Aufwand zum Beispiel durch eine schaltbare Stromversorgungseinheit der Netzübergangseinheit ohne eine Änderung in der Konfiguration oder Implementierung der Netzübergangseinheit selbst möglich. Somit können auch Netzübergangseinheiten, die keine expliziten Beschränkungsmechanismen unterstützten, durch dieses Verfahren überwacht und der Datenverkehr eingeschränkt werden.

**[0053]** In einer Ausführungsform des Verfahrens bleibt der restriktive, beschränkende Modus der Netzübergangseinheit so lange aktiviert, wie die Warnnachricht an der Netzübergangseinheit anliegt. Vorzugsweise bleibt der restriktive Modus jedoch so lange aktiv, bis ein expliziter Wechsel in einen regulären Modus durch eine administrative Handlung erfolgt. Beispielsweise kann der reguläre Modus durch einen Tastendruck eines physikalischen Tasters oder durch Betätigen eines Schlüsselschalters oder durch Eingabe über eine logische Administrationsschnittstelle durch Administrationspersonal ausgelöst werden. Dabei kann der reguläre Modus auch eine neue aktualisierte Filterregel umfassen. Das Verfahren geht dann in dem mit Stopp bezeichneten Endzustand über.

**[0054]** In **Fig. 2** ist nun ein System aus einer Netzübergangseinheit 23 und einer Überwachungseinheit 24 dargestellt. Die Netzübergangseinheit trennt zwei Datennetze mit beispielsweise unterschiedlichen Sicherheitseinstufungen. Dabei wird beispielsweise ein Datenstrom aus einem Netzwerk mit niedriger Sicherheitsanforderung, wie einem Büronetzwerk, über eine erste Schnittstelle 21 an die Netzübergangseinheit 23 angeschlossen. Die Netzübergangseinheit 23 überprüft die Datenpakete bzw. den Strom aus Datenpaketen und gibt diesen über eine zweite Schnittstelle 22 an ein zweites Netzwerk, das beispielsweise höhere Sicherheitsanforderungen aufweist, aus.

**[0055]** In der Ausführungsform in **Fig. 2** wird lediglich der ausgehende Datenstrom auf der zweiten Schnittstelle durch eine Auskoppeleinheit 25 dupliziert und in eine separate Leitung ausgekoppelt. Der ausgekoppelte Datenstrom wird an die Überprüfungseinheit 26 der Überwachungseinheit 24 weitergegeben und dort auf unzulässigen Datenverkehr überprüft. Dabei können insbesondere die Adressfelder im Kopf des Datenpakets auf unzulässige Herkunfts- beziehungsweise Zieladressen überprüft werden oder die Portnummer gegenüber zulässigen Portnummern verglichen werden. Liegt der Nutzinhalt des Datenpakets unverschlüsselt und somit in Klartext vor, so kann auch der Inhalt der Pakete auf

beispielsweise verdächtige bzw. unzulässige Muster überprüft werden und noch vor der Beendigung der Überprüfung des Datenpakets dessen weiterleiten verhindert werden.

**[0056]** Die Überprüfungseinheit 26 ist mit einer Kommunikationseinheit 27 verbunden. Wird in der Überprüfungseinheit 26 unzulässiger Datenverkehr erkannt, meldet die Überprüfungseinheit 26 dies der Kommunikationseinheit 27, die wiederum eine Warnnachricht 28 an die Netzübergangseinheit 23 sendet beziehungsweise anlegt. Die Warnnachricht kann beispielsweise als elektrisches Schaltsignal bereitgestellt werden.

**[0057] Fig. 3** zeigt eine Variante des Systems in **Fig. 2**, wobei hier neben dem ausgehenden Datenverkehr auf der zweiten Schnittstelle 22 auch der eingehende Datenstrom auf dem ersten Interface 21 durch eine zusätzliche Auskoppeleinheit 31 dupliziert und auf eine Leitung zur Überwachungseinheit 24 ausgekoppelt wird. Die Auskoppeleinheiten 25 und 31 befinden sich bevorzugt direkt an der Netzübergangseinheit 23, sodass insbesondere keine weiteren Komponenten im Datenstrom enthalten sind, die diesen verändern könnten.

