(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 109 358 B4** 2025.05.22

(12) # Patentschrift

(21) Aktenzeichen: **10 2016 109 358.0**
(22) Anmeldetag: **20.05.2016**
(43) Offenlegungstag: **24.11.2016**
(45) Veröffentlichungstag der Patenterteilung: **22.05.2025**

(51) Int Cl.: ***H04L 43/00*** (2022.01)
G05B 9/02 (2006.01)
G05B 19/418 (2006.01)
G05B 23/02 (2006.01)
G06F 21/55 (2013.01)
G06F 21/56 (2013.01)
H04L 9/40 (2022.01)
H04L 12/407 (2006.01)

(30) Unionspriorität:
14/719,946 **22.05.2015** **US**

(73) Patentinhaber:
Fisher-Rosemount Systems, Inc., Round Rock, Tex., US

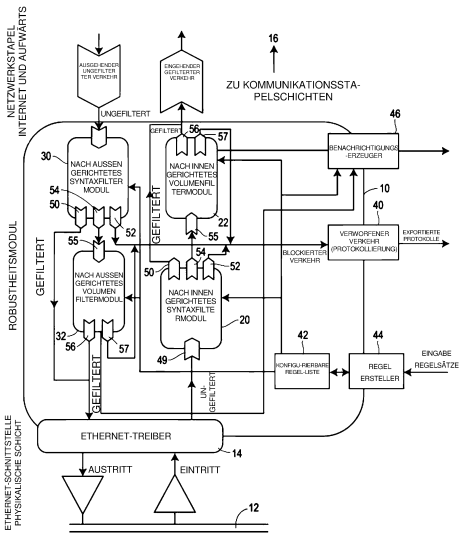
(74) Vertreter:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

(72) Erfinder:
Rayapeta, Vinaya S., Cedar Park, Tex., US; Peschansky, Jacob B., Austin, Tex., US; Bennett, William E., Georgetown, Tex., US

(56) Ermittelter Stand der Technik:
DE **11 2004 002 440** **T5**

(54) Bezeichnung: **Konfigurierbares Robustheitsmittel in einem Anlagensicherheitssystem**

(57) Hauptanspruch: Sicherheitssystem zur Verwendung in einem Kommunikationsnetzwerk, das eine Vielzahl von Netzwerkknoten aufweist, die kommunikativ über eine Kommunikationsverbindung gekoppelt sind, umfassend:
eine oder mehrere Nachrichtenmodulschnittstellen, wobei jede der Nachrichtenmodulschnittstellen an einem Prozessor an einem der Netzwerkknoten ausgeführt wird, um Nachrichtenverkehr an dem Netzwerkknoten zu detektieren und um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen;
einen Regelspeicher, der eine oder mehrere logische Regeln speichert; und
eine oder mehrere Filtereinheiten, die in einem Prozessor gespeichert und ausgeführt werden und mit dem Regelspeicher gekoppelt sind, wobei jede der Filtereinheiten Folgendes einschließt:
ein erstes Filtermodul und
ein zweites Filtermodul,
wobei das erste Filtermodul an dem Prozessor ausgeführt wird und eine oder mehrere logische Regeln, die in dem Regelspeicher gespeichert sind, auf Grundlage der Informationen über die Nachrichteneigenschaft zum Weiterleiten der Nachricht, zum Stoppen der Nachricht oder zum Weiterleiten der Nachricht an das zweite Filtermodul anwendet;
wobei das zweite Filtermodul die Anzahl der Nachrichten zählt, die einen bestimmten Satz von Nachrichteneigenschaften aufweisen, um eine Nachrichtenzählung zu bestimmen und auf Grundlage der Nachrichtenzählung die Nachricht weiterleitet oder die Nachricht stoppt, die den bestimmten Satz von Nachrichteneigenschaften aufweist
wobei die Nachrichtenzählung eine bestimmte Anzahl von Nachrichten ...



Beschreibung

TECHNISCHES GEBIET

[0001] Diese Anwendung betrifft im Allgemeinen Kommunikationssysteme von Prozessen oder Industrieanlagen und insbesondere das Detektieren des Eindringens in Kommunikationsnetzwerke für die Steuerung und Wartung, wie etwa denjenigen, die in Prozess- und industriellen Steuerungssystemen verwendet werden, auf Grundlage der Detektion und Filterung von Verkehr innerhalb der Kommunikationsnetzwerke der Anlage.

BESCHREIBUNG VERWANDTER TECHNIK

[0002] Steuerungs- und Wartungssysteme für Prozesse oder die Industrie, wie etwa verteilte oder skalierbare Prozesssteuerungssysteme wie diejenigen, die bei der Energiegewinnung, chemischen, Erdöl- oder anderen Herstellungsprozessen verwendet werden, schließen üblicherweise eine oder mehrere Steuerungen ein, die kommunikativ miteinander, über ein Prozesssteuerungsnetzwerk mit mindestens einem Host- oder Bedienarbeitsplatz und über analoge, digitale oder eine Kombination analoger/digitaler Busse mit einer oder mehreren Feldvorrichtungen gekoppelt sind. Die Feldvorrichtungen, bei denen es sich zum Beispiel um Ventile, Ventilstellungsregler, Schalter und Sender (z.B. Temperatur-, Druck- und Durchflusssensoren) handeln kann, führen innerhalb des Prozesses oder der Anlage Funktionen wie etwa das Öffnen oder Schließen von Ventilen, das Ein- und Ausschalten von Vorrichtungen und das Messen von Prozessparametern aus. Die Steuerungen empfangen Signale, die für von den Feldvorrichtungen durchgeführte Prozess- oder Anlagenmessungen bezeichnend sind und/oder andere Informationen in Bezug auf die Feldvorrichtungen, verwenden diese Informationen zum Implementieren von einer oder mehreren Steuerroutinen und erzeugen anschließend Steuersignale, die über die Busse oder Kommunikationskanäle des Anlagennetzwerks zu den Feldvorrichtungen übertragen werden, um den Betrieb des Prozesses oder der Anlage zu steuern. Informationen von den Feldvorrichtungen und der Steuerung werden üblicherweise über das Kommunikationsnetzwerk für eine oder mehrere Anwendungen zugänglich gemacht, die von dem Bedienarbeitsplatz ausgeführt werden, um es einem Bediener oder Wartungspersonal zu ermöglichen, eine beliebige gewünschte Funktion in Bezug auf den Prozess oder die Anlage auszuführen, wie etwa Anzeigen des aktuellen Zustands der Anlage, Modifizieren des Betriebs der Anlage, Kalibrieren von Vorrichtungen, Detektieren defekter Vorrichtungen usw.

[0003] Während des Betriebs werden die Prozesssteuerungen, die sich üblicherweise in der Umgebung der Prozessanlage befinden, gemäß einem Konfigurationsschema konfiguriert, um periodisch oder regelmäßig Signale zu empfangen, die für Prozessmessungen oder Prozessvariablen bezeichnend sind, die von den Feldvorrichtungen erzeugt werden oder damit verknüpft sind und/oder andere Informationen in Bezug auf die Feldvorrichtungen und führen unter Verwendung dieser Informationen Steuerungsanwendungen aus. Die Steuerungsanwendungen implementieren zum Beispiel unterschiedliche Steuermodule, die Entscheidungen über die Prozesssteuerung treffen, erzeugen auf Grundlage der empfangenen Informationen Steuersignale und koordinieren sich mit den Steuermodulen oder -blöcken in den Feldvorrichtungen, wie etwa HART® und FOUNDATION® Feldbus-Feldvorrichtungen. Ferner schicken die Steuermodule in den Prozesssteuerungen die Steuersignale über die Kommunikationsleitungen oder andere Signalwege zu den Feldvorrichtungen, wiederum gemäß einem Konfigurationsschema, um dadurch den Betrieb des Prozesses zu steuern.

[0004] Informationen von den Feldvorrichtungen und den Prozesssteuerungen werden außerdem üblicherweise über ein oder mehrere gesicherte Prozesssteuerungs- oder Wartungsnetzwerke für eine oder mehrere andere Hardware-Vorrichtungen innerhalb oder außerhalb der Anlage zugänglich gemacht, wie etwa zum Beispiel Bedienarbeitsplätze, Wartungsarbeitsplätze, Server, PCs, handgeführte Vorrichtungen, Verlaufsarchive für Daten oder Ereignisse, Reportgeneratoren, zentralisierte Datenbanken usw. Die Informationen, die über die Prozesssteuerungs- oder Wartungskommunikationsnetzwerke kommuniziert werden, ermöglichen es einem Bediener oder Wartungspersonal, gewünschte Funktionen in Bezug auf den Prozess auszuführen und/oder den Betrieb der Anlage oder der Vorrichtungen innerhalb der Anlage anzusehen. Zum Beispiel ermöglichen es die Steuerungsinformationen einem Bediener, Einstellungen von Prozesssteuerungsroutinen zu ändern, den Betrieb der Steuermodule innerhalb der Prozesssteuerungen oder der intelligenten Feldvorrichtungen zu modifizieren, den aktuellen Zustand des Prozesses oder den Status bestimmter Vorrichtungen innerhalb der Prozessanlage anzuzeigen, Alarme und/oder Benachrichtigungen anzuzeigen, die von Feldvorrichtungen und Prozesssteuerungen erzeugt wurden, den Betrieb des Prozesses zum Zwecke der Schulung von Personal oder dem Testen der Prozesssteuerungssoftware zu simulieren, Probleme oder Hardware-Fehler innerhalb der Prozessanlage zu diagnostizieren usw.

[0005] Die Feldvorrichtungen und Steuerungen kommunizieren mit den anderen Hardware-Vorrichtungen üblicherweise über ein oder mehrere gesicherte Prozesssteuerungs- oder Wartungskommunikationsnetzwerke, die zum Beispiel als Ethernet-konfigurierte LANs implementiert werden können. Die Prozesssteuerungs- oder Wartungskommunikationsnetzwerke schicken die Prozessparameter, Netzwerkinformationen und andere Prozesssteuerungsdaten durch verschiedene Netzwerkvorrichtungen und an verschiedene Einheiten in dem Prozesssteuerungssystem. Übliche Netzwerkvorrichtungen schließen Netzwerkschnittstellenkarten, Netzwerkschalter, Router, Server, Firewalls, Steuerungen, Bedienarbeitsplätze und Datenbanken ein. Die Netzwerkvorrichtungen erleichtern üblicherweise den Fluss von Daten durch das Netzwerk, indem das Routing, die Framerate, das Timeout und andere Netzwerkparameter gesteuert werden, ändern jedoch nicht die Prozessdaten an sich. Wenn das Prozesssteuerungsnetzwerk an Größe und Komplexität zunimmt, nehmen dementsprechend auch die Anzahl und Art von Netzwerkvorrichtungen zu. Als eine Folge von System- und Netzwerkwachstum werden die Sicherheit innerhalb dieser komplexen Systeme sowie ihre Verwaltung immer problematischer. Als ein Anfang werden diese Netzwerke jedoch im Allgemeinen von anderen externen Netzwerken isoliert und werden vor äußeren Angriffen durch eine oder mehrere Firewalls geschützt.

[0006] Im Allgemeinen werden die Arbeitsplätze/Server des Anlagensteuerungssystems in einem typischen industriellen Steuerungssystem strategisch zwischen externen Anlagennetzwerken, die verschiedene Funktionen ausführen, die mit der Anlage verknüpft sind und den eingebetteten Steuerungsvorrichtungen platziert, die Funktionen für die Steuerung und die Datenerfassung in dem Steuerungssystem ausführen (z.B. Steuerungen, PLCs, RTUs), um ein Eindringen in das Netzwerk einzuschränken. Ein wesentliches Sicherheitsziel für die Steuerungsarbeitsplätze/-server besteht darin, Malware am Eindringen in das Steuerungs- und Wartungssystem und der nachteiligen Beeinflussung der eingebetteten Vorrichtungen zu hindern sowie darin, Malware daran zu hindern, die Konfiguration und Verlaufsdaten, die in den Datenbanken der Anlagenprozesssteuerung gespeichert sind, zu ändern. Ferner verhindern diese Arbeitsplätze/Server einen unbefugten Zugriff auf das Steuerungssystem, um eine unbefugte Änderung der Anlagenkonfiguration, unbefugten Zugriff auf Anlagendaten usw. zu verhindern. Obwohl eine Anzahl von Sicherheitsmerkmalen, wie etwa Firewalls, „Antivirus“-Software und „Whitelisting“ verwendet werden können, um diese Sicherheitsziele anzugehen, sind diese Sicherheitsmerkmale üblicherweise nicht ausreichend. Zum Beispiel bietet Antivirus-Software keinen Schutz gegenüber „Zero-Day“-Viren und das Whitelisting hindert lediglich unerlaubte Anwendungen an ihrer Ausführung. Zusätzlich sind einige dieser Merkmale zu intrusiv, um in einem Prozesssteuerungssystem betrieblich praktisch zu sein, da diese Sicherheitsmerkmale das Potential haben, Aktivitäten von Anlagenbedienern oder der geplanten Steuerungsvorgänge zu behindern.

[0007] Ganz allgemein wird Malware, wie etwa die im Zentrum eines Zero-Day-Angriffs üblicherweise über eine unzulässige Kommunikationsverbindung zu einem externen Netzwerk über den Betrieb einer Anwendung oder eines Dienstes mit dem Privileg oder der Befugnis zum Zugriff auf die Speichervorrichtungen, die Netzwerkschnittstellen oder direkte Datenverbindungen innerhalb des Prozesssteuerungsnetzwerks in das gesicherte Steuerungssystemnetzwerk eingebracht. Alternativ kann Malware über lokales Personal in das gesicherte Steuerungssystemnetzwerk eingebracht werden, das infizierte tragbare Vorrichtungen und/oder Medien mit einer Steuerungssystemvorrichtung verbindet. Danach kann sich die Malware auf andere Vorrichtungen ausbreiten (z. B. über Kommunikationen) und/oder kann innerhalb einer Vorrichtung innerhalb des Prozesssteuerungsnetzwerks unter Verwendung der Sicherheitsprivilegien der Anwendungen oder Dienste ausgeführt werden, die mit der Malware infiziert werden. Zusätzlich kann die Malware lokal fortbestehen, damit sie nach einem Neustart vernetzter Vorrichtungen erneut ausgeführt werden kann. In einigen Fällen kann die Malware hinsichtlich der Privilegien eines Hosts, z. B. einer infizierten Anwendung oder einer Vorrichtung, unter Verwendung der Privilegien des Accounts aufsteigen, mit dem die Anwendung oder der Dienst ausgeführt wird und indem sie dies macht, kann die Malware dazu in der Lage sein, in der Prozesssteuerungsvorrichtung oder der Netzwerkvorrichtung Aktionen oder Operationen auszuführen, die ein höheres Privileg erforderlich machen und demnach für den Betrieb des Steuerungssystems üblicherweise schädlicher sind. Diese Angriffe können innerhalb einer Prozessanlage ernsthafte und möglicherweise zerstörerische oder sogar tödliche Folgen haben, wenn diese Angriffe den laufenden Betrieb des Anlagensteuerungssystems unterbrechen.

[0008] Es gab eine umfangreiche Forschungstätigkeit zur Definition und zum Erstellen von Hardware- und Softwarekonfigurationen, die agieren, um Angriffe auf Steuerungs- und Wartungssysteme für Prozesse oder die Industrie zu verhindern oder einzuschränken. Jedoch sind sogar dicht geschützte Netzwerke von Industriesteuerungssystemen (ICS) oder Netzwerke für die Überwachung-, Steuerung- und Datenerfassung (SCADA) immer noch anfällig gegenüber Sicherheitsbedrohungen, wie etwa einer Fehlkonfiguration der Sicherheitsabwehr, Benutzern mit berechtigtem Zugriff mit böswilliger Absicht und unbekannter aber bösartiger Software, die im Auftrag von Angreifern von außerhalb handelt. Zudem ist das automatische Detektieren

der Existenz von Viren oder Malware innerhalb einer Prozess- oder industriellen Steuerungsvorrichtung oder in Knoten für die Anlagenkommunikation nur begrenzt möglich, sobald ein Netzwerk infiziert wurde. Allgemein ausgedrückt, sobald ein Angriff in einer Anlagenumgebung erfolgreich war, wird im Allgemeinen ein Bediener, Wartungspersonal usw. benötigt, um zu detektieren, dass ein Knoten oder eine Vorrichtung für die Anlagenkommunikation infiziert ist. Obwohl es möglich ist, an jedem Knoten eines Kommunikationsnetzwerks eine Virensuchsoftware im Hintergrund auszuführen, nimmt diese Software viel Speicherplatz und Verarbeitungsressourcen in Anspruch, muss regelmäßig aktualisiert werden (was erhebliche Netzwerkwartungsressourcen und Zeit erforderlich macht) und ist dennoch nicht dazu in der Lage, Zero-Day-Viren zu detektieren.

[0009] In vielen Fällen können Viren oder unautorisierte Software an einer Anlagenvorrichtung oder einem Netzwerkknoten zu einer verringerten Leistung der Vorrichtung oder des Netzwerks führen, den normalen Anlagenbetrieb in ausreichendem Maße unterbrechen, um zu veranlassen, dass Fehler oder Alarme an diesem Knoten oder anderen Knoten innerhalb des Netzwerks generiert werden oder andere ernst zu nehmende und merkliche Probleme verursachen. In einigen dieser Fälle kann es für einen Bediener oder anderes Anlagenpersonal relativ einfach sein, die Existenz eines Virus zu detektieren, es kann aber dennoch schwierig sein, die Position des Virus zu detektieren. Zudem kann der Virus oder der Angriff in vielen anderen Fällen für einen beträchtlichen Zeitraum undetektiert agieren, während er Netzwerkoperationen geringfügig herabsetzen kann, diese Herabsetzung oder eine andere Auswirkung auf den Betrieb der Anlage kann unbedeutend und somit sehr schwer zu detektieren sein. Folglich können Viren in vielen Fällen für beträchtliche Zeiträume undetektiert bleiben, wobei die Viren in dieser Zeit agieren können, um die Effizienz von Anlagen zu reduzieren, um den Diebstahl von Anlagendaten zu ermöglichen, um ein ernster zu nehmendes Eindringen zu ermöglichen, um Netzwerkvorrichtungen gegenüber ernsthaften Angriffen oder Schäden freizulegen usw.

[0010] Das Dokument DE 11 2004 002 440 T5 offenbart ein IT-Sicherheitssystem zur Erkennung von Eindringlingen in ein privates Netz, das mit einem öffentlichen Netz verbunden ist und umfasst ein Verarbeitungssystem, ein Überwachungssystem und ein Schnittstellensystem. Das Verarbeitungssystem erkennt ein Eindringen oder einen unerwünschten Zugriff auf Ressourcen in einem privaten Netzwerk und alarmiert im Falle eines erkannten Eindringens oder unerwünschten Zugriffs auf Ressourcen, indem es quantitative Alarmdaten erzeugt. Das Überwachungssystem verarbeitet die Warnmeldungen automatisch oder leitet sie an einen Betreiber des Sicherheitssystems weiter. Das Schnittstellensystem überträgt die Warnmeldungen vom Verarbeitungssystem an das Überwachungssystem. Die verfügbaren Daten über die Netzaktivität können so dem Bediener auf intuitive und nichttechnische Weise präsentiert werden. Wenn der Betreiber den Verdacht hat, dass die Sicherheit des Netzes gefährdet ist, kann er das private Netz sicher von der Außenwelt isolieren, als einfache Reaktion auf jede Bedrohung, die die private Netzumgebung gefährdet.

