(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 124 866 A1** 2018.06.07

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 124 866.8**
(22) Anmeldetag: **24.10.2017**
(43) Offenlegungstag: **07.06.2018**

(51) Int Cl.: ***H04L 12/46*** (2006.01)
H04L 12/66 (2006.01)
H04L 9/14 (2006.01)

(30) Unionspriorität:
15/332,751 **24.10.2016** **US**

(71) Anmelder:
Fisher-Rosemount Systems, Inc., Round Rock, Tex., US

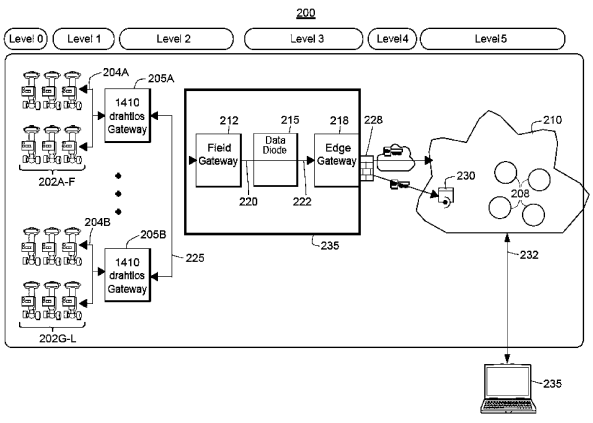
(74) Vertreter:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

(72) Erfinder:
Rotvold, Eric, West Saint Paul, Minn., US; Nixon, Mark J., Round Rock, Tex., US; Boudreaux, Michael J., Round Rock, Tex., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Gesicherte Prozesssteuerkommunikationen**

(57) Zusammenfassung: Das Sichern von Kommunikationen von einer Prozessanlage zu einem fernen System beinhaltet eine Datendiode, die dazwischen angeordnet ist und es zulässt, dass Daten von der Anlage austreten, aber ein Eintreten von Daten in die Anlage und ihre assoziierten Systeme verhindert. Daten werden über die Datendiode durch sicheres Provisionieren eines sendenden Geräts am Anlagenende der Diode zu einem empfangenden Gerät am Ende des fernen Systems gesichert. Das sendende und das empfangene Gerät nutzen Geheimschlüsselmaterial gemeinsam, dass rekurrent aktualisiert wird. Um die Vertraulichkeit von Kommunikationen über die unidirektionale Datendiode zu gewährleisten, stellt das sendende Gerät rekurrent Kontextinformationen bereit, die Datenquellen der Anlage beschreiben. Zusätzlich können von Anlagendatenquellen zu dem sendenden Gerät der Datendiode übertragene Daten mit einem/r jeweiligen Sicherheitsmechanismus/Technik gesichert werden, und von dem empfangenen Gerät der Datendiode zu dem fernen System übertragene Daten können mit einer/m jeweiligen Sicherheitsmechanismus/Technik gesichert werden.



Beschreibung

ZUGEHÖRIGE REFERENZEN

[0001] Die vorliegende Offenbarung ist verwandt mit der in Gemeinschaftsbesitz befindlichen US-Patentanmeldung Nr. 14/507,188, eingereicht am 6. Oktober 2014 unter dem Titel „Regional Big Data in Process Control Systems“; der in Gemeinschaftsbesitz befindlichen US-Patentanmeldung Nr. 15/274,519, eingereicht am 23. September 2016 unter dem Titel „Data Analytics Services for Distributed Industrial Performance Monitoring“; der US-Patentanmeldung Nr. 15/274,233, eingereicht am 23. September 2016 unter dem Titel „Distributed Industrial Performance Monitoring and Analytics“; und der in Gemeinschaftsbesitz befindlichen US-Patentanmeldung Nr. 15/332,521, eingereicht am 24. Oktober 2016 unter dem Titel „Process Device Condition and Performance Monitoring“, deren gesamte Offenbarungen hierin durch Bezugnahme eingeschlossen sind.

TECHNISCHER BEREICH

[0002] Die vorliegende Offenbarung betrifft allgemein Prozessanlagen und Prozesssteuersysteme und spezieller das Sichern von Kommunikationen zwischen lokalen Prozessanlagen/Prozesssteuersystemen und einem Fernsystem, das die lokalen Prozesssteueranlagen/-systeme bedient, wie zum Beispiel ein tiefgreifendes Sensorsystem.

HINTERGRUND

[0003] Verteilte Prozesssteuersysteme wie die, die in Chemie-, Erdöl- oder anderen Prozessanlagen zum Einsatz kommen, beinhalten typischerweise einen oder mehrere Prozesscontroller, die kommunikativ mit einem oder mehreren Feldgeräten über analoge, digitale oder kombinierte analoge/digitale Sammelschienen oder über ein(e) drahtlose(s) Kommunikationsverbindung oder -netzwerk gekoppelt sind. Die Feldgeräte, die beispielsweise Ventile, Ventilstellungsregler, Schalter und Sender (z.B. Temperatur-, Druck-, Füllstands- und Durchflussratensensoren) sein können, befinden sich in der Prozessumgebung und führen allgemein physische oder Prozesssteuerfunktionen wie Öffnen oder Schließen von Ventilen, Messen von Prozessparametern wie Druck, Temperatur usw. und dergleichen durch, um einen oder mehrere in der/dem Prozessanlage oder -system laufende Prozesse zu steuern. Intelligente Feldgeräte, wie zum Beispiel die Feldgeräte, die dem gut bekannten Fieldbus-Protokoll entsprechen, können ebenfalls Steuerberechnungen, Alarmierungsfunktionen und andere Steuerfunktionen ausführen, die üblicherweise im Controller implementiert werden. Die Prozesscontroller, die sich typischerweise ebenfalls in der Prozessumgebung befinden, empfangen Signale, die Prozessmessungen anzeigen, die von den Feldgeräten durchgeführt werden, und/oder andere Informationen in Bezug auf die Feldgeräte, und eine Controller-Anwendung ausführen, die beispielsweise unterschiedliche Steuermodule abarbeitet, die Prozesssteuerentscheidungen treffen, Steuersignale auf der Basis der empfangenen Informationen erzeugen und mit den Steuermodulen oder -blöcken koordinieren, die in den Feldgeräten ausgeführt werden, wie HART®, WirelessHART® und FOUNDATION® Fieldbus-Feldgeräte. Die Steuermodule im Controller senden die Steuersignale über die Kommunikationsleitungen oder -verbindungen zu den Feldgeräten, um dadurch den Betrieb wenigstens eines Teils der/des Prozessanlage oder -systems zu steuern.

[0004] Informationen von den Feldgeräten und dem Controller werden gewöhnlich über einen Daten-Highway einem oder mehreren anderen Hardware-Geräten zur Verfügung gestellt, wie zum Beispiel Operator-Workstations, Personal Computern oder Rechengeräten, Data-Historians, Berichtsgeneratoren, zentralisierten Datenbanken oder anderen zentralisierten administrativen Rechengeräten, die sich typischerweise in Kontrollräumen oder an anderen Orten fern von der rauheren Anlagenumgebung befinden. Jedes dieser Hardware-Geräte ist typischerweise über die Prozessanlage oder über einen Teil der Prozessanlage zentralisiert. Diese Hardware-Geräte arbeiten Anwendungen ab, die beispielsweise einen Bediener befähigen können, Funktionen mit Bezug auf das Steuern eines Prozesses und/oder das Bedienen der Prozessanlage auszuführen, wie zum Beispiel Ändern von Einstellungen der Prozesssteuerroutine, Modifizieren des Betriebs der Steuermodule in den Controllern oder den Feldgeräten, Betrachten des aktuellen Zustands des Prozesses, Betrachten von Alarmen, die von Feldgeräten und Controllern erzeugt wurden, Simulieren des Betriebs des Prozesses zwecks Ausbildung von Personal oder Testen der Prozesssteuer-Software, Führen und Aktualisieren einer Konfigurationsdatenbank usw. Der von den Hardware-Geräten, Controllern und Feldgeräten benutzte Data-Highway kann einen verdrahteten Kommunikationspfad, einen drahtlosen Kommunikationspfad oder eine Kombination aus verdrahteten und drahtlosen Kommunikationspfaden beinhalten.

[0005] Zum Beispiel, das von Emerson Process Management verkaufte Steuersystem DeltaV™ beinhaltet mehrere Anwendungen, die in unterschiedlichen Geräten gespeichert sind und von diesen abgearbeitet werden, die sich an diversen Stellen in der Prozessanlage befinden. Eine Konfigurationsanwendung, die sich in einer oder mehreren Workstations oder Rechengeräten befindet, befähigt Benutzer, Prozesssteuermodule zu erzeugen oder zu ändern und diese Prozesssteuermodule über einen Data-Highway auf dedizierte verteilte Controller herunterzuladen. Diese Steuermodule setzen sich typischerweise aus kommunikativ miteinander verbun-

denen Funktionsblöcken zusammen, die Objekte in einem objektorientierten Programmierungsprotokoll sind, die Funktionen in dem Steuerschema auf der Basis von Eingaben darin ausführen und Ausgänge zu anderen Funktionsblöcken in dem Steuerschema bereitstellen. Die Konfigurationsanwendung kann es auch einem Konfigurationsdesigner gestatten, Bedieneroberflächen zu erzeugen oder zu ändern, die von einer Betrachtungsanwendung benutzt werden, um einem Bediener Daten anzuzeigen und den Bediener zu befähigen, Einstellungen wie Sollwerte innerhalb der Prozesssteuerroutinen zu ändern. Jeder dedizierte Controller und, in einigen Fällen, ein oder mehrere Feldgeräte, speichert eine jeweilige Controller-Anwendung und arbeitet sie ab, die die ihr zugewiesenen und auf sie heruntergeladenen Steuermodule abarbeitet, um tatsächliche Prozesssteuerfunktionalität zu implementieren. Die Betrachtungsanwendungen, die auf einer oder mehreren Operator-Workstations (oder auf einem oder mehreren Fernrechengeräten in kommunikativer Verbindung mit den Operator-Workstations und dem Data-Highway) ausgeführt werden können, empfangen Daten von der Controller-Anwendung über den Data-Highway und zeigen diese Daten Prozesssteuersystem-Designern, Bedienern oder Benutzern an, die die Benutzeroberflächen benutzen, und können beliebige aus einer Reihe verschiedener Ansichten bereitstellen, wie zum Beispiel eine Bedieneransicht, eine Ingenieursansicht, einer Technikeransicht usw. Eine Data-Historian-Anwendung ist typischerweise in einem Data-Historian-Gerät gespeichert und wird davon ausgeführt, das einige oder alle der über den Data-Highway bereitgestellten Daten sammelt und speichert, während eine Konfigurationsdatenbank-Anwendung in einem noch weiteren Computer abgearbeitet werden kann, der am Data-Highway angeschlossen ist, um die aktuelle Prozesssteuerroutinenkonfiguration und damit assoziierte Daten zu speichern. Alternativ kann sich die Konfigurationsdatenbank in derselben Workstation befinden wie die Konfigurationsanwendung.

[0006] Allgemein ausgedrückt, ein Prozesssteuersystem einer Prozessanlage beinhaltet Feldgeräte, Controller, Workstations und andere Geräte, die über einen Satz von geschichteten Netzwerken und Sammelschienen miteinander verbunden sind. Das Prozesssteuersystem kann wiederum mit verschiedenen Geschäfts- und externen Netzwerken verbunden sein, z.B. zum Reduzieren von Herstellungs- und Betriebskosten, Verbessern von Produktivität und Effizienzen, Bereitstellen von rechtzeitigem Zugang zu Prozesssteuer- und/oder Prozessanlageninformationen usw. Andererseits erhöht die Verbindung von Prozessanlagen und/oder Prozesssteuersystemen mit Unternehmens- und/oder externen Netzwerken und Systemen das Risiko von Cyber-Eingriffen und/oder bösartigen Cyber-Attacken, die von erwarteten Schwachstellen in kommerziellen Systemen und Anwendungen wie denen entstehen können, die in Unternehmens- und/oder externen Netzwerken benutzt werden. Cyber-Eingriffe und bösartige Cyber-Attacken auf Prozessanlagen, Netzwerke und/oder Steuersysteme können Vertraulichkeit, Integrität und/oder Verfügbarkeit von Informationsbeständen negativ beeinflussen, die allgemein gesagt Schwachstellen ähnlich denen von universellen Rechennetzwerken sind. Im Gegensatz zu Universalcomputernetzen können Cyber-Eingriffe in Prozessanlagen, Netzwerke und/oder Steuersysteme jedoch auch zu Schäden, Zerstörung und/oder Verlust nicht nur von Anlagenausrüstung, Produkten und anderen physischen Vermögenswerten führen, sondern auch zu Verlust von menschlichem Leben. Zum Beispiel, ein Cyber-Eingriff kann verursachen, dass ein Prozess unkontrollierbar wird, und kann dadurch Explosionen, Brände, Überflutungen, Kontakt mit gefährlichen Materialien usw. hervorrufen. So ist das Sichern von Kommunikationen in Bezug auf Prozesssteueranlagen und -systeme von höchster Bedeutung.

[0007] **Fig. 1** zeigt ein Blockdiagramm 10 von beispielhaften Sicherheitsstufen für ein Prozesssteuer- oder industrielles Prozesssystem. Das Diagramm 10 veranschaulicht Verbindungen zwischen verschiedenen Komponenten des Prozesssteuersystems, dem Prozesssteuersystem selbst und anderen Systemen und/oder Netzwerken, mit denen das Prozesssteuersystem kommunikativ verbunden sein kann, sowie Sicherheitsschichten oder - stufen in Bezug auf Kommunikationen in und zwischen dem Prozesssteuersystem und den anderen Systemen/Netwerken. Die Sicherheitsstufen bieten einen geschichteten Ansatz zu Sicherheit über Segmentierung oder Trennung, und verschiedene Stufen werden durch eine oder mehrere Firewalls 12A, 12B, 12C geschützt, um nur befugten Verkehr zwischen den unterschiedlichen Stufen zuzulassen. In **Fig. 1** sind die Sicherheitsstufen mit den kleineren Nummern näher am Online-Prozess, der gesteuert wird, während die Sicherheitsstufen mit den höheren Nummern weiter vom laufenden Prozess entfernt sind. Demzufolge sind Vertrauensstufen (z.B. ein relativer Grad an Vertrauen in Sicherheit und Gültigkeit von Nachrichten, Paketen und anderen Kommunikationen) auf der Gerätestufe (Level 0) am höchsten, und Vertrauensstufen jenseits der Geschäftsnetzwerkebene (Level 5), z.B. am öffentlichen Internet und/oder an anderen öffentlichen Netzwerken, sind am tiefsten. Im Hinblick auf den Logikrahmen gemäß Purdue Model for Control Hierarchy, standardisiert von der ISA (International Society of Automation) 95.01 - IEC (International Electrotechnical Commission) 62264-1, fallen Prozesssteuersysteme im Allgemeinen in Sicherheitsstufen 0-2, und Herstellungs-, Corporate- und Unternehmenssysteme fallen im Allgemeinen in die Sicherheitsstufen 3-5.

[0008] Beispiele für unterschiedliche Funktionalitäten auf jeder der unterschiedlichen Sicherheitsstufen sind in **Fig. 1** dargestellt. Typischerweise beinhal-

tet Level 0 Feldgeräte und andere Geräte, die in einer Prozessanlage angeordnet sind und die direkten Kontakt mit dem Prozess und/oder Prozessablauf haben, zum Beispiel Sensoren, Ventile, Ventilstellungsregler, Schalter, Sender und andere Geräte, die physische und/oder Prozesssteuerfunktionen wie Öffnen oder Schließen von Ventilen, Messen von Prozessparametern wie Druck, Temperatur usw. und dergleichen ausführen. Zur Verdeutlichung zeigt **Fig. 1** keine Beispiele für Feldgeräte.

[0009] Level 1 beinhaltet Controller und andere Prozesssteuergeräte 15A-15D, die Basissteuerung von Echtzeitvorgängen des Prozesses bereitstellen, z.B. durch Empfangen von Eingängen von Feldgeräten, Verarbeiten der Eingänge mit Steuerschemata, Modulen oder sonstiger Logik, und Senden von resultierenden Ausgängen zu anderen Geräten. Im Allgemeinen sind solche Prozesssteuergeräte mit jeweiligen Steuerschemata programmiert und/oder konfiguriert. Zum Beispiel, Prozesssteuergeräte auf Level 1 können Prozess-Controller, programmierbare Logik-Controller (PLC), Fernbediednungsterminals (RTUs) und dergleichen beinhalten. Wie in **Fig. 1** gezeigt, können die Prozesssteuergeräte auf Level 1 diejenigen beinhalten, die Chargensteuerung 15A, diskrete Steuerung 15B, kontinuierliche Steuerung 15C, Hybridsteuerung 15D und/oder andere Steuertypen ausführen.

[0010] Level 2 beinhaltet Geräte und Ausrüstung 18A-18D, die Produktionsbereich-Aufsichtssteuerung für die Prozessanlage bereitstellen. Zum Beispiel, Level 2 kann Alarmierungs- und/oder Warnsysteme 18A, Operator-Workstations 18C, andere Mensch-Maschine-Schnittstellen (HMI) 18B, 18D und dergleichen beinhalten. Im Allgemeinen können Geräte und Ausrüstung auf Level 2 mit Geräten 15A-15D von Level 1 sowie mit Geräten und Ausrüstung von Level 3 z.B. über eine oder mehrere Firewalls 12A, 12B kommunizieren.

[0011] Level 3 beinhaltet Anlagensysteme und/oder -netzwerke, z.B. die Geräte, Ausrüstung und Systeme 20A-20D, die Standort/Anlagenvorgänge und -bedienung verwalten, um ein gewünschtes Endprodukt zu produzieren oder herzustellen. Zum Beispiel, Level 3 kann Produktionssysteme 20A beinhalten, die für Produktionssteuerung, Meldung, Planung usw. benutzt werden; Optimierungssysteme 20B, die zum Verbessern von Qualität, Produktivität, Effizienzen usw. benutzt werden; Historians 20C zum Historisieren von Daten, die von der Prozessanlage erzeugt werden und/oder diese anzeigen; und/oder Engineering-Workstations oder Rechengeräte 20D, die vom Personal für Design und Entwicklung von Steuerschemata und Modulen benutzt werden, Operator-Workstations und/oder HMI-Schnittstellen usw.

[0012] Nun übergehend zu Level 5, Level 5 beherbergt im Allgemeinen Geschäfts-, Corporate- oder Unternehmenssysteme und/oder -netzwerke. Typischerweise verwalten solche Systeme und/oder Netzwerke das Interfacing mit Systemen außerhalb des Unternehmens. Zum Beispiel, in Level 5 befinden sich ein Unternehmens-VPN (Virtual Private Network), Corporate- oder Unternehmens-Internet-Zugangsdienste und/oder andere IT-(Information Technology)-Infrastruktursysteme und Anwendungen.

[0013] Level 4, der als eine Einwärtserweiterung von Level 5 bezeichnet werden kann, beherbergt im Allgemeinen Corporate- oder Unternehmenssysteme, die sich innerhalb des Unternehmens befinden, zum Beispiel Corporate-Systeme, die Email, Intranet, Standortgeschäftsplanung und Logistik, Inventar, Planung und/oder andere Corporate/Unternehmens-Systeme und -netzwerke unterstützen.

[0014] Wie in **Fig. 1** gezeigt, ist die Schnittstelle zwischen Sicherheitsstufen 3 und 4 eine entmilitarisierte Zone (DMZ) 22, die Geschäfts- oder Unternehmenssysteme und/oder - netzwerke von Anlagen/Prozesssystemen und/oder -netzwerken trennt, um dadurch das Niveau an Sicherheitsrisiko zu minimieren, dem eine Prozessanlage ausgesetzt ist. Die DMZ 22 kann eine oder mehrere jeweilige Firewalls 12C beinhalten und kann verschiedene Geräte, Ausrüstung, Server und/oder Anwendungen 25A-25F beherbergen, die mit anlagenbezogenen Geräten, Ausrüstung und Anwendungen auf niedrigeren Sicherheitsstufen kommunizieren und/oder die mit unternehmensbezogenen Geräten, Ausrüstung und Anwendungen auf höheren Sicherheitsstufen kommunizieren. Zum Beispiel, die DMZ 22 kann Terminaldienste 25A, Patch-Management 25B, einen oder mehrere AV-Server 25C, einen oder mehrere Historians 25D (die zum Beispiel Spiegel-Historians beinhalten können), Web Services Operations 25E und/oder einen oder mehrere Anwendungsserver 25F beherbergen, um nur einige wenige zu nennen. Typischerweise dürfen für die Geräte, Ausrüstung und/oder Anwendungen auf Sicherheitsstufen über DMZ 22 nur diejenigen, die autorisiert sind, kommunikativ auf die Prozessanlage zugreifen, und müssen ferner über die Geräte, Ausrüstung, Server und/oder Anwendungen 25A-25F der DMZ 22 zugeschaltet sein. Die DMZ-Geräte 25A-25F wiederum führen separate Verbindungen mit den niedrigeren Stufen, um dadurch die Prozessanlage und das Steuersystem vor Attacken von den Unternehmens-(und höheren) Systemen und/oder Netzwerken zu schützen.

[0015] Nun zu einer kurzen Erörterung von Ferndiensten, Ferndienste werden immer häufiger von unterschiedlichen Benutzern und Systemen benutzt. Zum Beispiel, das vom Microsoft Windows® Betriebssystem bereitgestellte Remote Desktop Services Produkt ermöglicht es Benutzern, auf sitzungs-

gestützte Desktops, virtuelle maschinengestützte Desktops und/oder auf andere Anwendungen in einem Datenzentrum von einem Corporate-Netzwerk und/oder vom Internet aus zuzugreifen. Das von Intuit® bereitgestellte Online-Produkt QuickBooks® ermöglicht es Benutzern, Buchhaltungsfunktionen wie Cashflow-Management, Rechnungsstellung und Online-Durchführung von Zahlungen über das Internet durchzuführen. Allgemein ausgedrückt, Ferndienste werden von einer oder mehreren Anwendungen bereitgestellt, die fern von dem System oder Benutzer ablaufen, das/der auf den Ferndienst zugreift. Zum Beispiel, die ein oder mehreren Anwendungen führen Daten auf einer fernen Bank von Servern, im Cloud usw. aus und verwalten sie, und es wird über ein oder mehrere private und/oder öffentliche Netzwerke wie zum Beispiel ein Unternehmensnetzwerk und/oder das öffentliche Internet darauf zugegriffen.

ZUSAMMENFASSUNG

[0016] In einer Ausgestaltung beinhaltet ein System zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System eine Datendiode, die zwischen einem Netzwerk der Prozessanlage und einem Netzwerk des anderen Systems angeordnet ist. Die Datendiode ist zum Verhindern von Zweiweg-Kommunikationen zwischen dem Prozessanlagennetzwerk und dem Netzwerk des anderen Systems konfiguriert, so dass Daten, die von Geräten der Prozessanlage erzeugt werden, während die Prozessanlage in Betrieb ist, um einen industriellen Prozess zu steuern, verschlüsselt und sicher von dem Prozessanlagennetzwerk zum Netzwerk des anderen Systems über oder durch die Datendiode transportiert werden.

[0017] In einer Ausgestaltung beinhaltet ein Verfahren zum Sichern von Kommunikationen zwischen einer Prozessanlage und einem anderen System das Empfangen, an einem Field-Gateway von einem Prozessanlagennetzwerk, von Daten, die von einem oder mehreren Geräten der Prozessanlage erzeugt werden, während die Prozessanlage arbeitet, um einen industriellen Prozess zu steuern, wobei die Prozessanlagendaten zur Übertragung von den ein oder mehreren Geräten zum Field-Gateway über einen ersten Sicherheitsmechanismus gesichert werden. Das Verfahren beinhaltet auch das Sichern, durch den Field-Gateway, der Prozessanlagendaten über einen zweiten Sicherheitsmechanismus und das Transportieren der gesicherten Prozessanlagendaten über eine Datendiode zur Lieferung zu dem anderen System über einen Edge-Gateway. Der Edge-Gateway ist kommunikativ mit dem anderen System verbunden und die kommunikative Verbindung zwischen dem Edge-Gateway und dem anderen System wird über einen dritten Sicherheitsmechanismus gesichert. Die Datendiode ist so konfiguriert, dass sie das Eindringen von Daten verhindert, die vom Edge-Gateway in den Field-Gateway übertragen werden.

[0018] In einer Ausgestaltung beinhaltet ein Verfahren zum Sichern von Kommunikationen zwischen einer Prozessanlage und einem anderen System, das die Prozessanlage bedient, das Empfangen, an einem Edge-Gateway über eine Datendiode, die kommunikativ mit einem Field-Gateway der Prozessanlage verbunden ist, von Daten, die von einem oder mehreren Geräten der Prozessanlage erzeugt werden, während die Prozessanlage in Betrieb ist, um einen Industrieprozess zu steuern. Die Prozessanlagendaten werden zur Übertragung von den ein oder mehreren Geräten zum Field-Gateway über einen ersten Sicherheitsmechanismus gesichert und werden ferner für den Transport vom Field-Gateway über die Datendiode zum Edge-Gateway mit einem zweiten Sicherheitsmechanismus gesichert. Ferner ist die Datendiode so konfiguriert, dass sie das Eindringen von Daten verhindert, die vom Edge-Gateway in den Field-Gateway übertragen werden. Das Verfahren beinhaltet auch das Sichern, durch den Edge-Gateway, der Prozessanlagendaten über einen dritten Mechanismus, um das Übertragen, durch den Edge-Gateway, der gesicherten Prozessanlagendaten zu dem anderen System.