**[0058]** Der aus der ersten Schnittstelle 21 ausgekoppelte Datenstrom wird in der Vergleichseinheit 32, mit dem Datenstrom der zweiten Schnittstelle 22 verglichen. Der Datenstrom der zweiten Schnittstelle 22 kann über die Prüfungseinheit 26 beispielsweise an die Vergleichseinheit 32 weitergegeben werden. Die Vergleichseinheit 32 ist wiederum mit der Kommunikationseinheit 27 verbunden. Wird ein Unterschied zwischen dem Datenstrom der ersten und der zweiten Schnittstelle 21,22 detektiert, sendet die Kommunikationseinheit 27 eine Warnnachricht 28 an die Netzübergangseinheit 23. Die Verbindung zwischen Überwachungseinheit 24 und Netzübergangseinheit 23 kann dabei in Form einer Drahtverbindung oder aber einer drahtlosen Verbindung oder einer logischen Verbindung ausgeführt sein.

**[0059]** Alle beschriebenen und/oder gezeichneten Merkmale können im Rahmen der Erfindung vorteilhaft miteinander kombiniert werden. Des Weiteren kann die Überwachungseinheit als separate Komponente oder aber mit der Netzübergangseinheit integriert ausgeführt sein.

## Patentansprüche

1. Verfahren zur Überwachung einer Sicherheits-Netzübergangseinheit (23), die einen Strom von Datenpaketen über eine erste Schnittstelle (21) empfängt, diesen Datenstrom gegenüber Filterregeln überprüft und an eine zweite Schnittstelle (22) ausgibt, mit den Verfahrensschritten:
- Duplizieren und Auskoppeln (11) des Datenstroms an der zweiten Schnittstelle (22),
- Überprüfen (12) des ausgekoppelten Datenstroms auf unzulässigen Datenverkehr,
- Senden (14) einer Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23), wenn unzulässiger Datenverkehr (12) im Datenstrom erkannt wird, und
- Beschränken (15) des Datenstroms durch die Sicherheits-Netzübergangseinheit (23), wenn die Warnnachricht (28) in der Sicherheits-Netzübergangseinheit (23) empfangen wird.

2. Verfahren nach Anspruch 1, mit den zusätzlichen Verfahrensschritten:
- Duplizieren und Auskoppeln (16) des Datenstroms an der ersten Schnittstelle (21),
- Vergleichen (18) des Datenstroms an der ersten Schnittstelle (21) mit dem Datenstrom an der zweiten Schnittstelle (22),
- Senden (14') einer Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23), wenn sich der Datenstrom der zweiten Schnittstelle (22) von dem Datenstrom der ersten Schnittstelle (21) unterscheidet.

3. Verfahren nach Anspruch 1 oder 2, wobei das Beschränken des Datenstroms durch eine Aktivierung von Ersatz-Filterregeln der Sicherheits-Netzübergangseinheit (23) erfolgt.

4. Verfahren nach Anspruch 1 oder 2, wobei das Beschränken des Datenstroms durch einen Neustart der Sicherheits-Netzübergangseinheit (23) mit einer geschützten Start-Software oder durch einem Neustart der Sicherheits-Netzübergangseinheit (23) mit einer Ersatz-Firmware-Abbild oder durch einen Wechsel von einer aktiven Virtuellen Maschine zu einer Ersatz-Virtuellen Maschine in einer Sicherheits-Netzübergangseinheit (23) erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei das Beschränken des Datenstroms durch Deaktivieren der zweiten Schnittstelle (22) und/oder durch Deaktivieren der ersten Schnittstelle (21) der Sicherheits-Netzübergangseinheit (23) erfolgt.

6. Verfahren nach einem der Ansprüche 1 bis 5, wobei das Beschränken des Datenstroms durch Deaktivieren einer Stromversorgungseinheit der Netzübergangseinheit (23) erfolgt.

7. Verfahren nach einem der Ansprüche 1 bis 6, wobei die Beschränkung in der Sicherheits-Netzübergangseinheit (23) solange aktiv bleibt wie die Warnnachricht (28) an der Sicherheits-Netzübergangseinheit (23) empfangen wird.

8. Verfahren nach einem der Ansprüche 1 bis 6, wobei die Beschränkung der Sicherheits-Netzübergangseinheit (23) solange aktiv bleibt bis ein explizi-

tes Signal zur Aufhebung der Beschränkung, bevorzugt durch eine Handlung von Administrations-Personal, an der Sicherheits-Netzübergangseinheit (23) empfangen wird.