KURZDARSTELLUNG

[0011] Die der Erfindung zugrundeliegende Aufgabe wird durch ein Sicherheitssystem zur Verwendung in einem Kommunikationsnetzwerk mit den Merkmalen des unabhängigen Patentanspruchs 1 gelöst. Weiterhin wird das Problem durch das Verfahren nach Anspruch 10 gelöst. Weiterhin wird das Problem durch das Kommunikationsnetzwerk nach Anspruch 19 gelöst. Weiterhin wird das Problem durch das Computer-lesbares Speichermedium nach Anspruch 25 gelöst. Vorteilhafte Weiterbildungen ergeben sich aus den jeweiligen abhängigen Ansprüchen.

[0012] Bei einem Steuerungssystem, wie etwa einem Steuerungs- oder Wartungssystem für die Industrie oder Prozessanlagen, wird ein Kommunikationsnetzwerksystem zur Detektion von Bedrohungen implementiert, das eine robuste Analyse und Filterung von Kommunikationen bereitstellt, die über das Netzwerk gesendet werden, um einen Schutz gegenüber potenziell infizierten Netzwerkknoten bereitzustellen. Allgemein ausgedrückt, schließt das Analysesystem ein Robustheitsmittel ein, das an einer Schnittstelle zwischen einer Knotenvorrichtung (z. B. eine Steuerung, eine Benutzerschnittstelle, ein Schalter usw.) und dem Kommunikationsnetzwerk agiert, wobei das Robustheitsmittel Nachrichten analysiert und filtert, die von dem Netzwerk kommen oder dorthin gehen, um die Art der Nachrichten, die durch das Robustheitsmittel fließen oder Informationen darüber zu ermitteln. Das Robustheitsmittel kann konfiguriert sein, um zu ermöglichen, dass bestimmte Arten von Nachrichten (z. B. Nachrichten mit bestimmten vorher festgelegten Eigenschaften) durch das Mittel zu dem Netzwerk oder zu der Vorrichtung geleitet werden, kann verhindern, dass Nachrichten mit anderen vorher festgelegten Eigenschaften durch das Mittel geleitet werden, wie etwa durch das Verwerfen oder Filtern dieser Nachrichten und/oder kann noch weitere Nachrichten, die andere Eigenschaften aufweisen, zur Zählung zu einem Volumenfilter weiterleiten. Der Volumenfilter kann agieren, um die Anzahl von Nachrichten einer bestimmten Art (oder mit einem bestimmten Satz von Nachrichteneigenschaften) zu

zählen und kann agieren, um diese Nachrichten weiterzuleiten, wenn die Anzahl dieser detektierten Nachrichten über einen bestimmten Zeitraum hinweg kleiner ist als ein bestimmter Schwellenwert, kann diese Nachrichten jedoch filtern, wenn die Anzahl der gezählten Nachrichten über einen bestimmten Zeitraum hinweg größer ist als ein bestimmter Schwellenwert. Allgemein ausgedrückt, kann das Robustheitsmittel konfiguriert sein, sodass seine Filteroperationen im Laufe der Zeit auf Grundlage von Veränderungen, die am Netzwerk vorgenommen werden, geändert werden können, es kann für unterschiedliche Arten von Netzwerken oder für Netzwerke in unterschiedlichen Anlagen justiert oder eingestellt werden und es kann im Allgemeinen konfiguriert sein, um mit dem erwarteten Betrieb eines bestimmten Netzwerks übereinzustimmen, in dem das Robustheitsmittel oder das Sicherheitssystem, das eine Anzahl von Robustheitsmitteln aufweist, betrieben wird.

[0013] Ganz allgemein verhindert das Sicherheitssystem, das ein oder mehrere derartige Robustheitsmittel verwendet, Knoten, die durch das Weiterleiten von Nachrichten infiziert sein können, die zu einer Art gehören oder die Eigenschaften aufweisen, für die es äußerst wahrscheinlich ist, dass sie mit einem Eindringen verknüpft sind und es verhindert Knoten, die durch das Senden einer beträchtlichen Menge von Nachrichten infiziert sein können, die mit einem Eindringen in das Netzwerk verknüpft sein können. Zudem trägt dieses System dazu bei, Knoten, die von einem infizierten Knoten angegriffen werden, daran zu hindern, eine beträchtliche Menge von Nachrichten von dem Netzwerk anzunehmen oder zu empfangen, das mit dem Eindringen verknüpft sein oder dadurch verursacht werden kann. Insbesondere überprüft das Robustheitsmittel des Sicherheitssystems ausgehende Nachrichten (von einem Knoten), um zu bestimmen, ob diese Nachrichten mit erwarteten Arten von Nachrichten an dem Netzwerk auf Grundlage der Konfiguration des Netzwerks übereinstimmen, z. B. um zu bestimmen, ob die ausgehenden Nachrichten Nachrichten sind, die Sätze von Eigenschaften aufweisen, die innerhalb von Netzwerkkonfigurationen, wie konfiguriert, zu erwarten sind. In einigen Fällen kann das Sicherheitssystem konfiguriert sein, um alle Nachrichten bestimmter Arten (oder mit bestimmten Sätzen von Eigenschaften) weiterzuleiten, die Nachrichten der Art einschließen können, für die angenommen wird, dass sie für den Betrieb des Netzwerks benötigt werden oder wesentlich sind. In anderen Fällen kann das Sicherheitssystem konfiguriert sein, um alle Nachrichten bestimmter Arten oder mit bestimmten Eigenschaften zurückzuweisen oder herauszufiltern, wobei diese Nachrichten nicht während des normalen Betriebs des Netzwerks, wie konfiguriert, auftreten sollten und es demnach wahrscheinlich ist, dass sie von Malware oder einem infizierten Knoten innerhalb des Systems generiert wurden. In einem dritten Fall kann das Sicherheitssystem eingestellt sein, um Nachrichten bestimmter Arten oder mit bestimmten Sätzen von Eigenschaften bis zu einem bestimmten Umfang bzw. einer bestimmten Stufe bedingt weiterzuleiten und diese Nachrichten dann auf eine gewisse Weise zu filtern. In diesem Fall ist es möglich, dass erwartet wird, dass eine begrenzte Anzahl von Nachrichten dieser dritten Art innerhalb des Netzwerks, wie konfiguriert, auftritt, dass diese Nachrichten jedoch suspekt sind, insofern als, dass lediglich ein bestimmtes Niveau bzw. eine bestimmte Menge dieser Nachrichten erwartet wird. Die Existenz von Nachrichten dieser Art oberhalb eines bestimmten Niveaus bzw. einer bestimmten Menge während eines bestimmten Zeitraums kann demnach dafür bezeichnend sein, dass diese Nachrichten von Malware oder einer anderen Art von Infektion oder Intrusion in das Netzwerk generiert werden. Wenn eine derartige Menge detektiert wird, dann kann das Robustheitsmittel all diese Nachrichten filtern oder kann eine begrenzte Anzahl dieser Nachrichten weiterleiten, während andere gefiltert werden, um die Menge unterhalb einer bestimmten Stufe zu halten, es kann einen Benutzer benachrichtigen, es kann eine Intrusion Detection Software ausführen und/oder es kann die Vorrichtung, welche die Nachrichten generiert, von der Netzwerkverbindung trennen, um zu verhindern, dass eine infizierte Vorrichtung Zugriff auf das Netzwerk hat.

[0014] In jedem Fall kann jedes der Robustheitsmodule des Sicherheitssystems konfiguriert sein, um unter Verwendung einer Konfigurationsdatei zu agieren, welche die Arten oder Eigenschaften von Nachrichten, die weitergeleitet, gefiltert oder zu dem Volumenfilter weitergeleitet werden sollen, die bestimmten zulässigen Mengen verschiedener Arten von Nachrichten in dem Volumenfilter, die von dem Robustheitsmittel zu ergreifenden Maßnahmen, wenn ein Volumenschwellenwert erreicht oder überschritten wird usw. spezifiziert. Diese Konfiguration oder die damit verknüpften Regeln können in einem Read-Only Flash-Speicher gespeichert werden, der mit dem Robustheitsmittel oder der Vorrichtung, in welcher das Robustheitsmittel agiert, verbunden sein kann, wodurch die Konfigurationsdaten während des Betriebs des Robustheitsmittels unveränderlich werden oder in einem Lese-/Schreibspeicher, wodurch die Konfiguration veränderbar und demnach während des Betriebs des Netzwerks robuster wird, wodurch das Sicherheitssystem während des Betriebs auf Grundlage von Veränderungen, die an dem Netzwerk vorgenommen werden, erneut konfiguriert werden kann. Im letztgenannten Fall kann die Konfigurationsdatei jedoch gegenüber Malware anfälliger sein, die agieren kann, um die Konfigurationsdatei zu infizieren. In einigen Fällen kann ein Teil der Regeln in einem Flash-Speicher gespeichert werden, während einige Daten oder Listen, die in den Regeln verwendet werden, auf konfigurierbare Weise in anderen Arten von Speichern gespeichert werden können.

[0015] Allgemein ausgedrückt, kann die Konfiguration der Robustheitsmittel auf Grundlage der Netzwerkposition und der -vorrichtung, mit der jedes Robustheitsmittel verbunden ist, variieren. Zudem kann eine beliebige Anzahl von Robustheitsmitteln in einem Kommunikationsnetzwerk bereitgestellt werden, um ein Netzwerksicherheitssystem auszumachen. Obwohl es in einigen Fällen wünschenswert sein kann, ist es nicht immer notwendig, dass jede Vorrichtung in dem Netzwerk ihr eigenes Robustheitsmittel aufweist. Gleichermaßen kann die Konfiguration von jedem Robustheitsmittel so eingestellt sein, dass es aufgrund der relativ statischen Konfiguration der Netzwerkknoten sowie des apriorischen Wesens der Konfigurationen von Steuerungs- oder Wartungssystemen für Prozesse oder die Industrie, die in einer Anlage oder einem Anlagensteuerungsnetzwerk verwendet werden, angemessen arbeitet.

[0016] In einer oder mehreren Ausführungsformen schließt ein Sicherheitssystem zur Verwendung in einem Kommunikationsnetzwerk, das eine Vielzahl von Netzwerkknoten aufweist, die kommunikativ über eine Kommunikationsverbindung gekoppelt sind, eine oder mehrere Nachrichtenmodulschnittstellen ein, wobei jede der Nachrichtenmodulschnittstellen an einem Prozessor an einem der Netzwerkknoten ausgeführt wird, um Nachrichtenverkehr an dem Netzwerkknoten zu detektieren und um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen. Das Sicherheitssystem schließt außerdem einen Regelspeicher ein, in dem eine oder mehrere logische Regeln gespeichert werden und das Sicherheitssystem schließt eine oder mehrere Filtereinheiten ein, die in einem Prozessor gespeichert und an diesem ausgeführt werden und mit dem Regelspeicher gekoppelt sind, wobei jede der Filtereinheiten ein erstes Filtermodul und ein zweites Filtermodul einschließt. In diesem Fall wird das erste Filtermodul an dem Prozessor ausgeführt und wendet eine oder mehrere logische Regeln, die in dem Regelspeicher gespeichert sind, auf Grundlage der Informationen über die Nachrichteneigenschaft zum Weiterleiten der Nachricht, zum Stoppen der Nachricht oder zum Weiterleiten der Nachricht an das zweite Filtermodul an. Zudem zählt das zweite Filtermodul die Anzahl der Nachrichten, die einen bestimmten Satz von Nachrichteneigenschaften aufweisen, um eine Nachrichtenzählung zu bestimmen und auf Grundlage der Nachrichtenzählung die Nachricht weiterleitet oder die Nachricht stoppt, die den bestimmten Satz von Nachrichteneigenschaften aufweist.

[0017] Falls gewünscht, kann die Nachrichtenzählung eine bestimmte Anzahl von Nachrichten mit dem bestimmten Satz von Nachrichteneigenschaften umfassen, der innerhalb eines bestimmten Zeitraums empfangen wird. Ferner kann der Regelspeicher ein Read-Only Memory, ein Lese-/Schreibspeicher oder ein Speicher sein, der einen ersten Teil, der ein Read-Only Memory ist und einen zweiten Teil einschließt, der ein Lese-/Schreibspeicher ist. Zusätzlich kann der Regelspeicher ein Flash-Speicher, wie etwa ein entfernbarer Flash-Speicher sein.

[0018] Zudem kann das Sicherheitssystem ein Protokollierungsmodul einschließen, das mit den ersten und/oder den zweiten Filtermodulen gekoppelt ist und an dem Prozessor ausgeführt wird, um Informationen im Hinblick auf eine oder mehrere gestoppte Nachrichten zu empfangen und um Informationen im Hinblick auf die einen oder mehreren gestoppten Nachrichten in einem Protokoll oder einer Protokolldatei zu speichern. Das Protokollierungsmodul kann eine Kommunikationsschnittstelle einschließen, die ein oder mehrere Protokolle gestoppter Nachrichten zu einem Benutzer schickt und kann Metadaten im Hinblick auf die gestoppten Nachrichten speichern. Das Sicherheitssystem kann außerdem oder stattdessen ein Benachrichtigungserzeugungsmodul einschließen, das mit dem zweiten Filtermodul gekoppelt ist, wobei das Benachrichtigungserzeugungsmodul an dem Prozessor ausgeführt wird, um eine Benachrichtigung an einen Benutzer zu schicken, wenn die Nachrichtenzählung eine vorher festgelegte Stufe erreicht. Das Benachrichtigungserzeugungsmodul kann außerdem agieren, um eine Vorrichtung (wie etwa eine Vorrichtung an dem Netzwerk, die eine beträchtliche Anzahl von Nachrichten einer bestimmten Art oder mit einem bestimmten Satz von Eigenschaften generiert) von dem Kommunikationsnetzwerk zu trennen, wenn die Nachrichtenzählung eine vorher festgelegte Stufe erreicht. Ferner können die einen oder mehreren Filtereinheiten eine erste Filtereinheit, die Nachrichten empfängt und analysiert, die von der Kommunikationsverbindung in den Netzwerkknoten gelangen und eine zweite Filtereinheit einschließen, die Nachrichten empfängt und analysiert, die in dem Netzwerkknoten erzeugt und über die Kommunikationsverbindung zu einem anderen Netzwerkknoten geschickt werden.

[0019] In einer oder mehreren anderen Ausführungsformen schließt ein Verfahren zur Sicherung von Nachrichtenverkehr in einem Kommunikationsnetzwerk das Empfangen einer Reihe von Nachrichten an einer Vorrichtung, die mit dem Kommunikationsnetzwerk verbunden ist und das Analysieren, über einen Prozessor an der Vorrichtung, von jeder der Reihe von Nachrichten ein, um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen. Das Verfahren schließt ferner das Filtern von jeder der Nachrichten, über den Prozessor an der Vorrichtung, auf Grundlage einer Reihe von logischen Regeln, die an der Vorrichtung gespeichert sind, ein, wobei das Filtern das Weiterleiten von Nachrichten mit einem oder mehreren ers-

ten Sätzen von Nachrichteneigenschaften, das Stoppen von Nachrichten mit einem oder mehreren zweiten Sätzen von Nachrichteneigenschaften und das Zählen von Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften einschließt. Zudem schließt das Verfahren ferner das Weiterleiten oder Stoppen der Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften auf Grundlage von Zählungen ein, die mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften verknüpft sind.

[0020] In noch weiteren einen oder mehreren Ausführungsformen schließt ein Kommunikationsnetzwerk eine Kommunikationsverbindung und eine Vielzahl von Netzwerkknoten ein, wobei jeder der Netzwerkknoten eine Netzwerkvorrichtung einschließt, die mit der Kommunikationsverbindung gekoppelt ist und einen Prozessor und einen Kommunikationsstapel aufweist, der an dem Prozessor zur Verarbeitung von Nachrichten ausgeführt wird, die von der Kommunikationsverbindung kommen und dorthin gehen. Ferner schließt jeder einer Vielzahl der Netzwerkknoten ferner eine oder mehrere Nachrichtenmodulschnittstellen ein, wobei jede der Nachrichtenmodulschnittstellen an einem Prozessor an einem Netzwerkknoten ausgeführt wird, um Nachrichtenverkehr zu detektieren, der von dem Kommunikationsstapel oder von der Kommunikationsverbindung kommt, um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen. Jeder der Vielzahl von Netzwerkknoten schließt außerdem einen Regelspeicher ein, der eine oder mehrere logische Regeln speichert und schließt ein Filtermodul ein, das in einem Prozessor gespeichert und an diesem ausgeführt wird und mit dem Regelspeicher gekoppelt ist, das die Reihe logischer Regeln, die in dem Regelspeicher gespeichert sind, verwendet, um Nachrichten mit einem oder mehreren ersten Sätzen von Nachrichteneigenschaften weiterzuleiten, um Nachrichten mit einem oder mehreren zweiten Sätzen von Nachrichteneigenschaften zu stoppen und um Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften zu zählen. Das Filtermodul leitet ferner die Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften auf Grundlage von Zählungen, die mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften verknüpft sind, weiter oder stoppt sie.

KURZBESCHREIBUNG DER ZEICHNUNGEN

Fig. 1 bildet ein konfigurierbares Robustheitsmittel ab, das in einem Prozesssteuerungsnetzwerk verwendet werden kann, um die Auswirkungen eines Eindringens in ein Netzwerk einzugrenzen.

Fig. 2 ist ein beispielhaftes Blockdiagramm einer Prozess- oder Industrieanlage, die mehrere miteinander verbundene Kommunikationsnetzwerke aufweist, in denen ein oder mehrere auf einem Robustheitsmittel basierende Sicherheitssysteme implementiert werden können.

Fig. 3 ist ein beispielhaftes Schaubild von einem der Anlagennetzwerke aus **Fig.** 2 in Form eines verteilten Prozesssteuerungssystems und Prozessautomatisierungsnetzwerks, das verschiedene Netzwerkknoten aufweist, einschließend Bedien- und Wartungsarbeitsplätze, Server und Steuerungsknoten, wobei ein Sicherheitssystem, welches das Robustheitsmittel aus **Fig.** 1 verwendet, agiert, um die Auswirkungen von infizierten oder gefährdeten Knoten einzugrenzen und diese möglicherweise zu detektieren.

BESCHREIBUNG

[0021] Allgemein ausgedrückt, werden in einem hierin beschriebenen Netzwerksicherheitssystem eine Detektion von Bedrohungen und eine Wiedergutmachung von Bedrohungen implementiert, indem Netzwerkverkehr analysiert wird, der in eine oder mehrere Vorrichtungen an einem Kommunikationsnetzwerk hineingeht und/oder dort herauskommt, um auf Grundlage von einer oder mehreren Nachrichteneigenschaften, wie etwa einer Nachrichtenart, einem Sender, einem Empfänger, einem Sender-/Empfänger-Paar usw. zu bestimmen, ob die Nachricht weitergeleitet, gefiltert oder weiter verarbeitet werden soll, alles zum Zwecke der Umsetzung der Netzwerksicherheit. In einigen Fällen kann die weitere Verarbeitung das Zählen oder Detektieren einer Menge von Nachrichten einschließen, die eine bestimmte Art (oder einen anderen Satz von Eigenschaften) innerhalb eines bestimmten Zeitraums aufweisen. Die weitere Verarbeitung kann dazu führen, dass die Nachrichten mit der bestimmten Art oder einem anderen Satz von Eigenschaften entweder weitergeleitet oder gesperrt (z. B. gelöscht) werden und/oder kann dazu führen, dass eine andere Maßnahme ergriffen wird, wie etwa das Ausführen einer Intrusion Detection Software an dem Knoten, das Entfernen einer Vorrichtung aus dem Netzwerk, um das Netzwerk vor einer Infektion innerhalb der Vorrichtung zu schützen usw. Das hierin beschriebene Sicherheitssystem arbeitet effizient, da das apriorische Wesen der Konfiguration des industriellen Systems oder des Prozesssteuerungsnetzwerks auf Grundlage erwarteter oder bekannter Verkehrsstatistiken, die sich aus einer bestimmten Netzwerkkonfiguration ergeben, eine Analyse von grundlegendem Datenverkehr ermöglicht (und dass dieser relativ bekannt und statisch ist). Das heißt,

dass die Konfiguration von Netzwerkkommunikationen in Netzwerken für die Prozesssteuerung, für ein industrielles System oder die Anlagenautomatisierung im Allgemeinen vor der Implementierung oder dem Betrieb des Kommunikationsnetzwerks ziemlich wohlbekannt ist und die grundlegende Konfiguration des Netzwerkverkehrs demnach nicht dazu neigt, sich während der Verwendung oder des Betriebs dieser Netzwerke deutlich zu verändern. Stattdessen neigt der Verkehr der Netzwerkkommunikation dazu, während des Betriebs des Kommunikationsnetzwerks ziemlich statisch zu sein (im statistischen Sinne) und ändert sich demnach in den Arten oder Eigenschaften der Netzwerknachrichten oder Nachrichtenmuster, besonders im statistischen Sinne, können für ein Eindringen in das Netzwerk bezeichnend sein, das kein Teil der ursprünglichen oder gewünschten Konfiguration ist.