Figurenliste

Fig. 1 beinhaltet ein Blockdiagramm von beispielhaften Sicherheitsstufen für einen Prozesssteuer- oder Industrieprozesssystem, einschließlich u.a. Verbindungen zwischen verschiedenen beispielhaften Komponenten des Prozesssteuersystems, dem Prozesssteuersystem selbst und anderen beispielhaften Systemen und/oder Netzwerken;

Fig. 2 ist ein Blockdiagramm einer/s beispielhaften Prozessanlage oder Prozesssteuersystems, die/das u.a. Verbindungen zwischen verschiedenen beispielhaften Komponenten des Prozesssteuersystems, dem Prozesssteuersystem selbst und anderen beispielhaften Systemen und/oder Netzwerken illustriert;

Fig. 3 ist ein Blockdiagramm einer beispielhaften Sicherheitsarchitektur für eine Prozessanlage oder ein Prozesssteuersystem;

Fig. 4 zeigt einen beispielhaften Nachrichtenfluss, der zum Provisionieren von gesicherten Kommunikationen für ein/e Prozessanlage oder Prozesssteuersystem benutzt werden kann;

Fig. 5 veranschaulicht einen beispielhaften Nachrichtenfluss, der zum Liefern von Prozessanlagendaten über die Datendiode benutzt werden kann.

Fig. 6 ist ein Ablaufschema eines beispielhaften Verfahrens zum sicheren Transportieren

von Kommunikationen von einer Prozessanlage oder einem Prozesssteuersystem; und

Fig. 7 ist ein Ablaufschema eines beispielhaften Verfahrens zum sicheren Transportieren von Kommunikationen von einer Prozessanlage oder einem Prozesssteuersystem.

AUSFÜHRLICHE BESCHREIBUNG

[0019] Wie oben erörtert, wird beim Sichern von Prozesssteueranlagen und -systemen gegen Cyber-Eingriffe und bösartige Cyber-Attacken typischerweise eine geschichtete oder mehrstufige Sicherheitshierarchie benutzt, wobei wenigstens einige der Schichten oder Stufen mit Hilfe von Firewalls und anderen Sicherheitsmechanismen gesichert werden. Zum Beispiel, wie zuvor mit Bezug auf **Fig. 1** erörtert, können Prozessanlagensysteme, Netzwerke und Geräte auf den Sicherheitsstufen **0**-**3** gegen Bedrohungen von Unternehmensnetzen auf den Sicherheitsstufen **4**-**5** und/oder vor anderen externen Netzwerken höher als Stufe **5** geschützt werden, die die Unternehmensnetze nutzen, z.B. durch Verwenden einer DMZ **22** und von einer oder mehreren Firewalls **12A**-**12C**. Mit zunehmener Umstellung von immer mehr Diensten und Anwendungen, die auf Prozessanlagendaten wirken, auf Fernausführung, z.B. auf Netzwerken und Systemen außerhalb der Prozessanlage (z.B. auf den Stufen **4** und/oder **5** im Unternehmen oder Geschäft), und/oder selbst auf Netzwerken und Systemen, die sich außerhalb des Unternehmens oder Geschäfts befinden (z.B. über Level **5**, über das Internet oder ein anderes öffentliches Netzwerk), werden stärkere Techniken zum Verhüten einer Kompromittierung von Prozessanlagensystemen, Netzwerken und Geräten benötigt.

[0020] Die hierin beschriebenen neuen Systeme, Komponenten, Vorrichtungen, Methoden und Techniken gehen diese und andere Sicherheitsprobleme in Bezug auf Prozessanlagen und deren Netzwerke an und betreffen insbesondere das Sichern von Kommunikationen zwischen Prozessanlagen/Netzwerken und anderen Netzwerken oder Systemen.

[0021] Um dies zu verdeutlichen, **Fig. 2** ist ein Blockdiagramm einer beispielhaften Prozessanlage **100**, die zum Steuern eines Industrieprozesses bei Online-Vorgängen konfiguriert ist und mit beliebigen ein oder mehreren der hierin beschriebenen neuen Sicherheitstechniken gesichert werden können. Die Prozessanlage **100** (die hierin austauschbar auch als Prozesssteuersystem **100** oder als Prozesssteuerumgebung **100** bezeichnet wird), beinhaltet eine oder mehrere Prozesscontroller, die Signale empfangen, die von Feldgeräten vorgenommene Prozessmessungen anzeigen, diese Informationen zum Implementieren einer Steuerroutine verarbeiten und Steuersignale erzeugen, die über verdrahtete oder drahtlose Prozesssteuerkommunikationsverbindungen oder -netzwerke zu anderen Feldgeräten gesendet werden, um den Betrieb eines Prozesses in der Anlage **100** zu steuern. Typischerweise führt wenigstens ein Feldgerät eine physische Funktion (z.B. Öffnen oder Schließen eines Ventils, Erhöhen oder Verringern einer Temperatur, Vornehmen einer Messung, Erfassen eines Zustands usw.) durch, um den Betrieb eines Prozesses zu steuern. Einige Typen von Feldgeräten kommunizieren mit Controllern über E/A-Geräte. Prozesscontroller, Feldgeräte und E/A-Geräte können verdrahtet oder drahtlos sein, und es kann jede beliebige Anzahl und Kombination von verdrahteten und drahtlosen Prozesscontrollern, Feldgeräten und E/A-Geräten in der Prozessanlagenumgebung oder dem System **100** enthalten sein.

[0022] Zum Beispiel, **Fig. 2** illustriert einen Prozesscontroller **111**, der kommunikativ mit verdrahteten Feldgeräten **115**-**122** über Ein-/Ausgabe-(E/A)-Karten 126 und 128 verbunden ist und kommunikativ mit drahtlosen Feldgeräten **140**-**146** über einen drahtlosen Gateway 135 und einen Prozesssteuerdaten-Highway oder Backbone **110** verbunden ist. Der Prozesssteuerdaten-Highway **110** kann eine oder mehrere verdrahtete und/oder drahtlose Kommunikationsverbindungen beinhalten und kann mit einem beliebigen gewünschten oder geeigneten Kommunikationsprotokoll wie zum Beispiel einem Ethernet-Protokoll implementiert werden. In einigen Konfigurationen (nicht dargestellt) kann der Controller **111** kommunikativ mit dem drahtlosen Gateway **135** über ein oder mehrere andere Kommunikationsnetze verbunden werden als dem Backbone **110**, wie zum Beispiel durch Verwenden einer beliebigen Anzahl von anderen verdrahteten oder drahtlosen Kommunikationsverbindungen, die ein oder mehrere Kommunikationsprotokolle unterstützen, z.B. WiFi oder andere drahtlose Lokalnetzprotokolle gemäß IEEE **802.11**, mobile Kommunikationsprotokolle (z.B. WiMAX, LTE oder ein anderes ITU-R-kompatibles Protokoll), Bluetooth®, HART®, WirelessHART®, Profibus, FOUNDATION® Fieldbus, usw.

[0023] Der Controller **111**, der beispielsweise der von Emerson Process Management verkaufte Controller DeltaV™ sein kann, kann so arbeiten, dass er einen Chargenprozess oder einen kontinuierlichen Prozess unter Verwendung von wenigstens einigen der Feldgeräte **115**-**122** und **140**-**146** implementiert. In einer Ausgestaltung kann der Controller 111 nicht nur kommunikativ mit dem Prozesssteuerdaten-Highway **110** verbunden sein, sondern auch kommunikativ mit wenigstens einigen der Feldgeräte **115**-**122** und **140**-**146** mit einer gewünschten damit assoziierten Hardware und Software verbunden sein, zum Beispiel standardmäßigen 4-20 mA Geräten, E/A-Karten 126, 128 und/oder einem intelligenten Kommunikationsprotokoll wie dem FOUNDATION® Fieldbus Protokoll, dem HART® Protokoll, dem WirelessHART® Protokoll usw. In **Fig. 2** sind der Controller

111, die Feldgeräte **115**-**122** und die E/A-Karten 126, 128 verdrahtete Geräte, und die Feldgeräte **140**-146 sind drahtlose Feldgeräte. Die verdrahteten Feldgeräte **115**-**122** und die drahtlosen Feldgeräte **140**-**146** könnten natürlich jedem anderen gewünschten Standard oder Protokoll entsprechen, wie zum Beispiel beliebigen verdrahteten oder drahtlosen Protokollen, einschließlich beliebigen in der Zukunft entwickelten Standards oder Protokollen.

[0024] Der Prozess-Controller **111** von **Fig. 2** beinhaltet einen Prozessor **130**, der eine oder mehrere Prozesssteuerroutinen **138** implementiert oder überwacht (z.B. die in einem Speicher 132 gespeichert sind). Der Prozessor **130** ist zum Kommunizieren mit den Feldgeräten **115**-122 und 140-146 und mit anderen Knoten konfiguriert, die kommunikativ mit dem Controller 111 verbunden sind. Es ist zu bemerken, dass Teile von beliebigen der hierin beschriebenen Steuerroutinen oder -module von anderen Controllern oder anderen Geräten implementiert oder ausgeführt werden kann, wenn dies gewünscht wird. Ebenso können die hierin beschriebenen Steuerroutinen oder -module 138, die in dem Prozesssteuersystem **100** implementiert werden sollen, jede gewünschte Form annehmen, einschließlich Software, Firmware, Hardware usw. Steuerroutinen können in einem beliebigen gewünschten Software-Format implementiert werden, wie zum Beispiel unter Verwendung von objektorientierter Programmierung, Kontaktplan, sequentiellen Funktionsübersichten, Funktionsblockdiagrammen oder unter Verwendung einer beliebigen anderen Software-Programmiersprache oder Design-Paradigma. Die Steuerroutinen **138** können in einem beliebigen gewünschten Speichertyp **132** wie einem Arbeitsspeicher (RAM) oder einem Festwertspeicher (ROM) gespeichert werden. Ebenso können die Steuerroutinen **138** beispielsweise in eine oder mehrere EPROMs, EEPROMs, anwendungsspezifische integrierte Schaltungen (ASICs) oder beliebige andere Hardware- oder Firmware-Elemente festcodiert werden. So kann der Controller **111** zum Implementieren einer Steuerstrategie oder Steuerroutine auf eine beliebige gewünschte Weise konfiguriert werden.

[0025] Der Controller **111** implementiert eine Steuerstrategie unter Verwendung dessen, was üblicherweise als Funktionsblöcke bezeichnet wird, wobei jeder Funktionsblock ein Objekt oder ein anderer Teil (z.B. eine Subroutine) einer Gesamtsteuerroutine ist und zusammen mit anderen Funktionsblöcken (über als Links bezeichnete Kommunikationen) arbeitet, um Prozesssteuerschleifen im Prozesssteuersystem **100** zu implementieren. Steuerungsbasierte Funktionsblöcke führen typischerweise eine der folgenden Funktionen aus: eine Eingabefunktion, wie zum Beispiel die, die mit einem Sender, einem Sensor oder einem anderen Prozessparametermessgerät assoziiert ist; eine Steuerfunktion wie die, die mit einer Steuerroutine assoziiert ist, die PID ausführt, Fuzzy-Logic, usw; oder eine Ausgabefunktion, die den Betrieb eines Geräts steuert, wie zum Beispiel ein Ventil, um eine physische Funktion innerhalb des Prozesssteuersystems **100** auszuführen. Es existieren natürlich auch Hybrid- und andere Typen von Funktionsblöcken. Funktionsblöcke können im Controller **111** gespeichert sein und sie ausführen, was typischerweise dann der Fall ist, wenn diese Funktionsblöcke für standardmäßige 4-20 mA Geräte benutzt werden oder damit assoziiert sind, oder andere Typen von intelligenten Feldgeräten wie HART® Geräte, oder sie können in den Feldgeräten selbst gespeichert sein und von diesen implementiert werden, wie dies bei FOUNDATION® Fieldbus-Geräten der Fall sein kann. Der Controller **111** kann eine oder mehrere Steuerroutinen **138** beinhalten, die eine oder mehrere Steuerschleifen implementieren können, die durch Ausführen von einem oder mehreren der Funktionsblöcke durchgeführt werden.

[0026] Die verdrahteten Feldgeräte **115**-**122** können beliebige Typen von Geräten sein, wie Sensoren, Ventile, Sender, Stellungsregler usw., während die E/A-Karten 126 und 128 beliebige Typen von E/A-Geräten sein können, die einem gewünschten Kommunikations- oder Controller-Protokoll entsprechen. In **Fig. 2** sind die Feldgeräte **115**-**118** standardmäßige 4-20 mA Geräte oder HART® Geräte, die über Analogleitungen oder kombinierte Analog- und Digitalleitungen mit der E/A-Karte 126 kommunizieren, während die Feldgeräte **119**-**122** intelligente Geräte wie zum Beispiel FOUNDATION® Fieldbus-Feldgeräte sind, die über eine digitale Sammelschiene mit der E/A-Karte 128 mittels eines FOUNDATION® Fieldbus Kommunikationsprotokolls kommunizieren. In einigen Ausgestaltungen kommunizieren jedoch wenigstens einige der verdrahteten Feldgeräte **116**, **116** und **118**-**121** und/oder wenigstens einige der E/A-Karten 126, 128 zusätzlich oder alternativ mit dem Controller **111** über den Prozesssteuerdaten-Highway **110** und/oder über andere geeignete Steuersystemprotokolle (z.B. Profibus, DeviceNet, Foundation Fieldbus, ControlNet, Modbus, HART, usw.).

[0027] In **Fig. 2** kommunizieren die drahtlose Feldgeräte **140**-**146** über ein drahtloses Prozesssteuerkommunikationsnetz **170** über ein drahtloses Protokoll wie das WirelessHART® Protokoll. Solche drahtlosen Feldgeräte **140**-**146** können direkt mit einem oder mehreren anderen Geräten oder Knoten des drahtlosen Netzwerks **170** kommunizieren, die auch zum drahtlosen Kommunizieren konfiguriert sind (z.B. über das drahtlose Protokoll oder ein anderes drahtloses Protokoll). Zum Kommunizieren mit anderen Knoten, die nicht zum drahtlosen Kommunizieren konfiguriert sind, können die drahtlosen Feldgeräte **140**-**146** einen drahtlosen Gateway **135** benutzen, der mit dem Prozesssteuerdaten-Highway **110** oder mit einem anderen Prozesssteuerkommunikati-

onsnetz verbunden ist. Der drahtlose Gateway 135 bietet Zugang zu verschiedenen drahtlosen Geräten **140**-**158** des drahtlosen Kommunikationsnetzes **170**. Insbesondere stellt der drahtlose Gateway **135** eine kommunikative Kopplung zwischen den drahtlosen Geräten **140**-**158**, den verdrahteten Geräten **115**-**128** und/oder anderen Knoten oder Geräten der Prozesssteueranlage **100** bereit. Zum Beispiel, der drahtlose Gateway **135** kann kommunikative Kopplung unter Verwendung des Prozesssteuerdaten-Highway **110** und/oder mit Hilfe von einem oder mehreren anderen Kommunikationsnetzen der Prozessanlage **100** bereitstellen.

[0028] Ähnlich den verdrahteten Feldgeräten **115**-**122**, führen die drahtlosen Feldgeräte 140-146 des drahtlosen Netzwerks **170** physische Steuerfunktionen innerhalb der Prozessanlage **100** durch, z.B. Öffnen oder Schließen von Ventilen oder Vornehmen von Messungen von Prozessparametern. Die drahtlosen Feldgeräte **140**-**146** sind jedoch zum Kommunizieren mit dem drahtlosen Protokoll des Netzwerks **170** konfiguriert. Somit sind die drahtlosen Feldgeräte **140**-**146**, der drahtlose Gateway **135** und andere drahtlose Knoten **152**-158 des drahtlosen Netzwerks **170** Erzeuger und Verbraucher von drahtlosen Kommunikationspaketen.

[0029] In einigen Konfigurationen der Prozessanlage **100** beinhaltet das drahtlose Netzwerk **170** nicht drahtlose Geräte. Zum Beispiel, in **Fig. 2** ist ein Feldgerät **148** von **Fig. 2** ein 4-20 mA Legacy-Gerät und ein Feldgerät **150** ist ein verdrahtetes HART® Gerät. Zum Kommunizieren innerhalb des Netzwerks **170** werden die Feldgeräte **148** und **150** über einen jeweiligen drahtlosen Adapter **152A**, **152B** mit dem drahtlosen Kommunikationsnetz **170** verbunden. Die drahtlosen Adapter **152A**, **152B** unterstützen ein drahtloses Protokoll wie WirelessHART und können auch ein oder mehrere andere Kommunikationsprotokolle wie Foundation® Fieldbus, PROFIBUS, DeviceNet, usw. unterstützen. Zusätzlich beinhaltet das drahtlose Netzwerk **170** in einigen Konfigurationen einen oder mehrere Netzwerkzugangspunkte **155A**, **155B**, die separate physische Geräte in verdrahteter Kommunikation mit dem drahtlosen Gateway **135** oder mit dem drahtlosen Gateway **135** als integriertes Gerät vorgesehen sein können. Das drahtlose Netzwerk **170** kann auch einen oder mehrere Router **158** zum Weiterleiten von Paketen von einem drahtlosen Gerät zu einem anderen drahtlosen Gerät innerhalb des drahtlosen Kommunikationsnetzes **170** beinhalten. In **Fig. 2** kommunizieren die drahtlosen Geräte **140**-**146** und **152**-**158** miteinander und mit dem drahtlosen Gateway **135** über drahtlose Links **160** des drahtlosen Kommunikationsnetzes **170** und/oder über den Prozesssteuerdaten-Highway **110**.

[0030] In **Fig. 2** beinhaltet das Prozesssteuersystem **100** eine oder mehrere Operator-Workstations **171**, die kommunikativ mit dem Data-Highway **110** verbunden sind. Über die Operator-Workstations **171** können Bediener Laufzeitvorgänge der Prozessanlage **100** betrachten und überwachen und eventuelle diagnostische, korrektive, wartungsbezogene und/oder andere eventuell erforderliche Maßnahmen treffen. Wenigstens einige der Operator-Workstations **171** können sich in verschiedenen geschützten Bereichen in oder nahe der Anlage **100** befinden, z.B. in einer Backend-Umgebung der Anlage **100**, und in einigen Situationen können sich wenigstens einige der Operator-Workstations **171** an einer fernen Stelle, aber trotzdem in kommunikativer Verbindung mit der Anlage **100** befinden. Operator-Workstations **171** können verdrahtete oder drahtlose Rechengeräte sein.

[0031] Das beispielhafte Prozesssteuersystem **100** ist weiter so illustriert, dass es eine Konfigurationsanwendung **172A** und eine Konfigurationsdatenbank **172B** beinhaltet, die jeweils auch kommunikativ mit dem Data-Highway **110** verbunden sind. Wie oben erörtert, können verschiedene Instanzen der Konfigurationsanwendung **172A** auf einem oder mehreren Rechengeräten (nicht gezeigt) laufen, um Benutzer zu befähigen, Prozesssteuermodule zu erzeugen oder zu ändern und diese Module über den Data-Highway 110 auf die Controller **111** herunterzuladen, sowie Benutzer zu befähigen, Bedieneroberflächen zu erzeugen oder zu ändern, über die ein Bediener Daten betrachten und Dateneinstellungen innerhalb von Prozesssteuerroutinen ändern kann. Die Konfigurationsdatenbank **172B** speichert die erzeugten (z.B. konfigurierten) Module und/oder Bedieneroberflächen. Im Allgemeinen sind die Konfigurationsanwendung **172A** und Konfigurationsdatenbank **172B** zentralisiert und haben für das Prozesssteuersystem **100** ein einheitliches logisches Erscheinungsbild, obwohl mehrere Instanzen der Konfigurationsanwendung **172A** gleichzeitig in dem Prozesssteuersystem **100** laufen können und die Konfigurationsdatenbank **172B** über mehrere physische Datenspeichergeräte implementiert werden kann. Demgemäß umfassen die Konfigurationsanwendung **172A**, die Konfigurationsdatenbank **172B** und Benutzeroberflächen davon (nicht gezeigt) ein Konfigurations- oder Entwicklungssystem **172** für Steuer- und/oder Anzeigemodule. Typischerweise, aber nicht unbedingt, unterscheiden sich die Benutzeroberflächen für das Konfigurationssystem **172** von den Operator-Workstations **171**, da die Benutzeroberflächen für das Konfigurationssystem **172** von Konfigurations- und Entwicklungsingenieuren unabhängig davon benutzt werden, ob die Anlage **100** in Echtzeit arbeitet oder nicht, während die Operator-Workstations **171** von Bedienern bei Echtzeitvorgängen der Prozessanlage **100** benutzt werden (die hierin auch austauschbar als „Laufzeit“-Vorgänge der Prozessanlage **100** bezeichnet werden).

[0032] Das beispielhafte Prozesssteuersystem **100** beinhaltet eine Data-Historian-Anwendung **173A** und eine Data-Historian-Datenbank **173B**, die jeweils auch mit dem Data-Highway **110** kommunikativ verbunden sind. Die Data-Historian-Anwendung **173A** dient zum Sammeln einiger oder aller der über den Daten-Highway **110** bereitgestellten Daten und zum Historisieren oder Speichern der Daten in der Historian-Datenbank **173B** zur Langzeitspeicherung. Ähnlich wie die Konfigurationsanwendung **172A** und die Konfigurationsdatenbank **172B**, sind die Data-Historian-Anwendung **173A** und die Historian-Datenbank **173B** zentralisiert und haben für das Prozesssteuersystem **100** ein einheitliches logisches Erscheinungsbild, obwohl mehrere Instanzen einer Data-Historian-Anwendung **173A** gleichzeitig im Prozesssteuersystem **100** laufen können, und der Data-Historian **173B** kann über mehrere physische Datenspeichergeräte implementiert werden.

[0033] In einigen Konfigurationen beinhaltet das Prozesssteuersystem **100** einen oder mehrere andere drahtlose Zugangspunkte **174**, die mit anderen Geräten über andere drahtlose Protokolle wie WiFi oder andere drahtlose Lokalnetzprotokolle gemäß IEEE **802.11**, mobile Kommunikationsprotokolle wie WiMAX (Worldwide Interoperability for Microwave Access), LTE (Long Term Evolution) oder andere mit ITU-R (International Telecommunication Union Radiocommunication Sector) kompatible Protokolle, Kurzwellenlängen-Funkkommunikationen wie Nahfeldkommunikationen (NFC) und Bluetooth oder andere drahtlose Kommunikationsprotokolle kommunizieren. Typischerweise können es solche drahtlosen Zugangspunkte **174** zulassen, dass handgehaltene oder andere portable Rechengeräte (z.B. Benutzeroberflächengeräte **175**) über ein jeweiliges drahtlose Prozesssteuerkommunikationsnetz kommunizieren, das sich von dem drahtlosen Netzwerk 170 unterscheidet und ein anderes drahtloses Protokoll unterstützt als das drahtlose Netzwerk 170. Zum Beispiel, ein drahtloses oder portables Benutzeroberflächengerät **175** kann eine mobile Workstation oder ein Diagnosetestgerät sein, das von einem Bediener in der Prozessanlage **100** benutzt wird (z.B. eine Instanz von einer der Operator-Workstations **171**). In einigen Szenarios kommunizieren ein oder mehrere Prozesssteuergeräte (z.B. Controller 111, Feldgeräte **115**-**122** oder drahtlose Geräte **135**, **140**-**158**) nicht nur mit portablen Rechengeräten, sondern auch über das von den Zugangspunkten **174** unterstützte drahtlose Protokoll.

[0034] In einigen Konfigurationen beinhaltet das Prozesssteuersystem **100** einen oder mehrere Gateways **176**, **178** zu Systemen, die sich außerhalb des unmittelbaren Prozesssteuersystems **100** befinden. Solche Systeme sind typischerweise Kunden oder Zulieferer von Informationen, die von dem Prozesssteuersystem **100** erzeugt werden oder darauf wirken. Zum Beispiel, die Prozesssteueranlage **100** kann einen Gateway-Knoten **176** zum kommunikativen Verbinden der unmittelbaren Prozessanlage **100** mit einer anderen Prozessanlage beinhalten. Zusätzlich oder alternativ kann die Prozesssteueranlage **100** einen Gateway-Knoten **178** zum kommunikativen Verbinden der unmittelbaren Prozessanlage **100** mit einem externen öffentlichen oder privaten System wie einem Laborsystem (z.B. Laboratory Information Management System oder LIMS), einer Operator-Rounds-Datenbank, einem Materialhandhabungssystem, einem Wartungsmanagementsystem, einem Produktinventarsteuersystem, einem Produktionsplanungssystem, einem Wetterdatensystem, einem Versand- oder Handhabungssystem, einem Verpackungssystem, dem Internet, dem Prozesssteuersystem eines anderen Anbieters oder anderen externen Systemen kommunizieren.