9. Vorrichtung zur Überwachung einer Sicherheits-Netzübergangseinheit (23), die einen Strom von Datenpaketen über eine erste Schnittstelle (21) empfängt, diesen Datenstrom gegenüber Filterregeln überprüft und an eine zweite Schnittstelle (22) ausgibt, umfassend
- eine Auskoppeleinheit (25), die ausgebildet ist um den Datenstrom an der zweiten Schnittstelle (22) zu duplizieren und auszukoppeln,
- eine Überprüfungseinheit (26), die ausgebildet ist um den ausgekoppelten Datenstrom auf unzulässigen Datenverkehr zu überprüfen und
- eine Kommunikationseinheit (27), die ausgebildet ist um eine Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23) zu senden, wenn unzulässiger Datenverkehr im Datenstrom erkannt wird.

10. Vorrichtung nach Anspruch 9, umfassend zusätzlich eine
- Auskoppeleinheit (31), die ausgebildet ist um den Datenstrom auf der ersten Schnittstelle (21) zu duplizieren und auszukoppeln, und
- eine Vergleichseinheit (32), die ausgebildet ist um den ausgekoppelten Datenstrom der ersten Schnittstelle (21) mit dem Datenstrom der zweiten Schnittstelle (22) zu vergleichen und bei Erkennen von Unterschieden zwischen dem Datenstrom der zweiten Schnittstelle (22) und dem Datenstrom der ersten Schnittstelle (21) die Kommunikationseinheit (27) zu veranlassen eine Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23) zu senden.

11. Vorrichtung nach Anspruch 9 oder 10, wobei die Vorrichtung derart ausgebildet ist um das Verfahren gemäß den Ansprüchen 3 bis 8 auszuführen.

12. System zur Überwachung einer Sicherheits-Netzübergangseinheit (23) umfassend
- eine Sicherheits-Netzübergangseinheit (23), die derart ausgebildet um einen Strom von Datenpaketen über eine erste Schnittstelle (21) zu empfangen, diesen Datenstrom gegenüber Filterregeln zu überprüfen und an eine zweite Schnittstelle (22) auszugeben,
- eine Überwachungseinheit (24) mit einer Auskoppeleinheit (25), die ausgebildet ist zum Duplizieren und Auskoppeln des Datenstroms an der zweiten Schnittstelle (22), mit einer Überprüfungseinheit (26) zum Überprüfen des ausgekoppelten Datenstroms auf unzulässigen Datenverkehr, und einer Kommunikationseinheit (27), die ausgebildet ist zum Senden einer Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23), wenn unzulässiger Datenverkehr im Datenstrom erkannt wird, woraufhin die Sicherheits-Netzübergangseinheit (23) eingerichtet ist den Datenstrom zu beschränken.

13. System nach Anspruch 12, wobei die Überwachungseinheit (24) eine zusätzliche
- Auskoppeleinheit (31), die ausgebildet ist um den Datenstrom auf der ersten Schnittstelle (21) zu duplizieren und auszukoppeln, und
- eine Vergleichseinheit (32), die ausgebildet ist um den ausgekoppelten Datenstrom der ersten Schnittstelle (21) mit dem Datenstrom der zweiten Schnittstelle (22) zu vergleichen und bei Erkennen von Unterschieden zwischen dem Datenstrom der zweiten Schnittstelle (22) und dem Datenstrom der ersten Schnittstelle (21) die Kommunikationseinheit (27) zu veranlassen eine Warnnachricht (28) an die Sicherheits-Netzübergangseinheit (23) zu senden, umfasst.

14. System nach Anspruch 13, wobei die Sicherheits-Netzübergangseinheit (23) und die Überwachungseinheit (24) derart ausgebildet sind um das Verfahren gemäß den Ansprüchen 3 bis 8 auszuführen.