[0022] Allgemein ausgedrückt, unterliegen Vorrichtungen von Industriesteuerungssystemen, zum Beispiel mit Ethernet-Schnittstellen, verschiedenen Mustern und Bedingungen für den Netzwerkverkehr, die das Potential haben das Verhalten der Vorrichtung nachteilig zu beeinflussen. Ein Sicherheitssystem, wie hierin beschrieben, ist dazu in der Lage, mit Regeln konfiguriert oder aktualisiert zu werden, die spezifische Muster für den Nachrichtenverkehr an dem Netzwerk regulieren, wie etwa in die Vorrichtungen an dem Netzwerk hinein und aus diesen heraus. Bediener von Steuerungssystemen benötigen jedoch Vorrichtungen, die angesichts eines ungewöhnlichen Verkehrs robust sind und demnach kann das hierin beschriebene Sicherheitssystem spontan konfiguriert werden, um Verkehr auf angemessene Weise zu detektieren und zu handhaben, um ein nachteiliges Verhalten der Vorrichtung zu verhindern. In einigen Fällen können die Regeln dynamisch konfigurierbar sein, die Regeln können auf Grundlage von Bedingungen oder anderen Regeln Abhängigkeiten aufweisen, um einen vorausschauenden Schutz bereitzustellen, die Regeln können dynamisch andere Regeln aufrufen, um einen effizienten, robusten Betrieb zu ermöglichen und die Regeln können an spezifisch Verkehrsmuster in spezifischen Installationen anpassbar sein. Zudem kann das hierin beschriebene Sicherheitssystem automatisch Regeln zum Schutz vor dynamisch entdeckten nachteiligen Verkehrsmustern und/oder Zuständen erzeugen, während das Netzwerk betriebsbereit ist. Ferner ist das Sicherheitssystem in einigen Fällen dazu in der Lage, Angriffe von gefährdeten Vorrichtungen oder Knoten des Steuerungssystems zu identifizieren und zu verhindern, indem Austrittsverkehr analysiert wird, der aus diesen Vorrichtungen austritt und ungewöhnlicher Verkehr verworfen wird, der nicht mit den erlaubten Verkehrsregeln oder Nachrichtenarten übereinstimmt, wodurch die Verwendung dieser Vorrichtungen in dem Steuerungssystem zum Einleiten bösartiger Netzwerkangriffe verhindert wird.

[0023] Insbesondere schließt das hierin beschriebene Sicherheitssystem ein konfigurierbares Robustheitsmittel ein, das sich an einem oder mehreren Knoten eines Kommunikationsnetzwerks befindet, für das Sicherheit umgesetzt wird. Ganz allgemein agiert das konfigurierbare Robustheitsmittel, um den Fluss des Nachrichtenverkehrs in einen Kommunikationsknoten und/oder aus diesem heraus gemäß der Theorie zu verwalten (z. B. einschränken), dass die Existenz einer bestimmten Art bzw. eines Flusses oder Musters von Nachrichten mit bestimmten vorher festgelegten Eigenschaften für Malware bezeichnend sein kann, die in dem Knoten (oder in einem anderen Knoten und den Knoten angreifend) agiert oder andererseits für einen Angriff an oder von dem Knoten bezeichnend sein kann. Das Robustheitsmittel agiert, um die Auswirkungen eines derartigen Angriffs einzuschränken, indem jede der Nachrichten, die in den Knoten hinein oder aus diesem herausgeht analysiert wird, um zu bestimmen, ob die Nachrichten Eigenschaften aufweisen, die (1) erwartet, (2) nicht erwartet oder (3) in gewissem Maße, jedoch nur in einer bestimmten Menge oder Stufe, erwartet werden. Wenn eine eingehende Nachricht einen Satz von Eigenschaften (z. B. eine Nachrichtenart, einen bestimmten Sender oder Empfänger oder ein Sender-/Empfänger-Paar usw.) aufweist, der in den Netzwerkkommunikationen erwartet wird, kann das Robustheitsmittel die Nachricht einfach weiterleiten (entweder in den Knoten, wenn die Nachricht eine eingehende Nachricht von dem Netzwerk ist oder zu der Netzwerkverbindung, wenn die Nachricht eine ausgehende Nachricht von dem Knoten ist). Wenn eine eingehende Nachricht einen Satz von Eigenschaften (z. B. eine Nachrichtenart, einen bestimmten Sender oder Empfänger oder ein Sender-/Empfänger-Paar usw.) aufweist, der in den Netzwerkkommunikationen an der empfangenden oder sendenden Vorrichtung nicht erwartet wird, kann das Robustheitsmittel die Nachricht löschen, filtern oder sperren, um zu verhindern, dass die Nachricht die höheren Ebenen des Kommunikationsstapels in dem Knoten erreicht (wenn die Nachricht eine eingehende Nachricht von dem Netzwerk ist) oder dass sie an der Netzwerkverbindung platziert wird (wenn die Nachricht eine ausgehende Nachricht von dem Knoten ist). Wenn eine eingehende Nachricht einen Satz von Eigenschaften (z. B. eine Nachrichtenart, einen bestimmten Sender oder Empfänger oder ein Sender-/Empfänger-Paar usw.) aufweist, der in gewisser Hinsicht in dem Netzwerk erwartet wird, jedoch nur mit einer begrenzten Stufe oder Menge, kann das Robustheitsmittel die Nachrichten dieser Art oder mit diesem Satz von Eigenschaften zählen, um die Anzahl von Nachrichten dieser Art oder mit diesem Satz von Eigenschaften zu bestimmen, die durch das Robustheitsmittel über einen bestimmten Zeitraum hinweg hindurchgehen.

[0024] In diesem Fall kann das Robustheitsmittel die Nachricht weiterleiten, wenn die Menge unterhalb einer bestimmten Stufe liegt und kann die Nachricht blockieren oder sperren, wenn die Menge oberhalb einer bestimmten Stufe oder eines bestimmten Schwellenwerts liegt. Zudem kann das Robustheitsmittel, wenn die Menge oberhalb einer bestimmten Stufe liegt, was anzeigt, dass der Knoten angegriffen wird oder Malware oder eine Infektion aufweist, die das Netzwerk angreift, weitere Maßnahmen ergreifen, um das Kommunikationsnetzwerk zu schützen. Zum Beispiel kann das Robustheitsmittel den Knoten trennen, an dem sich das Robustheitsmittel befindet, wenn dieser Knoten zu viele Nachrichten einer bestimmten Art zu dem Netzwerk schickt. Alternativ, wenn das Robustheitsmittel einen Angriff von einem anderen Knoten detektiert (auf Grundlage der Anzahl oder der Menge verdächtiger Nachrichten von diesem anderen Knoten), kann das Robustheitsmittel ein Signal oder eine Nachricht zu dem anderen Knoten schicken (z. B. über das Kommunikationsnetzwerk), um zu veranlassen, dass der andere Knoten sich selbst von dem Netzwerk trennt. In diesen oder anderen Fällen kann das Robustheitsmittel einem Benutzer oder Bediener einen potenziellen Angriff und einige der Einzelheiten des Angriffs melden, kann Anwendungen für die Erkennung von Malware oder die Intrusion Detection an einem oder mehreren Knoten des Netzwerks aufrufen, um zu bestimmen, ob an diesen Knoten ein Virus, Malware oder eine andere Intrusion vorliegt oder kann eine beliebige andere gewünschte Maßnahme ergreifen.

[0025] Falls gewünscht, kann das Robustheitsmittel konfigurierbar sein, um es dem Robustheitsmittel zu ermöglichen, dass es besser für die bestimmte Netzwerkumgebung, in der es sich befindet, den bestimmten Knoten, an dem es sich befindet usw. geeignet ist. Insbesondere kann das Robustheitsmittel auf Grundlage des erwarteten Nachrichtenverkehrs in einen bestimmten Knoten hinein und aus diesem heraus konfigurierbar sein, der sich ändern oder auf Grundlage der Art des Knotens (z.B. ein Steuerungsknoten, ein Benutzerschnittstellenknoten, ein Datenbankknoten usw.), auf Grundlage der Position des Knotens usw. unterschiedlich sein kann. Zudem kann das konfigurierbare Wesen des Robustheitsmittels dem Robustheitsmittel ermöglichen, auf Grundlage detektierter Statistiken des Nachrichtenverkehrs an dem Knoten oder als Reaktion auf Veränderungen hinsichtlich der Konfiguration von einem oder mehreren Knoten der Kommunikationssysteme usw. besser zu agieren.

[0026] **Fig.** 1 veranschaulicht ein beispielhaftes Robustheitsmittel oder -modul 10, das in einem Kommunikationsnetzwerk verwendet werden kann, um die zuvor beschriebenen Funktionen auszuführen. Insbesondere ist das Robustheitsmodul 10 an einer Schnittstelle eines Netzwerkknotens (z. B. eine Netzwerkvorrichtung) und der physikalischen Schicht der Netzwerkverbindung 12 angeordnet. Insbesondere kann das Robustheitsmittel 10 zwischen einem Netzwerktreiber, wie etwa einem Ethernet-Treiber 14, der mit der Netzwerkverbindung 12 verbunden ist und den höheren Schichten des Netzwerkkommunikationsstapels 16 der Netzwerkvorrichtung gekoppelt sein. Wie in **Fig.** 1 veranschaulicht, kann das Robustheitsmodul 10 ein nach innen gerichtetes Syntaxfiltermodul 20 und ein nach innen gerichtetes Volumenfiltermodul 22 einschließen, die zwischen dem Treiber 14 und dem Netzwerkstapel 16 gekoppelt sind, um Nachrichten zu verarbeiten, die von der Netzwerkverbindung 12 zu der Netzwerkvorrichtung geschickt werden. Das Robustheitsmodul 10 kann außerdem ein nach außen gerichtetes Syntaxfiltermodul 30 und ein nach außen gerichtetes Volumenfiltermodul 32 einschließen, die zwischen dem Netzwerkstapel 16 und dem Treiber 14 gekoppelt sind, um Nachrichten zu verarbeiten, die von der Netzwerkvorrichtung (dem Netzwerkkommunikationsstapel 16) zu der Netzwerkverbindung 12 geschickt werden. Das Robustheitsmodul 10 schließt außerdem einen Protokollierungsblock 40 für verworfene Nachrichten, der mit jedem der Module 20, 22, 30 und 32 verbunden ist, einen Regelspeicher 42, der Konfigurationsregeln (z.B. logische Regeln) speichert, die von einem oder mehreren der Module 20, 22, 30 und 32 implementiert werden können und einen Regelerstellungsblock 44 ein, der verwendet werden kann, um die Regeln in dem Regelspeicher 42 zu erstellen (z. B. aufstellen oder ändern). Ferner kann das Robustheitsmodul 10 einen Benachrichtigungserzeuger 46 einschließen, der agieren kann, um Benachrichtigungen für Benutzer bereitzustellen, wenn einer der Volumenfilter 22 oder 32 eine beträchtliche Menge von Nachrichten einer bestimmten Art (z.B. mit einem bestimmten Satz von Eigenschaften) detektiert. Der Benachrichtigungserzeuger 46 kann außerdem oder stattdessen andere Aktionen ausführen, wie etwa das Initiieren von Malware- oder Viruserkennungssoftware an der Vorrichtung oder an einem anderen Knoten des Netzwerks, das Trennen der Vorrichtung von dem Netzwerk oder das Senden einer Nachricht zu einem Robustheitsmittel an einem anderen Knoten des Netzwerks, damit sich dieser Knoten selbst von dem Netzwerk trennt usw.

[0027] Während des Betriebs werden Nachrichten von der Kommunikationsverbindung 12 empfangen und werden an dem Treiber 14 verarbeitet, um zum Beispiel zu bestimmen, ob jede der Nachrichten an der Verbindung 12 an die bestimmte Netzwerkvorrichtung oder an eine Adresse oder Anwendung innerhalb dieser Vorrichtung oder damit verknüpft, gerichtet ist. Natürlich kann der Treiber 14 eine beliebige bekannte oder gewünschte Art eines Netzwerktreibers, wie etwa ein Ethernet-Treiber, wie in **Fig.** 1 veranschaulicht, sein

und kann auf eine beliebige bekannte Art und Weise agieren. Nachrichten, die für die Netzwerkvorrichtung bestimmt sind, werden dann zu einem Eingang 49 des nach innen gerichteten Syntaxfiltermoduls 20 weitergeleitet, welches diese Nachrichten analysiert, um eine oder mehrere Eigenschaften der Nachrichten zu bestimmten. Diese Eigenschaften können die Art der Nachricht (z. B. UDP, TCP usw.), einen Sender und/oder Empfänger, der mit der Nachricht verknüpft ist, eine Nachrichtenlänge, eine Parität, einen Sicherheitstyp, eine Priorität der Nachricht, einen Port, der die Nachricht sendet oder empfängt oder eine beliebige andere gewünschte Nachrichteneigenschaft einschließen. Diese eine oder mehreren Nachrichteneigenschaften sind im Allgemeinen in dem Header und/oder dem Endsegment oder einem anderen eingeschlossenen Bereich der Nachricht zu finden oder können durch darin enthaltene Informationen bestimmt werden, obwohl auch Eigenschaften der Nutzdaten oder des Datenabschnitts der Nachrichten untersucht und zum Filtern verwendet werden können.

[0028] Allgemein ausgedrückt, bestimmt das nach innen gerichtete Syntaxfiltermodul 20 einen oder mehrere Sätze von Eigenschaften jeder Nachricht (wobei diese Sätze von Eigenschaften in dem Regelspeicher 42 gespeichert oder dadurch bereitgestellt werden können oder in dem Syntaxmodulfilter 20 fest kodiert werden können). Nach der Bestimmung der einen oder mehreren Sätze von Eigenschaften, die mit einer Nachricht verknüpft sind, wird das Syntaxfiltermodul 20 eine oder mehrere logische Regeln anwenden, die auf Grundlage dieser bestimmten Eigenschaften agieren, um zu entscheiden, wie die Nachricht weiter verarbeitet werden soll. Insbesondere auf Grundlage der bestimmten Nachrichteneigenschaften und der Regeln in dem Regelspeicher 42 kann das Syntaxfiltermodul 20 eine Nachricht (für die angenommen wird, dass sie sicher ist oder eine erwartete Nachricht) von einem Ausgang 50 direkt zu dem Ausgang des Robustheitsmoduls 10 und demnach zu der nächsten Schicht des Netzwerkkommunikationsstapels 16 der Netzwerkvorrichtung weiterleiten, wo die Nachricht entschlüsselt, verarbeitet und zu dem geeigneten Empfänger in der Netzwerkvorrichtung auf eine beliebige standardmäßige Art und Weise weitergeleitet wird. In anderen Fällen kann das Syntaxfiltermodul 20 auf Grundlage der bestimmten Nachrichteneigenschaften und der Regeln in dem Regelspeicher 42 eine Nachricht (für die angenommen wird, dass sie unsicher oder definitiv in dem Netzwerk nicht erlaubt ist) von einem Ausgang 52 zu dem Protokollierungsblock 40 für verworfenen Verkehr weiterleiten, welcher diese Nachricht, Metadaten über diese Nachricht oder andere Informationen über die Nachricht für eine zukünftige Verwendung bei der Analyse von Netzwerkintrusionen, eine Änderung der Regeln in dem Regelspeicher 42, um eine bessere oder genauere Filterung auszuführen usw. protokollieren kann. In noch weiteren Fällen kann das Syntaxfiltermodul 20 auf Grundlage der bestimmten Nachrichteneigenschaften und der Regeln in dem Regelspeicher 42 eine Nachricht (für die angenommen wird, dass sie möglicherweise nicht sicher ist) von einem Ausgang 54 zu einem Eingang 55 des nach innen gerichteten Volumenfiltermoduls 22 weiterleiten.

[0029] Allgemein ausgedrückt, bearbeitet das nach innen gerichtete Volumenfiltermodul 22 Nachrichten, die Eigenschaften aufweisen, die anzeigen, dass diese Nachrichten, jedoch nicht zwangsläufig, zulässig sein können, da diese Nachrichten zu einer Art gehören oder Eigenschaften aufweisen können, die in einem zulässigen Netzwerkverkehr verwendet werden und die außerdem von typischer Malware oder typischen Viren verwendet werden, um ein System anzugreifen, besonders mengenmäßig. Das nach innen gerichtete Volumenfiltermodul 22 empfängt diese Nachrichten (wie von dem nach innen gerichteten Syntaxfiltermodul 20 detektiert) und zählt diese Nachrichten (unter Verwendung von einem oder mehreren Zählern) und kann zusätzlich nachverfolgen, wie viele derartige Nachrichten über einen bestimmten Zeitraum oder innerhalb eines bestimmten Zeitabschnitts in der Vergangenheit empfangen werden. Demnach bestimmt das nach innen gerichtete Volumenfiltermodul 22 die Menge des Nachrichtenverkehrs (z. B. Anzahl von Nachrichten über einen oder innerhalb eines bestimmten Zeitraum(s)) von Nachrichten mit einem bestimmten Satz von Nachrichteneigenschaften. Natürlich kann das nach innen gerichtete Volumenfiltermodul 22 Nachrichtenmengen für eine beliebige Anzahl unterschiedlicher Sätze von Nachrichteneigenschaften nachverfolgen.