[0035] Es ist anzumerken, dass **Fig. 2** zwar nur einen einzigen Controller **111** mit einer finiten Anzahl von Feldgeräten **115**-**122** und **140**-**146**, drahtlosen Gateways **35**, drahtlosen Adaptern **152**, Zugangspunkten **155**, Routern **1158** und drahtlosen Prozesssteuerkommunikationsnetzen **170** illustriert, die in der beispielhaften Prozessanlage 100 enthalten sind, aber dies ist lediglich eine illustrative und nichtbegrenzende Ausgestaltung. Es kann eine beliebige Anzahl von Controllern **111** in der/dem Prozesssteueranlage oder -system 100 enthalten sein und beliebige der Controller **111** können mit einer beliebigen Anzahl von verdrahteten oder drahtlosen Geräten und Netzwerken **115**-122, 140-146, 135, 152, 155, 158 und 170 kommunizieren, um einen Prozess in der Anlage 100 zu steuern.

[0036] **Fig. 3** illustriert ein Blockdiagramm einer beispielhaften Sicherheitsarchitektur **200** für die beispielhafte Prozessanlage **100** von **Fig. 1**. Zur Bezugnahme sind die verschiedenen Sicherheitsstufen **0**-**5** von **Fig. 1** am oberen Rand von **Fig. 3** dargestellt, um anzuzeigen, in welchen Sicherheitsstufen verschiedene Teile der Sicherheitsarchitektur **200** enthalten sein können, aber diese Referenz ist lediglich eine Richtlinie, da verschiedene Teile der Sicherheitsarchitektur **200** in anderen Sicherheitsstufen als den in **Fig. 3** gezeigten beherbergt sein können.

[0037] Wie in **Fig. 3** gezeigt, sind ein oder mehrere Geräte **202** kommunikativ mit einem oder mehreren drahtlosen Gateways **205A**, **205B** verbunden, die beispielsweise Instanzen des drahtlosen Gateway **135** von **Fig. 1** sein können. Wie zuvor erörtert, können sich die drahtlosen Gateways **205A**, **205B** in Sicherheitsstufe **1** und/oder Sicherheitsstufe **2** befinden, z.B. in der Prozessanlage **100** selbst. Die kommunikativen Verbindungen zwischen den Gateways **205A**, **205B** und den Geräten **202** sind mit den Bezugszeichen **204A**, **204B** denotiert.

[0038] Der Satz von Geräten **202** ist in Sicherheitsstufe **0** der Prozessanlage **100** gezeigt und so dargestellt, dass er eine finite Anzahl von drahtlosen Feldgeräten umfasst. Es ist jedoch zu verstehen, dass die hierin mit Bezug auf die Geräte **202** beschriebenen Konzepte und Merkmale leicht auf jede beliebige Anzahl von Feldgeräten der Prozessanlage **100** sowie auf beliebige Typen von Feldgeräten anwendbar sind. Zum Beispiel, die Feldgeräte **202** können ein oder mehrere der verdrahteten Feldgeräte **115**-**122** beinhalten, die kommunikativ über ein oder mehrere verdrahtete Kommunikationsnetze **110** der Prozessanlage **100** mit den drahtlosen Gateways **204A**, **205B** verbunden sind, und/oder die Feldgeräte **202** können die verdrahteten Feldgeräte **148**, **150** beinhalten, die mit drahtlosen Adaptern **152A**, **152B** und dadurch mit den drahtlosen Gateways **205A**, **205B** gekoppelt sind.

[0039] Ferner ist zu verstehen, dass der Satz von Geräten **202** nicht nur auf Feldgeräte begrenzt ist, die Prozessdaten erzeugen, sondern zusätzlich oder alternativ auch jede(s) Gerät oder Komponente in der Prozessanlage **100** beinhalten kann, die Daten infolge davon erzeugt, dass die Prozessanlage **100** den Online-Prozess steuert. Zum Beispiel, der Satz von Geräten 202 kann ein(e) Diagnosegerät oder -komponente enthalten, das/die Diagnosedaten erzeugt, ein(e) Netzwerkroutinggerät oder -komponente, das/die Informationen zwischen verschiedenen Komponenten und/oder Geräten der Prozessanlage **100** überträgt, und dergleichen. In der Tat können beliebige ein oder mehrere der in **Fig. 2** gezeigten Komponenten (z.B. Komponenten **111**, **115**-**122**, **126**, **128**, **135**, **140**-**146**, **152**, **155**, **158**, **160**, 170, 171-176, 178) und andere nicht in **Fig. 2** gezeigte Komponenten ein Gerät oder eine Komponente **202** sein, das/die Daten zur Lieferung an das ferne System **210** erzeugt. Somit wird der Satz von Geräten **202** hierin austauschbar als „Datenquellen 202“ oder „Datenquellgeräte 202“ bezeichnet.

[0040] **Fig. 3** illustriert ferner einen Satz von fernen Anwendungen oder Diensten **208**, die mit Bezug auf die Prozessanlage **100** benutzt werden können und/oder die die Prozessanlage 100 nutzt. Der Satz von fernen Anwendungen oder Diensten **208**, die an einem oder mehreren fernen Systemen **210** laufen oder gehostet werden können, und der Satz von fernen Anwendungen/Diensten **208** werden allgemein ausgedrückt als auf Sicherheitsstufe **5** oder darüber befindlich angesehen. Wenigstens einige der Anwendungen oder Dienste **208** arbeiten in Echtzeit an Echtzeitdaten, sobald die Echtzeitdaten von der Prozessanlage **100** erzeugt und von den Anwendungen oder Diensten **208** empfangen wurden. Andere Anwendungen oder Dienste **208** können an Prozessanlagen-erzeugten Daten mit weniger stringenten Zeitanforderungen arbeiten oder laufen. Beispiele für Anwendungen/Dienste **208**, die an dem fernen System **210** laufen oder gehostet werden können und die Verbraucher von von der Prozessanlage **100** erzeugten Daten sind, beinhalten Anwendungen, die an der Prozessanlage **100** auftretende Zustände und/oder Ereignisse überwachen und/oder erfassen, und Anwendungen oder Dienste, die wenigstens einen Teil des Online-Prozesses selbst überwachen, während dieser an der Prozessanlage **100** läuft. Zu anderen Beispielen von Anwendungen/Diensten **208** gehört deskriptive und/oder präskriptive Analytik, die an von der Prozessanlage **100** erzeugten Daten arbeiten und in einigen Fällen auf Wissen wirken kann, das von der Analyse der Prozessanlage-erzeugten Daten gesammelt oder entdeckt wurde, sowie an Daten, die von anderen Prozessanlagen erzeugt und empfangen wurden. Noch andere Beispiele von Anwendungen/Diensten **208** beinhalten eine oder mehrere Routinen, die präskriptive Funktionen, Modifikationen von Konfigurationen und/oder andere Daten implementieren, und/oder andere präskriptive Änderungen, die zurück in die Prozessanlage **100** implementiert werden sollen, z.B. infolge eines/r anderen Dienstes oder Anwendung. Einige Beispiele für Anwendungen und Dienste **208** sind in der US-Patentanmeldung Nr. 15/274,519, die am 23. September **2016** unter dem Titel „Data Analytics Services for Distributed Industrial Performance Monitoring“ eingereicht wurde, in der US-Patentanmeldung Nr. 15/274, 233, die am 23. September **2016** unter dem Titel „Distributed Industrial Performance Monitoring and Analytics“ eingereicht wurde, und in der US-Patentanmeldung Nr. 15/332,521 beschrieben, die am 24. Oktober **2016** unter dem Titel „Process Device Condition and Performance Monitoring“ eingereicht wurde, deren gesamte Offenbarungen hierin durch Bezugnahme eingeschlossen sind.

[0041] Die ein oder mehreren fernen Systeme **210** können auf eine beliebige gewünschte Weise implementiert werden, wie zum Beispiel von einer fernen Bank von vernetzten Servern, einem oder mehreren Cloud-Computing-Systemen, einem oder mehreren Netzwerken usw. Zum Erleichtern der Erörterung werden die ein oder mehreren fernen Systeme **210** hierin im Singular bezeichnet, d.h. „fernes System 210“, obwohl zu verstehen ist, dass der genannte Begriff sich auf ein System, auf mehr als ein System oder auf eine beliebige Anzahl von Systemen beziehen kann.

[0042] Allgemein ausgedrückt, die Sicherheitsarchitektur **200** bietet dem fernen System 210, das Anwendungen und/oder Dienste **208** bereitstellt, die von der Prozessanlage **100** erzeugte Daten verbraucht und daran arbeitet, Ende-zu-Ende-Sicherheit vor der Feldumgebung der Prozessanlagen **100**, in denen Geräte **202** installiert sind und arbeiten. Somit können Daten, die von den Geräten **202** und anderen Komponenten der Prozessanlage 100 erzeugt werden, sicher zum Fernsystem **210** zur Verwendung durch die

fernen Anwendungen/Dienste **208** transportiert werden, während die Anlage **100** vor Cyber-Attacken, Eingriffen und/oder anderen bösartigen Ereignissen geschützt wird. Insbesondere beinhaltet die Sicherheitsarchitektur **200** einen Field-Gateway **212**, eine Datendiode **215** und einen Edge-Gateway **218**, angeordnet zwischen der Prozessanlage **100** (z.B. zwischen den drahtlosen Gateways **205A**, **205B** der Prozessanlage **100**) und dem fernen System **210**. Typischerweise, aber nicht unbedingt, sind der Field-Gateway **212**, die Datendiode **215** und der Edge-Gateway **218** in den Sicherheitsstufen **2**-**5** enthalten.

[0043] Ein Hauptaspekt der Sicherheitsarchitektur **200** ist die Datendiode **215**. Die Datendiode **215** ist eine Komponente, die in Hardware, Firmware und/oder Software implementiert und insbesondere so konfiguriert ist, dass sie Zweiweg-Kommunikationen zwischen der Prozessanlage **100** und dem fernen System **210** verhindert. Das heißt, die Datendiode **215** lässt den Austritt von Datenverkehr vom Prozesssteuersystem **100** zum fernen System **210** zu und verhindert den Eintritt von Datenverkehr (z.B. der von dem fernen System **210** oder anderen Systemen übertragen oder gesendet wird) in das Prozesssteuersystem **100**.

[0044] Demgemäß beinhaltet die Datendiode **215** wenigstens einen Eingangsport **220**, der kommunikativ mit dem Field-Gateway **212** verbunden ist, und wenigstens einen Ausgangsport **222**, der kommunikativ mit dem Edge-Gateway **218** verbunden ist. Die Datendiode **215** beinhaltet auch eine Lichtwellenleiter- oder Kommunikationsverbindung einer beliebigen anderen geeigneten Technologie, die ihren Eingangsport **222** mit ihrem Ausgangsport **222** verbindet. Um den Fluss von Datenverkehr zu (z.B. den Eintritt in das) dem Prozesssteuersystem **100** zu verhindern, schließt die Datendiode **215** in einer beispielhaften Implementation einen Eingangsport aus oder lässt ihn weg, um Daten vom Edge-Gateway **218** (oder einer anderen Komponente auf einer höheren Sicherheitsstufe) zu empfangen, und/oder schließt einen Ausgangsport aus oder lässt ihn weg, um Daten zum Field-Gateway **212** (oder zu einer anderen Komponente auf einer tieferen Sicherheitsstufe) zu übertragen. In einer zusätzlichen oder alternativen Implementation schließt die Datendiode 215 Transceiver, die sonst den Fluss von Daten vom Ausgangsport **222** zum Eingangsport 220 zulassen würden, aus, lässt sie weg und/oder sperrt sie, und/oder schließt einen physischen Kommunikationspfad für Daten vom Fluss vom Ausgangsport **222** zum Eingangsport **220** aus. Darüber hinaus oder alternativ kann die Datendiode **215** nur einen unidirektionalen Datenfluss vom Eingangsport **220** zum Ausgangsport **222** über Software unterstützen, z.B. durch Fallenlassen oder Blockieren von Nachrichten, die am Ausgangsport 222 vom Edge-Gateway **218** (oder einer Komponente einer höheren Sicherheitsstufe) empfangen werden, und/oder durch Fallenlassen oder Blockieren von Nachrichten, die an den Field-Gateway **212** (oder eine Komponente einer tieferen Sicherheitsstufe) adressiert sind.

[0045] Daten, die aus der Prozessanlage **100** austreten und über die Datendiode **215** vom Eingangsport **220** zum Ausgangsport **222** übertragen werden, können ferner durch Verschlüsseln über die Datendiode **215** weiter gesichert werden. In einem Beispiel verschlüsselt der Field-Gateway **212** Daten und liefert verschlüsselte Daten zum Eingangsport **220**. In einem anderen Beispiel empfängt die Datendiode **215** Datenverkehr vom Field-Gateway **212** und die Datendiode **215** verschlüsselt den empfangenen Datenverkehr vor dem Übertragen der Daten zum Ausgangsport **222**. Der Datenverkehr, der über die Datendiode **215** verschlüsselt und transportiert wird, kann in einem Beispiel UDP-(User Datagram Protocol)-Datenverkehr und in einem anderen Beispiel JSON-Datenverkehr oder ein anderes allgemeines Kommunikationsformat sein.

[0046] Der Field-Gateway **212** verbindet die Niedersicherheitsseite der Datendiode **215** kommunikativ mit der Prozesssteueranlage **100**. Wie in **Fig. 3** gezeigt, ist der Field-Gateway 212 kommunikativ mit den drahtlosen Gateways **205A**, **205B** verbunden, die in der Feldumgebung der Prozessanlage **100** angeordnet und kommunikativ mit einem oder mehreren Geräten oder Datenquellen **202** verbunden sind. Wie zuvor erörtert, können die Geräte oder Datenquellen **202** und die drahtlosen Gateways **205A**, **205B** mit dem industriellen WirelessHART-Protokoll oder einem anderen geeigneten drahtlosen Protokoll kommunizieren, das zum Bereitstellen von gesicherten Kommunikationen über einen oder mehrere Sicherheitsmechanismen strukturiert ist. Zum Beispiel, das Industrieprotokoll WirelessHART bietet 128-Bit-AES-Verschlüsselung und die Kommunikationspfade **204A**, 204B können entsprechend gesichert werden.

[0047] Zusätzlich wird die kommunikative Verbindung **225** zwischen den drahtlosen Gateways **205A**, **205B** und dem Field-Gateway **212** jeweils mit demselben oder einem anderen Sicherheitsmechanismus wie dem gesichert, der für die kommunikativen Verbindungen **204A**, **204B** benutzt wird. In einem Beispiel wird die kommunikative Verbindung **225** durch einen TLS-(Transport Layer Security)-Wrapper gesichert. Zum Beispiel, die drahtlosen Gateways **205A**, **205B** erzeugen Pakete im HART-IP-Format, die von einem TLS-Wrapper für die Übertragung zum Field-Gateway **212** gesichert werden.

[0048] So können in einer Ausgestaltung, wie oben beschrieben, von den Geräten **202** erzeugte Daten oder Pakete für den Transit **204A**, **204B** zu den drahtlosen Gateways **205A**, 205B mit einem ersten Sicherheitsmechanismus gesichert und nachfol-

gend für den Transit 225 von den drahtlosen Gateways **205A**, **205B** zum Field-Gateway **212** mit einem zweiten Sicherheitsmechanismus gesichert und dann nachfolgend für den Transit über die Datendiode 215 mit einem dritten Sicherheitsmechanismus gesichert werden.

[0049] Nun mit Bezug auf die Seite der Datendiode **215** mit höherer Sicherheit, der aus der Datendiode **215** austretende Datenverkehr kann für den Transit zum Edge-Gateway **218** bei Bedarf durch Verwenden eines vierten Sicherheitsmechanismus oder durch Verwenden eines der Sicherheitsmechanismen gesichert werden, die auf der Seite der Datendiode **215** mit geringerer Sicherheit wie oben erörtert eingesetzt werden. Zusätzlich oder alternativ, und wie in **Fig. 3** gezeigt, kann der Edge-Gateway **218** durch eine Firewall **228** geschützt werden, die die Firewall **12C** von **Fig. 1** oder eine andere Firewall sein kann.

[0050] Vom Edge-Gateway **218** zum fernen System **210** fließende Daten können mit einem oder mehreren öffentlichen und/oder privaten Netzwerken geliefert werden, wie zum Beispiel einem privaten Unternehmensnetz, dem Internet, einem zellulären Router, einem Backhaul-Internet oder einer Backhaul-Verbindung eines anderen Typs. Signifikanterweise werden die vom Edge-Gateway **218** zum fernen System **210** fließenden Daten durch Verwenden eines fünften Sicherheitsmechanismus oder durch Verwenden von einem der zuvor oben erörterten Sicherheitsmechanismen gesichert. **Fig. 3** zeigt den vom Edge-Gateway 218 zum fernen System **210** gelieferten Datenverkehr als über ein SAS- (Shared Access Signature)-Token gesichert, das durch einen am fernen System **210** bereitgestellten Token-Service **230** verwaltet werden kann. Der Edge-Gateway **218** authentifiziert sich beim Token-Server **230** und fordert ein SAS-Token an, das möglicherweise nur für eine begrenzte Zeitperiode wie z.B. zwei Minuten, fünf Minuten, dreißig Minuten, maximal eine Stunde usw. gültig ist. Der Edge-Gateway **218** empfängt und benutzt das SAS-Token zum Sichern und Authentifizieren einer AMQP-(Advanced Message Queuing Protocol) -Verbindung beim fernen System **210**, über die Inhaltsdaten vom Edge-Gateway **218** zum fernen System **210** übertragen werden. Natürlich ist die Verwendung von SAS-Tokens und des AMQP-Protokolls zum Sichern von zwischen dem Edge-Gateway **218** und dem fernen System **210** fließenden Daten nur einer von vielen möglichen Sicherheitsmechanismen. Zum Beispiel, es können beliebige ein oder mehrere geeignete IOT-(Internet-Of-Things)-Sicherheitsmechanismen zum Sichern von Daten benutzt werden, die zwischen dem Edge-Gateway **218** und dem fernen System **210** fließen, z.B. X.509-Zertifikate, andere Token-Typen, andere IOT-Protokolle wie MQTT (MQ Telemetry Transport) oder XMPP (Extensible Messaging and Presence Protocol), und dergleichen. In diesen anderen Ausgestaltungen stellt der Dienst **230** die entsprechenden Sicherheit-Tokens oder Zertifikate zum Beispiel bereit und/oder gibt sie aus.

[0051] Am fernen System **210** wird Benutzerauthentifizierung und/oder -autorisierung durch einen oder mehrere geeignete Authentifizierungs- und/oder Autorisierungssicherheitsmechanismen **232** bereitgestellt. Zum Beispiel, sicherer Zugang zum fernen System **210** kann von einem Domänenauthentifizierungsservice, einem API-Benutzerauthentifizierungsservice und/oder einem beliebigen anderen geeigneten Authentifizierungs- und/oder Autorisierungsservice **232** bereitgestellt werden. So können nur Benutzer **235**, die über den Authentifizierungs- und/oder Autorisierungsservice **232** authentifiziert und/oder autorisiert sind, auf wenigstens einige der Daten zugreifen, die am fernen System **210** zur Verfügung stehen, die u.a. die von den Geräten **202** erzeugten Daten beinhalten.

[0052] So bietet, wie oben beschrieben, die Sicherheitsarchitektur **200** Ende-zu-Ende-Sicherheit für Daten, die von Geräten oder Datenquellen **210** während des Betriebs in der Prozessanlage **100** zum Steuern eines Prozesses erzeugt werden, z.B. ab der Erzeugung der Daten durch die Datenquellen **202** über ihre Übertragung zum fernen System **210**, um von einer/m oder mehreren fernen Anwendungen oder Diensten **208** verarbeitet zu werden. Bedeutsamerweise bietet die Sicherheitsarchitektur **200** diese Ende-zu-Ende-Sicherheit und verhindert gleichzeitig bösartige Attacken an der Prozessanlage **100**.

[0053] Es wird angemerkt, dass **Fig. 3** zwar drahtlose Gateways **205A**, **205B** als die Geräte oder Datenquellen **202** kommunikativ mit dem Field-Gateway **212** verbindend darstellt, aber in einigen Anordnungen sind ein oder mehrere der drahtlosen Gateways **205A**, **205B** weggelassen und Quelldaten werden von den Datenquellen **202** direkt zum Field-Gateway 212 übertragen. Zum Beispiel, die Datenquellen **202** können Quelldaten über ein großes Datennetz der Prozessanlage **100** direkt zum Field-Gateway **212** übertragen. Allgemein ausgedrückt, ein großes Datennetz der Prozessanlage **100** ist nicht das Backbone-Anlagennetz **110**, noch ist das große Datennetz ein Industrieprotokollnetz, das zum Übertragen von Steuersignalen zwischen Geräten mit einem industriellen Kommunikationsprotokoll benutzt wird (z.B. Profibus, DeviceNet, Foundation Fieldbus, ControlNet, Modbus, HART, usw.). Stattdessen kann ein großes Datennetz der Prozessanlage **100** ein Overlay-Netzwerk sein, das für die Prozessanlage **100** implementiert wird, das Daten beispielsweise zwischen Knoten zur Datenverarbeitung und für analytische Zwecke streamt. Die Knoten eines großen Datennetzes können beispielsweise die Datenquellen **202**, die drahtlosen Gateways **205A**, **205B** und den Field-Gateway **212** sowie beliebige eine oder mehrere der Komponenten **111**, **115**-**122**, **126**, **128**, **135**, **140**-**146**,

152, 155, 158, 160, 170, 171-176, 178 wie in **Fig. 2** gezeigt und andere Komponenten beinhalten. Demgemäß beinhaltet für viele Knoten einer Prozessanlage das Datennetz jeweils eine designierte Schnittstelle für Prozessanlagenoperationen, die typischerweise ein industrielles Kommunikationsprotokoll nutzt, und eine andere designierte Schnittstelle für Datenverarbeitungs-/Analytikoperationen, die beispielsweise ein Streaming-Protokoll nutzen können. Ein Beispiel für ein großes Datennetz, das in einer Prozessanlage **100** benutzt werden kann, ist in der US-Patentanmeldung Nr. 14/507,188 mit dem Titel „Regional Big Data in Process Control Systems“ beschrieben, die am 6. Oktober **2014** eingereicht wurde und deren gesamte Offenbarung hierin durch Bezugnahme eingeschlossen ist.

[0054] Es wird ferner mit Bezug auf **Fig. 3** bemerkt, dass in einigen Ausgestaltungen ein verdrahtetes Gateway (nicht gezeigt) anstelle von einem der drahtlosen Gateways **205A**, 205B benutzt werden kann. Darüber hinaus können sich der Field-Gateway **212**, die Datendiode **215** und der Edge-Gateway **218** physisch an derselben Stelle befinden, wie durch den in **Fig. 3** gezeigten Kasten **235** angedeutet, oder eine oder mehrere der Komponenten 212, 215, 218 können sich physisch an mehreren Stellen befinden. Zum Beispiel, ein oder mehrere aus Field-Gateway **212**, Datendiode **215** oder Edge-Gateway **218** könn an der Prozessanlage **100** angeordnet sein. Zusätzlich oder alternativ können eines oder mehrere aus Field-Gateway **212**, Datendiode **215** oder Edge-Gateway **218** fern von der Prozessanlage **100** angeordnet sein.

[0055] Die Prozessanlage **100** kann bei Bedarf von mehr als einem Field-Gateway **212** bedient werden und jede beliebige Anzahl von Field-Gateways **212** kann von einem einzigen Edge-Gateway **218** bedient werden. In einigen Ausgestaltungen wird das ferne System **210** bei Bedarf von mehr als einem Edge-Gateway **218** bedient.

[0056] Wie zuvor erörtert, wird der über die Datendiode **215** transportierte Datenverkehr gesichert. Ein derartiger Datenverkehr kann über die Datendiode **215** beispielsweise durch Verwenden von serieller Kommunikation oder UDP-Kommunikation kommuniziert werden. Das Sichern solcher Kommunikationen ohne Zweiweg-Kommunikationen ist jedoch schwierig und aufwändig, da typischerweise sowohl UDP- als auch serielle Kommunikationen erfordern, dass beide Seiten nicht nur bidirektional kommunizieren (was mit der Datendiode **215** nicht möglich ist), sondern auch dass sie sich lange Schlüsselfolgen merken und eingeben. So können die transportierten Daten, anstatt traditionelle Zweiweg-Kommunikationen zum Sichern von Datentransport über die unidirektionale Datendiode **215** zu benutzen, über einen Sicherheitsprovisionierungsprozess gesichert werden, der zwischen dem Edge-Gateway **218** und dem Field-Gateway **212** benutzt wird. Der Sicherheitsprovisionierungsprozess erzeugt eindeutiges anfängliches Schlüssel- oder Geheimmaterial, das von Edge-Gateway **218** und Field-Gateway **212** gemeinsam genutzt wird (z.B. ein symmetrischer Schlüssel oder symmetrisches Material), wie zum Beispiel ein Join-Key. Mit Hilfe des Join-Key stellen der Edge-Gateway **218** und der Field-Gateway **212** eine sichere Verbindung her, die zum Austauschen von weiterem Key- oder Geheimmaterial benutzt wird, das wiederum zum sicheren Transportieren von Datenverkehr über die Datendiode **215** benutzt wird.