15. Computerprogramm mit Programmbefehlen zur Durchführung des Verfahrens nach Ansprüchen 1-8.

16. Datenträger, der das Computerprogramm nach Anspruch 15 speichert.

Es folgen 4 Seiten Zeichnungen

**Anhängende Zeichnungen**

FIG 1A

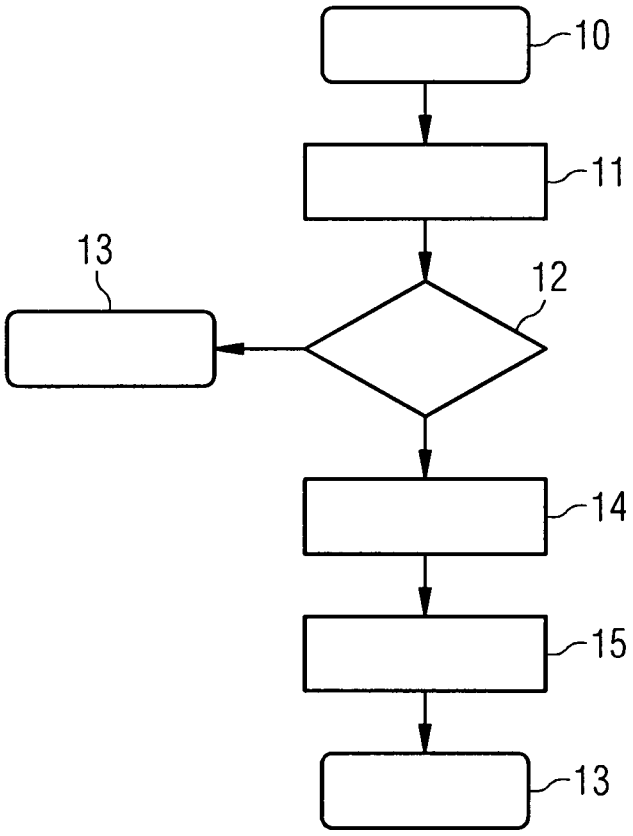


FIG 1B

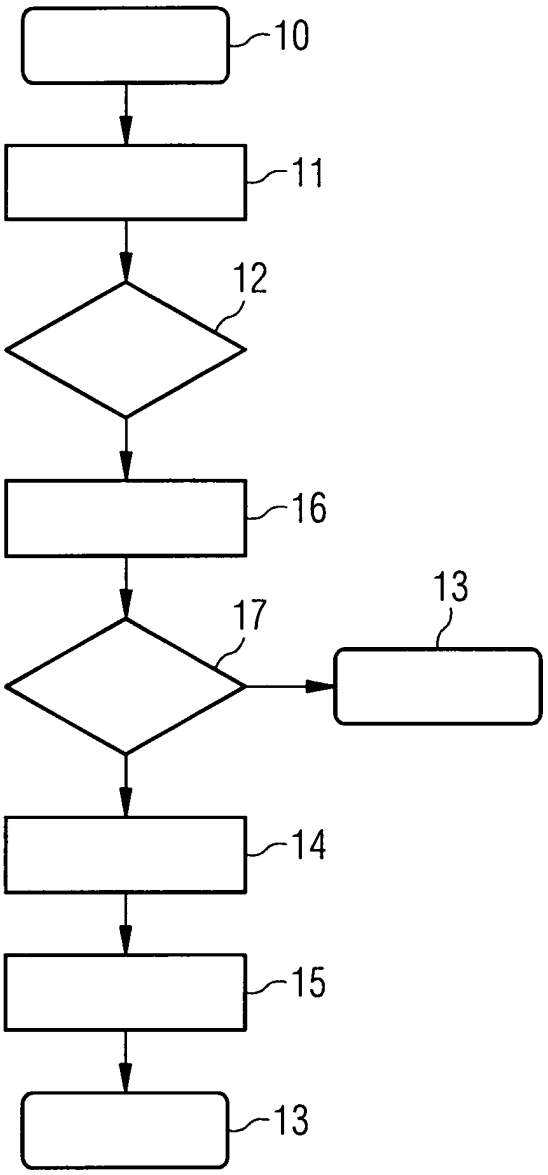


FIG 1C

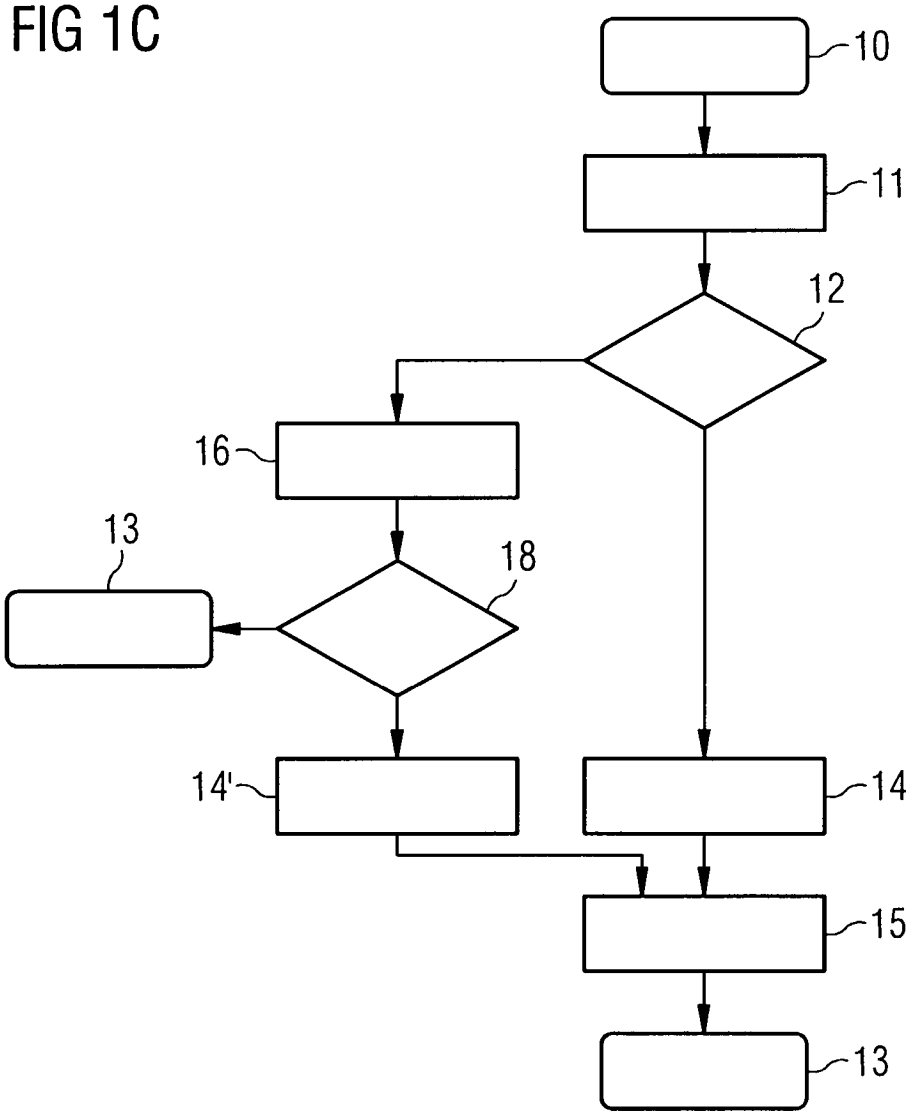


FIG 2

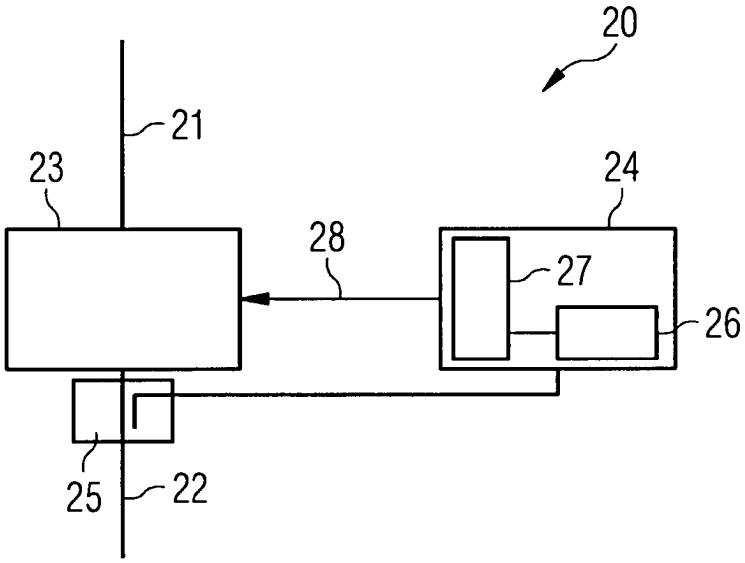



FIG 3