[0030] In jedem Fall kann das nach innen gerichtete Volumenfiltermodul 22, wenn die aktuelle Menge einer Nachrichtenart (d. h. Nachrichten mit einem bestimmten Satz von Eigenschaften) unterhalb eines vorher festgelegten Schwellenwerts (wobei dieser Schwellenwert in dem Regelspeicher 42 gespeichert werden kann) liegt, die Nachricht zur Verarbeitung in der Netzwerkvorrichtung über einen Ausgang 56 zu dem Stapel 16 weiterleiten. Andererseits kann das nach innen gerichtete Volumenfiltermodul 22, wenn die aktuelle Menge einer Nachrichtenart (d. h. Nachrichten mit einem bestimmten Satz von Eigenschaften) oberhalb eines vorher festgelegten Schwellenwerts (wobei dieser Schwellenwert in dem Regelspeicher 42 gespeichert werden kann) liegt, die Nachricht blockieren oder verwerfen, indem die Nachricht zum Beispiel über einen Ausgang 57 für den Protokollierungsblock 40 für verworfenen Verkehr bereitgestellt wird. Hier kann der Block 40 wiederum die Nachricht und/oder Metadaten über die Nachricht protokollieren, um Statistiken über diese blockierten Nachrichten zu ermitteln. Ferner kann das nach innen gerichtete Volumenfiltermodul 22 die aktuelle

Menge einer Nachrichtenart mit mehreren Schwellenwerten vergleichen oder es kann mehrere Schwellenwerte verwenden, um zu ergreifende Maßnahmen zu bestimmen. Wenn eine Nachricht zum Beispiel an dem Volumenfiltermodul 22 empfangen wird und die aktuelle detektierte Menge dieser Art einer Nachricht unterhalb eines ersten (z. B. niedrigeren) Schwellenwerts liegt, kann das Volumenfiltermodul 22 diese Nachricht an den Stapel 16 der Netzwerkvorrichtung weiterleiten. Wenn eine Nachricht jedoch an dem Volumenfiltermodul 22 empfangen wird und die aktuelle detektierte Menge dieser Art einer Nachricht größer ist als der erste (z. B. niedrigere) Schwellenwert, aber kleiner als ein zweiter (z.B. höherer) Schwellenwert, kann das Volumenfiltermodul 22 die Nachricht blockieren, indem die Nachricht an den Protokollierungsblock 40 geschickt wird. Wenn eine Nachricht jedoch an dem Volumenfiltermodul 22 empfangen wird und die aktuelle detektierte Menge dieser Art einer Nachricht größer ist als der zweite (z. B. höhere) Schwellenwert, kann das Volumenfiltermodul 22 die Nachricht blockieren (indem die Nachricht an den Protokollierungsblock 40 geschickt wird) und kann außerdem einige weitere Aktionen ausführen, um das Netzwerk zu schützen. Wenn zum Beispiel ein zweiter oder höherer Mengenschwellenwert überschritten wird, kann der Volumenfilter 22 mit dem Benachrichtigungserzeuger 46 kommunizieren, der eine Benachrichtigung an einen Benutzer schicken kann, in der ein potenzieller Angriff auf die Netzwerkvorrichtung angezeigt wird, er kann die Netzwerkvorrichtung von der Netzwerkverbindung 12 trennen, um die Vorrichtung vor einem Angriff zu schützen, er kann eine Nachricht zu einer anderen Vorrichtung schicken, wie etwa einer Vorrichtung, welche die Nachrichten sendet, damit sich diese Vorrichtung selbst von dem Netzwerk trennt, um das Netzwerk zu schützen, er kann eine Malware- oder Viruserkennungssoftware innerhalb einer Vorrichtung initiieren usw. Natürlich kann eine beliebige Anzahl von unterschiedlichen Schwellenwerten auf der Mengenebene eingeführt werden, um zu ermöglichen oder zu veranlassen, dass der Benachrichtigungserzeuger 46 in dem Netzwerk unterschiedliche Maßnahmen ergreift.

[0031] Wie in **Fig.** 1 veranschaulicht, schließt das Robustheitsmodul 10 außerdem einen nach außen gerichteten Filterpfad ein, der von dem nach außen gerichteten Syntaxfiltermodul 30 und dem nach außen gerichteten Volumenfiltermodul 32 definiert wird. In diesem Fall agiert das nach außen gerichtete Syntaxfiltermodul 30 ähnlich wie das nach innen gerichtete Syntaxfiltermodul 20 und das nach außen gerichtete Volumenfiltermodul 32 agiert ähnlich wie das nach innen gerichtete Volumenfiltermodul 22, mit der Ausnahme, dass die Module 30 und 32 ausgehende Nachrichten bearbeiten, die von dem Kommunikationsstapel 16 empfangen wurden und über die Netzwerkverbindung 12 zu einer anderen Vorrichtung geschickt werden. Zudem, obwohl die Module 30 und 32 die gleichen Regeln anwenden können wie diejenigen, die jeweils von den Modulen 20 und 22 angewendet werden, können die Module 30 und 32 andere Regeln verwenden, um andere Filteroperationen für ausgehende Nachrichten zu ermöglichen als diejenigen, die für eingehende Nachrichten angewendet werden. Demnach arbeiten die Module 30 und 32 für ausgehende Nachrichten im Wesentlichen auf die gleiche Art und Weise zusammen, wie zuvor in Bezug auf die Module 20 und 22 beschrieben, die eingehenden Nachrichten bearbeiten, um dadurch andere Vorrichtungen an dem Netzwerk vor potenzieller Malware und Infektionen zu schützen, die sich in dem Knoten oder der Vorrichtung befinden, an dem bzw. der sich das Robustheitsmodul 10 befindet. Die ausgehenden Module 30 und 32 können demnach agieren, um die Existenz von Malware, Viren oder anderen Quellen eines Eindringens zu detektieren, die sich in der Vorrichtung befinden, die mit dem Robustheitsmittel 10 verknüpft ist und können agieren, um mit dem Benachrichtigungserzeuger 46 zu kommunizieren, damit der Benachrichtigungserzeuger eine Benachrichtigung an einen Benutzer schickt und/oder um diese Vorrichtung von dem Netzwerk zu trennen, wenn zum Beispiel der Volumenfilter 32 eine vorher festgelegte Stufe oder Menge ausgehender Nachrichten einer bestimmten Art oder Konfiguration detektiert, die von der Vorrichtung gesendet werden.

[0032] Während des Betriebs kann der Protokollierungsblock 40 agieren, um verworfene Nachrichten zu empfangen, zu analysieren und nachzuverfolgen. Insbesondere kann der Protokollierungsblock 40 verschiedene Metadaten über jede der verworfenen Nachrichten bestimmen, einschließend den zeitlichen Ablauf, den Sender/Empfänger, die Art der Nachricht, die Länge der Nachricht, den Grund dafür, dass die Nachricht an einem Syntax- oder Volumenfiltermodul verworfen wurde usw. und kann ein Protokoll für die Nachrichten erstellen. Der Block 40 kann getrennte Protokolle für eingehende und ausgehende Nachrichten, für jede Art einer Nachricht, für jeden Sender/Empfänger von Nachrichten usw. erstellen. Natürlich kann der Protokollierungsblock 40 beliebige andere Arten von Protokollen erstellen und kann diese Protokolle an eine Benutzerschnittstelle, eine Datenbankvorrichtung oder eine beliebige andere Vorrichtung auf Anfrage, periodisch, wenn ein Protokoll eine bestimmte Länge aufweist oder als Reaktion auf ein beliebiges anderes auslösendes Ereignis schicken. Ferner kann der Protokollierungsblock 40 Informationen protokollieren und/oder protokollierte Informationen über die verworfenen Nachrichten auf Grundlage von zuvor konfigurierten und fest kodierten Regeln oder auf Grundlage von Regeln aus der Regelliste 42, wenn so gewünscht, schicken. Auf diese Weise kann auch die Protokollierung verworfener Nachrichten konfiguriert werden. Der Protokollierungsblock 42 kann Protokolle über die Netzwerkverbindung 12, wenn so gewünscht, exportieren oder kann

Protokolle über eine beliebige andere Kommunikationsverbindung zu dem Robustheitsmodul 10 exportieren, wie etwa eine lokale Verbindung.

[0033] Gleichermaßen, wie zuvor angegeben, können in der konfigurierbaren Regelliste 42 Regeln für jedes bzw. jeden des nach innen gerichteten Syntaxfiltermoduls 20, des nach innen gerichteten Volumenfiltermoduls 22, des nach außen gerichteten Syntaxfiltermoduls 30, des nach außen gerichteten Volumenfiltermoduls 32, des Protokollierungsblocks 40 und des Benachrichtigungserzeugers 46 gespeichert werden. Diese Regeln können über das Regelerstellungsmodul 44 konfigurierbar sein, das mit einer anderen Anwendung (über die Netzwerkverbindung 12 oder über eine beliebige andere Kommunikationsverbindung zu dem Robustheitsmodul 10, wie etwa eine Bluetooth-Verbindung, eine drahtlose Internetverbindung, eine intermittierende festverdrahtete Verbindung von einer handgeführten Vorrichtung usw.) kommunizieren kann, um einen oder mehrere Regelsätze zu empfangen, die verwendet werden, um die Regeln aufzustellen, die in der Regelliste 42 gespeichert werden. Die andere Anwendung kann eine Regelerstellungsanwendung sein, die in einer Benutzerschnittstelle (wie etwa einer Konfigurationsschnittstelle) an der Netzwerkverbindung 12 gespeichert wird oder in einer handgeführten Vorrichtung gespeichert wird, die sich mit dem Modul 10 periodisch zum Beispiel über eine festverdrahtete oder eine drahtlose Kommunikationsverbindung usw. verbindet. Falls gewünscht, kann der Regelersteller 44 eine Kommunikationsschnittstelle zu dem Modul 10 sein, um eine Online- oder spontane Konfiguration der Regeln zu ermöglichen, die in der Regelliste 42 gespeichert sind, um dadurch zu ermöglichen, dass das Robustheitsmodul 10 angesichts neuer Konfigurationen an dem Netzwerk, sich ändernder Statistiken des Nachrichtenverkehrs usw. erneut konfiguriert wird. Jedoch kann der Regelersteller 44, falls gewünscht ein schreibgeschützter Flash-Speicher sein, der in Bezug auf die Vorrichtung intern sein kann oder der an einer Schnittstelle (z. B. ein USB-Port oder ein anderer externer Speicherport) der Vorrichtung angeschlossen sein kann, in welcher sich das Robustheitsmodul 10 befindet. Da ein derartiger Flash-Speicher während der Verwendung nicht beschrieben werden kann, können die Regeln, die in dem Flash-Speicher gespeichert sind, nicht geändert werden, wodurch das Robustheitsmodul 10 davor geschützt wird, über eine Veränderung in der Regelliste 42 infiziert zu werden. Das heißt, um die Regelliste 42 zu ändern, muss der Flash-Speicher 44 entfernt und mit neuen Regeln darin zur Verwendung in dem Robustheitsmodul 10 ersetzt werden. Während diese Konfiguration der Regelliste 42 das Robustheitsmodul 10 gegenüber einem Eindringen sicherer macht, kann dadurch auch das System nicht mehr so spontan konfiguriert werden. Natürlich kann der Regelspeicher 42, falls gewünscht, in das gleiche Modul integriert werden, wie der Regelersteller 44. In einem Fall können einige der Regeln in der Regelliste 42 in einem Flash-Speicher gespeichert und demnach nicht konfigurierbar sein, während diese Regeln Listen verwenden können, die in dem Speicher, wie etwa in der Regelliste 42, abgelegt sind, die sich während des Betriebs ändern können, um dadurch eine gewisse spontane Konfiguration des Robustheitsmoduls 10 zu ermöglichen. Lediglich beispielhalber stellt die nachfolgende Tabelle 1 eine beispielhafte Reihe von Regeln bereit, die für jeden der nach innen gerichteten und nach außen gerichteten Syntax- und Volumenfilter eines Robustheitsmoduls verwendet werden können. Tabelle 1 definiert außerdem für jede Regel, ob die Regel in dem Flash-Speicher gespeichert wird, ob die Regel konfigurierbar ist, ob die Regel eine Implementierung eines Windows Betriebssystems verwendet und ob die Regel in eingebetteten Vorrichtungen in dem Netzwerk (z. B. Steuerungen) verwendet wird. Natürlich stellt Tabelle 1 nur ein einzelnes Beispiel für eine Reihe von Regeln bereit, die in einem bestimmten Robustheitsmodul 10 verwendet werden können und beliebige andere Arten und Anzahlen von Regeln können in einem bestimmten Robustheitsmodul 10 verwendet werden.

Tabelle 1

Regelbeschreibung	**Flash-Speicher?**	**Konfigurierbar?**	**Windows?**	**Eingebettet?**
Nach innen gerichteter Syntaxfilter				
Alle Pakete verwerfen, die auf einen bestimmten Port gerichtet sind (z. B. Pakete zu UDP-Port 199 verwerfen).	JA	JA* (z. B. können neue UDP-Ports in der Liste zum Verwerfen von nach innen gerichtetem Port-Verkehr eingeschlossen werden)	JA	JA

Regelbeschreibung	**Flash-Speicher?**	**Konfigurierbar?**	**Windows?**	**Eingebettet?**
Alle Pakete verwerfen, die eine ungültige Länge aufweisen (z. B. wenn die Länge in dem IP-Header für ein TCP-Paket zu kurz ist).	JA	NEIN	NEIN	JA
Pakete mit technisch gültiger Länge, die aber nicht in die erwartete Länge für eine Steuerungsnetzwerkumgebung fallen, verwerfen (z. B. UDP-Pakete verwerfen, die oberhalb der minimalen UDP-Länge, wie durch das Protokoll spezifiziert, liegen, aber kürzer/-länger sind als das, was für einen Steuerungsverkehr erwartet wird). Diese Regel kann ferner durch einen IP-Adressbereich und einen Port definiert werden.	JA	JA	JA - Kann auf den IP-Adressbereich und den Port des Steuerungsnetzwerks begrenzt sein	JA
Nach innen gerichteter Volumenfilter				
Pakete einer spezifischen Art von einer einzigen Quelle verwerfen, nachdem innerhalb eines Zeitraums zu viele empfangen wurden (z. B. TCP SYNs).	JA	JA* (z. B. können neue Source IPs in einer separaten Liste zum Verwerfen von Port-Verkehr eingeschlossen werden)	JA	JA
Alle Pakete verwerfen, nachdem eine Obergrenze zum Verwerfen von Paketen erreicht wurde. Die Arten von	JA	JA	JA	JA
Paketen, die dieser Grenze zum Verwerfen gegengerechnet werden, können konfigurierbar sein (z. B. falsche TCP SYNs, TCP URGs).				
Pakete verwerfen, nachdem innerhalb eines bestimmten Zeitraums zu viele empfangen wurden (z. B. TCP URGs).	JA	JA* (z. B. können Grenzen für die Paketzählung für spezifische Pakettypen abgestimmt werden)	JA	JA
Grenzen für die Paketrate für UDP-Verkehr umsetzen, der erwartete Höchstwerte übersteigt. Die Grenzen für die Rate können konfigurierbar sein.	JA	JA	JA	JA
Nach außen gerichteter Syntaxfilter				
Pakete verwerfen, die zu einem Port geschickt werden würden, an dem oder durch den die Vorrichtung normalerweise nicht kommunizieren würde.	JA	JA* (z. B. können neue Ports in einer separaten Liste zum Verwerfen von nach außen gerichtetem Port-Verkehr eingeschlossen werden)	JA	JA
Pakete mit ungültiger Länge verwerfen (z. B. ist die Länge in dem IP-Header für ein TCP-Paket zu kurz).	JA	NEIN	NEIN	JA

Regelbeschreibung	**Flash-Speicher?**	**Konfigurierbar?**	**Windows?**	**Eingebettet?**
Pakete mit technisch gültiger Länge, die aber nicht in die erwartete Länge für eine Steuerungsumgebung fallen, was auf ein fehlerhaftes Verhalten an der Vorrichtung/dem System hindeutet, verwerfen (z. B. UDP-Pakete verwerfen, die oberhalb der minimalen UDP-Länge, wie durch das Protokoll spezifiziert, liegen, aber kürzer/länger sind als das, was für den Verkehr im Steuerprotokoll erwartet wird). Diese Regel kann ferner durch einen IP-Adressbereich und einen Port definiert werden.	JA	JA	JA - begrenzt auf den IP-Adressbereich und den Port des Steuerungsnetzwerks	JA
Ausgehenden Verkehr zu bekannten Teilnetz-IP-Adressbereichen des Netzwerks einschränken (z. B. Verkehr blockieren, der zu den IP-Adressen 8.8.8.8 und 8.8.4.4 geht).	JA	JA	JA	JA
Nach außen gerichteter Volumenfilter				
Ausgehende TCP SYNs verwerfen, nachdem eine bestimmte Menge in einer bestimmten Zeitspanne oder einem bestimmten Zeitraum empfangen wurde, in Abhängigkeit davon, wie viel TCP-Verkehr erwartet wird	JA	JA* (z. B. schließen konfigurierbare Parameter im Allgemeinen Grenzen für die Menge ein und ein Abgleich für spezifische Paketsignaturen kann ein-/ausgeschaltet werden)	NEIN	JA
Eine überschüssige Anzahl von Paketen verwerfen, die üblicherweise nicht verwendet werden, wie ICMP-Pings	JA	JA* (z. B. schließen konfigurierbare Parameter im Allgemeinen Grenzen für die Menge ein oder schließen neue Paketsignaturen ein, die in dem Regelsatz eingeschlossen werden können)	JA	JA
Überschüssige Anzahl von UDP-Paketen mit maximaler Länge verwerfen, welche die konfigurierbaren Grenzen übersteigen.	JA	JA	JA	JA

[0034] Lediglich beispielhalber veranschaulichen **Fig.** 2 und 3 beispielhafte Anlagennetzwerke, in denen ein Netzwerksicherheitssystem, das aus einem oder mehreren der Robustheitsmodule 10 aus **Fig.** 1 besteht, installiert und verwendet werden kann. Insbesondere veranschaulicht **Fig.** 2 eine Anlage oder ein industrielles Kommunikationssystem 10, einschließend eine Anzahl unterschiedlicher, aber miteinander verbundener Kommunikationsnetzwerke 112, 114, 116 und 118, die jeweils verschiedene Netzwerkknoten aufweisen. Das Kommunikationsnetzwerk 112 aus **Fig.** 2 kann ein Unternehmenskommunikationsnetzwerk sein, einschließend mehrere Knoten 122A-122H, die durch einen Kommunikationsbus 124 miteinander verbunden sind, der zum Beispiel ein Ethernet-Bus oder ein beliebiger anderer verdrahteter oder drahtloser bzw. ein beliebiges anderes verdrahtetes oder drahtloses Kommunikationsbus oder Netzwerk sein kann. Die Knoten 122A, 122B können zum Beispiel Computer, Server, Arbeitsplätze usw. einschließen, an denen Unternehmensanwendungen oder Programme ausgeführt werden und der Knoten 122C kann zum Beispiel eine Datenbank

sein, die Unternehmensdaten, Konfigurationsdaten für industrielle Anlagen oder beliebige andere gewünschte Daten in Bezug auf die Anlage speichert. Gleichermaßen können die Knoten 122D, 122E und 122F Gateway-Knoten sein, die das Netzwerk 112 jeweils mit den anderen Kommunikationsnetzwerken 114, 116, 118 verbinden und um netzübergreifende Kommunikationen zu ermöglichen. Ferner kann ein Knoten 122G ein Gateway-Knoten sein, der das Netzwerk 112 mit dem Internet, der Cloud oder einem anderen Weitverkehrsnetzwerk verbindet, damit das Netzwerk 112 mit entfernten Servern, Anlagen oder anderen Computern kommunizieren kann.

[0035] In diesem Beispiel sind die Netzwerke 114, 116 und 118 Steuerungsnetzwerke für Anlagen (wie etwa eine Prozessanlage oder eine industrielle Anlage), die verschiedene Knoten einschließen, die durch einen verdrahteten oder drahtlosen Kommunikationsbus oder eine verdrahtete oder drahtlose Netzwerkverbindung miteinander verbunden sind. Jedes der Anlagensteuerungsnetzwerke114, 116, 118 kann beliebige von verschiedenen Arten von Vorrichtungen an den diesbezüglichen Knoten einschließen. Zum Beispiel werden die Anlagensteuerungsnetzwerke 114 und 116 als verdrahtete Kommunikationsnetzwerke veranschaulicht, die jeweils eine oder mehrere Benutzerschnittstellenvorrichtung 130, eine Datenbank oder ein Verlaufsarchiv 132, welche(s) Konfigurationsdaten des Anlagensteuerungsnetzwerks für die Netzwerke 114 und/oder 116 speichern kann, einen oder mehrere Prozesssteuerungsknoten 134, die über einen Kommunikationsbus 136, in diesem Fall in Form eines Ethernet-Kommunikationsbusses, miteinander verbunden sind und einen oder mehrere Server- oder Prozessorknoten 138 einschließen. Die Prozesssteuerungsknoten 134 können eine oder mehrere Prozesssteuerungen einschließen, die kommunikativ mit anderen Vorrichtungen, wie etwa Eingabe-/Ausgabe- (E/A) und Feldvorrichtungen (z.B. Sensoren, Ventilen, gesteuerten Vorrichtungen usw.) über ein oder mehrere verdrahtete oder drahtlose Teilnetze 140 gekoppelt sind. Die Feldvorrichtung in den Teilnetzen 140 kann zum Beispiel die Form von Ventilen, Sensoren, Sendern oder anderen Mess- oder Steuerungsvorrichtungen annehmen, die einen Parameter oder eine Prozessvariable in der Anlage messen oder die eine physikalische Steueraktion in Bezug auf den Materialbetrieb oder den Materialfluss in der Anlage ausführen. Die Teilnetze 140 der Feldvorrichtungen können zum Beispiel ein beliebiges gewünschtes Kommunikationsprotokoll oder -paradigma für die Prozesssteuerung verwenden, wie etwa das Highway Addressable Remote Transmitter (HART®) Protokoll, das FOUNDATION® Feldbus-Protokoll, das Profibus-Protokoll, das CAN-Protokoll usw. Ferner können die Teilnetze 140 der Feldvorrichtungen als verdrahtete oder drahtlose Netzwerke implementiert werden, wie etwa WirelessHART®-Netzwerke. Die Netzwerke 114 und 116 können außerdem Gateway-Vorrichtungen an den Knoten 122D, 122E einschließen, welche die Netzwerke 114 und 116 mit dem Netzwerk 112, mit dem Internet oder anderen WANs usw. verbinden. Natürlich können diese Gateway-Vorrichtungen eine Firewall und andere Sicherheitsmerkmale oder -anwendungen bereitstellen.