[0057] **Fig. 4** veranschaulicht einen beispielhaften Nachrichtenfluss **250**, der für den Sicherheitsprovisionierungsprozess benutzt werden kann. In **Fig. 4** sind der Field-Gateway und der Edge-Gateway **218** beide auf einem Provisionierungsnetz enthalten (z.B. im selben Subnetz, nicht gezeigt), wie auch ein Provisionierungsserver oder Rechengerät **252**, der/das von einem Benutzer betrieben wird, um dem Edge-Gateway **218** den Field-Gateway **212** zu provisionieren. Über das Provisionierungsnetzwerk können der Field-Gateway **212** und der Edge-Gateway **218** in einer Ausgestaltung vorübergehend bidirektional miteinander kommunizieren, um Provisionierung z.B. mit einer Kommunikation des TCP-Typs einzurichten.

[0058] Zum Beispiel, bei Bezugsziffer **255** loggt sich der Benutzer über das Provisionierungsgerät **252** bei der Benutzeroberfläche UI des Edge-Gateway **218** ein und wird gegenüber diesem authentifiziert. Zum Beispiel, die UI des Edge-Gateway **218** kann eine Webschnittstelle oder eine andere geeignete UI sein. Über die Provisionierungsseite oder Display-Ansicht des Edge-Gateway **218** gibt der Benutzer die Adresse des Field-Gateway 212 (Bezugsziffer **258**) ein (die in einem Beispiel eine IP-Adresse sein kann), um dadurch zu bewirken, dass der Edge-Gateway **218** einen Weißlisteneintrag für den Field-Gateway **212** erzeugt (Bezugsziffer **260**). Demzufolge fordert der Edge-Gateway **218** beim Provisionierungsgerät **252** die Anmeldedaten des Field-Gateway **212** an, die bei der Datenübertragung benutzt werden sollen (Bezugsziffer **262**).

[0059] Als Reaktion auf die Anforderung des Edge-Gateway stellt der Benutzer, über das Provisionierungsgerät **252**, Authorisierungs- und Sicherheitsinformationen für den Field-Gateway **212** bereit (Bezugsziffer **265**). Die genannten Authorisierungs- und Sicherheitsinformationen beinhalten typischerweise (aber nicht unbedingt) anfängliches Schlüsselmaterial, das mit dem Field-Gateway **212** gemeinsam zu benutzen ist. In einem Beispiel beinhaltet das anfängliche Schlüsselmaterial einen 128-Bit, 192-Bit oder 256-Bit Join-Key und beinhaltet einen 32-Bit oder 64-Bit Paketzähler, der als Teil einer Nonce für Paket-Verschlüsselung/Entschlüsselung und in einigen Fällen für MIC-(Message Integrity Check)-Berechnun-

gen benutzt wird, die an Paketen durchgeführt werden. Zum Beispiel, ein Wert des Paketzählers wird in der Nonce jeder Übertragung inkrementiert, geändert oder aktualisiert, um gegen Netzwerkwiedergabeattacken zu schützen. In jedem Fall verschlüsselt und speichert der Edge-Gateway **218** eine lokale Kopie des anfänglichen Schlüsselmaterials und sendet das anfängliche Schlüsselmaterial sowie eine oder mehrere Adressen des Edge-Gateway **218** (z.B. die IP-Adresse und/oder die MAC-Adresse des Edge-Gateway **218**) zum Field-Gateway **212** (Bezugsziffer **268**). Am Field-Gateway **212** verschlüsselt und speichert der Field-Gateway **212** eine lokale Kopie des anfänglichen Schlüsselmaterials sowie die Adressen des Edge-Gateway **218** und bestätigt den Empfang dem Edge-Gateway **218** (Bezugsziffer **270**).

[0060] Nachfolgend leitet der Field-Gateway **212** unidirektionale Kommunikationen mit dem Edge-Gateway **218** über die Datendiode **215** z.B. mit UDP ein. Insbesondere überträgt der Field-Gateway **212** eine Anfangsnachricht zum Edge-Gateway **218**, die einen neuen zufällig erzeugten Netzwerkschlüssel und zufällig erzeugten Paketzähler enthält (z.B. der in der Nonce und für MIC-Berechnungen benutzt werden soll), die zum Verschlüsseln und Integritätsprüfen von nachfolgenden Nachrichten zu benutzen sind. Der neue Netzwerkschlüssel und jeweilige Paketzähler werden mit dem anfänglichen Schlüsselmaterial verschlüsselt, z.B. dem Join-Key und seinem jeweiligen Paketzähler (Bezugsziffer **272**). Der Edge-Gateway **218** entschlüsselt die empfangene anfängliche Nachricht mit seinem lokal gespeicherten anfänglichen Schlüsselmaterial, speichert den neuen Netzwerkschlüssel und Paketzähler (Bezugsziffer **275**) und benutzt den gespeicherten Netzwerkschlüssel im Paketzähler zum Entschlüsseln von Nachrichten oder Paketen, die nachfolgend vom Field-Gateway **212** empfangen werden.

[0061] Man beachte, dass, wie in **Fig. 4** illustriert, wenn der Edge-Gateway **218** vom Field-Gateway **212** die erste Nachricht empfangen hat, die mit dem neuen Netzwerkschlüssel verschlüsselt wurde und den neuen Paketzähler enthält (Bezugsziffern **278**, **280**), der gesicherte Provisionierungsprozess als abgeschlossen angesehen werden kann und das Provisionierungsgerät **252** nicht länger am Nachrichtenfluss **250** beteiligt zu sein braucht. Folglich wird in einer Ausgestaltung ein vorübergehender Kommunikationskanal, der für Kommunikationen vom Edge-Gateway **218** zum Field-Gateway **212** benutzt wurde (z.B. der bei Bezugsziffer **268** benutzt wurde), abgebaut, gesperrt oder auf andere Weise unverfügbar gemacht. Der Field-Gateway **212** sendet jedoch weiter Daten über die unidirektionale Datendiode **215** zum Edge-Gateway **218** unter Verwendung des gespeicherten Netzwerkschlüssels und Paketzählers (Bezugsziffer **282**, der Edge-Gateway **218** entschlüsselt weiter empfangene Nachrichten mit seinem gespeicherten Netzwerkschlüssel und Paketzähler (Bezugsziffer **285**)).

[0062] In einigen Ausgestaltungen kehren jedoch der Field-Gateway **212** und der Edge-Gateway **218** zu unidirektionalen Kommunikationen über die Datendiode **215** nach dem Abtrennen des Provisionierungsgeräts **252** vom Netzwerk oder früher während des Nachrichtenflusses **250** zurück. Zum Beispiel, der Edge-Gateway **218** kann nach dem Übertragen des anfänglichen Join-Key-Materials zum Field-Gateway **212** (Bezugsziffer **268**) zu unidirektionalen Kommunikationen zurückkehren, und der Field-Gateway **212** kann nach dem Übertragen der Bestätigung des Empfangs des anfänglichen Schlüsselmaterials zu unidirektionalen Kommunikationen zurückkehren (Bezugsziffer **270**).

[0063] Für Robustheit und Zuverlässigkeit von Datenübertragungen über die unidirektionale Datendiode **216** erzeugt der Field-Gateway **212** eine andere Initialisierungsnachricht und einen jeweiligen zufälligen Paketzähler zum Einrichten eines neuen oder aktualisierten Netzwerkschlüsselmaterials mit dem Edge-Gateway **218**. Zum Beispiel, der Field-Gateway **212** überträgt eine andere Initialisierungsnachricht, die mit dem anfänglichen Join-Key-Material verschlüsselt wurde und einen neuen oder aktualisierten Netzwerkschlüssel und einen entsprechenden neuen oder aktualisierten Paketzähler (Bezugsziffer **288**) enthält. Das anfängliche Join-Key-Material wurde zuvor am Field-Gateway **212** und am Edge-Gateway **218** gespeichert (siehe z.B. Bezugsziffern **265**, **268**, 270), und der aktualisierte Netzwerkschlüssel und zufällige Paketzähler werden zum Beispiel zufällig am Field-Gateway **212** erzeugt.

[0064] Bei Bezugsziffer **290** verifiziert der Edge-Gateway **218** die empfangene Initialisierungsnachricht, z.B. durch Prüfen der Weißliste und/oder der Adressen, von denen die neue Initialisierungsnachricht empfangen wurde. Wenn der Edge-Gateway **218** feststellt, dass die empfangene neue Initialisierungsnachricht gültig ist, dann entschlüsselt der Edge-Gateway **218** die Initialisierungsnachricht mit seinem lokal gespeicherten anfänglichen Join-Key-Material und speichert den neuen/aktualisierten Netzwerkschlüssel und den darin enthaltenen zufälligen Paketzähler zur Nutzung bei der Verarbeitung zukünftiger Nachrichten, die vom Field-Gateway **212** empfangen werden. Zum Beispiel, der Field-Gateway **212** kann nachfolgende Nachrichten senden (Bezugsziffern **292**, **295**), die mit dem neuen/aktualisierten Netzwerkschlüssel und zufälligen Paketzähler verschlüsselt werden, und der Edge-Gateway **218** entschlüsselt die empfangenen Nachrichten mit dem gespeicherten neuen aktualisierten Netzwerkschlüssel und zufälligen Paketzähler (Bezugsziffern **298**, **300**).

[0065] Der Field-Gateway **212** wiederholt das Senden einer neuen oder aktualisierten Initialisierungsnachricht (z.B. Bezugsziffern **275**, **288** usw.), um einen aktualisierten oder neuen Netzwerkschlüssel und jeweiligen zufälligen Paketzähler rekurrent, periodisch oder bei Bedarf z.B. als Ergebnis eines Benutzerbefehls oder des Auftretens eines anderen Ereignisses einzurichten. Da Kommunikationen zwischen dem Field-Gateway **212** und dem Edge-Gateway **218** unidirektional über die Datendiode **215** sind, hat der Field-Gateway **212** keine explizite Bestätigung dafür, dass der Edge-Gateway **218** die vom Field-Gateway **212** übertragenen Daten tatsächlich empfängt. So kann, indem der Field-Gateway **212** rekurrent eine neue/aktualisierte Initialisierungsnachricht sendet, die einen neuen/aktualisierten Netzwerkschlüssel und jeweiligen zufälligen Paketzähler enthält, das zwischen dem Field-Gateway **212** und dem Edge-Gateway **218** gemeinsam genutzte Netzwerkschlüsselmaterial neu synchronisiert werden. Diese Neusynchronisierungstechnik lässt eine Wiederherstellung bei Fehler- oder Ausfallzuständen wie dann zu, wenn der Edge-Gateway versagt und ersetzt oder neu gestartet wird und/oder wenn ein Paket fehlt. Die Länge der Zeitperiode für Netzwerkschlüsselmaterial-Neusynchronisation kann anwendungsabhängig sein, z.B. kann durch eine Toleranz einer Anwendung (z.B. einer der Anwendungen oder Dienste **208**) für verlorene Pakete oder Daten bestimmt werden, und kann konfigurierbar sein.

[0066] Demgemäß werden, wie oben beschrieben, der/das anfänglich provisionierte Join-Key und zufällige Paketzähler oder Nonce-Material, die am Edge-Gateway **218** (Bezugsziffer 268) und am Field-Gateway **212** (Bezugsziffer **270**) gespeichert sind, zum Ver-/Entschlüsseln der anfänglichen Initialisierungsnachricht benutzt werden, die den anfänglichen zufälligen Netzwerkschlüssel und den zufälligen Paketstartzähler (Bezugsziffer **275**) bereitstellt, und nachfolgende Kommunikationen nutzen den zufälligen Netzwerkschlüssel und Paketzähler wie in der Initialisierungsnachricht enthalten zum Ver-/Entschlüssel der darin übertragenen Daten. Rekurrent, periodisch und/oder nach Bedarf erzeugt der Field-Gateway **212** eine neue oder aktualisierte Initialisierungsnachricht, die mit dem anfänglichen Join-Key-Material ver-/entschlüsselt ist, und dies ergibt einen neuen/aktualisierten zufälligen Netzwerkschlüssel und zufälligen Paketstartzähler (Bezugsziffer **288**). Kommunikationen, die nach der neuen/aktualisierten Initialisierungsnachricht gesendet werden, unterliegen dem neuen/aktualisierten zufälligen Netzwerkschlüssel und Paketzähler zum Ver-/Entschlüsseln der darin übertragenen Daten. So kann der Edge-Gateway **218** gleichzeitig zuvor benutzte Netzwerkschlüsselinformationen und neue Netzwerkschlüsselinformationen für eine finite Zeitdauer speichern, um evtl. außer der Reihe ankommende Pakete beim Übergang auf die neuen Netzwerkschlüsselinformationen verarbeiten zu können.

[0067] Wie in **Fig. 4** illustriert, nutzt der Nachrichtenfluss **250** ein Provisionierungsnetzwerk und Provisionierungsgerät **252** zum Durchführen des sicheren Provisionierungsprozesses zwischen dem Feld-Gateway **212** und dem Edge-Gateway **218**. Dies ist jedoch nur eine von vielen möglichen Ausgestaltungen.

[0068] Zum Beispiel, in einer anderen Ausgestaltung sind der Field-Gateway **212** und der Edge-Gateway **218** nicht auf einem Provisionierungsnetzwerk und sind evtl. nicht einmal auf demselben Netzwerk. In dieser Ausgestaltung authentifiziert sich ein Benutzer, zum sicheren Provisionieren des Field-Gateway **212** und des Edge-Gateway **218**, direkt beim Edge-Gateway **218** und stellt Sicherheitsinformationen oder Daten bereit, die den Field-Gateway 212 beschreiben. Zum Beispiel, der Benutzer stellt die IP-Adresse des Field-Gateway **212** für seinen Weißlisteneintrag am Edge-Gateway **218** bereit und der Benutzer stellt die Sicherheitsinformationen oder das anfängliche Schlüsselmaterial z.B. auf eine Weise ähnlich wie oben mit Bezug auf Bezugsziffer **265** in **Fig. 4** erörtert bereit. Die Sicherheitsinformationen werden verschlüsselt und am Edge-Gateway **218** zur Verwendung bei Kommunikationen mit dem Field-Gateway **212** gespeichert. Zusätzlich werden die verschlüsselten Sicherheitsinformationen auf einer separaten Datei gespeichert, die ebenfalls jeweils verschlüsselt sein kann. Die separate Datei wird z.B. vom Benutzer zum Field-Gateway **212** transportiert. Der Benutzer authentifiziert sich direkt beim Field-Gateway **212** und stellt die separate Datei zur Verwendung am Field-Gateway **212** bereit. Der Field-Gateway **212** verifiziert die separate Datei (und entschlüsselt die Datei falls nötig), holt die darin gespeicherten Sicherheitsinformationen ein (z.B. das anfängliche Schlüsselmaterial), verschlüsselt die erhaltenen Sicherheitsinformationen und speichert die verschlüsselten Sicherheitsinformationen lokal zur Verwendung bei zukünftigen Kommunikationen mit dem Edge-Gateway **218** über die Datendiode **215**.

[0069] In einer anderen Ausgestaltung werden Daten anstatt mit UDP mit seriellen Kommunikationen über die Datendiode **215** transportiert. In dieser Ausgestaltung kann der gesicherte Provisionierungsprozess dem oben zum Provisionieren des Field-Gateway **212** und des Edge-Gateway **218** beschriebenen ähnlich sein, während die Gateway **212**, **218** nicht auf einem Provisionierungsnetzwerk sind oder auf separaten Netzwerken sind.

[0070] In einigen Implementationen, unterhalb der gesicherten TCP-, UDP- und/oder seriellen Kommunikationen über die Datendiode **215**, kann das zum Übertragen von Prozessanlagen-erzeugten Da-

ten über die Datendiode **215** benutzte Kommunikationsprotokoll ein modifiziertes HART-IP-Protokoll sein oder kann eine Modifikation an einem bekannten industriellen Kommunikationsprotokoll sein, wie zum Beispiel Fieldbus.

[0071] Zum Benutzen des HART-IP Protokolls als illustratives, aber nicht begrenzendes Beispiel, kann das HART-IP Protokoll nutzbar gemacht werden, um ferner zusätzliche Sicherheit für Ende-zu-Ende-Kommunikationen von den in der Prozessanlage **100** arbeitenden Geräten **102** zu dem fernen System **210** bereitzustellen. Insbesondere wird der in HART-IP und HART enthaltene Publishing-Mechanismus auf eine einzigartige Weise nutzbar gemacht, um die unidirektionalen Kommunikationen über die Datendiode **215** zu unterstützen, so dass an der Prozessanlage **100** erzeugte Daten zu den fernen Anwendungen 208 über Nachrichten oder Pakete geliefert werden können, die zwischen dem Field-Gateway 212 und dem Edge-Gateway **218** über die Datendiode **215** übertragen werden (z.B. wie durch Bezugsziffern **278**, **282**, **292**, **295** in **Fig. 4** angezeigt).

[0072] Die modifizierten HART-IP-Protokoll-Pakete können von einem Token-Passing Data-Link Layer Frame Format und/oder von einem Direct/Wireless Packet Format sein. Zum Beispiel, der HART-IP-Header kann so modifiziert werden, dass er Sicherheitsinformationen wie eine Anzeige eines Sicherheitstyps enthält (z.B. als ein Wert im Message Type Feld des Headers), die Hart-IP-Sitzungsinitialisierungsnachricht kann so modifiziert werden, dass sie die anfänglichen Sicherheitsschlüsselmaterialinformationen enthält, und/oder andere HART-Nachrichtentypen (z.B. Request, Response, usw.), können so modifiziert werden, dass sie ein Netzwerksicherheitsschlüsselfeld und ein Netzwerksicherheitszählerfeld enthalten.

[0073] Eine beispielhafte Nutzung des modifizierten HART-IP-Protokolls zum Sichern von Kommunikationen über die Datendiode **215** ist in **Fig. 5** dargestellt. **Fig. 5** zeigt einen beispielhaften Nachrichtenfluss **400**, der zum Liefern von Prozessanlagendaten benutzt werden kann, die von einem oder mehreren sendenden Geräten **402** über die Datendiode **215** zu einem oder mehreren empfangenen Geräten **405** erzeugt werden. Allgemein ausgedrückt, ein sendendes Gerät **402** sendet zunächst Entdeckungsinformationen zu einem empfangenen Gerät **405**, um den Kontext für Inhalts- oder Nutzlastdaten festzulegen, die über die Datendiode **215** übertragen werden sollen. Die Entdeckungsinformationen lassen es zu, dass das empfangende Gerät **405** weiß, welche datenerzeugenden Komponenten oder Geräte sich auf der Prozessanlagenseite der Datendiode **215** befinden, die Typen und/oder Identitäten der Daten, die von den prozessanlagenseitigen Komponenten erzeugt werden, die erwarteten Ankunftsraten der erzeugten Daten an dem empfangenden Gerät **405**, Statuse der verschiedenen datenerzeugenden Komponenten oder Geräte usw. Bedeutsamerweise lassen es die Entdeckungsinformationen zu, dass das empfangende Gerät **405** diese Kenntnis erlangt, ohne dass das empfangende Gerät **405** Geräte auf der Prozessanlagenseite der Datendiode **215** abfragen muss, was das empfangende Gerät **405** aufgrund der unidirektionalen Natur der Datendiode **215** nicht tun kann.

[0074] Nach dem Senden der Entdeckungsinformationen durch das sendende Gerät **402** zum empfangenden Gerät **405** veröffentlicht das sendende Gerät **402** anhand des modifizierten HART-IP-Protokolls Inhalts- oder Nutzlastdaten über die Datendiode **215** gemäß dem in den Entdeckungsinformationen in Echtzeit festgelegten Kontext, z.B. während das sendende Gerät **402** die Quelldaten erzeugt und/oder während das sendende Gerät **402** Quelldaten von einer oder mehreren anderen Komponenten in der Prozessanlage **100** empfängt. Somit kann das empfangende Gerät **405** ein Abonnent für Daten sein, die vom sendenden Gerät **402** veröffentlicht werden.

[0075] Zusätzlich, ebenso aufgrund der unidirektionalen Natur der Datendiode **215**, kann das sendende Gerät **402** den Status des empfangenden Geräts **405** nicht erkennen (z.B. ob das empfangende Gerät **405** in Betrieb, eingeschaltet, abgetrennt usw. ist) und kann nicht explizit bestimmen, ob das empfangende Gerät **405** die gesendeten Daten empfangen hat oder nicht. Demgemäß stellt das sendende Gerät **402** rekurrent (z.B. periodisch und/oder nach Bedarf) Entdeckungsinformationen dem empfangenden Gerät **405** bereit, sendet sie dorthin oder annonciert sie, so dass, wenn das empfangende Gerät **405** zufällig unverfügbar ist, das empfangende Gerät **405** nach Wiederherstellung den Kontext der vom sendenden Gerät **402** gesendeten Inhalts- oder Nutzlastdaten schnell (wieder) verstehen kann. Die Länge der Zeitperiode zwischen dem Senden von Entdeckungsinformationen kann von der Toleranz einer Client-Anwendung (t.B. eine der fernen Anwendungen oder Dienste **208**) auf der Empfangsgeräteseite der Datendiode **215** für verlorene Pakete oder Daten abhängig sein und kann konfigurierbar sein. Entdeckungsinformationen können auch dann gesendet werden, wenn eine Änderung seitens des sendenden Geräts **402** auftritt, wie zum Beispiel dann, wenn Datenquellen **202** und/oder drahtlose Gateways **205** zur Prozessanlage **100** hinzugefügt oder davon weggenommen werden.

[0076] Das sendende Gerät **402** kann ein Field-Gateway **212**, ein drahtloser Gateway **205**, ein Datenquellgerät **202** und/oder eine beliebige andere Komponente sein, die von einer/m oder mehreren in der Prozessanlage **100** arbeitenden Komponenten oder Geräten erzeugt werden. Das empfangende Gerät

405 kann ein Edge-Gateway **218**, ein oder mehrere der Geräte, die das ferne System **210** umfassen, und/oder eine Client-Anwendung sein, die ein Verbraucher von Quelldaten ist (z.B. eine(r) der fernen Anwendungen oder Dienste **208**). In **Fig. 5** wird jedoch zum Vereinfachen der Erörterung der Nachrichtenfluss **400** unter der Annahme erörtert, dass das sendende Gerät **402** der Field-Gateway **212** von **Fig. 3** ist und das empfangende Gerät **405** der Edge-Gateway **218** von **Fig. 3** ist, obwohl zu verstehen ist, dass dies nur eine von zahlreichen möglichen Ausgestaltungen ist.

[0077] Während der Kontexteinstellphase **408** überträgt das sendende Gerät **402** jeweilige Informationen, die jede Datenquelle der Prozessanlage **100** beschreiben, deren Daten über die Datendiode **215** übertragen werden sollen. Die deskriptiven Datenquellinformationen beinhalten zum Beispiel eine Identität der Datenquelle (z.B. eindeutiger Identifikator, Geräte-Tag usw.); eine Identität der Daten (die beispielsweise Mapping-Informationen zu einer oder mehreren ihrer dynamischen Variablen enthalten, wie Primary Variable (PV), Secondary Variable (SV), Tertiary Variable (TV), Quaternary Variable (QV) usw.); eine Anzeige der erwarteten Ankunftsrate der identifizierten Daten (z.B. Burst-Konfigurationsinformationen); und/oder andere Informationen, die die Daten und/oder die Datenquelle beschreiben, wie Daten, die den bestimmten Gateway anzeigen, mit dem die Datenquelle kommunikativ verbunden ist, Status der Datenquelle, Status ihres Gateway usw. Wie in **Fig. 5** illustriert, iteriert das sendende Gerät **402** in einer Ausgestaltung pro drahtlosem Gateway **204** pro drahtlosem Quellgerät **202** während der Kontexteinstellphase **408**. Zum Beispiel, das sendende Gerät **402** sendet deskriptive Informationen für den drahtlosen Gateway **0** (Bezugsziffer **410**), der beispielsweise einer der drahtlosen Gateways **205A**, **205B** sein kann. Das sendende Gerät **402** kann deskriptive Informationen über den drahtlosen Gateway **0** zum Beispiel mit Hilfe eines modifizierten HART-IP Befehls **0**, **20** oder **74** senden. Nachfolgend sendet das sendende Gerät **402** jeweilige deskriptive Informationen für jedes der N Geräte, die kommunikativ mit dem Gateway **0** verbunden sind (Bezugsziffer **412**), zum Beispiel mitels des/der modifizierten HART-IP Befehls(e) 0, 20, 50, 105(n), und optional Befehle **74** und **101** für Subgerät-Burst-Mapping. Diese Folge wird für jeden der M Gateways wiederholt und die Kontexteinstellphase **408** endet, nachdem die deskriptiven Informationen für Gateway M und seine jeweiligen N Geräte zum empfangenden Gerät **405** gesendet wurden (Bezugsziffern **415**, **418**).

[0078] Während der Veröffentlichungsphase **420** veröffentlicht das sendende Gerät **402** Quelldaten über die Datendiode **215** für beliebige der Datenquellgeräte **202**, deren Kontext während der Kontexteinstellphase **408** eingestellt wurde. In einem Beispiel veröffentlicht das sendende Gerät **402** die Quelldaten über die Datendiode **215** mit Hilfe eines modifizierten HART-IP-Befehls **48** oder eines anderen geeigneten Hart-IP-Befehls. Bestimmte Quelldaten werden mit der Rate veröffentlicht, mit der die Quelldaten am sendenden Gerät **402** empfangen werden, z.B. von dem Gerät **202** über seinen jeweiligen drahtlosen Gateway **205**. Das heißt, bei Online-Operationen der Prozessanlage **100** werden von der Prozessanlage **100** erzeugte Quelldaten über die Datendiode **215** in Echtzeit veröffentlicht, während sie vom sendenden Gerät **402** empfangen werden. Es wird bemerkt, dass einige datenerzeugenden Komponenten der Prozessanlage **100** (z.B. einige der Datenquellgeräte **202** und/oder einige der drahtlosen Gateways **205**) Daten direkt zum Field-Gateway **212** zur Lieferung über die Datendiode **215** veröffentlichen können. Andere datenerzeugenden Komponenten der Prozessanlage **100** (z.B. andere der Datenquellgeräte **202** und/oder drahtlosen Gateways **205**) können keine Veröffentlichung unterstützen und der Field-Gateway **212** kann diese Typen von Geräten/Gateways abfragen, um ihre jeweiligen Quelldaten zu empfangen. Zum Beispiel, der Field-Gateway **212** kann auf der Basis einer Burst-Konfiguration des Geräts/Gateway abfragen, das/der keine Veröffentlichung unterstützt, z.B. durch Verwenden von HART-IP-Befehl **3** oder **9**.

[0079] Wie zuvor erörtert, nach dem Verstreichen einer vordefinierten Zeitperiode, oder nach Bedarf, werden wenigstens einige der Kontextinformationen **410**-**418** vom sendenden Gerät **402** zum empfangenden Gerät **405** neu gesendet oder aktualisiert. In einer Ausgestaltung wird die Gesamtheit der Kontextdaten **410**-**418** der Gateways **0-M** und jeweiligen Geräte **1-N** neu gesendet oder aktualisiert. In einer anderen Ausgestaltung werden bestimmte Kontextdaten für bestimmte Geräte zu mehreren verschiedenen Zeiten je nach Bedarf für einen bestimmten Verbraucher der Daten neu gesendet oder aktualisiert, z.B. auf der Basis einer Toleranz des bestimmten Verbrauchers für verlorene Daten oder Pakete. In diesen Ausgestaltungen können verschiedene Geräte unterschiedliche Periodizitäten oder Intervalle haben, in denen ihre jeweiligen Kontextdaten neu gesendet oder aktualisiert werden.

[0080] Zusätzlich wird festgestellt, dass der obige Nachrichtenfluss **400** in einer Ausgestaltung beschrieben wird, in der die Datendiode **215** eine Ethernet-verbundene Datendiode ist. Ähnliche Techniken können jedoch leicht auch bei Bedarf auf eine seriell geschaltete Datendiode angewendet werden. Ferner wurde der obige Nachrichtenfluss **400** zwar anhand des HART-IP-Protokolls beschrieben, aber es können auch andere Kommunikationsprotokolle während der Kontextphase **408** und der Datenlieferphase **420** des Nachrichtenflusses **400** benutzt werden. In einigen beispielhaften Konfigurationen können ande-

re industrielle Kommunikationsprotokolle als HART-IP (z.B. Profibus, DeviceNet, Foundation Fieldbus, ControlNet, Modbus, HART, usw.) benutzt werden. In anderen Konfigurationsbeispielen können andere Protokolle, die nicht speziell für industrielle Kommunikationen ausgelegt sind, während der Kontextphase **408** und der Datenlieferphase 420 des Nachrichtenflusses **400** benutzt werden.

[0081] Zum Beispiel, in einer Ausgestaltung können Pakete anstatt mit HART-IP mit einem JSON (JavaScript Object Notation) Format über die Datendiode **215** übertragen werden. In dieser Ausgestaltung konvertiert der Field-Gateway **212** Daten, die von verschiedenen Geräten und Komponenten in der Prozessanlage **100** empfangen werden, in ein JSON-Format zur Lieferung über die Datendiode **215**. Falls gewünscht, können Erweiterungen zu den JSON-Paketdaten hinzugefügt werden, wie beispielsweise Labels, die zusätzliche Bedeutung haben (z.B. „PRESSURE“ anstatt „PV“, gerätespezifische Labels für verschiedene Datenwerte und dergleichen).

[0082] Ferner beschreibt die obige Erörterung von **Fig. 5** zwar den Nachrichtenfluss **400** so wie er auftritt, wenn der sendende Gateway **402** der Field-Gateway **212** ist und das empfangende Gerät **405** der Edge-Gateway **218** ist, aber dies ist nur eine von zahlreichen Ausgestaltungen. Zum Beispiel, in anderen Ausgestaltungen des Nachrichtenflusses **400** kann das sendende Gerät **402** ein Field-Gateway **212**, ein drahtloser Gateway **205**, ein Datenquellgerät **202** und/oder eine beliebige andere Komponente sein, die Daten bereitstellt, die von einer oder mehreren in der Prozessanlage **100** arbeitenden Komponenten oder Geräten erzeugt werden, und das empfangende Gerät **405** kann ein Edge-Gateway **218**, ein oder mehrere das ferne System **210** umfassende Geräte und/oder eine Client-Anwendung sein, die ein Verbraucher von Quelldaten ist (z.B. eine(r) der fernen Anwendungen oder Dienste **208**). Zum Beispiel, eine erste der Client-Anwendungen **208** kann Daten abonnieren, die von einem bestimmten Gerät **202** erzeugt werden, die über die Datendiode **215** veröffentlicht wird, und eine zweite der Client-Anwendungen **28** kann Daten abonnieren, die von einem anderen bestimmten Gerät **202** erzeugt werden. In diesem Beispiel kann der Edge-Gateway **218** als Router zum Verteilen von empfangenen Daten zu jeweiligen Datenabonnenten dienen. In einem anderen Beispiel veröffentlicht der Edge-Gateway **218** alle Daten, die er über die Datendiode **215** empfängt, und verschiedene Anwendungen **208** abonnieren spezifische Daten, die vom Edge-Gateway **218** veröffentlicht werden. Es sind auch andere Veröffentlicher/Abonnenten-Beziehungen möglich und können von einer oder mehreren beliebigen der hierin beschriebenen gesicherten Kommunikationstechniken unterstützt werden.

[0083] Darüber hinaus können eine oder mehrere beliebige der gesicherten Kommunikationstechniken leicht zum Sichern von Daten angewendet werden, die zu Systemen und/oder Geräten gesendet werden, die lokal zur Prozessanlage **100** sind. Zum Beispiel, eine jeweilige Datendiode **215** und/oder Instanz der Sicherheitsarchitektur **200** kann zum Veröffentlichen von gewählten (oder sogar allen) Daten über die DMZ **22** der Prozessanlage **100** benutzt werden, so dass die Daten auf den Sicherheitsstufen **0**-**3** der Prozessanlage **100** sicher über die DMZ **22** zu Unternehmenssystemen auf den Stufen **4**-**5** über eine jeweilige Datendiode geliefert werden. In einem anderen Beispiel kann eine jeweilige Datendiode **215** und/oder Instanz der Sicherheitsarchitektur **200** zum Veröffentlichen von gewählten (oder sogar allen) Daten von einer oder mehreren in der Prozessanlage **100** angeordneten Datenquellen **202** zu einem oder mehreren lokalen Servern benutzt werden, die ebenfalls in oder lokal zu der Prozessanlage **100** angeordnet sind und die lokale Dienste und Anwendungen hosten oder bereitstellen. Eine solche Konfiguration ist zum Beispiel dann nützlich, wenn lokale Dienste und Anwendungen lokale präskriptive Änderungen erzeugen, die auf die Online-Prozessanlage **100** heruntergeladen oder anderweitig darin implementiert werden sollen, obwohl im Allgemeinen präskriptive Funktionen, Modifikationen an Konfigurationen und/oder andere Daten und/oder andere Änderungen in der Prozessanlage **100** durch entfernt befindliche Anwendungen und Dienste 208 implementiert werden können.

[0084] Es wird jedoch bemerkt, dass beliebige präskriptive Änderungen, die von den Anwendungen/Diensten **208** bestimmt werden, typischerweise in der Prozessanlage **100** über einen anderen Kommunikationsmechanismus als die Datendiode **215** implementiert werden, da die Datendiode **215** in Austrittsrichtung mit Bezug auf die Prozessanlage **100** unidirektional ist. Zum Beispiel, zum Implementieren einer präskriptiven Änderung an der Prozessanlage **100** kann ein(e) Anwendung/Dienst **208** eine andere gesicherte Kommunikationsverbindung als über die Datendiode **215** mit einer oder mehreren administrativen oder Backend-Komponenten der Prozessanlage einrichten, wie die Operator-Workstation **171**, die Konfigurationsanwendungen **172A**, die Konfigurationsdatenbank **173B** usw., und die präskriptive Änderung kann auf die Prozessanlage **100** heruntergeladen oder ihr auf andere Weise geliefert werden. In der Tat kann in einer Ausgestaltung eine andere Instanz der Datendiode **215** und/oder der Sicherheitsarchitektur **200** in Eintrittsrichtung eingerichtet werden, um beliebige präskriptive Änderungen von der/dem fernen Anwendung/Dienst **208** der Prozessanlage **100** sicher zu liefern.

[0085] Ferner nutzt, allgemein ausgedrückt, jede Eintrittskommunikation vom fernen System **210** zur Prozessanlage **210** typischerweise einen anderen

Kommunikationsmechanismus als die Ausgangsdatendiode **215** und/oder die Austrittssicherheitsarchitektur **200**. Zum Beispiel kann das ferne System **210** eine andere Instanz von Datendiode **215** und/oder die Sicherheitsarchitektur **200** in Eintrittsrichtung angewandt oder eine(n) andere(n) geeignete(n) gesicherte(n) Verbindung oder Kommunikationspfad nutzen.

[0086] Nun wieder zurück zu gesicherten Austrittskommunikationen von der Prozessanlage **100**, **Fig. 6** veranschaulicht ein Ablaufdiagramm eines beispielhaften Verfahrens **450** zum sicheren Transportieren von Kommunikationen von einer Prozessanlage wie der Prozessanlage **100** von **Fig. 2**. In einigen Ausgestaltungen wird wenigstens ein Teil des Verfahrens **450** durch Ausführen eines Satzes von computerausführbaren oder computerlesbaren Befehlen implementiert, die auf einem oder mehreren nichtflüchtigen computerlesbaren Speichern gespeichert sind und von einem oder mehreren Prozessoren wie z.B. dem System **200** ausgeführt werden. Zum Beispiel, wenigstens ein Teil des Verfahrens 450 kann von einer oder mehreren Komponenten des Systems **200** wie in den **Fig. 1**-**Fig. 5** veranschaulicht durchgeführt werden, wie zum Beispiel dem Field-Gateway **212** oder dem sendenden Gerät **402**. Demgemäß wird das Verfahren **450** nachfolgend mit gleichzeitiger Bezugnahme auf die **Fig. 1**-**Fig. 5** beschrieben; dies soll jedoch lediglich die Erläuterung vereinfachen und ist nicht für Begrenzungszwecke.

[0087] Im Block **452** beinhaltet das Verfahren **450** das Provisionieren eines sendenden Geräts einer Prozessanlage mit einem empfangenden Gerät. Das sendende Gerät ist kommunikativ mit der Prozessanlage (z.B. über ein oder mehrere geeignete Netzwerke) verbunden und das empfangende Gerät ist kommunikativ mit einem anderen System (z.B. über ein oder mehrere geeignete Netzwerke), zum Beispiel, verbunden. Das andere System hostet eine oder mehrere Anwendungen oder Dienste, die zum Wirken an Daten konfiguriert sind, die von der Prozessanlage während ihrer Laufzeitoperationen erzeugt werden, und optional an anderen von der Prozessanlage erzeugten Daten. Das sendende Gerät kann beispielsweise das sendende Gerät **402** sein und das empfangende Gerät kann beispielsweise das in **Fig. 5** illustrierte empfangende Gerät **405** sein. Somit kann das sendende Gerät **402** der Field-Gateway **212**, ein Datenquellgerät **202**, ein drahtloser Gateway **205** oder eine andere Komponente der Prozessanlage **100** sein, und das empfangende Gerät kann kann der Edge-Gateway **218**, ein im fernen System **210** enthaltenes Rechengerät oder ein(e) Anwendung oder Dienst **208** sein, die/der auf dem fernen System **210** läuft. Es sind natürlich auch andere Ausgestaltungen des sendenden Geräts und/oder des empfangenden Geräts möglich, wie z.B. beliebige der zuvor oben erörterten.

[0088] Das sendende Gerät und das empfangende Gerät sind über eine Datendiode wie die Datendiode **215** von **Fig. 3** miteinander verbunden. Die Datendiode ist so konfiguriert, dass sie das Übertragen von unidirektionalen Kommunikationen vom sendenden Gerät zum empfangenden Gerät zulässt und das Übertragen von Kommunikationen vom empfangenden Gerät zum sendenden Gerät verhindert (abgesehen von anfänglichen Provisionierungsnachrichten in einer Ausgestaltung).

[0089] Das Provisionieren des sendenden Geräts zum empfangenden Gerät (Block **452**) erfolgt mit einem ersten Schlüssel, der auch als Join-Key bezeichnet wird. Der Join-Key kann ein Geheimschlüssel oder ein Gemeinschaftsgeheimnis sein und kann von einem Benutzer bereitgestellt werden, z.B. über ein Provisionierungsgerät, das kommunikativ mit dem sendenden Gerät und/oder dem empfangenden Gerät verbunden ist, oder über einen manuellen Datentransfer. In einigen Anordnungen wird ein erster Paketzähler (der auch als Join-Paketzähler bezeichnet wird) oder ein anderes jeweiliges Nonce-Material in Verbindung mit dem Join-Key bereitgestellt. Der Join-Key und/oder der Join-Paketzähler kann/können bei Bedarf zufällig erzeugt werden.

[0090] In einigen Ausgestaltungen beinhaltet das Provisionieren des sendenden Gerät des empfangenden Geräts [sic] (Block **452**) das Einrichten eines temporären Kommunikationskanals, um Kommunikationen vom empfangenden Gerät zum sendenden Gerät Übertragen und/oder Verifizieren des Join-Key zuzulassen. Der temporäre Kommunikationskanal kann über die Datendiode eingerichtet werden oder kann über eine andere kommunikative Verbindung wie zum Beispiel eine externe verdrahtete oder drahtlose Verbindung, einen manuellen Trasfer über ein portables Speichergerät oder dergleichen eingerichtet werden. In diesen Ausgestaltungen kann der temporäre Kommunikationskanal nach dem Übertragen des Join-Key durch das empfangene Gerät und/oder dem Empfang des Join-Key am sendenden Gerät abgetrennt, abgebaut oder auf andere Weise gesperrt werden. Allgemein ausgedrückt, der temporäre Kommunikationskanal dient nur zum gemeinsamen Nutzen des ersten oder Join-Key zwischen sendenden und empfangenden Geräten. Nach dem gemeinsamen Nutzen des anfänglichen Schlüsselmaterials (z.B. dem Join-Key und seinem jeweiligen Paketzähler oder sonstigen Nonce-Material) wird das anfängliche Schlüsselmaterial lokal verschlüsselt und jeweils sowohl am sendenden Gerät als auch am empfangenden Gerät gespeichert.

[0091] Das Verfahren **450** beinhaltet das Verschlüsseln, z.B. durch das sendende Gerät, einer Initialisierungsnachricht anhand des ersten oder Join-Key (Block **455**) und das Übertragen der verschlüsselten Initialisierungsnachricht über die Datendiode zu

dem empfangenden Gerät (Block **458**). Die Initialisierungsnachricht beinhaltet einen zweiten Schlüssel, der hierin auch als Netzwerkschlüssel bezeichnet wird, der durch die sendenden und empfangenden Geräte zum Verarbeiten von nachfolgenden Nachrichten oder Paketen zu benutzen ist, die von dem sendenden Gerät zu dem empfangenden Gerät über die Datendiode übertragen werden. Der zweite Schlüssel kann zum Beispiel ein anderer Geheimschlüssel oder Gemeinschaftsgeheimnis sein. Zumindest einige der nachfolgenden Nachrichten oder Pakete, die mit dem zweiten oder Netzwerkschlüssel verarbeitet werden, beinhalten Inhalt oder Nutzlast mit Daten, die von der Prozessanlage erzeugt werden, während sie in Echtzeit zum Steuern eines Prozesses arbeitet, wie erzeugte Prozessdaten, Diagnosedaten und andere Datentypen. In einigen Anordnungen wird ein zweiter Paketzähler (der auch als Netzwerkpaketzähler bezeichnet wird) oder sonstiges jeweiliges Nonce-Material verschlüsselt und in Verbindung mit dem Netzwerkschlüssel zur Verwendung beim Verarbeiten der nachfolgenden Nachrichten/Pakete bereitgestellt. Der Netzwerkschlüssel und/oder der Netzwerkpaketzähler können bei Bedarf zufällig erzeugt werden.

[0092] Demgemäß beinhaltet das Verfahren **450** ferner das Empfangen, am sendenden Gerät, von Daten, die von der Prozessanlage erzeugt werden, während diese in Echtzeit zum Steuern des Prozesses arbeitet (Block **460**); Verschlüsseln, durch das sendende Gerät und anhand des Netzwerkschlüssels und optional des Netzwerkpaketzählers, von nachfolgenden Nachrichten/Paketen, die die Prozessanlagen-erzeugten Daten als Nutzlast enthalten (Block 562); und das Bereitstellen der verschlüsselten nachfolgenden Nachrichten/Pakete über die Datendiode zum empfangenden Gerät (Block **465**). Somit werden an den Blöcken **462**, **465** die nachfolgenden Nachrichten/Pakete, von denen wenigstens einige von der Prozessanlage erzeugte Daten enthalten, für einen Transport über die Datendiode mit Hilfe des Gemeinschaftsgeheimnis-Netzwerkschlüssels gesichert. In einigen Ausgestaltungen werden die nachfolgenden Nachrichten/Pakete weiter für einen Transport über die Datendiode bei Bedarf durch zusätzliche Verschlüsselung gesichert (nicht gezeigt).

[0093] Das Empfangen der Daten, die von der Prozessanlage bei Echtzeit- oder Online-Operationen zum Steuern des Prozesses erzeugt werden (Block **460**), kann das Empfangen von Daten direkt von einer Datenerzeugungsquelle (z.B. einem Gerät oder einer Komponente 202) und/oder das Empfangen, von einem Gateway (z.B. einem drahtlosen Gateway **205**) von Daten beinhalten, die von einer Datenerzeugungsquelle (z.B. einem Gerät oder einer Komponente **202**) zu dem Gateway übertragen wurden. Die Prozessanlagen-erzeugten Daten, die am sendenden Gerät empfangen werden, wurden möglicherweise von der Datenerzeugungsquelle (z.B. dem Gerät oder der Komponente **202**) und/oder vom Gateway (z.B. dem drahtlosen Gateway **205**) zum Beispiel auf eine Weise wie zuvor beschrieben verschlüsselt, wrapped und/oder auf andere Weise gesichert.

[0094] Die Prozessanlagen-erzeugten Daten, die empfangen werden (Block **460**), können veröffentlichte Daten enthalten, da einige Datenerzeugungsquellgeräte ihre jeweiligen erzeugten Daten veröffentlichen können, z.B. zu dem drahtlosen Gateway **205** und/oder zum dem sendenden Gerät **402**. Andere datenerzeugende Quellgeräte können abgefragt werden (z.B. durch den drahtlosen Gateway **205** und/oder durch das sendende Gerät **402**), so dass ihre jeweiligen erzeugten Daten am sendenden Gerät empfangen werden können (Block **460**). Ferner können die Prozessanlagen-erzeugten Daten, ob veröffentlicht, abgefragt oder auf andere Weise empfangen (Block **460**), in einem HART-kompatiblen Format, in einem JSONkompatiblen Format oder einem anderen geeigneten Format gemäß einem beliebigen geeigneten industriellen Kommunikationsprotokoll oder einem Universal-Kommunikationsprotokoll vorliegen.

[0095] Wie zuvor erörtert, beinhaltet das Verschlüsseln von Nachrichten/Paketen, die Prozessanlagenerzeugte Daten als Nutzlast enthalten (Block **462**), das Verschlüsseln der genannten Nachrichten/Pakete mit dem Netzwerkschlüssel und optional dem Netzwerkpaketzähler, z.B. als Nonce-Material, und der Transport der Nachrichten/Pakete über die Datendiode wird ferner durch die unidirektionale Kommunikationskonfiguration der Datendiode gesichert.

[0096] Zusätzlich kann das Bereitstellen oder das Senden der verschlüsselten nachfolgenden Nachrichten über die Datendiode zu dem empfangenden Gerät (Block **465**) zum Beispiel das rekurrente Annoncieren oder Senden, zu dem empfangenden Gerät über die Datendiode, von jeweiligen Kontextinformationen beinhalten, die jedes von einem oder mehreren datenerzeugenden Geten der Prozessanlage beschreiben. Die jeweiligen Kontextinformationen können einen Identifikator des gegenständlichen datenerzeugenden Geräts, eine jeweilige Rate, mit der von dem gegenständlichen Gerät erzeugte Daten übertragen oder veröffentlicht werden sollen, eine Anzeige eines aktuellen Status des gegenständlichen datenerzeugenden Geräts und/oder andere Informationen enthalten, die das gegenständliche datenerzeugende Gerät beschreiben, wie oben mit Bezug auf **Fig. 5** erörtert wurde.

[0097] Das rekurrente Annoncieren von Kontextinformationen kann in einem Beispiel das periodische Senden von Kontextinformationen zu dem empfangenden Gerät über die Datendiode beinhalten. Die Dauer der Periodizität kann sich für unterschiedliche Typen von Inhaltsdaten, für unterschiedliche daten-

erzeugende Quellen der Prozessanlage und/oder für unterschiedliche Verbraucher der Inhaltsdaten unterscheiden (z.B. eine ferne Anwendung 208). Zum Beispiel, eine Dauer der Periodizität für bestimme Typen von Inhaltsdaten kann auf einer Toleranz eines Verbrauchers der Daten für verlorene Pakete und/oder Verzögerung basieren. Kontextinformationen können natürlich dem empfangenden Gerät nach Bedarf über die Datendiode annonciert werden, wie zum Beispiel nach dem Rebooten des sendenden Geräts, wenn ein neues Datenerzeugungsgerät zur Prozessanlage hinzugefügt wird, nach Anzeige durch den Benutzer usw.

[0098] Ferner kann das Annoncieren von Kontextinformationen das Benutzen von einem oder mehreren Nachrichtentypen eines industriellen Kommunikationsprotokolls in einer Ausgestaltung beinhalten. Zum Beispiel, wenn ein Typ von HART-Kommunikationsprotokoll über die Datendiode benutzt wird, dann kann das Annoncieren von Kontextinformationen das Benutzen von HART-Befehlen **0**, **20**, **50**, **74**, **105** und optional Befehlen **74** und **101** beinhalten. In einer anderen Ausgestaltung kann das Annoncieren von Kontextinformationen mit einem Universal-Kommunikationsprotokoll wie JSON oder einem anderen geeigneten Universal-Kommunikationsprotokoll implementiert werden. Verschiedene Nachrichtentypen von verschiedenen industriellen Kommunikationsprotokollen können zum Aufnehmen der Annoncierungen in einem Beispiel modifiziert werden.

[0099] Das Bereitstellen der verschlüsselten nachfolgenden Nachrichten über die Datendiode zum empfangenden Gerät (Block **465**) beinhaltet auch das Übertragen oder Transportieren von Inhaltsdaten über die Datendiode gemäß den zuvor gesendeten Kontextinformationen. Wie zuvor erörtert, beinhalten die Inhaltsdaten dynamische Daten, die von der Prozessanlage erzeugt werden, während diese online zum Steuern des Prozesses arbeitet, wie Prozessdaten, Diagnosedaten und dergleichen. In einer Ausgestaltung beinhaltet das Bereitstellen der verschlüsselten nachfolgenden Nachrichten über die Datendiode das Veröffentlichen der Inhaltsdaten über die Datendiode z.B. in einer Weise wie oben beschrieben.

[0100] Das Verfahren **450** beinhaltet ferner das Verschlüsseln einer zweiten (z.B. einer nachfolgenden) Initialisierungsnachricht mit dem ersten oder Join-Key (Block **468**), und das Bereitstellen der verschlüsselten, zweiten Initialisierungsnachricht über die Datendiode zum empfangenden Gerät (Block **470**). Die zweite Initialisierungsnachricht beinhaltet einen aktualisierten oder neuen Netzwerkschlüssel, der von den sendenden und empfangenden Geräten zum Verarbeiten von nachfolgenden Nachrichten oder Paketen zu benutzen ist, die über die Datendiode vom sendenden Gerät zum empfangenden Gerät übertragen werden. Der aktualisierte oder neue Netzwerkschlüssel kann ein anderer Gemeinschaftsschlüssel oder Gemeinschaftsgeheimnis sein, der sich von dem mit Bezug auf Block **452** erörterten Join-Key unterscheidet und ein anderer ist als der mit Bezug auf die Blöcke **455**, **458** erörterte Netzwerkschlüssel. Ein aktualisierter oder neuer Netzwerkpaketzähler, der auch zur Verwendung zum Verarbeiten von nachfolgenden Nachrichten/Paketen dient, kann erzeugt und über die Datendiode in Verbindung mit dem aktualisierten oder neuen Netzwerkschlüssel transportiert werden. Der neue oder aktualisierte Netzwerkschlüssel und/oder Paketzähler kann/können bei Bedarf auch zufällig erzeugt werden.