[0036] Auf ähnliche Weise wird das Kommunikationsnetzwerk 118 als ein drahtloses Kommunikationsnetzwerk veranschaulicht, das ein drahtloses Kommunikationsprotokoll, wie etwa ein drahtloses Ethernet-Protokoll, das WirelessHART®-Protokoll, das drahtlose ISA100-Protokoll usw. verwenden kann. Das Kommunikationsnetzwerk 118 wird so veranschaulicht, dass es verschiedene Vorrichtungen, wie etwa Benutzerschnittstellenvorrichtungen oder - Arbeitsplätze 130, Datenbanken 132, Prozesssteuerungen 134, Server 136, Teilnetze 140 von Feldvorrichtungen, Gateway-Vorrichtungen 139 usw. einschließt. Natürlich kann sich eine beliebige Anzahl dieser und anderer Arten von Vorrichtungen an den verschiedenen Knoten der Kommunikationsnetzwerke 114, 116 und 118 befinden. Es versteht sich, dass beliebige oder alle der Netzwerkvorrichtungen in den Netzwerken 112, 114, 116, 118 einen oder mehrere computerlesbare Speicher und Prozessoren einschließen können, an denen verschiedene Softwaremodule, einschließend beliebige der Module, die mit dem Robustheitsmodul 10 aus **Fig.** 1 verknüpft sind und hierin beschrieben werden, gespeichert und ausgeführt werden können.

[0037] Zudem kann ein hierin beschriebenes Sicherheitssystem in beliebigen und allen der Netzwerke 112, 114, 116 und 118 aus **Fig.** 2 implementiert werden, um die Auswirkungen des Eindringens in diese Netzwerke, zum Beispiel in der Form von Malware oder anderen unzulässigen Anwendungen, die in verschiedenen Knoten dieser Netzwerke ausgeführt werden, zu begrenzen. Allgemein ausgedrückt, kann es für jedes der Netzwerke 112, 114, 116 und 118 oder sogar für jeden der Knoten in einem beliebigen der Netzwerke 112, 114, 116, 118 ein auf einem separaten Robustheitsmodul basierendes Sicherheitssystem geben. Andererseits kann in einigen Fällen ein einzelnes Sicherheitssystem verwendet werden, um mehrere der Netzwerke 112-118, wie etwa die Netzwerke 114 und 116 oder die Netzwerke 112 und 114 usw. abzudecken.

[0038] Als ein Beispiel, wie im Allgemeinen in den Netzwerken 114, 116 und 118 aus **Fig.** 2 veranschaulicht, schließt ein auf einem Robustheitsmodul basierendes Sicherheitssystem ein Robustheitsmodul 210 ein, das sich an der Schnittstelle (z. B. in dem Kommunikationsstapel) von jedem der Knoten dieser Netzwerke und

der Kommunikationsverbindung befindet, mit der diese Netzwerke verbunden sind. Hier können die Robustheitsmodule 210 (hierin auch als Transitverkehr-Analysemittel bezeichnet) die Form aufweisen, die zuvor als das Robustheitsmodul oder -mittel 10 aus **Fig.** 1 beschrieben wurde. Zusätzlich, obwohl **Fig.** 2 ein Robustheitsmodul an jedem Knoten von jedem Netzwerk veranschaulicht, muss es nicht notwendig sein, ein separates Robustheitsmodul in jedem Knoten eines Netzwerks, das geschützt wird, bereitzustellen. Stattdessen können für die hierin beschriebene Sicherheit ein oder mehrere Robustheitsmodule in einem Netzwerk verwendet werden, ohne dass sich zwangsläufig an jedem Knoten eines Netzwerks ein Robustheitsmodul befinden muss. Zum Beispiel kann ein Sicherheitssystem Robustheitsmodule 210 an der Netzwerkschnittstelle von eingebetteten Vorrichtungen eines Netzwerks, wie etwa Steuerungen, einschließen, ohne dass es ein Robustheitsmodul 210 an komplizierteren Vorrichtungen, wie etwa Benutzerschnittstellenvorrichtungen, aufweist. In jedem Fall können die Robustheitsmodule 210 an beliebigen gewünschten Vorrichtungen in einem Netzwerk auf eine beliebige gewünschte Art und Weise installiert werden und ein Sicherheitssystem, das diese Robustheitsmodule verwendet, ist nicht auf die spezifisch hierin beschriebenen Beispiele begrenzt. Zudem kann das Sicherheitssystem ein Konfigurations- und Benutzerschnittstellen-Supportmodul 211 einschließen, das sich in einem oder mehreren der Knoten der Netzwerke 112, 114, 116 und 118 befindet. Die Benutzerschnittstellensupport- und Konfigurationsanwendung 211 wird in einem computerlesbaren Speicher gespeichert und an einem Prozessor dieser Vorrichtungen ausgeführt, um den Benutzer zu befähigen, die Regeln in der Regelliste 42 von einem beliebigen der Robustheitsmodule 210 zu konfigurieren, kann es einem Benutzer ermöglichen, die verworfenen Verkehrsprotokolle von beliebigen oder allen Robustheitsmodulen 210 des Netzwerks, das geschützt wird, anzusehen, kann es einem Benutzer ermöglichen, zu sehen, welche Vorrichtungen oder Knoten offline genommen werden oder aktuell im Hinblick auf das Senden oder Empfangen großer Mengen von verdächtigem Nachrichtenverkehr verdächtig sind und können eine Umgebung bereitstellen, die es dem Benutzer ermöglicht, beliebige der Robustheitsmodule 210 zu konfigurieren, um eine bessere oder verstärkte Sicherheit zu gewährleisten.

[0039] Allgemein ausgedrückt, betrachtet oder analysiert jedes der Robustheitsmodule 210 eingehende und ausgehende Nachrichten gemäß den Regeln innerhalb des Moduls, um eine Weiterleitung von Nachrichten zu ermöglichen, um verdächtige Nachrichten zu blockieren und/oder um Nachrichten zu zählen und eine Mengenfilterung dafür durchzuführen. Die Robustheitsmodule 210 können unabhängig arbeiten oder sie können in einem bestimmten Netzwerk oder sogar über Netzwerke hinweg koordiniert werden, um eine koordinierte Nachrichtenfilterung bereitzustellen.

[0040] Als ein weiteres Beispiel veranschaulicht **Fig.** 3 das Kommunikationsnetzwerk 114 aus **Fig.** 2 ausführlicher. In diesem Beispiel schließt das Kommunikationsnetzwerk 114 einen verdrahteten Ethernet-Bus 200 ein, der einen oder mehrere Schalter 202 einschließen kann, die verschiedene Vorrichtungen, wie etwa Gateway-Vorrichtungen (z. B. ein Gateway mit anderen Netzwerken 226, ein Gateway mit externen Systemen 228, wie etwa mit dem Internet), eine oder mehrere Benutzerschnittstellenvorrichtungen oder -Arbeitsplätze 230, eine Konfigurationsdatenbank 232, einen Server 233 und zwei Prozesssteuerungsknoten 234A und 234B miteinander verbinden. Hier schließt der erste Prozesssteuerungsknoten 234A eine oder mehrere redundante Prozesssteuerungen 260 ein, die über Eingabe-/Ausgabe- (E/A) Karten 236 und 238 kommunikativ mit verdrahteten Feldvorrichtungen 215-422 verbunden ist/sind und über ein drahtloses Gateway 235 und den Netzwerk-Backbone 200 kommunikativ mit den drahtlosen Feldvorrichtungen 240-458 verbunden ist/sind. In diesem Fall ist das drahtlose Gateway 235 der zweite Steuerungsknoten 234B des Netzwerks 114. In einer anderen Ausführungsform kann die Steuerung 260 an dem Knoten 234A jedoch unter Verwendung eines Kommunikationsnetzwerks, das sich von dem Backbone 200 unterscheidet, kommunikativ mit dem drahtlosen Gateway 235 verbunden sein, wie etwa in dem eine andere verdrahtete oder eine drahtlose Kommunikationsverbindung bzw. ein E/A-Modul verwendet wird.

[0041] Die Steuerung 260, welche beispielsweise eine von Emerson Process Management verkaufte DeltaV™-Steuerung sein kann, kann betrieben werden, um einen oder mehrere Batch-Prozesse oder kontinuierliche Prozesse, Wartungsanwendungen, Sicherheitssystemanwendungen usw. unter Verwendung von mindestens einigen der Feldvorrichtungen 215-222 und 240-258 zu implementieren. Die Steuerung 260 kann mit den Feldvorrichtungen 215-222 und 240-258 unter Verwendung beliebiger gewünschter Hardware und Software kommunikativ verbunden werden, die zum Beispiel mit standardmäßigen 4-20 mA-Vorrichtungsprotokollen und/oder einem beliebigen intelligenten Kommunikationsprotokoll, wie etwa dem FOUNDATION® Feldbus-Protokoll, dem HART®-Protokoll, dem WirelessHART®-Protokoll usw. verknüpft sind. Die Steuerung 260 kann zusätzlich oder alternativ über die Eingabe-/Ausgabe- (E/A) Karten 236, 238 mit mindestens einigen der Feldvorrichtungen 215-222 und 240-258 über andere Arten von Verbindungen kommunikativ verbunden sein. In dem Netzwerk 114, das in **Fig.** 3 veranschaulicht wird, sind Steuerung 260, die Feldvorrichtungen 215-222 und die E/A-Karten 236, 238 verdrahtete Vorrichtungen und die Feldvorrichtungen 240-258

sind drahtlose Feldvorrichtungen. Natürlich können die verdrahteten Feldvorrichtungen 215-222 und die drahtlosen Feldvorrichtungen 240-258 (einem) beliebigen anderen gewünschten Standard(s) oder Protokollen entsprechen, wie etwa beliebigen verdrahteten oder drahtlosen Protokollen, einschließend beliebige in der Zukunft entwickelte Standards oder Protokolle.

[0042] Die Steuerung 260 aus **Fig.** 3 schließt einen Prozessor 270 ein, der eine oder mehrere Prozesssteuerungsroutinen (die in einem Speicher 272 gespeichert sind) implementiert oder überwacht, die Steuerschleifen umfassen können. Der Prozessor 270 kann mit den Feldvorrichtungen 215-222 und 240-258 und mit anderen Knoten kommunizieren, die mit dem Netzwerk-Backbone oder der - verbindung 200 kommunikativ verbunden sind, um Steuerungsaktivitäten oder andere Aktivitäten, wie etwa Wartungs-, Überwachungs- und Sicherheitssystemaktivitäten, auszuführen. Es wird vermerkt, dass beliebige der Steuerroutinen oder -module diesbezügliche Teile aufweisen können, die, falls gewünscht, von anderen Steuerungen oder anderen Vorrichtungen implementiert oder ausgeführt werden. Gleichermaßen können die Steuerroutinen oder -module, die in dem Prozesssteuerungssystem implementiert werden sollen, jede Form annehmen, einschließend Software, Firmware, Hardware usw. Steuerroutinen können in jedem gewünschten Softwareformat implementiert werden, wie etwa unter Verwendung von objektorientierter Programmierung, Leiterlogik, sequentiellen Funktionsplänen, Funktionsblockdiagrammen oder unter Verwendung einer anderen Sprache für die Softwareprogrammierung oder eines anderen Designparadigmas. Die Steuerroutinen können in jeder gewünschten Form eines Speichers gespeichert werden, wie etwa einem Random Access Memory (RAM) oder einem Read Only Memory (ROM). Gleichermaßen können die Steuerroutinen zum Beispiel in einem bzw. einer oder mehreren EPROMs, EEPROMs, anwendungsspezifischen integrierten Schaltungen (ASICs) oder beliebigen anderen Hardware- oder Firmware-Elementen fest kodiert werden. Demnach kann die Steuerung 260 konfiguriert werden, um eine Steuerstrategie oder eine Steuerroutine auf eine gewünschte Weise zu implementieren.

[0043] In einigen Ausführungsformen implementiert die Steuerung 260 eine Steuerstrategie unter der Verwendung von dem, was gemeinhin als Funktionsblöcke bezeichnet wird, wobei jeder Funktionsblock ein Objekt oder ein anderer Teil (z. B. eine Subroutine) einer gesamten Steuerroutine ist und zusammen mit anderen Funktionsblöcken arbeitet (über Kommunikationen, die Verbindungen genannt werden), um Prozesssteuerschleifen in dem Prozesssteuerungssystem zu implementieren. Steuerungsbasierte Funktionsblöcke führen üblicherweise eine einer Eingabefunktion wie diejenige, die mit einem Sender, einem Sensor oder anderen Messvorrichtungen für Prozessparameter verknüpft ist, einer Steuerfunktion, wie diejenige, die mit einer Steuerroutine verknüpft ist, die eine Steuerung mit einer proportionalen, integralen, derivativen (PID) Logik, Fuzzy Logic usw. ausführt oder einer Ausgabefunktion aus, welche den Betrieb einer Vorrichtung, wie etwa eines Ventil steuert, um in dem Prozesssteuerungssystem eine physikalische Funktion auszuführen. Natürlich existieren Mischformen und andere Arten von Funktionsblöcken. Funktionsblöcke können in der Steuerung 260 gespeichert und von dieser ausgeführt werden, was üblicherweise der Fall ist, wenn diese Funktionsblöcke für standardmäßige 4-20 mA-Vorrichtungen und einige Arten von intelligenten Feldvorrichtungen wie HART-Vorrichtungen verwendet werden oder mit diesen verknüpft sind oder sie können in den Feldvorrichtungen an sich gespeichert und von diesen implementiert werden, was bei Feldbus-Vorrichtungen der Fall sein kann. Die Steuerung 260 kann eine oder mehrere Steuerroutinen 280 umfassen, die eine oder mehrere Steuerschleifen implementieren können. Jede Steuerschleife wird üblicherweise als ein Steuermodul bezeichnet und kann durch die Ausführung von einem oder mehreren der Funktionsblöcke ausgeführt werden.

[0044] Die verdrahteten Feldvorrichtungen 215-222 können jede Art von Vorrichtungen sein, wie etwa Sensoren, Ventile, Sender, Stellungsregler usw., während die E/A-Karten 236 und 238 jede Art von E/A-Vorrichtungen sein können, die einem gewünschten Kommunikations- oder Steuerprotokoll entsprechen. In der in **Fig.** 3 veranschaulichten Ausführungsform sind die Feldvorrichtungen 215-218 standardmäßige 4-20 mA-Vorrichtungen oder HART-Vorrichtungen, die über analoge Leitungen oder eine Kombination aus analogen und digitalen Leitungen mit der E/A-Karte 226 kommunizieren, während die Feldvorrichtungen 219-222 intelligente Vorrichtungen wie FOUNDATION®-Feldbus-Feldvorrichtungen sind, die unter Verwendung eines FOUNDATION® Feldbus-Kommunikationsprotokolls über einen digitalen Bus mit der E/A-Karte 238 kommunizieren. In einigen Ausführungsformen kommunizieren jedoch zumindest einige der verdrahteten Feldvorrichtungen 215-222 und/oder zumindest einige der E/A-Karten 236, 238 unter Verwendung eines Big-Data-Netzwerks mit der Steuerung 260. In einigen Ausführungsformen können zumindest einige der verdrahteten Feldvorrichtungen 215-222 und/oder zumindest einige der E/A-Karten 236, 238 Knoten des Prozesssteuerungssystemnetzwerks 114 sein.

[0045] In der in **Fig.** 3 veranschaulichten Ausführungsform kommunizieren die drahtlosen Feldvorrichtungen 240-258 in einem Drahtlosnetzwerk 290 unter der Verwendung eines drahtlosen Protokolls, wie etwa dem WirelessHART®-Protokoll. Solche drahtlosen Feldvorrichtungen 240-258 können direkt mit einem oder mehreren anderen Knoten des Netzwerks 114 kommunizieren, die ebenso konfiguriert sind, um drahtlos zu kommunizieren (zum Beispiel unter Verwendung des drahtlosen Protokolls). Um mit einem oder mehreren anderen Knoten zu kommunizieren, die nicht konfiguriert sind, um drahtlos zu kommunizieren, können die drahtlosen Feldvorrichtungen 240-258 das drahtlose Gateway 235 verwenden, das mit dem Kommunikations-Backbone 200 oder mit einem anderen Kommunikationsnetz für die Prozesssteuerung verbunden ist. In einigen Ausführungsformen können zumindest einige der drahtlosen Feldvorrichtungen 240-258 Knoten des Prozesssteuerungssystemnetzwerks 114 sein.

[0046] Das drahtlose Gateway 235 ermöglicht eine kommunikative Kopplung zwischen den drahtlosen Vorrichtungen 240-258, den verdrahteten Vorrichtungen 215-222 und/oder anderen Knoten des Prozesssteuerungsnetzwerks 114. Das drahtlose Gateway 235 ermöglicht eine kommunikative Kopplung, in einigen Fällen durch die Verwendung des Routings, des Zwischenspeicherns und die zeitliche Steuerung von Diensten in unteren Schichten der verdrahteten und drahtlosen Protokollstapel (z. B. Adressumwandlung, Routing, Paketsegmentierung, Priorisierung usw.), während für eine geteilte Schicht bzw. Schichten der verdrahteten und drahtlosen Protokollstapel ein Tunneling-Vorgang ausgeführt wird. In anderen Fällen kann das drahtlose Gateway 235 Befehle zwischen verdrahteten und drahtlosen Protokollen umwandeln, die keine Protokollschichten teilen. Zusätzlich zu der Umwandlung von Protokollen und Befehlen kann das drahtlose Gateway 235 eine synchronisierte Taktung bereitstellen, die von Zeitschlitzen und Superframes (Sätze von Kommunikationszeitschlitzen, die zeitlich gleichmäßig beabstandet sind) eines Planungsschemas verwendet wird, das mit dem drahtlosen Protokoll verknüpft ist, das in dem Drahtlosnetzwerk 290 implementiert wird. Zudem kann das drahtlose Gateway 235 eine Netzwerkführung und administrative Funktionen für das Drahtlosnetzwerk 290 bereitstellen, wie Ressourcenmanagement, Leistungsanpassungen, die Abschwächung von Netzwerkfehlern, die Überwachung von Verkehr, Sicherheit und Ähnliches.

[0047] Ähnlich wie die verdrahteten Feldvorrichtungen 215-222 können die drahtlosen Feldvorrichtungen 240-258 des Drahtlosnetzwerks 290 in der Prozessanlage physikalische Steuerfunktionen ausführen, z. B. das Öffnen oder Schließen von Ventilen oder das Vornehmen von Messungen für Prozessparameter oder die Ausführung anderer Funktionen. Die drahtlosen Feldvorrichtungen 240-258 sind jedoch konfiguriert, um unter der Verwendung des drahtlosen Protokolls des Netzwerks 290 zu kommunizieren. Als solche sind die drahtlosen Feldvorrichtungen 240-258, das drahtlose Gateway 235 und andere drahtlose Knoten des Drahtlosnetzwerks 290 üblicherweise Erzeuger und Konsumenten von drahtlosen Kommunikationspaketen.

[0048] In einigen Szenarien kann das Drahtlosnetzwerk 290 nicht-drahtlose Vorrichtungen einschließen. Zum Beispiel kann eine Feldvorrichtung 248 aus **Fig.** 3 eine ältere 4-20 mA-Vorrichtung sein und eine Feldvorrichtung 250 kann eine herkömmliche verdrahtete HART-Vorrichtung sein. Um in dem Netzwerk 290 zu kommunizieren, können die Feldvorrichtungen 248 und 250 über einen Drahtlosadapter (WA) 252a oder 252b mit dem drahtlosen Kommunikationsnetz 290 verbunden sein. Zusätzlich können die Drahtlosadapter 252a, 252b andere Kommunikationsprotokolle unterstützen, wie etwa FOUNDATION®-Feldbus, PROFIBUS, DeviceNet usw. Zudem kann das Drahtlosnetzwerk 290 einen oder mehrere Netzwerkzugriffspunkte 255a, 255b einschließen, die getrennte physikalische Vorrichtungen in verdrahteter Kommunikation mit dem drahtlosen Gateway 235 sein oder in dem drahtlosen Gateway 235 als eine integrierte Vorrichtung bereitgestellt werden können. Das Drahtlosnetzwerk 290 kann außerdem einen oder mehrere Router 258 einschließen, um Pakete in dem drahtlosen Kommunikationsnetz 290 von einer drahtlosen Vorrichtung zu einer anderen drahtlosen Vorrichtung weiterzuleiten. Die drahtlosen Vorrichtungen 240-258 können miteinander und mit dem drahtlosen Gateway 235 über drahtlose Verbindungen des drahtlosen Kommunikationsnetzes 290, in **Fig.** 3 durch gestrichelte Linien veranschaulicht, kommunizieren.

[0049] Obwohl das Netzwerk 114 aus **Fig.** 3 lediglich eine einzelne Steuerung 260 mit einer endlichen Anzahl von Feldvorrichtungen 215-222 und 240-258 veranschaulicht, ist dies lediglich eine veranschaulichende und nicht-einschränkende Ausführungsform. Eine beliebige Anzahl von Steuerungen kann an dem Netzwerk 114 eingeschlossen sein und die Steuerung 260 kann mit einer beliebigen Anzahl von verdrahteten oder drahtlosen Feldvorrichtungen 215-222, 240-258 kommunizieren, um zum Beispiel einen Prozess in der Anlage zu steuern. Ferner kann die Prozessanlage außerdem eine beliebige Anzahl von drahtlosen Gateways 235, Routern 258, Zugriffspunkten 255 und drahtlosen Kommunikationsnetzen für die Prozesssteuerung 290 einschließen.

[0050] Allgemein ausgedrückt, kann ein Sicherheitssystem in dem Netzwerk 114 auf eine beliebige gewünschte Art und Weise unter Verwendung von einem oder mehreren Robustheitsmodulen installiert oder implementiert werden, die, wie in Bezug auf **Fig.** 1 beschrieben, konfiguriert sind. Insbesondere, wie in **Fig.** 3 veranschaulicht, schließt das Sicherheitssystem Robustheitsmodule 210 ein, die in jedem der Netzwerkknoten 226, 228, 230, 232, 233, 234A und 234B und in beliebigen der Schalter 202 oder anderen Endpunktvorrichtungen des Netzwerks 114 angeordnet sind. Obwohl in **Fig.** 3 nicht mit allen Einzelheiten gezeigt, können die Robustheitsmodule 210 in beliebigen der Unterknotenvorrichtungen, wie etwa in den E/A-Vorrichtungen 236 und 238, in einer oder mehreren der verdrahteten Feldvorrichtungen 215-222 oder in beliebigen oder allen der drahtlosen Vorrichtungen 240-258, installiert werden. In **Fig.** 3 ist jedes der Robustheitsmodule 210 in einer Unterknotenvorrichtung mit der Bezugsziffer 210a gekennzeichnet, um zu zeigen, dass es sich in einem Unterknoten eines größeren Knotens des Netzwerks 114 befindet. Wie in Bezug auf **Fig.** 1 angezeigt, analysieren die Robustheitsmodule 210 und 210a den Verkehr, der in jeden der Knoten hinein und aus diesen hinausgeht und können eine Filterung durchführen und Metadaten über den Verkehr sammeln, während eine Nachrichten- und Mengenfilterung durchgeführt werden.

[0051] In diesem beispielhaften Sicherheitssystem können die Robustheitsmodule 210 unabhängig arbeiten, können jedoch miteinander kommunizieren, um zum Beispiel gegenseitig die Trennung ihrer entsprechenden Vorrichtung von dem Netzwerk anzuweisen, wenn ihre Vorrichtung viele verdächtige Nachrichten sendet, wie durch einen Mengenfilter ermittelt oder um einander oder einem Benutzerschnittstellenmodul 211 (in den Benutzerschnittstellenvorrichtungen 230 veranschaulicht) Protokolle für verworfene Nachrichten bereitzustellen. Ferner kann ein Benutzer ein Benutzerschnittstellenmodul 211 verwenden, um eines oder mehrere der Robustheitsmodule 210 zu konfigurieren und ein Benutzer benötigt möglicherweise eine passende Sicherheits-ID oder Sicherheitsberechtigung, um dies zu tun. Natürlich kann das Benutzerschnittstellenmodul 211 über eine oder mehrere Netzwerkverbindungen 200 kommunizieren und das Benutzerschnittstellenmodul 211 kann in einer beliebigen der anderen Computervorrichtungen an dem Netzwerk 114, wie etwa in der Konfigurationsdatenbank 232, den Gateway-Vorrichtungen 226, 228, den Schaltern 202 usw. an dem Netzwerk installiert werden. Zusätzlich können Kommunikationen (wie etwa Benachrichtigungen und Protokolle über das Verwerfen) von den Teilnetzvorrichtungen, wie etwa den Feldvorrichtungen 215-222, E/A-Vorrichtungen 236, 238 und drahtlosen Feldvorrichtungen 240-258 zu einer primären Netzwerkknotenvorrichtung, wie etwa der Steuerung 260 oder der Gateway-Vorrichtung 235, gesendet werden und diese Vorrichtungen können dann diese Kommunikationen an das Benutzerschnittstellenmodul 211 oder andere Robustheitsmodule 210 weiterleiten. Ferner, wie in **Fig.** 3 veranschaulicht, schließt die Konfigurationsdatenbank 232 ein Konfigurationsänderungsmodul 370 ein, das Konfigurationsänderungen in dem Netzwerk detektieren kann und das Regelsätze für das Robustheitsmodul auf Grundlage dieser Konfigurationsänderungen auf eine beliebige gewünschte Art und Weise an die Robustheitsmodule 210 kommunizieren kann. Wie in mindestens einigen der Knoten aus **Fig.** 3 veranschaulicht, schließt jede der Knotenvorrichtungen einen Prozessor 309 ein, der ein Mikroprozessor, eine ASIC oder ein anderer Prozessor sein kann, der die verschiedenen Robustheitsmodule 210 implementiert und ausführt und schließt einen computerlesbaren Speicher 311 ein, der diese Module zur Ausführung an dem Prozessor 309 speichert.

[0052] Ganz allgemein spiegeln die Regeln für die Nachrichtenanalyse, die in dem Regelspeicher 42 der Robustheitsmodule 210 gespeichert sind, das erwartete oder normale Verhalten des Nachrichtenverkehrs wider, der in die Knoten des Netzwerks 114 hinein- und aus diesen hinausgeht. Insbesondere können die Regeln, die in den Regeldatenbanken 42 gespeichert sind, generiert werden, indem Metadaten über Nachrichten oder den Verkehr innerhalb eines bestimmten Zeitraums von den Knoten des Netzwerks 114 gesammelt und analysiert werden, wie wenn das Netzwerk seit längerem funktioniert, jedoch direkt nachdem es eingerichtet wurde, wenn eine relative Sicherheit dafür besteht, dass das Netzwerk nicht gefährdet ist. Während dieser Zeit spiegeln die generierten oder gesammelten Daten über den Nachrichtenverkehr den „normalen“ oder „erwarteten“ Betrieb des Netzwerks im statistischen Sinne wider. Aus den Daten über den Nachrichtenverkehr, die während dieser Zeit gesammelt werden, können verschiedene Parameter oder Statistiken für Verkehrsmuster gesammelt oder generiert werden und diese Daten können in einer Verkehrsmusterdatenbank zur Verwendung bei der Erstellung von einem oder mehreren Regelsätzen für die verschiedenen Robustheitsmodule 210 gespeichert werden. Die gesammelten oder generierten und in der Datenbank gespeicherten Verkehrsmusterparameter können zum Beispiel statistische Messungen des Verkehrs an einem bestimmten Knoten oder Gruppen von Knoten in einer beliebigen Granularität einschließen. Das heißt, dass die gespeicherten Verkehrsmusterparameter eine statistische Messung von Daten (z. B. Mittelwert, Standardabweichung, Durchschnitt, Median, Anzahl usw.) anzeigen können, die für eine beliebige Art von Daten, einen Zeitrahmen, Knoten oder Gruppenknoten, eingehend oder ausgehend, Sender/Empfänger, Länge usw. gruppiert oder durchgeführt wurde und sie können in einer beliebigen gewünschten Hierarchie gespeichert werden, wie etwa einer Hierarchie, welche die Konfigurationshierarchie des Netzwerks wider-

spiegelt. Die Verkehrsmusterparameter können außerdem Bereiche oder Grenzen für beliebige Arten oder Gruppen von Kommunikationen einschließen, die in einen Knoten oder eine Gruppe von Knoten hinein- oder aus diesen hinausgehen, wobei diese, wenn sie überschritten werden, einen Schwellenwert für die Mengenfilterung, eine Warnung, eine Trennung von dem Netzwerk usw. widerspiegeln oder auslösen. Diese Bereiche oder Grenzen können absolute Grenzen sein, zum Beispiel in der Form einer festgelegten Anzahl oder sie können auf Grundlage von oder in Bezug auf andere(n) statistische(n) Messungen relative Grenzen sein, wie etwa das Dreifache eines durchschnittlichen Werts, zählend zu der ersten oder zweiten Standardabweichung, eine vorher festgelegte Menge oberhalb oder unterhalb eines Medians oder Mittelwerts usw.

[0053] Es versteht sich, dass die Regeln innerhalb der Regeldatenbanken 42 aufgestellt und verwendet werden, um die Art und Weise zu definieren, auf welche die aktuellen oder gesammelten Nachrichten analysiert werden sollen, um Anomalien oder Intrusionen in dem Netzwerk festzustellen. Insbesondere wird mit den Regeln in der Regeldatenbank 42 die Art und Weise spezifiziert, auf welche der gesammelte Nachrichtenverkehr analysiert werden soll, zum Beispiel durch einen Vergleich der gesammelten Metadaten oder von Statistiken über die gesammelten Nachrichten mit Verkehrsmusterdaten und/oder unter Verwendung von Grenzen oder Bereichen für Verkehrsmuster. Ganz allgemein werden in den Filtermodulen 20, 22, 30, 32 aus **Fig.** 1 die Regeln implementiert, die in der Regeldatenbank 42 gespeichert sind, um die gesammelten Nachrichtendaten oder Metadaten mit bekannten, gewünschten oder erwarteten Verkehrsmusterparametern zu vergleichen.

[0054] Gleichermaßen, wie in **Fig.** 1 angezeigt, kann das Robustheitsmodul 10 einen Benachrichtigungserzeuger 46 einschließen, der auf Grundlage der Ergebnisse der Analysen, die von den Modulen 20, 22, 30 und 32 durchgeführt wurden, eine(n) oder mehrere Benachrichtigungen, Alarme oder Nachrichten generieren kann. Die Benachrichtigungen, Alarme oder Nachrichten, die von dem Benachrichtigungserzeuger 46 erzeugt werden, können über die Netzwerkverbindung oder über eine beliebige andere Kommunikationsverbindung, die für diesen Zweck bereitgestellt oder dafür verwendet wird, zu gewünschtem Personal, wie etwa Bedienern, Sicherheitspersonal, IT-Personal usw. geschickt werden. Als ein Beispiel können Benachrichtigungen, Alarme oder Nachrichten zu dem E-Mail-Account einer bestimmten Person, zu einer Bedien- oder Sicherheitsschnittstelle, die außerdem andere Daten über die Anlage veranschaulicht, geschickt werden, sie können als ein Telefonanruf oder eine Textnachricht geschickt werden, die über private oder öffentliche Netzwerke einer bestimmten Person oder Gruppe von Personen, auf einer beliebigen gewünschten Vorrichtung, wie etwa einer mobilen Vorrichtung usw., zugestellt wird. Gleichermaßen können diese Benachrichtigungen, Alarme oder Nachrichten Alarme oder Mitteilungen auf handgeführten Vorrichtungen, wie etwa Telefonen, Uhren, tragbaren Vorrichtungen, Laptops, Tablets usw. einer bestimmten Person auslösen, die für die Antwort auf und die Untersuchung von mögliche(n) Intrusionen in ein Netzwerk verantwortlich ist. In einigen Fällen kann der Alarm- oder Benachrichtigungserzeuger 46 agieren, um den Zugriff auf einen infizierten oder möglicherweise infizierten Knoten einzuschränken, kann einen Knoten abschalten oder kann in sehr kritischen Situationen das Kommunikationsnetz selbst abschalten oder von anderen Netzwerken isolieren, um Schäden zu begrenzen, die der Anlage oder einem Teilsystem in der Anlage durch das Eindringen zugefügt werden. Natürlich kann der Benachrichtigungserzeuger 46 Software oder Logik einschließen, die mit anderen Vorrichtungen in dem Netzwerk kommunizieren kann, um derartige automatische Operationen auszuführen. In einigen Fällen kann der Benachrichtigungserzeuger 46 einen Benutzer, zum Beispiel über das Benutzerschnittstellenmodul 211, zur Autorisierung auffordern, bevor derartige automatische Aktionen in dem Anlagennetzwerk ausgeführt werden, er kann jedoch in anderen Fällen die Aktionen in dem Netzwerk ausführen, bevor er einen Benutzer über ein Eindringen oder ein potenzielles Eindringen informiert oder zeitgleich damit. Zudem kann der Benachrichtigungserzeuger 46, wenn automatische Aktionen ausgeführt werden, mit dem infizierten oder möglicherweise infizierten Knoten kommunizieren, um Kommunikationen von (hinein und/oder hinaus) diesem Knoten einzuschränken, zum Beispiel um bestimmte Arten von Nachrichten von diesem Knoten einzuschränken oder zu stoppen, um den Betrieb bestimmter Anwendungen an diesem Knoten zu stoppen oder einzuschränken (die den ungewöhnlichen Nachrichtenverkehr generieren können), um Kommunikationen über bestimmte Ports einer Vorrichtung zu stoppen oder einzuschränken usw. Demnach kann der Benachrichtigungserzeuger 46 von einem Robustheitsmodul 10 oder 210 die Regeln des Regelspeichers 42 eines anderen Robustheitsmoduls ändern oder modifizieren, um dazu beizutragen, das letztgenannte Robustheitsmodul daran zu hindern, die verdächtigen Nachrichten über die ursprüngliche Verbindung zu senden. Stattdessen oder zusätzlich kann der Benachrichtigungserzeuger 46 mit anderen Knoten, wie etwa Gateway-Knoten, die mit anderen Netzwerken verbunden sind, kommunizieren, um Nachrichten zwischen dem Netzwerk und anderen Netzwerken einzuschränken oder zu stoppen. Diese Maßnahme kann es ermöglichen, dass die kritischen Operationen (wie etwa Steueroperationen) an dem Netzwerk stattfinden, während das Netzwerk von äußeren Quellen getrennt wird, um den ungewöhnlichen Nachrichtenverkehr zumindest zeitweise daran zu hindern, das Netzwerk zu verlassen oder in dieses hineinzugehen, wodurch

Datendiebstahl eingeschränkt werden kann, der Virus innerhalb des Netzwerks daran gehindert werden kann, andere Netzwerke zu infizieren, ein weiteres Eindringen in das Netzwerk über den infizierten Knoten gestoppt werden kann usw. Zum Beispiel kann der Benachrichtigungserzeuger 46 alle Kommunikationen zwischen externen Unternehmenssystemen und dem betroffenen industriellen Steuerungssystemnetzwerk unterbrechen, bis die Anomalie vor Ort von Sicherheitspersonal untersucht werden konnte. Natürlich kann der Benachrichtigungserzeuger 46 mit anderen Systemen, wie etwa Sicherheitssystemen, verknüpft (kommunikativ verbunden) sein, um diese Funktionen auszuführen.

[0055] Die Regeldatenbank 42 kann beliebige gewünschte Regelsätze speichern, die von einem oder mehreren von Sicherheitspersonal, Konfigurationspersonal, Benutzern, Bedienern usw. erstellt oder generiert werden, die Analysen definieren, die für den Nachrichtenverkehr oder Nachrichtenmetadaten ausgeführt werden sollen, die von dem Kommunikationsnetzwerkknoten oder von der Kommunikationsverbindung empfangen wurden, um zu bestimmen, ob in dem Nachrichtenverkehr oder den Verkehrsmustern eine Anomalie vorliegt und demnach, ob eine Benachrichtigung oder ein Alarm generiert werden oder eine andere Filterung stattfinden soll. Die Regeln, die von den Modulen 20, 22, 30 und 32 angewendet werden, können demnach agieren, um die Nachrichtendaten, die von einem Knoten gesammelt wurden, mit dem standardmäßigen oder Ausgangssatz von Daten für den Knoten zu vergleichen, um zu bestimmen, ob es dazwischen erhebliche Unterschiede gibt, wie durch andere Verkehrsmusterparameter definiert, wie etwa eine Grenze oder Differenzvariable usw.

[0056] Es versteht sich, dass beliebige gewünschte Arten von Daten für die Nachrichten an den Robustheitsmodulen 10 und 210 erhalten und analysiert werden können und dass die Regeln in der Regeldatenbank 42 aufgestellt werden können, um die Daten auf eine beliebige gewünschte Art und Weise zu analysieren. Zum Beispiel können die Nachrichtendaten Folgendes einschließen: allgemeine Informationen über die Nachricht an sich, z. B. Art der Nutzdaten, Länge, Quellen (wie etwa konfigurierte gegenüber nicht konfigurierten Knoten, Ursprungsanschlüsse usw.), Adressen (wie etwa Quell- und Zieladressen und Ports), Umfang (wie etwa Unicast, Multicast, Broadcast), Art der Nutzdaten (wie etwa TCP, UDP, Sonstige) und den zeitlichen Ablauf (wie etwa Tageszeit, relative Zeit, Häufigkeit der Versuche usw.); Kommunikationsinformationen, z. B. Nachrichtenzeiteinteilung (wie etwa Häufigkeiten, Tageszeiten, Sequenzfehler usw.), Sicherheitsfehler (wie etwa eine fehlgeschlagene Integrität, Authentifizierung oder Entschlüsselung), Nachrichteninhalt (wie etwa Größe, Formatfehler usw.); und zweifelhafte Informationen, z. B. Informationen über die Ratenbegrenzung (wie etwa Zustand, Verfahren, Rate der Begrenzung usw.) und Verbindungsversuche (wie etwa außer der Reihe, deformiert, Aufräumen usw.). Natürlich können beliebige andere Arten von Nachrichtendaten oder Metadaten gewonnen und ebenso oder stattdessen in den Regeln 42 verwendet werden und es versteht sich, dass die hierin bereitgestellte Liste nicht umfassend ist.