[0101] Demgemäß wird an den Blöcken **468**, **470** der vom sendenden Gerät und vom empfangenden Gerät zum Verarbeiten von Nachrichten/Paketen benutzte Netzwerkschlüssel neu synchronisiert. Diese Neusynchronisation ist zumindest deshalb wichtig, weil die Datendiode unidirektional ist, und somit kann das empfangende Gerät kein Feedback über seinen Betriebsstatus, den erfolgreichen oder erfolglosen Empfang von Nachrichten usw. zum sendenden Gerät senden. Über die Blöcke **468**, **470** kann das Verfahren **450** jedoch kommunikative Abtrennungen zwischen dem sendenden Gerät und dem empfangenden Gerät durch Neusynchronisieren von Netzwerkschlüsselmaterial angehen. In der Tat werden in einigen Ausgestaltungen die Blöcke **468**, **470** rekurrent, periodisch und/oder auf der Basis des Auftretens bestimmter Ereignisse (z.B. ein Neubooten des sendenden Geräts, wenn ein Benutzer dies anzeigt, nach Bedarf, usw.) wiederholt. Die Dauer der Periodizität kann auf einer Toleranz von einem oder mehreren Verbrauchern der Inhaltsdaten zum Beispiel für verlorene Pakete und/oder Verzögerung basieren.

[0102] Es wird mit Bezug auf die Blöcke **468**, **470** angemerkt, dass das empfangende Gerät möglicherweise sowohl den ersten Netzwerkschlüssel/Paketzähler als auch den zweiten Netzwerkschlüssel/Paketzähler beispielsweise für eine finite Zeitperiode führen muss, zum Beispiel zum Verarbeiten von Paketen, die über die Datendiode in einer anderen Reihenfolge als der ankommen, in der sie gesendet wurden.

[0103] **Fig. 7** zeigt ein Ablaufdiagramm eines beispielhaften Verfahrens **500** zum sicheren Transportieren von Kommunikationen von einer Prozessanlage wie der Prozessanlage **100** von **Fig. 2**. In einigen Ausgestaltungen wird wenigstens ein Teil des Verfahrens **500** durch Ausführen eines Satzes von computerausführbaren oder computerlesbaren Befehlen implementiert, die auf einem oder mehreren nichtflüchtigen computerlesbaren Speichern gespeichert sind und von einem oder mehreren Prozessoren wie z.B. dem System **200** ausgeführt werden. Zum Beispiel, wenigstens ein Teil des Verfahrens 500 kann von einer oder mehreren Komponenten des Systems

200 wie in den **Fig. 1**-**Fig. 5** veranschaulicht durchgeführt werden, wie zum Beispiel dem Edge-Gateway **218** oder dem empfangenden Gerät **405**. Demgemäß wird das Verfahren **500** nachfolgend mit gleichzeitiger Bezugnahme auf die **Fig. 1**-**Fig. 5** beschrieben, aber dies dient lediglich zum Erleichtern der Erläuterung und nicht für Begrenzungszwecke.

[0104] Im Block **502** beinhaltet das Verfahren **500** das Empfangen, über eine Datendiode, von Daten, die von der Prozessanlage erzeugt werden, während sie in Echtzeit zum Steuern des Prozesses arbeitet. Die Datendiode ist so konfiguriert, dass sie es zulässt, dass unidirektionale Kommunikationen von einem sendenden Gerät zu dem empfangenden Gerät übertragen werden, während sie Übertragungen von Kommunikationen vom empfangenden Gerät zum sendenden Gerät verhindert. Die Prozessanlagen-erzeugten Daten, die über die Datendiode empfangen werden (Block **502**), können erzeugte Prozessdaten, Diagnosedaten und andere Datentypen beinhalten und können am empfangenden Gerät wie dem Edge-Gateway **218** oder dem empfangenden Gerät **405** empfangen werden. Die empfangenen Prozessanlagen-erzeugten Daten können gesicherte Daten sein, z.B. Daten, die mit den oben erörterten Verschlüsselungstechniken gesichert wurden, oder mit einem anderen Sicherheitsmechanismus.

[0105] In Block **505** beinhaltet das Verfahren **500** das Sichern der empfangenen Prozessanlagen-erzeugten Daten mit einem oder mehreren Sicherheitsmechanismen, die denselben Sicherheitsmechanismus beinhalten können, der über die Datendiode benutzt wurde, oder können einen oder mehrere unterschiedliche Sicherheitsmechanismen beinhalten. In Block **508** beinhaltet das Verfahren **500** das Übertragen der an Block **505** gesicherten Prozessanlagen-erzeugten Daten zu einem anderen System, das kommunikativ mit dem empfangenden Gerät verbunden ist. Zum Beispiel, die gesicherten, Prozessanlagen-erzeugten Daten werden zu einem oder mehreren fernen Systemen **210** übertragen, auf denen eine oder mehrere Anwendungen, Dienste oder andere Verbraucher der Prozessanlagen-erzeugten Daten **208** resident sind und laufen. Die Anwendungen, Dienste oder anderen Verbraucher können auf wenigstens einigen der Prozessanlagen-erzeugten Daten wirken.

[0106] In einer Ausgestaltung beinhaltet das Sichern der empfangenen Prozessanlagen-erzeugten Daten (Block **505**) und das Übertragen der gesicherten Prozessanlagen-erzeugten Daten zu dem anderen System (Block **508**) das Einrichten einer gesicherten Verbindung zwischen dem empfangenden Gerät und dem anderen System. Das Übertragen der gesicherten Prozessanlagen-erzeugten Daten zu dem anderen System (Block **508**) kann das Übertragen der Daten über ein oder mehrere öffentliche oder private Netzwerke wie zum Beispiel das öffentliche Internet, ein privates Unternehmensnetzwerk usw. beinhalten. Somit beinhaltet das Einrichten der gesicherten Verbindung zwischen dem empfangenden Gerät und dem anderen System das Einrichten einer gesicherten Verbindung durch ein oder mehrere öffentliche und/oder private Netzwerke. Es können bei Bedarf unterschiedliche gesicherte Verbindungen für unterschiedliche Typen von Inhaltsdaten, unterschiedliche datenerzeugende Quellen der Prozessanlage und/oder unterschiedliche Verbraucher der Inhaltsdaten eingerichtet werden.

[0107] In einem Beispiel wird die Verbindung zwischen dem empfangenden Gerät und dem anderen System mit einem Token-Service gesichert. Das empfangende Gerät authentifiziert sich bei einem Token-Service, der von dem anderen System bereitgestellt wird, und das empfangende Gerät empfängt als Reaktion auf die Authentifizierung ein SAS-(Shared Access Signature)-Token von dem anderen System. Das empfangende Gerät benutzt dann das SAS-Token beim Übertragen von Inhaltsdaten (z.B. Prozessanlagen-erzeugte Daten) zu dem anderen System. Zum Beispiel, das empfangende Gerät benutzt das SAS-Token zum Sichern und Authentifizieren einer Verbindung mit dem anderen System, z.B. über eine AMQP (Advanced Message Queuing Protocol)-Verbindung. Zusätzlich können bei Bedarf die Inhaltsdaten und das SAS-Token vor dem Übertragen zu dem anderen System verschlüsselt werden.

[0108] Das Verfahren **500** kann auch das Neusichern einer Verbindung zwischen dem empfangenden Gerät und dem anderen System beinhalten (Block **510**). Das Neusichern einer Verbindung zwischen dem empfangenden Gerät und dem anderen System **510** beinhaltet beispielsweise das Empfangen eines aktualisierten oder anderen SAS-Tokens von dem anderen System (z.B. von dem Token-Service an dem anderen System) zur Verwendung zum Übertragen von nachfolgenden Inhaltsdaten. Ein bestimmtes SAS-Token kann eine vordefinierte Ablaufperiode (z.B. fünf Minuten, zehn Minuten, weniger als eine Stunde oder eine andere Ablaufperiode, die konfigurierbar sein kann) haben. Nach Ablauf eines Tokens kann das empfangende Gerät das neue SAS-Token zur Verwendung für nachfolgende Nachrichten anfordern oder abrufen. Alternativ kann das andere System automatisch ein aktualisiertes oder neues SAS-Token für das empfangene Gerät zur Verwendung nach Ablauf des vorherigen Tokens senden.

[0109] Das Sichern und Neusichern von Verbindungen zwischen dem empfangenden Gerät und dem anderen System (z.B. Blöcke **505**, **508** und **510**) wurde zwar oben als SAS-Tokens und das AMQP-Protokoll benutzend beschrieben, aber dies ist nur eine von vielen möglichen Ausgestaltungen des Verfahrens **500**. Es können beliebige ein oder mehrere ge-

eignete IOT-Sicherheitsmechanismen mit dem Verfahren **500** benutzt werden, wie zum Beispiel X.509 Zertifikate, andere Token-Typen, andere IOT-Protokolle wie MQTT oder XMPP usw.

[0110] Ausgestaltungen der in der vorliegenden Offenbarung beschriebenen Techniken können jede beliebige Anzahl der folgenden Aspekte beinhalten, entweder allein oder in Kombination:

1. Ein System zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System, wobei das gesicherte Kommunikationstransportsystem Folgendes umfasst: eine Datendiode, die zwischen einem Netzwerk der Prozessanlage und einem Netzwerk des anderen Systems angeordnet ist, wobei die Datendiode konfiguriert ist, um zwei Weg-Kommunikationen zwischen dem Prozessanlagennetzwerk und dem Netzwerk des anderen Systems zu verhindern, wobei Daten, die von Geräten der Prozessanlage erzeugt werden, während die Prozessanlage zum Steuern eines Industrieprozesses arbeitet, von dem Prozessanlagennetzwerk verschlüsselt und über die Datendiode zu dem Netzwerk des anderen Systems transportiert werden.

2. Das System des vorherigen Aspekts, wobei Hardware der Datendiode zum Ausschließen eines physischen Kommunikationspfades zum Liefern von Kommunikationen konfiguriert ist, die vom Netzwerk des anderen Systems zu dem Prozessanlagennetzwerk gesendet werden.

3. Das System nach einem der vorherigen Aspekte, wobei Software der Datendiode konfiguriert ist zum Verhindern des Eintritts von vom Netzwerk des anderen Systems ausgesendeten Kommunikationen in das Prozessanlagennetzwerk.

4. Das System nach einem der vorherigen Aspekte, wobei die verschlüsselten Prozessanlagendaten über die Datendiode auf der Basis von TCP (Transmission Control Protocol), UDP (User Datagram Protocol) oder seriellen Kommunikationen transportiert werden.

5. Das System nach einem der vorherigen Aspekte, das ferner einen Field-Gateway umfasst, der das Prozessanlagennetzwerk mit der Datendiode verbindet, wobei der Field-Gateway die Prozessanlagendaten für den Transport über die Datendiode verschlüsselt.

6. Das System nach einem der vorherigen Aspekte, wobei der Field-Gateway an der Prozessanlage angeordnet ist.

7. Das System nach einem der vorherigen Aspekte, wobei die Datendiode an der Prozessanlage angeordnet ist.

8. Das System nach einem der vorherigen Aspekte, das ferner einen lokalen Anlagen-Gateway umfasst, der das Prozessanlagennetzwerk mit dem Field-Gateway verbindet, wobei der lokale Anlagen-Gateway die Prozessanlagendaten mit einem TLS-(Transport Layer Security)-Wrapper sichert.

9. Das System nach einem der vorherigen Aspekte, wobei wenigstens eines der Folgenden gilt: wenigstens ein erster Teil der von den in der Prozessanlage enthaltenen Geräte erzeugten Daten wird zu dem lokalen Anlagen-Gateway gestreamt; oder wenigstens ein zweiter Teil der von den in der Prozessanlage enthaltenen Geräte erzeugten Daten wird als Reaktion auf eine Abfrage zu dem lokalen Anlagen-Gateway gesendet.

10. Das System nach einem der vorherigen Aspekte, wobei die von dem Field-Gateway durchgeführte Verschlüsselung eine erste Verschlüsselung ist und wobei eine zweite Verschlüsselung von wenigstens einigen der von den Geräten erzeugten Daten an den Geräten durchgeführt wird.

11. Das System nach einem der vorherigen Aspekte, wobei die wenigstens einigen der von den Geräten erzeugten und verschlüsselten Daten über ein drahtloses Netzwerk und/oder ein verdrahtetes Netzwerk der Prozessanlage zum lokalen Anlagen-Gateway übertragen werden.

12. Das System nach einem der vorherigen Aspekte, das ferner einen Edge-Gateway umfasst, der die Datendiode mit dem Netzwerk des anderen Systems verbindet, wobei der Edge-Gateway die Prozessanlagendaten zum Übertragen zum Netzwerk des anderen Systems sichert.

13. Das System nach einem der vorherigen Aspekte, wobei der Edge-Gateway an der Prozessanlage angeordnet ist.

14. Das System nach einem der vorherigen Aspekte, wobei der Edge-Gateway die Lieferung der Prozessanlagendaten zum anderen System mit einem Token oder Zertifikat sichert.

15. Das System nach einem der vorherigen Aspekte, wobei: das Token oder Zertifikat von einem in dem anderen System enthaltenen Token-Sicherheitsdienst verwaltet wird; das Token oder Zertifikat für eine finite Zeitperiode gültig ist; und die finite Zeitperiode eine Dauer von maximal einer Stunde hat.

16. Das System nach einem der vorherigen Aspekte, wobei die gesicherten Prozessanlagendaten vom Edge-Gateway zum Netzwerk des anderen Systems mit wenigstens einem der Folgenden übertragen wird: einer Internet-Verbin-

dung, einem zellulären Router oder einem anderen Typ von Backhaul-Internet-Verbindung.

17. Das System nach einem der vorherigen Aspekte, wobei die Prozessanlagendaten an dem anderen System gespeichert werden und der Zugang zu den gespeicherten Daten an dem anderen System nur autorisierten Benutzern des anderen Systems gewährt wird.

18. Das System nach einem der vorherigen Aspekte, das ferner Folgendes umfasst: einen Field-Gateway, der das Prozessanlagennetzwerk mit der Datendiode verbindet; und einen Edge-Gateway, der die Datendiode mit dem Netzwerk des anderen Systems verbindet, wobei die über die Datendiode transportierten Prozessanlagendaten mit Schlüsselmaterial verschlüsselt werden, die von dem Field-Gateway und dem Edge-Gateway gemeinsam genutzt werden.

19. Das System nach einem der vorherigen Aspekte, wobei der Field-Gateway in der Prozessanlage enthalten ist.

20. Das System nach einem der vorherigen Aspekte, wobei der Edge-Gateway in der Prozessanlage enthalten ist.

21. Das System nach einem der vorherigen Aspekte, wobei das andere System in der Prozessanlage enthalten ist.

22. Das System nach einem der vorherigen Aspekte, wobei das andere System in einer oder mehreren Computing-Clouds enthalten ist.

23. Das System nach einem der vorherigen Aspekte, wobei das andere System über das öffentliche Internet zugänglich ist.

24. Das System nach einem der vorherigen Aspekte, wobei das andere System nicht über das öffentliche Internet zugänglich ist.

25. Das System nach einem der vorherigen Aspekte, wobei das andere System einen oder mehrere der Prozessanlage entsprechende Dienste bereitstellt, wobei die ein oder mehreren Dienste wenigstens eines der Folgenden beinhalten: Überwachen von Zuständen und/oder Ereignissen, die an der Prozessanlage auftreten; Erfassen der Zustände und/oder Ereignisse, die an der Prozessanlage auftreten; Überwachen wenigstens eines Teils eines von der Prozessanlage gesteuerten Prozesses; deskriptive Analytik; präskriptive Analytik; oder eine oder mehrere präskriptive Änderungen zum Modifizieren wenigstens eines Teils der Prozessanlage.

26. Das System nach einem der vorherigen Aspekte, wobei: wenigstens eines der Geräte mit einem anderen Gerät in der Prozessanlage über ein in der Prozessanlage enthaltenes Kommunikationsnetzwerk kommuniziert, zum Steuern wenigstens eines Teils eines Prozesses in der Prozessanlage, wobei sich das Kommunikationsnetzwerk von dem Prozessanlagennetzwerk unterscheidet, und das Kommunikationsnetzwerk wenigstens eines der Folgenden unterstützt: WiFi-Protokoll, ein Ethernet-Protokoll, und ein Protokoll gemäß IEEE **802.11**, mobiles Kommunikationsprotokoll, ein Kurzwellenlängen-Funkkommunikationsprotokoll, 4-20 ma Signalisierung, das HART® Protokoll, das WirelessHART® Protokoll, das FOUNDATION® Fieldbus Protokoll, das PROFIBUS Protokoll oder das DeviceNet Protokoll.

27. Das System nach einem der vorherigen Aspekte, wobei das in der Prozessanlage enthaltene Kommunikationsnetzwerk ein erstes Kommunikationsnetzwerk ist und wobei die Datendiode die erzeugten Daten von den ein oder mehreren Geräten über das Prozessanlagennetzwerk empfängt.

28. Das System nach einem der vorherigen Aspekte, wobei das Prozessanlagennetzwerk das HART-IP® Protokoll unterstützt.

29. Ein Verfahren zum Sichern von Kommunikationen zwischen einer Prozessanlage und einem anderen System, wobei das Verfahren Folgendes beinhaltet: Empfangen, an einem Field-Gateway von einem Prozessanlagennetzwerk, von Daten, die von einem oder mehreren Geräten der Prozessanlage erzeugt werden, während die Prozessanlage in Betrieb ist, um einen Industrieprozess zu steuern, wobei die Prozessanlagendaten zum Übertragen von den ein oder mehreren Geräten zu dem Field-Gateway über einen ersten Sicherheitsmechanismus gesichert werden; Sichern, durch den Field-Gateway, der Prozessanlagendaten über einen zweiten Sicherheitsmechanismus; und Transportieren der gesicherten Prozessanlagendaten über eine Datendiode zur Lieferung zu dem anderen System über einen Edge-Gateway, wobei der Edge-Gateway kommunikativ mit dem anderen System verbunden ist, wobei die kommunikative Verbindung zwischen dem Edge-Gateway und dem anderen System über einen dritten Sicherheitsmechanismus gesichert wird und wobei die Datendiode zum Verhindern des Eintretens von vom Edge-Gateway übertragenen Daten in den Field-Gateway konfiguriert ist.

30. Das Verfahren nach dem vorherigen Aspekt, von dem wenigstens ein Teil von dem System nach einem der Aspekte **1**-**28** ausgeführt wird.

31. Das Verfahren nach einem der Aspekte **29**-**30**, wobei der erste Sicherheitsmechanismus, der zweite Sicherheitsmechanismus und

der dritte Sicherheitsmechanismus unterschiedliche Sicherheitsmechanismen sind.

32. Das Verfahren nach einem der Aspekte **29**-**31**, das ferner das Provisionieren des Field-Gateway und des Edge-Gateway einschließlich des Erzeugens eines Schlüssels beinhaltet, der von dem Field-Gateway und dem Edge-Gateway gemeinsam genutzt wird; und wobei das Sichern, durch den Field-Gateway, der Prozessanlagendaten über den zweiten Sicherheitsmechanismus ferner das Sichern, durch den Field-Gateway, der Prozessanlagendaten mit dem gemeinsamen Schlüssel beinhaltet.

33. Das Verfahren nach einem der Aspekte **29**-**32**, wobei das Sichern, durch den Field-Gateway, der Prozessanlagendaten über den zweiten Sicherheitsmechanismus ferner das Verschlüsseln, durch den Field-Gateway, der Prozessanlagendaten beinhaltet.

34. Das Verfahren nach einem der Aspekte **29**-**33**, wobei der erste Sicherheitsmechanismus ein Verschlüsseln, durch die ein oder mehreren Geräten, der von den ein oder mehreren Geräten erzeugten Daten beinhaltet.

35. Das Verfahren nach einem der Aspekte **29**-**34**, wobei der erste Sicherheitsmechanismen ferner ein Wrapping der verschlüsselten Prozessanlagendaten in einer in der Prozessanlage implementierten Sicherheitsschicht beinhaltet.

36. Das Verfahren nach einem der Aspekte **29**-**35**, wobei der dritte Sicherheitsmechanismus ein Sicherheits-Token oder -Zertifikat beinhaltet.

37. Das Verfahren nach einem der Aspekte **29**-**36**, wobei der dritte Sicherheitsmechanismus ein vom Edge-Gateway durchgeführtes Verschlüsseln beinhaltet.

38. Ein Verfahren zum Sichern von Kommunikationen zwischen einer Prozessanlage und einem anderen System, das die Prozessanlage bedient, wobei das Verfahren Folgendes beinhaltet: Empfangen, an einem Edge-Gateway über eine Datendiode, die kommunikativ mit einem Field-Gateway der Prozessanlage verbunden ist, von Daten, die von einem oder mehreren Geräten der Prozessanlage erzeugt werden, während die Prozessanlage zum Steuern eines Industrieprozesses arbeitet, wobei: die Prozessanlagendaten zum Übertragen von den ein oder mehreren Geräten zu dem Field-Gateway über einen ersten Sicherheitsmechanismus gesichert werden und ferner für einen Transport vom Field-Gateway über die Datendiode zum Edge-Gateway über einen zweiten Sicherheitsmechanismus gesichert werden, und die Datendiode zum Verhindern des Eintretens von vom Edge-Gateway übertragenen Daten in den Field-Gateway konfiguriert ist. Das Verfahren beinhaltet ferner das Sichern, durch den Edge-Gateway, der Prozessanlagendaten über einen dritten Mechanismus; und Übertragen, durch den Edge-Gateway , der gesicherten Prozessanlagendaten zu dem anderen System.

39. Das Verfahren des vorherigen Aspekts in Kombination mit einem der Verfahren der Aspekte **29**-**37**.

40. Das Verfahren nach Aspekt **38** oder Aspekt **39**, von dem wenigstens ein Teil von dem System nach einem der Aspekte **1**-**28** ausgeführt wird.

41. Das Verfahren nach einem der Aspekte **38**-**40**, wobei der erste Sicherheitsmechanismus, der zweite Sicherheitsmechanismus und der dritte Sicherheitsmechanismus unterschiedliche Sicherheitsmechanismen sind.

42. Das Verfahren nach einem der Aspekte **38**-**41**, wobei der erste Sicherheitsmechanismus und/oder der zweite Sicherheitsmechanismus eine jeweilige Verschlüsselung der Prozessanlagendaten beinhaltet/beinhalten.

43. Das Verfahren nach einem der Aspekte **38**-**42**, wobei der erste Sicherheitsmechanismus ein Wrapping der Prozessanlagendaten in einer Sicherheitsschicht beinhaltet.

44. Das Verfahren nach einem der Aspekte **38**-**43**, das ferner das Einrichten einer gesicherten Verbindung zwischen dem Edge-Gateway und dem Field-Gateway über die Datendiode mit einem Geheimschlüssel beinhaltet und wobei der zweite Sicherheitsmechanismus die zwischen dem Edge-Gateway und dem Field-Gateway eingerichtete gesicherte Verbindung umfasst.

45. Das Verfahren nach einem der Aspekte **38**-**44**, wobei der zweite Sicherheitsmechanismus ferner ein Verschlüsseln, durch den Field-Gateway, der Prozessanlagendaten umfasst.

46. Das Verfahren nach einem der Aspekte **38**-**45**, das ferner das Einrichten einer gesicherten Verbindung zwischen dem Edge-Gateway und dem anderen System umfasst und wobei der dritte Sicherheitsmechanismus die zwischen dem Edge-Gateway und dem anderen System eingerichtete gesicherte Verbindung beinhaltet.

47. Das Verfahren nach einem der Aspekte **38**-**46**, wobei das Einrichten der gesicherten Verbindung zwischen dem Edge-Gateway und dem anderen System Folgendes beinhaltet: Authentifizieren bei einem von dem anderen System bereitgestellten Sicherheitsdienst; und Empfangen, als Reaktion auf die Authentifizierung, eines Sicherheits-Tokens oder -Zertifikats.

48. Das Verfahren nach einem der Aspekte **38**-**47**, wobei das Übertragen der gesicherten Prozessanlagendaten zu dem anderen System das Übertragen des Sicherheits-Tokens oder -Zertifikats zu dem anderen System in Verbindung mit den Prozessanlagendaten beinhaltet.

49. Das Verfahren nach einem der Aspekte **38**-**48**, wobei das Sicherheits-Token oder -Zertifikat ein erstes Sicherheit-Token oder -Zertifikat ist und das Verfahren ferner das Empfangen eines anderen Sicherheits-Tokens oder -Zertifikats beinhaltet, das beim Übertragen von nachfolgenden von den ein oder mehreren Geräten erzeugten Daten zu dem anderen System zu benutzen ist.

50. Das Verfahren nach einem der Aspekte **38**-**49**, wobei das Sichern, durch den Edge-Gateway, der Prozessanlagendaten über den dritten Mechanismus das Verschlüsseln, durch den Edge-Gateway, der Prozessanlagendaten beinhaltet.

51. Das Verfahren nach einem der Aspekte **38**-**50**, wobei das Übertragen der gesicherten Prozessanlagendaten zu dem anderen System das Übertragen der gesicherten Prozessanlagendaten zu einem in der Prozessanlage enthaltenen System beinhaltet.

52. Das Verfahren nach einem der Aspekte **38**-**51**, wobei das Übertragen der gesicherten Prozessanlagendaten zu dem anderen System das Übertragen der gesicherten Prozessanlagendaten zu einem System beinhaltet, das in einer oder mehreren Computing-Clouds implementiert wird.