[0057] Zudem können Nachrichtendaten auf Grundlage von anderen Faktoren oder Parametern in dem Netzwerk oder in Knoten gesammelt und gespeichert werden, wie etwa den Rollen der sendenden oder empfangenden Knoten (z. B. ob diese Knoten Arbeitsplätze, Server, Gateways, Steuerungen, E/A-Server, Remote Terminal Units (RTUs) usw. sind). Demnach versteht es sich, dass Nachrichten- und Verkehrsmetadaten auf oder für verschiedene(n) unterschiedliche(n) hierarchische(n) Ebenen des Netzwerks erstellt werden können, wie etwa an einer Vorrichtung oder Knotenbasis, einer Vorrichtung oder Knotenrollenbasis, einer Nachrichtenbasis usw. oder in Bezug auf eine andere hierarchische Ebene des Netzwerks. Ferner können die Konfigurationsinformationen des Steuerungs- oder Kommunikationsnetzwerks verwendet werden, um Regeln für die Analyse von Nachrichtenmetadaten anfangs zu erstellen oder zu modifizieren oder um die Analyse der Nachrichtenmetadaten zu organisieren. Ganz allgemein schließen die Konfigurationsinformationen für das Netzwerk Informationen hinsichtlich der Anzahl von Anwendungen, Modulen, Steuerroutinen usw. an jedem der Knoten (Vorrichtungen) und die Art und Weise auf die diese verschiedenen logischen Elemente, Software-Elemente und Hardware-Elemente miteinander kommunizieren ein, einschließend Kommunikationspaare (Sender-/Empfänger-Paare), Kommunikationszeiteinteilung, Frequenzen, Arten von Nachrichten, Steuerungssystemrolle oder Vorrichtungsart usw. Diese Konfigurationsinformationen können verwendet werden, um die Regeln zu erstellen oder zu modifizieren, die verwendet werden, um die Nachrichten an einem beliebigen der Knoten zu analysieren. Das heißt, dass die Konfigurationsinformationen, einschließend die Konfigurationshierarchieinformationen (z. B. welche Vorrichtungen und Module mit welchen anderen Modulen und Vorrichtungen in dem Netzwerk im Zusammenhang stehen), verwendet werden können, um Parameter von Regeln zu Analyse von Nachrichten zu erstellen, zu modifizieren oder einzutragen. Als ein Beispiel können die Konfigurationsinformationen verwendet werden, um zum Beispiel eine Teilmenge (d. h. ein Profil) der generalisierten Regeln zur Analyse von Nachrichten auszuwählen. Die Konfigurationsinformationen können außerdem verwendet werden, um spezifische Werte in einem oder mehreren Parametern mit generalisierten Regeln einzusetzen (z. B. können die Konfigurationsinformationen dort, wo eine Regel einen

Platzhalter für <Teilnehmer> aufweist, verwendet werden, um die Adresse und Portinformationen für die spezifischen Teilnehmer auszufüllen, die in der Konfiguration aufgelistet werden). Auf diese Weise können die effektiven logischen Regeln auf Grundlage der Konfiguration des Steuerungssystems einer Vorrichtung oder eines Knotens aus einem größeren Satz allgemeiner Regeln auf eine Teilmenge spezifischer Regeln zugeschnitten werden.

[0058] Ferner, wie in **Fig.** 2 und 3 veranschaulicht, kann das Sicherheitssystem ein Netzwerkkonfigurationsänderungsmodul 370 einschließen, das zum Beispiel in einer Netzwerkkonfigurationsdatenbank oder Servervorrichtung 122C oder 232 gespeichert werden kann. Ganz allgemein agiert das Konfigurationsänderungsmodul 370, um Änderungen in der Netzwerkkonfiguration für das Kommunikationsnetzwerk zu detektieren und schickt dann diese Änderungen und/oder Mitteilungen über diese Änderungen zum Beispiel über die Netzwerkverbindung an das Benutzerschnittstellenmodul 211. Wie hierin verwendet, kann eine Konfigurationsänderung eine beliebige Änderung einschließen, die hinsichtlich des Betriebs einer Vorrichtung oder einer Reihe von Vorrichtungen an dem Netzwerk vorgenommen wird, einschließend das Hinzufügen neuer Vorrichtungen, Anwendungen, Module usw.; das Entfernen beliebiger Vorrichtungen, Anwendungen, Module usw.; und die Änderungen von Parametern, Einstellungen oder anderen Konfigurationen (einschließend die Änderung von Hardware-, Software- oder Firmware-Einstellungen) in einer bzw. einem Vorrichtung, Anwendung, Modul usw., einschließend die Änderung von Einstellungen für die Kommunikations- und Prozesssteuerung, wie etwa zum Beispiel die Änderung einer Rezeptur, die zum Beispiel in einem Batch-Prozess usw. verwendet wird. In diesem Fall detektiert das Netzwerkkommunikationsänderungsmodul 370, immer wenn ein Konfigurationstechniker oder ein anderer Benutzer die Netzwerkkonfiguration ändert, zum Beispiel indem neue Anwendungen oder Module zu dem Netzwerk hinzugefügt werden, die Art und Weise geändert wird, auf die Anwendungen oder Module in dem Netzwerk miteinander kommunizieren usw., eine derartige Änderung und schickt eine Benachrichtigung an das Benutzerschnittstellenmodul 211, womit es den Benutzer über die Änderung hinsichtlich der Netzwerkkonfiguration informiert. Natürlich kann sich das Konfigurationsmodul 370, obwohl das Änderungsmodul 370 so veranschaulicht wird, dass es sich in der Konfigurationsdatenbank (z. B. der Datenbank 232 aus **Fig.** 3) befindet, in einer anderen Vorrichtung bzw. einem Computer (wie etwa einer Benutzerschnittstellenvorrichtung oder einem Server) befinden, die bzw. der Zugriff auf eine Konfigurationsanwendung (welche die Konfiguration des Netzwerks ändert oder einem Benutzer ermöglicht, diese zu ändern) hat oder eine solche implementiert oder die bzw. der anderweitig über Konfigurationsänderungen benachrichtigt wird und kann auf eine beliebige gewünschte Art und Weise agieren, um Änderungen der Netzwerkkonfiguration zu detektieren.

[0059] In jedem Fall kann das Änderungsdetektionsmodul 370, immer wenn eine Änderung hinsichtlich der Konfiguration des Netzwerks vorgenommen wird (z. B. Ausführen der Hinzufügung, Streichung oder Änderung von Kommunikationsaspekten von Software, Funktionsblöcken, Modulen usw. in beliebigen der Vorrichtungen an dem Netzwerk oder die mit dem Netzwerk verknüpft sind), eine Mitteilung an das Benutzerschnittstellenmodul 211 schicken, um den Benutzer darüber zu informieren, dass Änderungen oder mögliche Änderungen hinsichtlich der Netzwerkverkehrsmuster oder -spezifika zu erwarten sind. Diese Mitteilung kann es dem Benutzer ermöglichen, neue Regeln zu erstellen oder Regeln zu ändern, die bereits in einem oder mehreren der Robustheitsmodule 210 vorhanden sind, um dadurch die Robustheitsmodule 210 angesichts der neuen Netzwerkkonfiguration besser zu konfigurieren.

[0060] Demnach versteht es sich, dass durch eine Änderung der Netzwerkkonfiguration der Nachrichtenfluss im Netzwerk geändert werden kann, zum Beispiel indem Netzwerknachrichten bestimmter Arten vermehrt oder verringert werden, bestimmte Arten von Netzwerkkommunikationen geändert werden (z. B. durch die Änderung der Eigenschaften oder Mengen bestimmter Arten von Kommunikationen zwischen verschiedenen Vorrichtungen an dem Netzwerk oder zwischen Anwendungen, die in den verschiedenen Vorrichtung an den Knoten des Netzwerks ausgeführt werden). Unter gewissen Umständen kann es wünschenswert sein, Regeln in der Regeldatenbank 42 von einem oder mehreren Robustheitsmodulen 210 als ein Ergebnis der neuen Konfiguration zu ändern, hinzuzufügen oder zu löschen, um zum Beispiel die Regeln auf die neue Konfiguration zuzuschneiden, wie etwa durch die Implementierung eines Profil-Plugins innerhalb von einer oder mehreren Regeln der Regeldatenbank, um Parameter der neuen Konfiguration zuzuordnen oder widerzuspiegeln. Zum Beispiel können von der neuen Konfiguration neue Arten von Kommunikationen hinzugefügt werden und eine Regel kann auf Grundlage der neuen Kommunikation mit einem Profil-Plug-in aktualisiert werden und diese Regel kann dann verwendet werden, um die Nachrichten zu analysieren, die mit diesen neuen Arten von Kommunikationen verknüpft sind.

[0061] Zudem, obwohl das hierin beschriebene Sicherheitssystem so veranschaulicht wird, dass es separate Syntax- und Volumenfilter aufweist, kann ein einzelner Filter die Funktionen ausführen, die für jeden dieser

unterschiedlichen Filter beschrieben werden. Zum Beispiel kann ein einzelnes Filtermodul an einem Prozessor einer Netzwerkvorrichtung ausgeführt werden, um die logischen Regeln zu verwenden, die in dem Regelspeicher der Vorrichtung gespeichert sind, um Nachrichten mit einem oder mehreren ersten Sätzen von Nachrichteneigenschaften weiterzuleiten, um Nachrichten mit einem oder mehreren zweiten Sätzen von Nachrichteneigenschaften zu stoppen und um Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften zu zählen und kann ferner agieren, um die Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften auf Grundlage der Zählungen, die mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften verknüpft sind, weiterzuleiten oder zu stoppen.

[0062] Obwohl die hierin beschriebenen Sicherheitsmethoden so beschrieben wurden, dass sie in Verbindung mit vernetzten Prozesssteuerungsvorrichtungen und -systemen unter Verwendung von Ethernet und verschiedenen bekannten Prozesssteuerungsprotokollen, wie etwa Feldbus, HART und standardmäßigen 4-20 mA-Protokollen, verwendet werden, können die hierin beschriebenen Sicherheitsmethoden natürlich in einer beliebigen Art einer Steuervorrichtung unter Verwendung eines beliebigen anderen Kommunikationsprotokolls für die Prozesssteuerung oder einer beliebigen anderen Programmierungsumgebung implementiert werden und können mit beliebigen anderen Arten von Vorrichtungen, Funktionsblöcken oder Steuerungen verwendet werden. Obwohl die hierin beschriebenen Sicherheitsmerkmale vorzugsweise in Software implementiert werden, können sie auch in Hardware, Firmware usw. implementiert werden und können von einem beliebigen anderen Prozessor ausgeführt werden, der mit einer Computervorrichtung verknüpft ist. Demnach können die hierin beschriebenen Verfahren und Routinen und Systeme in einer standardmäßigen Mehrzweck-CPU oder in speziell konzipierter Hardware oder Firmware, wie etwa zum Beispiel ASICs, falls gewünscht, implementiert werden. Bei einer Implementierung in Software kann die Software in einem computerlesbaren Speicher, wie etwa auf einer Magnetscheibe, einer Laserdisc, einer optischen Scheibe oder einem anderen Speichermedium, in einem RAM oder ROM eines Computers oder Prozessors usw. gespeichert werden. Gleichermaßen kann diese Software einem Benutzer oder einem Prozesssteuerungssystem über eine bekannte oder gewünschte Liefermethode geliefert, einschließend zum Beispiel auf einer computerlesbaren Scheibe oder einem anderen transportierbaren Computerspeichermechanismus oder moduliert über einen Kommunikationskanal, wie etwa eine Telefonleitung, das Internet usw.

[0063] Zudem, obwohl die vorliegende Erfindung in Bezug auf spezifische Beispiele beschrieben wurde, die lediglich der Veranschaulichung dienen und die Erfindung nicht einschränken sollen, wird es für einen gewöhnlichen Fachmann deutlich, dass an den offenbarten Ausführungsformen Veränderungen, Hinzufügungen oder Streichungen vorgenommen werden können, ohne dass von dem Geist und dem Umfang der Erfindung abgewichen wird.

Patentansprüche

1. Sicherheitssystem zur Verwendung in einem Kommunikationsnetzwerk, das eine Vielzahl von Netzwerkknoten aufweist, die kommunikativ über eine Kommunikationsverbindung gekoppelt sind, umfassend:
eine oder mehrere Nachrichtenmodulschnittstellen, wobei jede der Nachrichtenmodulschnittstellen an einem Prozessor an einem der Netzwerkknoten ausgeführt wird, um Nachrichtenverkehr an dem Netzwerkknoten zu detektieren und um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen;
einen Regelspeicher, der eine oder mehrere logische Regeln speichert; und
eine oder mehrere Filtereinheiten, die in einem Prozessor gespeichert und ausgeführt werden und mit dem Regelspeicher gekoppelt sind, wobei jede der Filtereinheiten Folgendes einschließt:
ein erstes Filtermodul und
ein zweites Filtermodul,
wobei das erste Filtermodul an dem Prozessor ausgeführt wird und eine oder mehrere logische Regeln, die in dem Regelspeicher gespeichert sind, auf Grundlage der Informationen über die Nachrichteneigenschaft zum Weiterleiten der Nachricht, zum Stoppen der Nachricht oder zum Weiterleiten der Nachricht an das zweite Filtermodul anwendet;
wobei das zweite Filtermodul die Anzahl der Nachrichten zählt, die einen bestimmten Satz von Nachrichteneigenschaften aufweisen, um eine Nachrichtenzählung zu bestimmen und auf Grundlage der Nachrichtenzählung die Nachricht weiterleitet oder die Nachricht stoppt, die den bestimmten Satz von Nachrichteneigenschaften aufweist
wobei die Nachrichtenzählung eine bestimmte Anzahl von Nachrichten mit dem bestimmten Satz von Nachrichteneigenschaften, der innerhalb eines bestimmten Zeitraums empfangen wird, umfasst.

2. Sicherheitssystem nach Anspruch 1,
wobei der Regelspeicher ein Read-Only Memory ist; und/oder
wobei der Regelspeicher ein Lese-/Schreibspeicher ist.

3. Sicherheitssystem nach einem der vorhergehenden Ansprüche, insbesondere nach Anspruch 1, wobei der Regelspeicher einen ersten Teil einschließt, der ein Read-Only Memory ist und einen zweiten Teil einschließt, der ein Lese-/Schreibspeicher ist.

4. Sicherheitssystem nach einem der vorhergehenden Ansprüche, insbesondere nach Anspruch 1, wobei der Regelspeicher ein Flash-Speicher ist.

5. Sicherheitssystem nach einem der vorhergehenden Ansprüche, insbesondere nach Anspruch 4, wobei der Regelspeicher ein entfernbarer Flash-Speicher ist.

6. Sicherheitssystem nach einem der vorhergehenden Ansprüche, insbesondere nach Anspruch 1, ferner einschließend ein Protokollierungsmodul, das mit den ersten oder den zweiten Filtermodulen gekoppelt ist und an dem Prozessor ausgeführt wird, um Informationen im Hinblick auf eine oder mehrere gestoppte Nachrichten zu empfangen und um Informationen im Hinblick auf die einen oder mehreren gestoppten Nachrichten zu speichern.

7. Sicherheitssystem nach Anspruch 6, wobei das Protokollierungsmodul ferner eine Kommunikationsschnittstelle einschließt, die ein oder mehrere Protokolle gestoppter Nachrichten zu einem Benutzer schickt; und/oder wobei das Protokollierungsmodul Metadaten im Hinblick auf die gestoppten Nachrichten speichert.

8. Sicherheitssystem nach einem der vorhergehenden Ansprüche, insbesondere nach Anspruch 1, ferner einschließend ein Benachrichtigungserzeugungsmodul, das mit dem zweiten Filtermodul gekoppelt ist, wobei das Benachrichtigungserzeugungsmodul an dem Prozessor ausgeführt wird, um eine Benachrichtigung an einen Benutzer zu schicken, wenn die Nachrichtenzählung eine vorher festgelegte Stufe erreicht; und/oder wobei das Benachrichtigungserzeugungsmodul an dem Prozessor ausgeführt wird, um eine Vorrichtung von dem Kommunikationsnetzwerk zu trennen, wenn die Nachrichtenzählung eine vorher festgelegte Stufe erreicht.

9. Sicherheitssystem nach einem der vorhergehenden Ansprüche, insbesondere nach Anspruch 1, wobei die eine oder mehrere Filtereinheiten eine erste Filtereinheit, die Nachrichten empfängt und analysiert, die von der Kommunikationsverbindung in den Netzwerkknoten gelangen und eine zweite Filtereinheit einschließen, die Nachrichten empfängt und analysiert, die in dem Netzwerkknoten erzeugt und über die Kommunikationsverbindung zu einem anderen Netzwerkknoten geschickt werden.

10. Verfahren zum Sichern des Nachrichtenverkehrs in einem Kommunikationsnetzwerk, umfassend:
Empfangen einer Reihe von Nachrichten an einer Vorrichtung, die mit dem Kommunikationsnetzwerk verbunden ist;
Analysieren, über einen Prozessor an der Vorrichtung, jeder der Nachrichten, um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen; und
Filtern von jeder der Nachrichten, über den Prozessor an der Vorrichtung, auf Grundlage einer Reihe von logischen Regeln, die an der Vorrichtung gespeichert sind, wobei das Filtern das Weiterleiten von Nachrichten mit einem oder mehreren ersten Sätzen von Nachrichteneigenschaften, das Stoppen von Nachrichten mit einem oder mehreren zweiten Sätzen von Nachrichteneigenschaften und das Zählen von Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften einschließt und ferner das Weiterleiten oder Stoppen der Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften auf Grundlage von Zählungen einschließt, die mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften verknüpft sind;
wobei das Zählen von Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften das Zählen der Anzahl von Nachrichten einschließt, bei denen einer der dritten Sätze von Nachrichteneigenschaften innerhalb eines bestimmten Zeitraums empfangen wurde; und/oder
wobei das Zählen von Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften das Behalten einer Zählung der Anzahl von Nachrichten von jedem der dritten Sätze von Nachrichteneigenschaften einschließt, der innerhalb eines bestimmten Zeitraums empfangen wurde; und/oder
wobei das Zählen von Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften das Behalten einer Zählung der Anzahl von Nachrichten von jedem der dritten Sätze von Nachrichteneigenschaften einschließt.

11. Verfahren nach Anspruch 10, ferner einschließend das Speichern der logischen Regeln in einem Read-Only Memory in der Vorrichtung; und/oder
ferner einschließend das Speichern der logischen Regeln in einem Lese-/Schreibspeicher in der Vorrichtung; und/oder
ferner einschließend das Speichern eines ersten Teils der logischen Regeln in einem Read-Only Memory und das Speichern eines zweiten Teils der logischen Regeln in einem Lese-/Schreibspeicher; und/oder
ferner einschließend das Speichern von mindestens einem Teil der logischen Regeln in einem Flash-Speicher an der Vorrichtung.

12. Verfahren nach Anspruch 10, ferner einschließend das Protokollieren von Informationen im Hinblick auf eine oder mehrere gestoppte Nachrichten, um eine oder mehrere Protokolldateien zu erzeugen.

13. Verfahren nach Anspruch 12, ferner einschließend das Kommunizieren der einen oder mehreren Protokolldateien mit den Protokollierungsinformationen über das Kommunikationsnetzwerk an einen Benutzer; und/oder wobei das Protokollieren von Informationen das Speichern von Metadaten im Hinblick auf die gestoppten Nachrichten in einem Speicher an der Vorrichtung einschließt; und/oder ferner einschließend das Erzeugen einer Benachrichtigung zum Senden an einen Benutzer, wenn eine Nachrichtenzählung von Nachrichten mit einem der einen oder mehreren dritten Sätze von Nachrichteneigenschaften eine vorher festgelegte Stufe erreicht.

14. Verfahren nach Anspruch 10, ferner einschließend das Einleiten einer Sicherheitsmaßnahme, wenn eine Nachrichtenzählung von Nachrichten mit einem der einen oder mehreren dritten Sätze von Nachrichteneigenschaften eine vorher festgelegte Stufe erreicht.

15. Verfahren nach Anspruch 14, wobei das Einleiten der Sicherheitsmaßnahme das Initiieren einer Viruserkennungs- oder einer Intrusion Detection Software in einer Vorrichtung an dem Kommunikationsnetzwerk einschließt; und/oder
wobei das Einleiten der Sicherheitsmaßnahme das Trennen einer Vorrichtung von einer Kommunikationsverbindung des Kommunikationsnetzwerks einschließt; und/oder
wobei das Einleiten der Sicherheitsmaßnahme das Trennen einer anderen Vorrichtung an dem Kommunikationsnetzwerk von der Kommunikationsverbindung des Kommunikationsnetzwerks einschließt.

16. Verfahren nach einem der Ansprüche 10-15, insbesondere nach Anspruch 10, wobei das Weiterleiten der Nachrichten mit den einen oder mehreren ersten Sätzen von Nachrichteneigenschaften und das Weiterleiten der Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften das Weiterleiten der Nachrichten an einen Kommunikationsstapel der Vorrichtung zur Verarbeitung an der Vorrichtung einschließt; und/oder wobei das Weiterleiten der Nachrichten mit den einen oder mehreren ersten Sätzen von Nachrichteneigenschaften und das Weiterleiten der Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften das Weiterleiten der Nachrichten an eine Kommunikationsverbindung des Kommunikationsnetzwerks zur Übertragung an eine andere Vorrichtung an dem Kommunikationsnetzwerk einschließt.

17. Verfahren nach Anspruch 10, wobei das Empfangen der Reihe von Nachrichten an einer Vorrichtung, die mit dem Kommunikationsnetzwerk verbunden ist, das Empfangen einer ersten Reihe von Nachrichten, die in der Vorrichtung erzeugt werden und das Empfangen einer zweiten Reihe von Nachrichten einschließt, die von einer Kommunikationsverbindung des Kommunikationsnetzwerks empfangen werden, wobei das separate Analysieren von jeder der Reihe von Nachrichten das Analysieren von jeder der ersten Reihe von Nachrichten und der zweiten Reihe von Nachrichten einschließt und wobei das Filtern von jeder der Nachrichten das separate Filtern von jeder der ersten Reihe von Nachrichten und der zweiten Reihe von Nachrichten einschließt.

18. Verfahren nach Anspruch 17, wobei das separate Filtern von jeder der ersten Reihe von Nachrichten und der zweiten Reihe von Nachrichten das Filtern der ersten Reihe von Nachrichten unter Verwendung eines ersten Satzes von logischen Regeln und das Filtern der zweiten Reihe von Nachrichten unter Verwendung eines zweiten und anderen Satzes von logischen Regeln einschließt.

19. Kommunikationsnetzwerk, umfassend:
eine Kommunikationsverbindung;
eine Vielzahl von Netzwerkknoten, wobei jeder der Netzwerkknoten eine Netzwerkvorrichtung einschließt, die mit der Kommunikationsverbindung gekoppelt ist und einen Prozessor und einen Kommunikationsstapel

aufweist, der an dem Prozessor zur Verarbeitung von Nachrichten ausgeführt wird, die von der Kommunikationsverbindung kommen und dorthin gehen;
wobei jeder einer Vielzahl der Netzwerkknoten ferner Folgendes einschließt:
eine oder mehrere Nachrichtenmodulschnittstellen, wobei jede der Nachrichtenmodulschnittstellen an einem Prozessor an einem Netzwerkknoten ausgeführt wird, um Nachrichtenverkehr zu detektieren, der von dem Kommunikationsstapel oder von der Kommunikationsverbindung kommt, um eine oder mehrere Nachrichteneigenschaften von jeder der Nachrichten zu bestimmen;
einen Regelspeicher, der eine oder mehrere logische Regeln speichert; und
ein Filtermodul, das in einem Prozessor gespeichert und an diesem ausgeführt wird und mit dem Regelspeicher gekoppelt ist, das den Satz von logischen Regeln verwendet, der in dem Regelspeicher gespeichert ist, um Nachrichten mit einem oder mehreren ersten Sätzen von Nachrichteneigenschaften weiterzuleiten, um Nachrichten mit einem oder mehreren zweiten Sätzen von Nachrichteneigenschaften zu stoppen und um Nachrichten mit einem oder mehreren dritten Sätzen von Nachrichteneigenschaften zu zählen und das ferner die Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften auf Grundlage von Zählungen, die mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften verknüpft sind, weiterleitet oder stoppt;
wobei das Filtermodul die Nachrichtenzählungen für die Nachrichten mit den einen oder mehreren dritten Sätzen von Nachrichteneigenschaften als eine Anzahl von Nachrichten mit einem bestimmten Satz von Nachrichteneigenschaften erzeugt, der innerhalb eines bestimmten Zeitraums empfangen wurde.

20. Kommunikationsnetzwerk nach Anspruch 19, wobei der Regelspeicher ein Read-Only Memory ist; und/oder
wobei der Regelspeicher ein Lese-/Schreibspeicher ist; und/oder
wobei der Regelspeicher einen ersten Teil einschließt, der ein Read-Only Memory ist und einen zweiten Teil einschließt, der ein Lese-/Schreibspeicher ist.

21. Kommunikationsnetzwerk nach einem der Ansprüche 19-20, insbesondere nach Anspruch 19, wobei jeder der Vielzahl von Netzwerkknoten ferner ein Protokollierungsmodul einschließt, das mit dem Filtermodul gekoppelt ist, wobei das Protokollierungsprotokoll an dem Prozessor ausgeführt wird, um Informationen im Hinblick auf eine oder mehrere gestoppte Nachrichten zu empfangen und um Informationen im Hinblick auf die einen oder mehreren gestoppten Nachrichten in einem oder mehreren Protokollen zu speichern.

22. Kommunikationsnetzwerk nach Anspruch 21, wobei das Protokollierungsmodul ferner eine Kommunikationsschnittstelle einschließt, welche die einen oder mehreren Protokolle gestoppter Nachrichten zu einem Benutzer schickt.

23. Kommunikationsnetzwerk nach einem der Ansprüche 20-22, insbesondere nach Anspruch 22, wobei das Protokollierungsmodul Metadaten im Hinblick auf die gestoppten Nachrichten speichert.

24. Kommunikationsnetzwerk nach einem der Ansprüche 19-23, insbesondere nach Anspruch 19, wobei jeder der Vielzahl von Netzwerkknoten ferner ein Benachrichtigungserzeugungsmodul einschließt, das mit dem Filtermodul gekoppelt ist, wobei das Benachrichtigungserzeugungsmodul an dem Prozessor ausgeführt wird, um eine Benachrichtigung an einen Benutzer zu schicken, wenn eine der Nachrichtenzählungen eine vorher festgelegte Stufe erreicht; und/oder
wobei jeder der Vielzahl von Netzwerkknoten ferner ein Benachrichtigungserzeugungsmodul einschließt, das mit dem Filtermodul gekoppelt ist, wobei das Benachrichtigungserzeugungsmodul an dem Prozessor ausgeführt wird, um eine Vorrichtung von dem Kommunikationsverbindungsnetzwerk zu trennen, wenn eine der Nachrichtenzählungen eine vorher festgelegte Stufe erreicht; und/oder
wobei jeder der Vielzahl von Netzwerkknoten zwei oder mehr Filtermodule einschließt, wobei ein erstes der zwei oder mehr Filtermodule eingehende Nachrichten an dem Netzwerkknoten von der Kommunikationsverbindung in die Netzwerkvorrichtung empfängt und analysiert und ein zweites der zwei oder mehr Filtermodule Nachrichten empfängt und analysiert, die in der Netzwerkvorrichtung an dem Netzwerkknoten erzeugt wurden und an einem anderen Netzwerkknoten über die Kommunikationsverbindung zu einer anderen Netzwerkvorrichtung geschickt werden.

25. Computer-lesbares Speichermedium, welches Instruktionen aufweist, die zumindest einen Prozessor dazu veranlassen, ein Verfahren nach einem der Ansprüche 10 bis 18 zu implementieren, wenn die Instruktionen durch den Prozessor ausgeführt werden.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

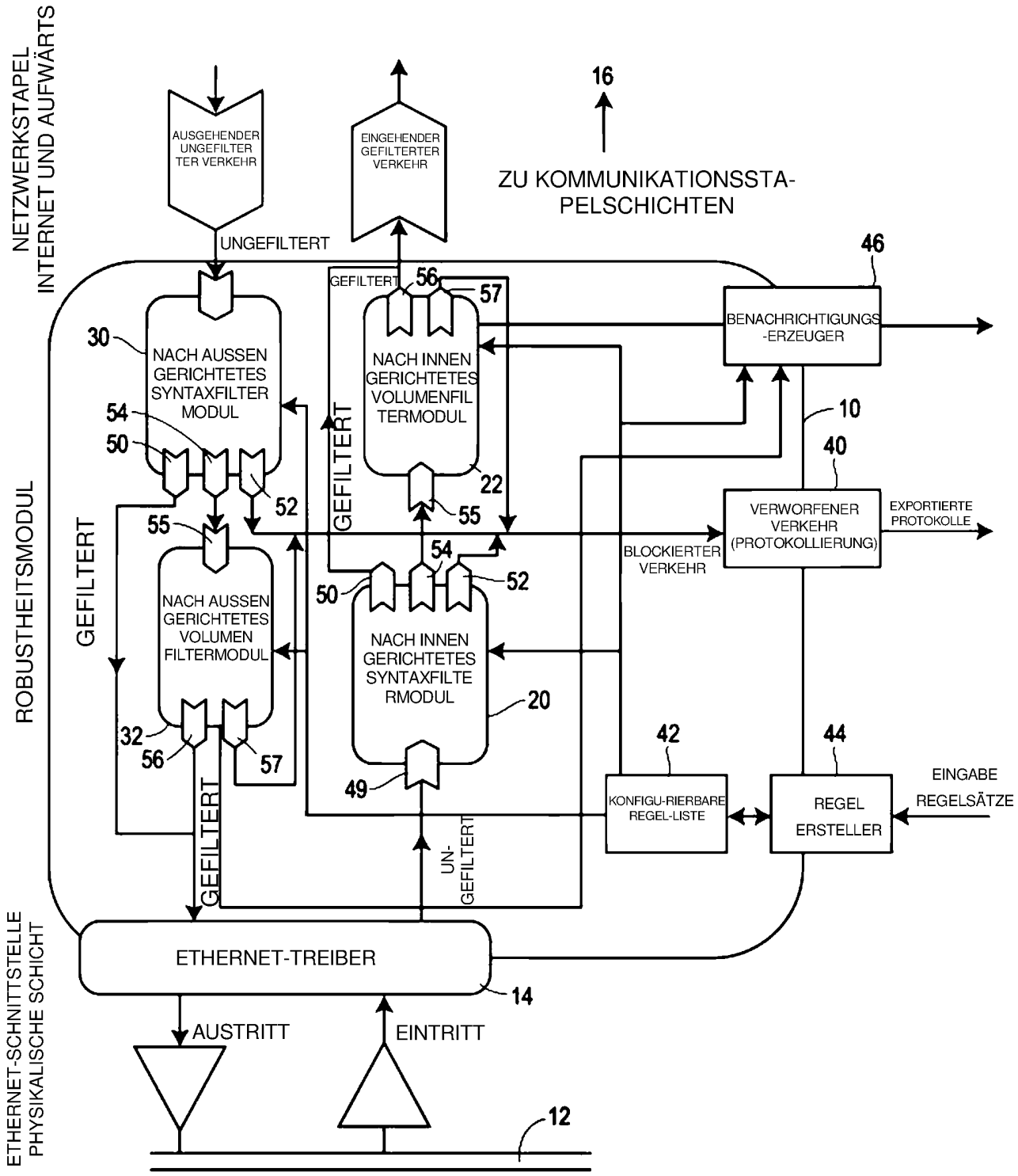


FIG. 1

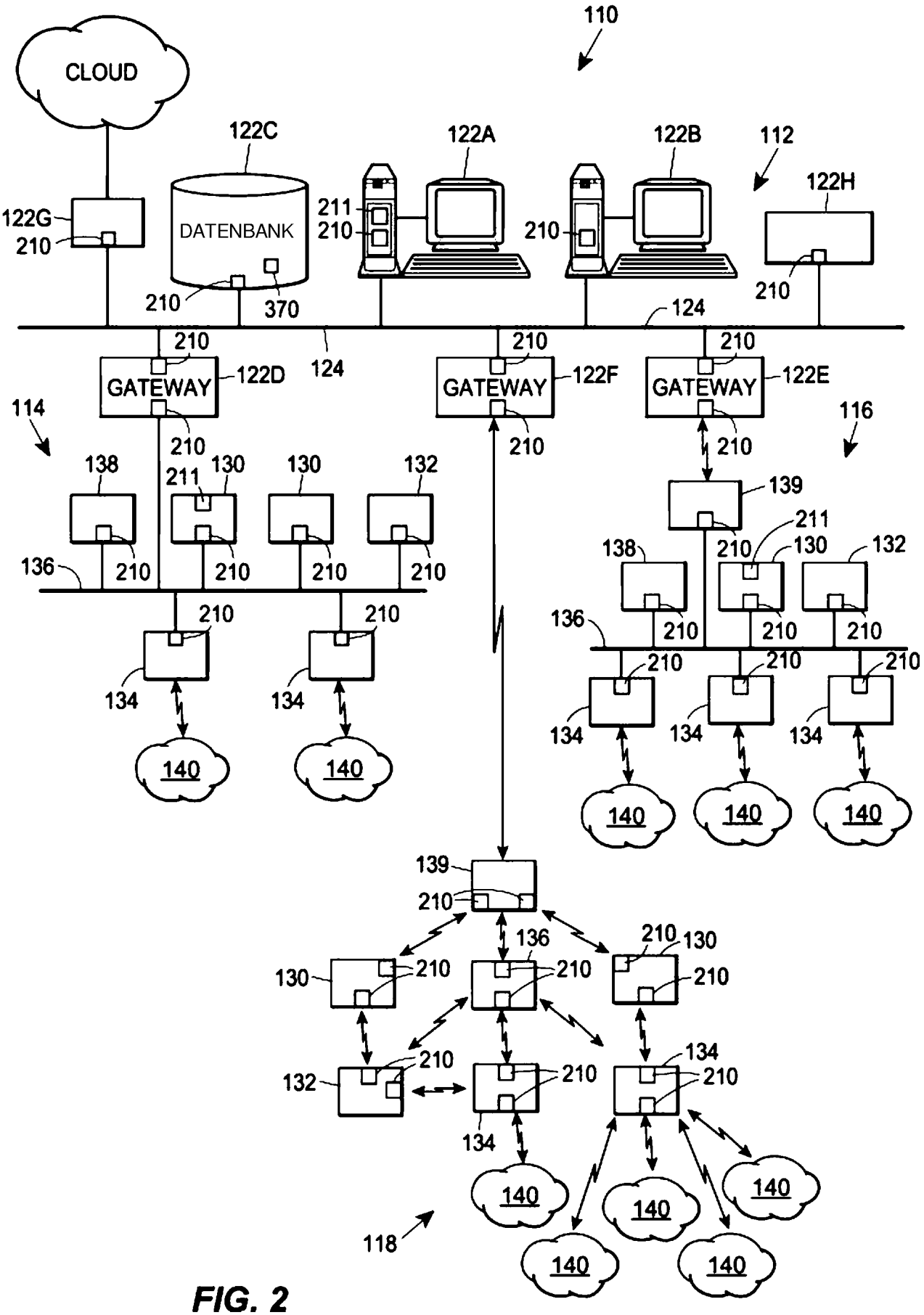

110
CLOUD
122C
DATENBANK
122A
122B
112
122H
122G
210
211
370
124
GATEWAY
122D
122F
122E
114
116
138
130
132
136
134
139
140
118

FIG. 2

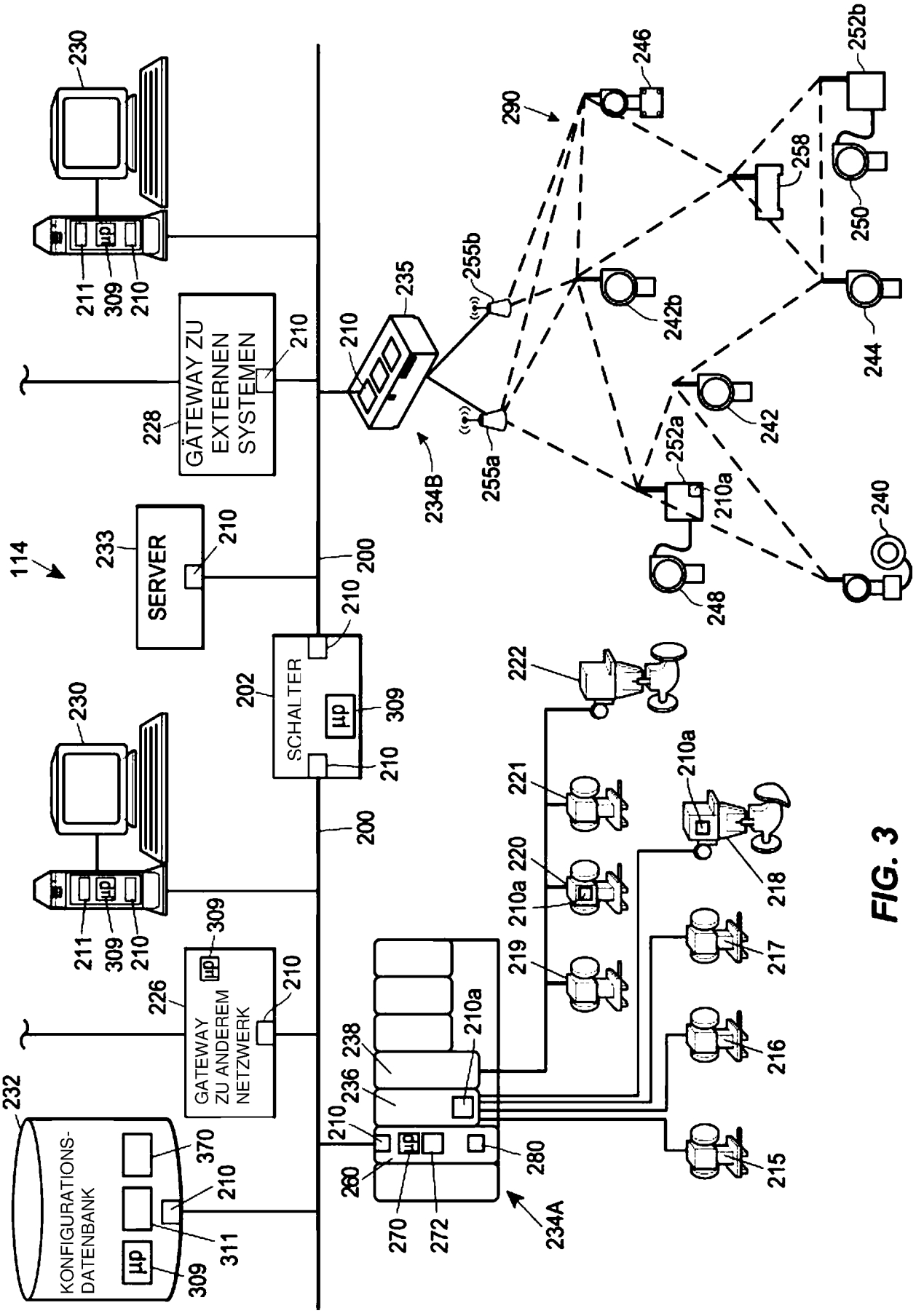


FIG. 3