53. Das Verfahren nach einem der Aspekte **38**-**52**, wobei das Übertragen der Prozessanlagendaten zu dem anderen System das Übertragen der Prozessanlagendaten zu dem anderen System über eine gesicherte Verbindung über das öffentliche Internet beinhaltet.

54. Das Verfahren nach einem der Aspekte **38**-**53**, wobei das Übertragen der Prozessanlagendaten zu dem anderen System das Übertragen der Prozessanlagendaten zu einem System beinhaltet, das wenigstens eines der Folgenden bereitstellt: Überwachen von Zuständen und/oder Ereignissen, die an der Prozessanlage auftreten; Erfassen der Zustände und/oder Ereignisse, die an der Prozessanlage auftreten; Überwachen wenigstens eines Teils eines von der Prozessanlage ausgeführten Prozesses; deskriptive Analytik; präskriptive Analytik; oder eine präskriptive Änderung zum Modifizieren wenigstens eines Teils der Prozessanlage.

55. Ein beliebiger der vorherigen Aspekte in Kombination mit einem beliebigen anderen der vorherigen Aspekte.

[0111] Wenn in Software implementiert, dann können beliebige der hierin beschriebenen Anwendungen, Dienste und Engines in einem beliebigen fassbaren, nichtflüchtigen, computerlesbaren Speicher wie auf einer Magnetplatte, einer Laserplatte, einem Solid-State-Speichergerät, einem Molekularmemory-Speichergerät oder einem anderen Speichergerät, in einem RAM oder ROM eines Computers oder Prozessors usw. gespeichert werden. Die hierin offenbarten beispielhaften Systeme sind zwar so offenbart, dass sie u.a. auf Hardware ausgeführte Komponenten, Software und/oder Firmware beinhalten, aber es ist zu bemerken, dass solche Systeme lediglich illustrativ sind und nicht als begrenzend anzusehen sind. Zum Beispiel, es ist vorgesehen, dass beliebige oder alle dieser Hardware-, Software- und Firmware-Komponenten ausschließlich in Hardware, ausschließlich in Software oder in einer beliebigen Kombination aus Hardware und Software ausgestaltet sein könnten. Demgemäß wurden die hierin beschriebenen beispielhaften Systeme zwar als in Software implementiert beschrieben, ausgeführt auf einem Prozessor von einem oder mehreren Computergeräten, aber die durchschnittliche Fachperson wird leicht erkennen, dass die gegebenen Beispiele nicht die einzige Möglichkeit sind, um solche Systeme zu implementieren.

[0112] Während also die vorliegende Erfindung mit Bezug auf spezifische Beispiele beschrieben wurde, die lediglich illustrativ sein und die Erfindung nicht begrenzen sollen, wird die durchschnittliche Fachperson erkennen, dass Änderungen, Hinzufügungen oder Weglassungen an den offenbarten Ausgestaltungen vorgenommen werden können, ohne von Wesen und Umfang der Erfindung abzuweichen.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- US 14/507188 [0001, 0053]
- US 15/274519 [0001, 0040]
- US 15/274233 [0001, 0040]
- US 15/332521 [0001, 0040]

Patentansprüche

1. System zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System, wobei das gesicherte Kommunikationstransportsystem Folgendes umfasst:
eine Datendiode, die zwischen einem Netzwerk der Prozessanlage und einem Netzwerk des anderen Systems angeordnet ist, wobei die Datendiode zum Verhindern von Zweiweg-Kommunikationen zwischen dem Prozessanlagennetzwerk und dem Netzwerk des anderen Systems konfiguriert ist,
wobei Daten, die von Geräten der Prozessanlage erzeugt werden, während die Prozessanlage zum Steuern eines Industrieprozesses arbeitet, von dem Prozessanlagennetzwerk verschlüsselt und über die Datendiode zu dem Netzwerk des anderen Systems transportiert werden.

2. System nach Anspruch 1, wobei Hardware der Datendiode zum Ausschließen eines physischen Kommunikationspfades zum Liefern von vom Netzwerk des anderen Systems ausgesendeten Kommunikationen zum Prozessanlagennetzwerk konfiguriert ist.

3. System nach einem der Ansprüche 1 oder 2, insbesondere nach Anspruch 1, wobei Software der Datendiode zum Verhindern des Eintritts von vom Netzwerk des anderen Systems ausgesendeten Kommunikationen in das Prozessanlagennetzwerk konfiguriert ist.

4. System nach einem der Ansprüche 1 bis 3, insbesondere nach Anspruch 1, wobei die verschlüsselten Prozessanlagendaten über die Datendiode auf der Basis von TCP (Transmission Control Protocol), UDP (User Datagram Protocol) oder seriellen Kommunikationen transportiert werden.

5. System nach einem der Ansprüche 1 bis 4, insbesondere nach Anspruch 1, das ferner einen Field-Gateway umfasst, der das Prozessanlagennetzwerk mit der Datendiode verbindet, wobei der Field-Gateway die Prozessanlagendaten für einen Transport über die Datendiode verschlüsselt, und/oder
wobei der Field-Gateway an der Prozessanlage angeordnet ist, und, insbesondere
, wobei die Datendiode an der Prozessanlage angeordnet ist, und/oder
das ferner einen lokalen Anlagen-Gateway umfasst, der das Prozessanlagennetzwerk mit dem Field-Gateway verbindet, wobei der lokale Anlagen-Gateway die Prozessanlagendaten mit einem TLS-(Transport Layer Security)-Wrapper sichert, und, insbesondere
wobei wenigstens eines der Folgenden gilt:
wenigstens ein erster Teil der von den in der Prozessanlage enthaltenen Geräten erzeugten Daten wird zu dem lokalen Anlagen-Gateway gestreamt; oder
wenigstens ein zweiter Teil der von den in der Prozessanlage enthaltenen Geräten erzeugten Daten wird als Reaktion auf eine Abfrage zum lokalen Anlagen-Gateway gesendet, und/oder
wobei die vom Field-Gateway durchgeführte Verschlüsselung eine erste Verschlüsselung ist und wobei eine zweite Verschlüsselung von wenigstens einigen der von den Geräten erzeugten Daten an den Geräten durchgeführt wird, und, insbesondere,
wobei die wenigstens einigen der von den Geräten erzeugten und verschlüsselten Daten über ein drahtloses Netzwerk und/oder ein verdrahtetes Netzwerk der Prozessanlage zu dem lokalen Anlagen-Gateway übertragen werden.

6. System nach einem der Ansprüche 1 bis 5, insbesondere nach Anspruch 1, das ferner einen Edge-Gateway umfasst, der die Datendiode mit dem Netzwerk des anderen Systems verbindet, wobei der Edge-Gateway die Prozessanlagendaten zur Übertragung zum Netzwerk des anderen Systems sichert, und/oder
wobei der Edge-Gateway an der Prozessanlage angeordnet ist, und/oder
wobei der Edge-Gateway die Lieferung der Prozessanlagendaten zu dem anderen System mit einem Token oder Zertifikat sichert, und, insbesondere
, wobei:
das Token oder Zertifikat von einem in dem anderen System enthaltenen Sicherheitsdienst verwaltet wird;
das Token oder Zertifikat für eine finite Zeitperiode gültig ist; und
die finite Zeitperiode eine Dauer von maximal einer Stunde hat, und/oder
wobei die gesicherten Prozessanlagendaten vom Edge-Gateway zum Netzwerk des anderen Systems mit wenigstens einem der Folgenden übertragen wird: einer Internet-Verbindung, einem zellulären Router oder einem anderen Typ von Backhaul-Internet-Verbindung.

7. System nach einem der Ansprüche 1 bis 6, insbesondere nach Anspruch 1, wobei die Prozessanlagendaten an dem anderen System gespeichert werden und der Zugang zu den gespeicherten Daten an dem anderen System nur autorisierten Benutzern des anderen Systems gewährt wird.

8. System nach einem der Ansprüche 1 bis 7, insbesondere nach Anspruch 1, das ferner Folgendes umfasst:
einen Field-Gateway, der das Prozessanlagennetzwerk mit der Datendiode verbindet; und
einen Edge-Gateway, der die Datendiode mit dem Netzwerk des anderen Systems verbindet,
wobei die Prozessanlagendaten, die über die Datendiode transportiert werden, mit Schlüsselmaterial verschlüsselt werden, das von dem Field-Gateway und dem Edge-Gateway gemeinsam genutzt wird, und/oder

wobei der Field-Gateway in der Prozessanlage enthalten ist und/oder
wobei der Edge-Gateway in der Prozessanlage enthalten ist und/oder
wobei das andere System in der Prozessanlage enthalten ist und/oder
wobei das andere System in einer oder mehreren Computing-Clouds implementiert wird und/oder
wobei das andere System über das öffentliche Internet zugänglich ist und/oder
wobei das andere System nicht über das öffentliche Internet zugänglich ist.

9. System nach einem der Ansprüche 1 bis 8, insbesondere nach Anspruch 1, wobei das andere System einen oder mehrere der Prozessanlage entsprechende Dienste bereitstellt, wobei die ein oder mehreren Dienste wenigstens eines der Folgenden beinhalten:
Überwachen von Zuständen und/oder Ereignissen, die an der Prozessanlage auftreten;
Erfassen der Zustände und/oder Ereignisse, die an der Prozessanlage auftreten;
Überwachen wenigstens eines Teils eines von der Prozessanlage gesteuerten Prozesses;
deskriptive Analytik;
präskriptive Analytik; oder
eine oder mehrere präskriptive Änderungen zum Modifizieren wenigstens eines Teils der Prozessanlage.

10. System nach einem der Ansprüche 1 bis 9, insbesondere nach Anspruch 1, wobei:
wenigstens eines der Geräte mit einem anderen Gerät in der Prozessanlage über ein Kommunikationsnetzwerk kommuniziert, das in der Prozessanlage enthalten ist, um wenigstens einen Teil eines Prozesses in der Prozessanlage zu steuern,
das Kommunikationsnetzwerk sich vom Prozessanlagennetzwerk unterscheidet, und
das Kommunikationsnetzwerk wenigstens eines der Folgenden unterstützt: ein WiFi-Protokoll, ein Ethernet-Protokoll, und ein Protokoll gemäß IEEE 802.11, mobiles Kommunikationsprotokoll, ein Kurzwellenlängen-Funkkommunikationsprotokoll, 4-20 ma Signalisierung, das HART® Protokoll, das Wireless-HART® Protokoll, das FOUNDATION® Fieldbus Protokoll, das PROFIBUS Protokoll oder das DeviceNet Protokoll, und/oder
wobei das in der Prozessanlage enthaltene Kommunikationsnetzwerk ein erstes Kommunikationsnetzwerk ist und wobei die Datendiode die erzeugten Daten von den ein oder mehreren Geräten über das Prozessanlagennetzwerk empfängt, und/oder
wobei das Prozessanlagennetzwerk das HART-IP® Protokoll unterstützt.

11. Verfahren zum Sichern von Kommunikationen zwischen einer Prozessanlage und einem anderen System, wobei das Verfahren Folgendes beinhaltet:
Empfangen, an einem Field-Gateway von einem Prozessanlagennetzwerk, von Daten, die von einem oder mehreren Geräten der Prozessanlage erzeugt werden, während die Prozessanlage zum Steuern eines Industrieprozesses arbeitet, wobei die Prozessanlagendaten zur Übertragung von den ein oder mehreren Geräten zu dem Field-Gateway über einen ersten Sicherheitsmechanismus gesichert werden;
Sichern, durch den Field-Gateway, der Prozessanlagendaten über einen zweiten Sicherheitsmechanismen; und
Transportieren der gesicherten Prozessanlagendaten über eine Datendiode zur Lieferung zu dem anderen System über einen Edge-Gateway, wobei der Edge-Gateway kommunikativ mit dem anderen System verbunden ist, wobei die kommunikative Verbindung zwischen dem Edge-Gateway und dem anderen System über einen dritten Sicherheitsmechanismus gesichert wird und die Datendiode zum Verhindern des Eintretens von vom Edge-Gateway übertragenen Daten in den Field-Gateway konfiguriert ist.

12. Verfahren nach Anspruch 11, wobei der erste Sicherheitsmechanismus, der zweite Sicherheitsmechanismus und der dritte Sicherheitsmechanismus unterschiedliche Sicherheitsmechanismen sind.

13. Verfahren nach einem der Ansprüche 11 oder 12, insbesondere nach Anspruch 1,
das ferner das Provisionieren des Field-Gateway und des Edge-Gateway beinhaltet, einschließlich des Erzeugens eines Schlüssels, der von dem Field-Gateway und dem Edge-Gateway gemeinsam benutzt wird; und
wobei das Sichern, durch den Field-Gateway, der Prozessanlagendaten über den zweiten Sicherheitsmechanismus das Sichern, durch den Field-Gateway, der Prozessanlagendaten mit dem Gemeinschaftsschlüssel beinhaltet, und/oder
wobei das Sichern, durch den Field-Gateway, der Prozessanlagendaten über den zweiten Sicherheitsmechanismus ferner das Verschlüsseln, durch den Field-Gateway, der Prozessanlagendaten beinhaltet.

14. Verfahren nach einem der Ansprüche 11 bis 13, insbesondere nach Anspruch 11, wobei der erste Sicherheitsmechanismus eine Verschlüsselung, durch die ein oder mehreren Geräte, der von den ein oder mehreren Geräten erzeugten Daten beinhaltet, und/oder
wobei der erste Sicherheitsmechanismus ferner ein Wrapping der verschlüsselten Prozessanlagendaten in einem in der Prozessanlage implementierten Sicherheitsschicht beinhaltet, und/oder
wobei der dritte Sicherheitsmechanismus ein Sicherheits-Token oder -Zertifikat umfasst und/oder
wobei der dritte Sicherheitsmechanismus eine durch den Edge-Gateway durchgeführte Verschlüsselung umfasst.

15. Verfahren zum Sichern von Kommunikationen zwischen einer Prozessanlage und einem anderen System, das die Prozessanlage bedient, wobei das Verfahren Folgendes beinhaltet:
Empfangen, an einem Edge-Gateway, über eine Datendiode, die kommunikativ mit einem Field-Gateway der Prozessanlage verbunden ist, von Daten, die von einem oder mehreren Geräten der Prozessanlage erzeugt werden, während die Prozessanlage zum Steuern eines Industrieprozesses arbeitet, wobei:
die Prozessanlagendaten zum Übertragen von den ein oder mehreren Geräten zu dem Field-Gateway über einen ersten Sicherheitsmechanismus gesichert werden und ferner für einen Transport vom Field-Gateway über die Datendiode zum Edge-Gateway über einen zweiten Sicherheitsmechanismen muss gesichert werden, und
die Datendiode zum Verhindern des Eintritts von vom Edge-Gateway übertragenen Daten in den Field-Gateway konfiguriert ist;
Sichern, durch den Edge-Gateway, der Prozessanlagendaten über einen dritten Mechanismus; und
Übertragen, durch den Edge-Gateway, der gesicherten Prozessanlagendaten zu dem anderen System.

16. Verfahren nach Anspruch 15, wobei der erste Sicherheitsmechanismus, der zweite Sicherheitsmechanismus und der dritte Sicherheitsmechanismus unterschiedliche Sicherheitsmechanismen sind.

17. Verfahren nach einem der Ansprüche 15 oder 16, insbesondere nach Anspruch 15, wobei der erste Sicherheitsmechanismus und/oder der zweite Sicherheitsmechanismus eine jeweilige Verschlüsselung der Prozessanlagendaten beinhaltet/beinhalten, und/oder wobei der erste Sicherheitsmechanismus ein Wrapping der Prozessanlagendaten in einer Sicherheitsschicht beinhaltet.

18. Verfahren nach einem der Ansprüche 15 bis 17, insbesondere nach Anspruch 15, das ferner das Einrichten einer gesicherten Verbindung zwischen dem Edge-Gateway und dem Field-Gateway über die Datendiode mit einem Geheimschlüssel beinhaltet und wobei der zweite Sicherheitsmechanismus die zwischen dem Edge-Gateway und dem Field-Gateway eingerichtete gesicherte Verbindung umfasst, und/oder wobei der zweite Sicherheitsmechanismus ferner eine Verschlüsselung, durch den Field-Gateway, der Prozessanlagendaten beinhaltet.

19. Verfahren nach einem der Ansprüche 15 bis 18, insbesondere nach Anspruch 15, das ferner das Einrichten einer gesicherten Verbindung zwischen dem Edge-Gateway und dem anderen System beinhaltet, und wobei der dritte Sicherheitsmechanismus muss die zwischen dem Edge-Gateway und dem anderen System eingerichtete gesicherte Verbindung beinhaltet, und/oder wobei das Einrichten der gesicherten Verbindung zwischen dem Edge-Gateway und dem anderen System Folgendes beinhaltet:
Authentifizieren bei einem von dem anderen System bereitgestellten Sicherheitsdienst; und
Empfangen, als Reaktion auf die Authentifizierung, eines Sicherheits-Tokens oder - Zertifikats, und, insbesonders
, wobei das Übertragen der gesicherten Prozessanlagendaten zu dem anderen System das Übertragen des Sicherheits-Tokens oder -Zertifikats zu dem anderen System in Verbindung mit den Prozessanlagendaten beinhaltet, und, spezifischer
wobei das Sicherheits-Token oder -Zertifikat ein erstes Sicherheits-Token oder - Zertifikat ist und das Verfahren ferner das Empfangen eines anderen Sicherheits-Tokens oder -Zertifikats beinhaltet, das beim Übertragen von nachfolgenden von den ein oder mehreren Geräten erzeugten Daten zu dem anderen System zu benutzen ist.

20. Verfahren nach einem der Ansprüche 15 bis 19, insbesondere nach Anspruch 15, wobei das Sichern, durch den Edge-Gateway, der Prozessanlagendaten über den dritten Mechanismus das Verschlüsseln, durch den Edge-Gateway, der Prozessanlagendaten beinhaltet.

21. Verfahren nach einem der Ansprüche 15 bis 20, insbesondere nach Anspruch 15, wobei das Übertragen der gesicherten Prozessanlagendaten zu dem anderen System das Übertragen der gesicherten Prozessanlagendaten zu einem in der Prozessanlage enthaltenen System beinhaltet, und/oder
wobei das Übertragen der gesicherten Prozessanlagendaten zu dem anderen System das Übertragen der gesicherten Prozessanlagendaten zu einem in einer oder mehreren Computing-Clouds implementierten System beinhaltet, und/oder
wobei des Übertragen der Prozessanlagendaten zu dem anderen System das Übertragen der Prozessanlagendaten zu dem anderen System über eine gesicherte Verbindung über das öffentliche Internet beinhaltet, und/oder
wobei das Übertragen der Prozessanlagendaten zu dem anderen System das Übertragen der Prozessanlagendaten zu einem System beinhaltet, das wenigstens eines der Folgenden bereitstellt:
Überwachen von Zuständen und/oder Ereignissen, die an der Prozessanlage auftreten;
Erfassen der Zustände und/oder Ereignisse, die an der Prozessanlage auftreten;
Überwachen wenigstens eines Teils eines von der Prozessanlage ausgeführten Prozesses;
deskriptive Analytik;
präskriptive Analytik; oder
eine präskriptive Änderung zum Modifizieren wenigstens eines Teils der Prozessanlage.

22. Computerlesbares Speichermedium, welches Instruktionen enthält, die mindestens einen Prozes-

sor dazu veranlassen, ein Verfahren nach einem der Ansprüche 15 bis 21 zu implementieren, wenn die Instruktionen durch mindestens einen Prozessor ausgeführt werden

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

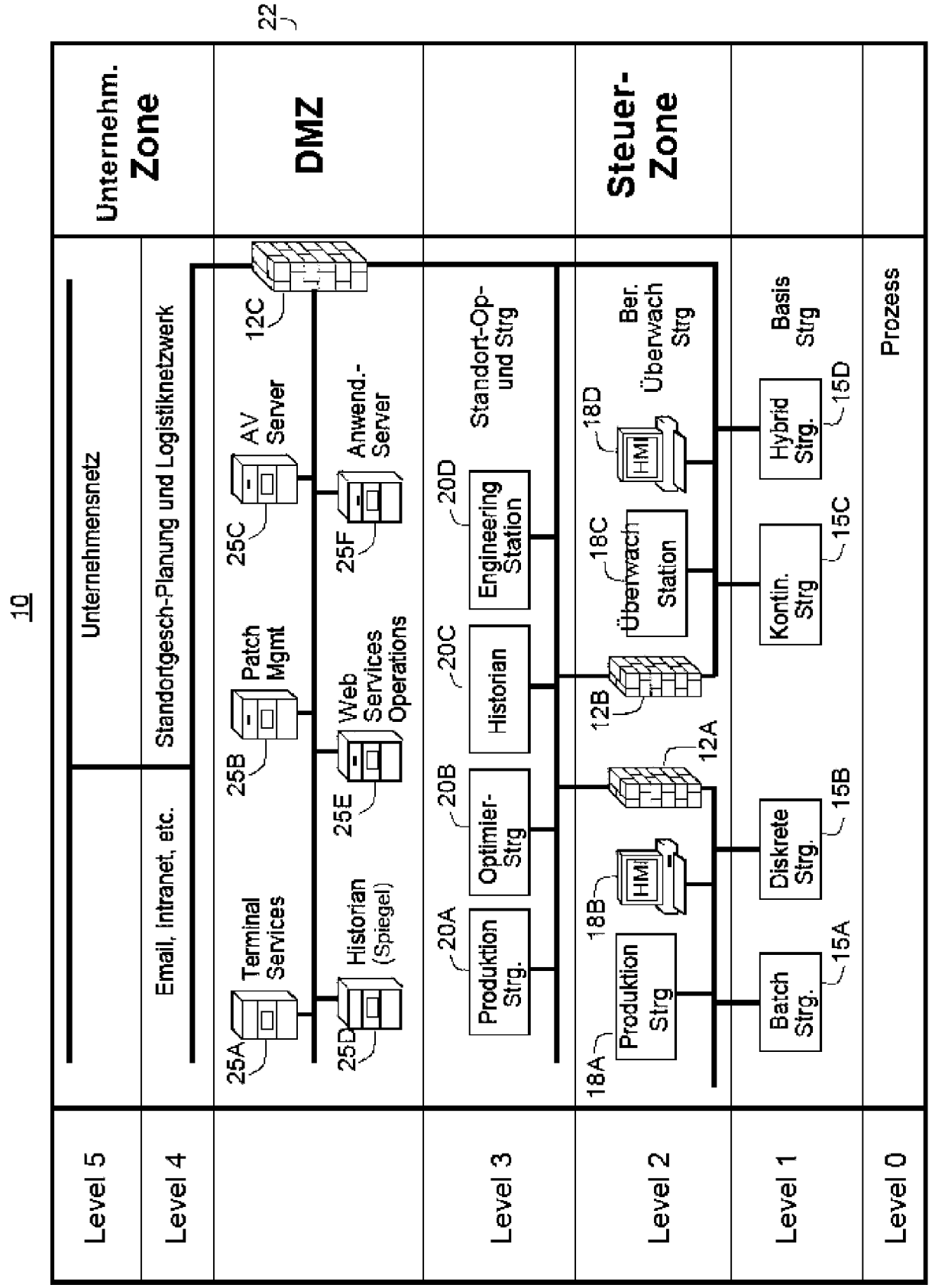


FIG. 1

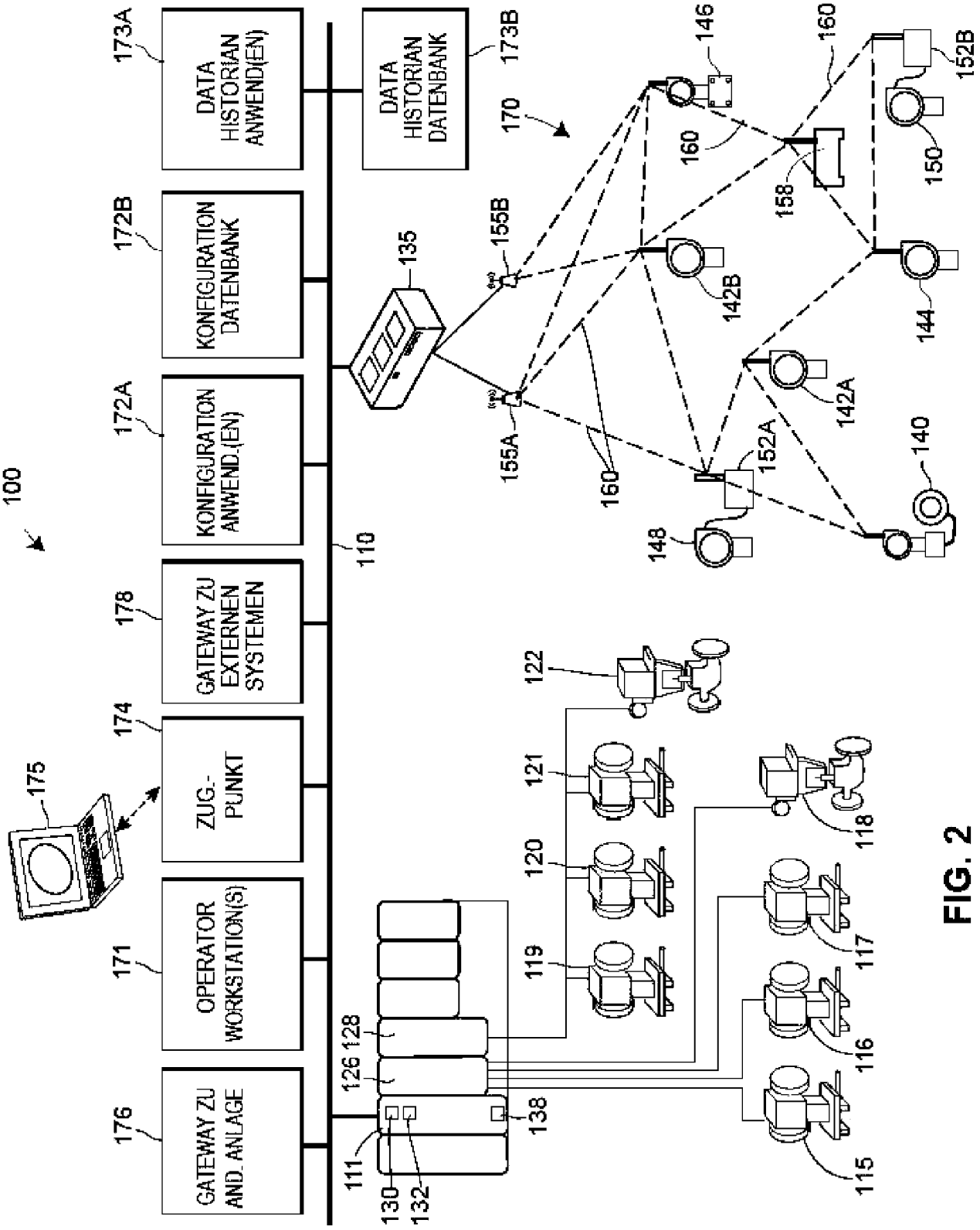

100
110
DATA HISTORIAN ANWEND(EN)
173A
DATA HISTORIAN DATENBANK
173B
KONFIGURATION DATENBANK
172B
KONFIGURATION ANWEND.(EN)
172A
GATEWAY ZU EXTERNEN SYSTEMEN
178
ZUG.-PUNKT
174
OPERATOR WORKSTATION(S)
171
GATEWAY ZU AND. ANLAGE
176
135
170
155A
155B
160
146
148
150
152A
152B
140
142A
142B
144
158
111
126
128
130
132
138
115
116
117
118
119
120
121
122
175

FIG. 2

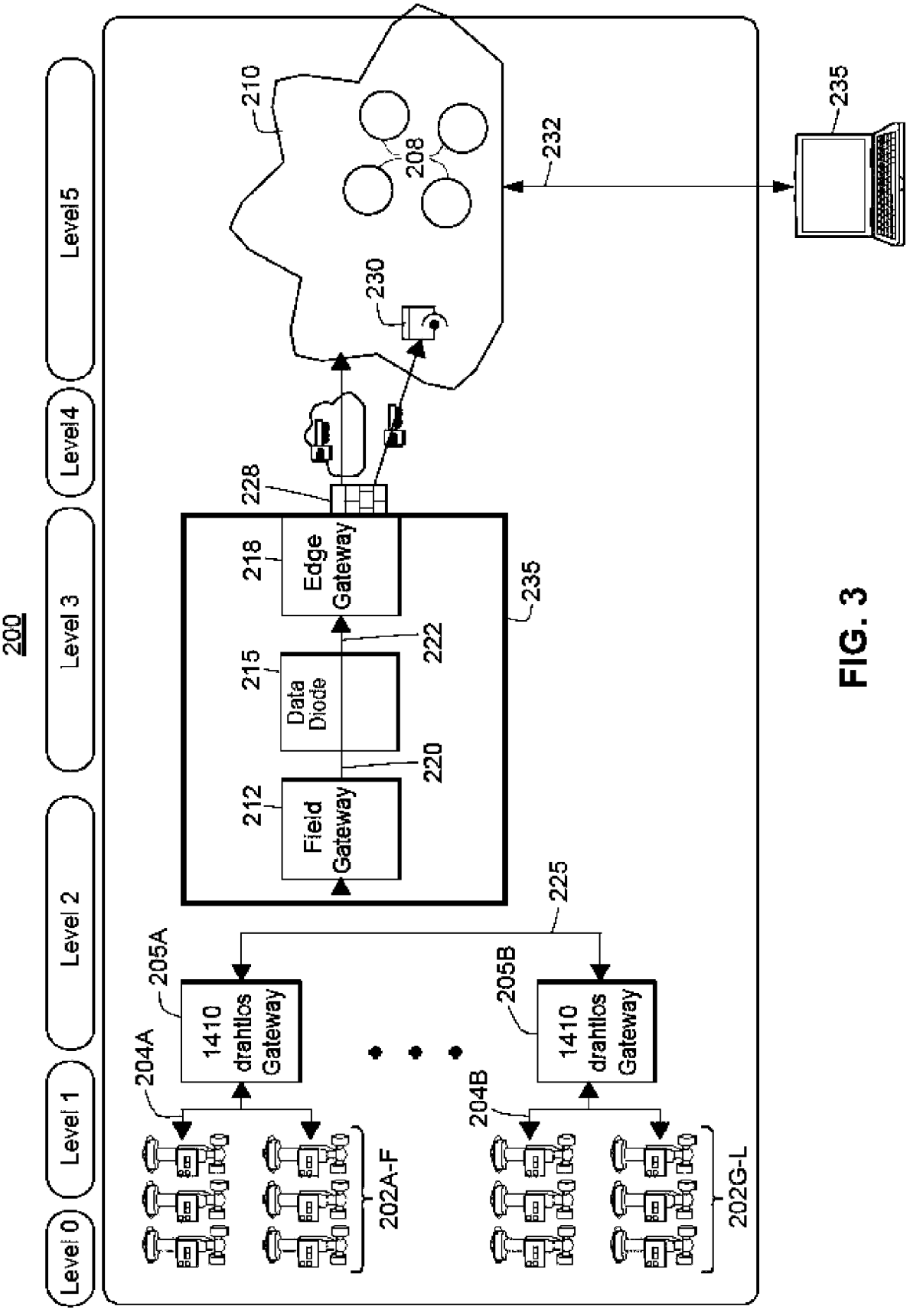

200
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
210
208
232
235
230
228
218
Edge Gateway
215
Data Diode
222
220
212
Field Gateway
235
225
205A
1410 drahtlos Gateway
205B
1410 drahtlos Gateway
204A
204B
202A-F
202G-L

FIG. 3

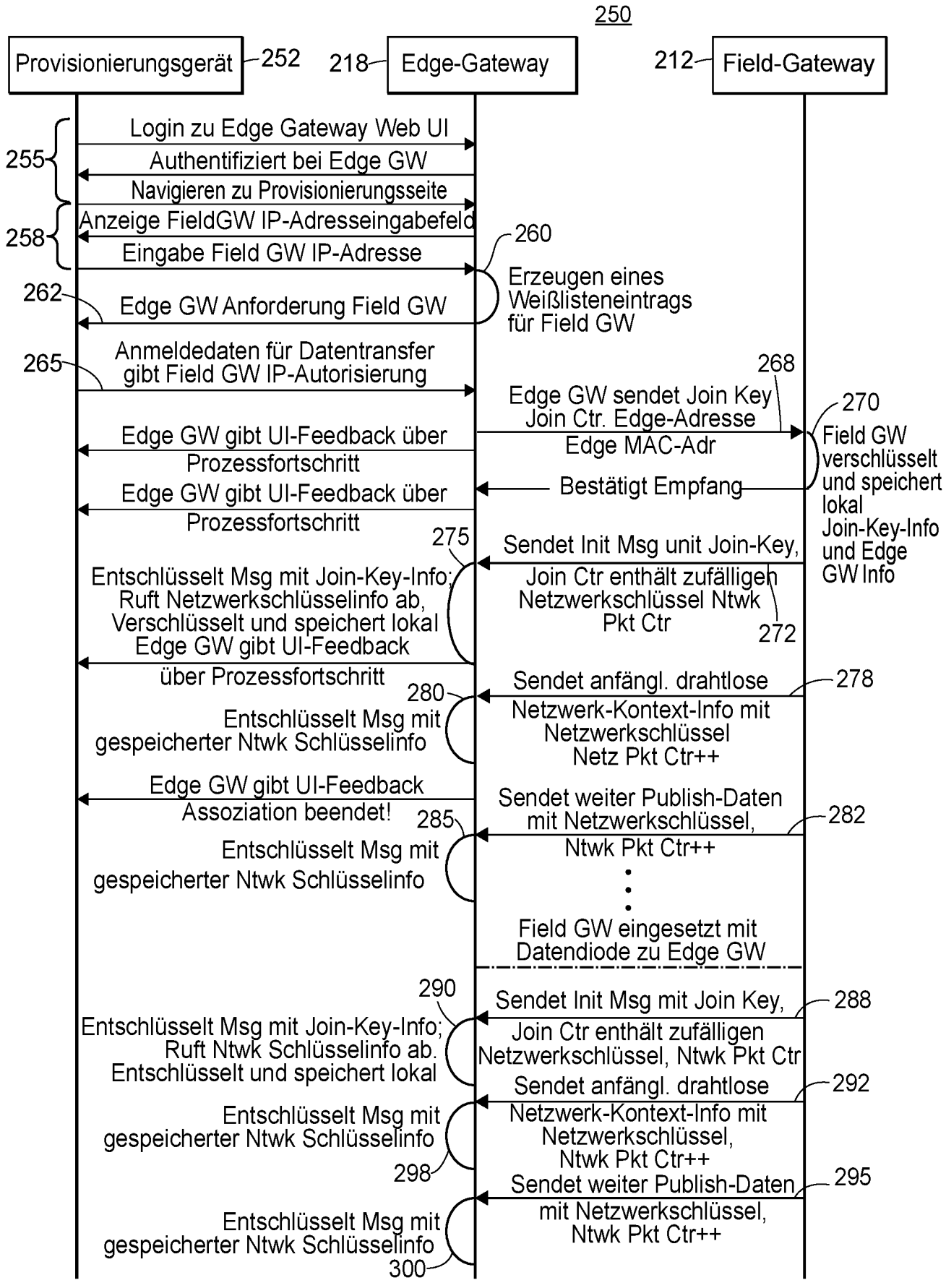

250
Provisionierungsgerät
252
218
Edge-Gateway
212
Field-Gateway
Login zu Edge Gateway Web UI
255
Authentifiziert bei Edge GW
Navigieren zu Provisionierungsseite
Anzeige FieldGW IP-Adresseingabefeld
258
Eingabe Field GW IP-Adresse
260
Erzeugen eines Weißlisteneintrags für Field GW
262
Edge GW Anforderung Field GW
Anmeldedaten für Datentransfer gibt Field GW IP-Autorisierung
265
268
Edge GW sendet Join Key Join Ctr. Edge-Adresse Edge MAC-Adr
270
Field GW verschlüsselt und speichert lokal Join-Key-Info und Edge GW Info
Bestätigt Empfang
Edge GW gibt UI-Feedback über Prozessfortschritt
Edge GW gibt UI-Feedback über Prozessfortschritt
275
Sendet Init Msg unit Join-Key,
Join Ctr enthält zufälligen Netzwerkschlüssel Ntwk Pkt Ctr
272
Entschlüsselt Msg mit Join-Key-Info; Ruft Netzwerkschlüsselinfo ab, Verschlüsselt und speichert lokal Edge GW gibt UI-Feedback über Prozessfortschritt
278
Sendet anfängl. drahtlose Netzwerk-Kontext-Info mit Netzwerkschlüssel Netz Pkt Ctr++
280
Entschlüsselt Msg mit gespeicherter Ntwk Schlüsselinfo
Edge GW gibt UI-Feedback Assoziation beendet!
Sendet weiter Publish-Daten mit Netzwerkschlüssel, Ntwk Pkt Ctr++
282
285
Entschlüsselt Msg mit gespeicherter Ntwk Schlüsselinfo
Field GW eingesetzt mit Datendiode zu Edge GW
290
Sendet Init Msg mit Join Key,
288
Join Ctr enthält zufälligen Netzwerkschlüssel, Ntwk Pkt Ctr
Entschlüsselt Msg mit Join-Key-Info; Ruft Ntwk Schlüsselinfo ab. Entschlüsselt und speichert lokal
Sendet anfängl. drahtlose Netzwerk-Kontext-Info mit Netzwerkschlüssel, Ntwk Pkt Ctr++
292
Entschlüsselt Msg mit gespeicherter Ntwk Schlüsselinfo
298
Sendet weiter Publish-Daten mit Netzwerkschlüssel, Ntwk Pkt Ctr++
295
Entschlüsselt Msg mit gespeicherter Ntwk Schlüsselinfo
300

FIG. 4

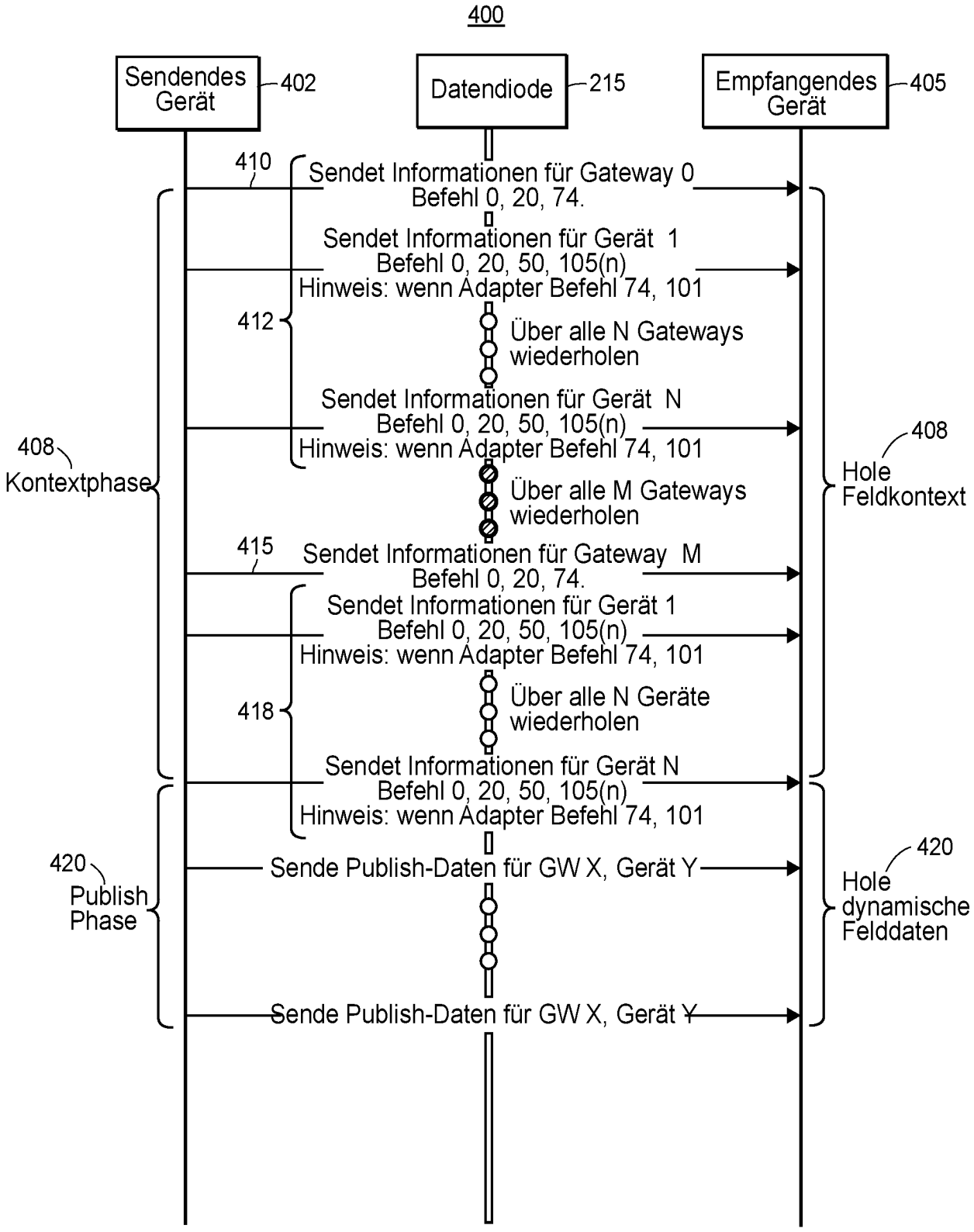

400
Sendendes Gerät
402
Datendiode
215
Empfangendes Gerät
405
410
Sendet Informationen für Gateway 0
Befehl 0, 20, 74.
Sendet Informationen für Gerät 1
Befehl 0, 20, 50, 105(n)
Hinweis: wenn Adapter Befehl 74, 101
412
Über alle N Gateways wiederholen
Sendet Informationen für Gerät N
Befehl 0, 20, 50, 105(n)
Hinweis: wenn Adapter Befehl 74, 101
408
Kontextphase
Über alle M Gateways wiederholen
408
Hole Feldkontext
415
Sendet Informationen für Gateway M
Befehl 0, 20, 74.
Sendet Informationen für Gerät 1
Befehl 0, 20, 50, 105(n)
Hinweis: wenn Adapter Befehl 74, 101
418
Über alle N Geräte wiederholen
Sendet Informationen für Gerät N
Befehl 0, 20, 50, 105(n)
Hinweis: wenn Adapter Befehl 74, 101
420
Publish Phase
Sende Publish-Daten für GW X, Gerät Y
420
Hole dynamische Felddaten
Sende Publish-Daten für GW X, Gerät Y

FIG. 5

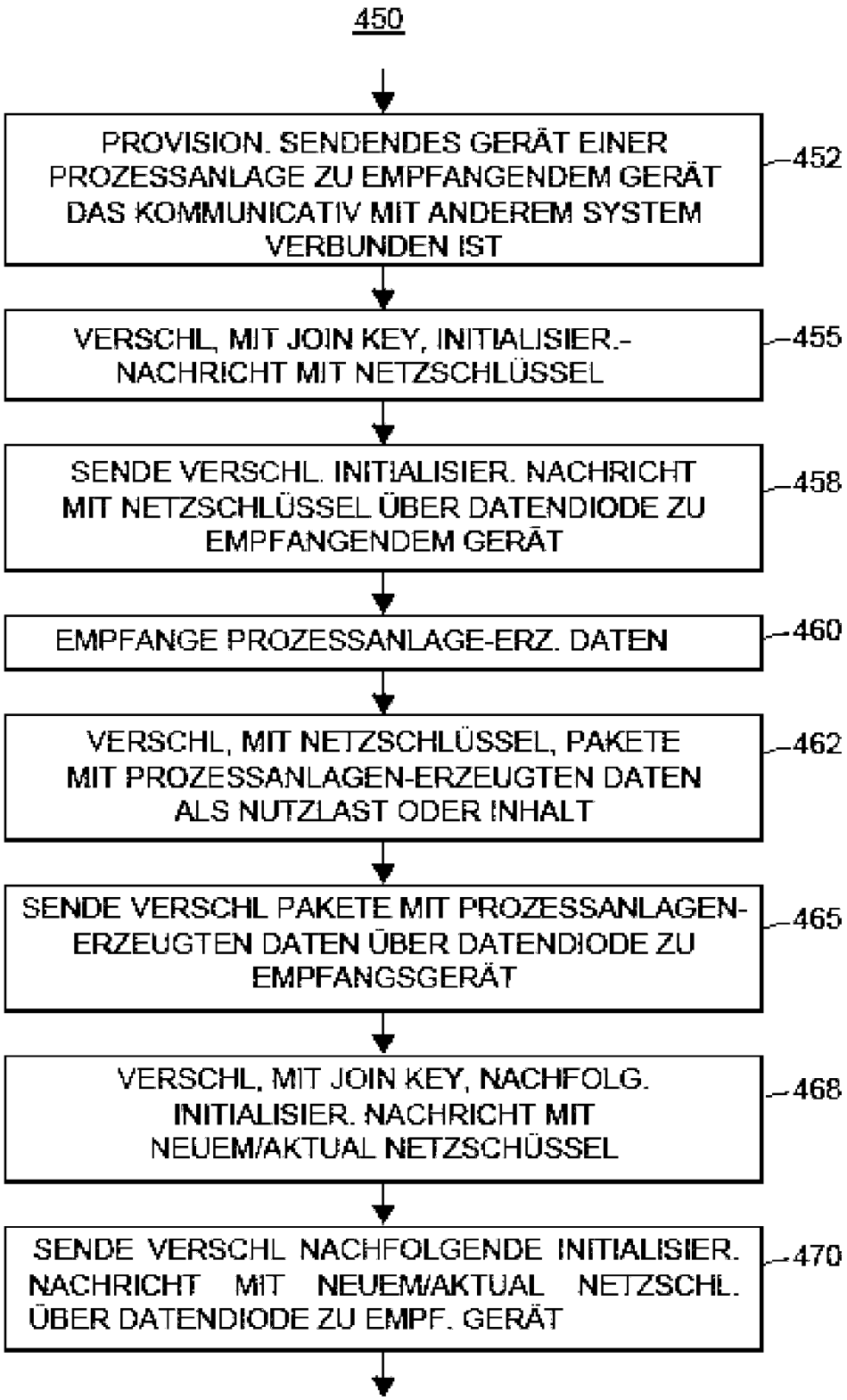

450
PROVISION. SENDENDES GERÄT EINER PROZESSANLAGE ZU EMPFANGENDEM GERÄT DAS KOMMUNICATIV MIT ANDEREM SYSTEM VERBUNDEN IST
452
VERSCHL, MIT JOIN KEY, INITIALISIER.-NACHRICHT MIT NETZSCHLÜSSEL
455
SENDE VERSCHL. INITIALISIER. NACHRICHT MIT NETZSCHLÜSSEL ÜBER DATENDIODE ZU EMPFANGENDEM GERÄT
458
EMPFANGE PROZESSANLAGE-ERZ. DATEN
460
VERSCHL, MIT NETZSCHLÜSSEL, PAKETE MIT PROZESSANLAGEN-ERZEUGTEN DATEN ALS NUTZLAST ODER INHALT
462
SENDE VERSCHL PAKETE MIT PROZESSANLAGEN-ERZEUGTEN DATEN ÜBER DATENDIODE ZU EMPFANGSGERÄT
465
VERSCHL, MIT JOIN KEY, NACHFOLG. INITIALISIER. NACHRICHT MIT NEUEM/AKTUAL NETZSCHÜSSEL
468
SENDE VERSCHL NACHFOLGENDE INITIALISIER. NACHRICHT MIT NEUEM/AKTUAL NETZSCHL. ÜBER DATENDIODE ZU EMPF. GERÄT
470

FIG. 6

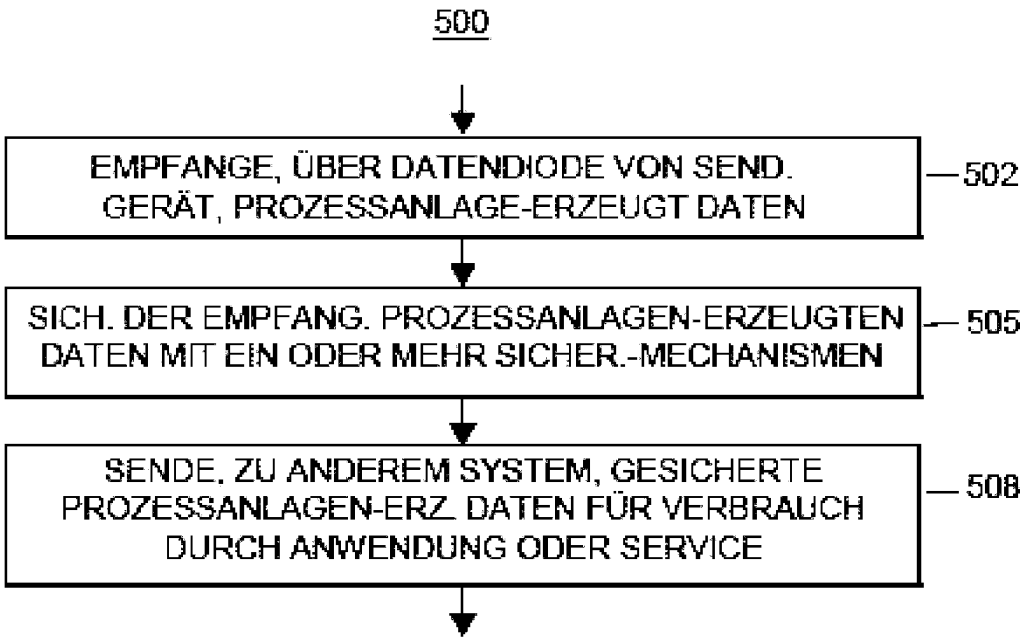

500
EMPFANGE, ÜBER DATENDIODE VON SEND. GERÄT, PROZESSANLAGE-ERZEUGT DATEN
502
SICH. DER EMPFANG. PROZESSANLAGEN-ERZEUGTEN DATEN MIT EIN ODER MEHR SICHER.-MECHANISMEN
505
SENDE, ZU ANDEREM SYSTEM, GESICHERTE PROZESSANLAGEN-ERZ. DATEN FÜR VERBRAUCH DURCH ANWENDUNG ODER SERVICE
508

FIG. 7