(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 124 821 A1** 2018.05.17

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 124 821.8**
(22) Anmeldetag: **24.10.2017**
(43) Offenlegungstag: **17.05.2018**

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

(30) Unionspriorität:
15/332,622 **24.10.2016** **US**

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

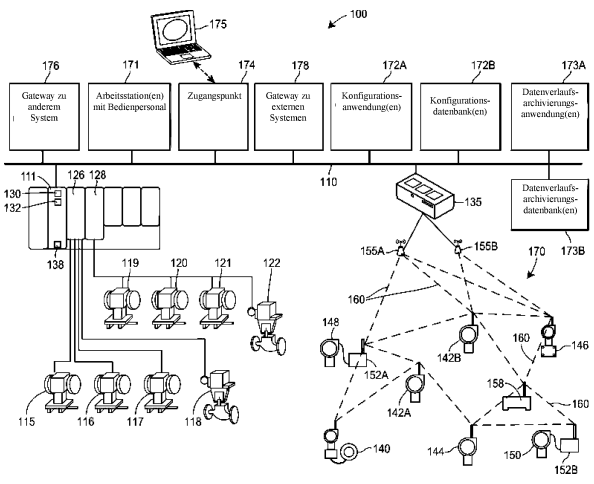
(74) Vertreter:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

(72) Erfinder:
Rotvold, Eric D., West St. Paul, Minn., US; Nixon, Mark John, Round Rock, Tex., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **VERÖFFENTLICHUNG VON DATEN ÜBER EINE DATENDIODE FÜR GESICHERTE PROZESSSTEUERUNGSKOMMUNIKATIONEN**

(57) Zusammenfassung: Um Kommunikationen von einer Prozessanlage über eine unidirektionale Datendiode an ein entferntes System zu sichern, veröffentlicht eine anlagenseitige Sendevorrichtung Daten über die Diode gegenüber einer Empfangsvorrichtung auf der entfernten Seite. Die Veröffentlichung der verschiedenen Daten geschieht entsprechend gemäß Kontextinformationen (z. B. Identifizierung von Datenquellen, entsprechende Rate der Datenerzeugung/-ankunft usw.), die Datenquellen der Anlage beschreiben und die wiederkehrend über die Diode durch die Sendevorrichtung bereitgestellt werden. Ein Rekurrenzintervall kann auf einer Toleranz für verlorene Daten oder einer anderen Eigenschaft einer Anwendung, eines Dienstes oder eines Konsumenten der Daten bei dem entfernten System beruhen. Die Veröffentlichung kann ein industrielles Kommunikationsprotokoll (z. B. HART-IP) und/oder ein geeignetes Universal-Kommunikationsprotokoll (z. B. JSON) nutzen.



Beschreibung

VERWANDTE REFERENZEN

[0001] Die vorliegende Offenbarung ist mit der gemeinsam gehaltenen US-Patentanmeldung Nr. 14/507,188, eingereicht am 6. Oktober 2014, mit dem Titel „Regional Big Data in Process Control Systems“; der gemeinsam gehaltenen US-Patentanmeldung Nr. 15/274,519, eingereicht am 23. September 2016, mit dem Titel „Data Analytics Services for Distributed Industrial Performance Monitoring“; der US-Patentanmeldung Nr. 15/274,233, eingereicht am 23. September 2016, mit dem Titel „Distributed Industrial Performance Monitoring and Analytics“; und der gemeinsam gehaltenen US-Patentanmeldung Nr. 15/332,521, eingereicht am 24. Oktober 2016, mit dem Titel „Process Device Condition and Performance Monitoring“ verwandt, wobei die gesamten Offenbarungen davon durch Bezugnahme in diese Schrift aufgenommen werden.

TECHNISCHES GEBIET

[0002] Die vorliegende Offenbarung betrifft im Allgemeinen Prozessanlagen und Prozesssteuerungssysteme und insbesondere das Sichern von Kommunikationen zwischen lokalen Prozessanalagen/Prozesssteuerungssystemen und einem entfernten System, das die lokalen Prozesssteuerungsanlagen/-systeme bedient, wie zum Beispiel ein tiefgreifendes Erfassungssystem.

ALLGEMEINER STAND DER TECHNIK

[0003] Verteilte Prozesssteuerungssysteme wie diejenigen, die in chemischen, mineralöltechnischen oder anderen Prozessanlagen verwendet werden, umfassen üblicherweise eine oder mehrere Prozesssteuerungen, die über analoge, digitale oder eine Kombination analoger/digitaler Busse oder über eine drahtlose Kommunikationsverbindung bzw. ein Netzwerk kommunikativ mit einer oder mehreren Feldvorrichtungen gekoppelt sind. Die Feldvorrichtungen, die zum Beispiel Ventile, Ventilstellungsregler, Schalter und Sender (z. B. Temperatur-, Druck-, Füllstands- und Durchflussmengensensoren) sein können, befinden sich in der Prozessumgebung und führen im Allgemeinen physische oder Prozesssteuerungsfunktionen wie das Öffnen oder Schließen von Ventilen, das Messen von Prozessparametern, wie zum Beispiel Druck, Temperatur usw., und dergleichen aus, um einen oder mehrere Prozesse zu steuern, die in der Prozessanlage oder dem -system ausgeführt werden. Intelligente Feldvorrichtungen wie die Feldvorrichtungen, die dem hinreichend bekannten Feldbus-Protokoll entsprechen, können außerdem Steuerungsberechnungen, Alarmfunktionen und andere Steuerfunktionen ausführen, die gemeinhin in der Steuerung umgesetzt werden. Die Prozesssteuerungen, die sich ebenso üblicherweise in der Anlagenumgebung befinden, empfangen Signale, die von den Feldvorrichtungen durchgeführte Messungen und/oder andere Informationen anzeigen, welche die Feldvorrichtungen betreffen und führen eine Steuerungsanwendung aus, die zum Beispiel verschiedene Steuermodule ablaufen lässt, die Prozesssteuerungsentscheidungen treffen, auf der Grundlage der empfangenen Informationen Steuersignale generieren und sich mit den Steuermodulen oder Blöcken koordinieren, die in den Feldvorrichtungen ausgeführt werden, wie zum Beispiel HART®-, WirelessHART®- und FOUNDATION®-Feldbus-Feldvorrichtungen. Die Steuermodule in der Steuerung senden die Steuersignale über die Kommunikationsleitungen oder -verbindungen an die Feldvorrichtungen, um so den Betrieb von mindestens einem Teil der Prozessanlage oder des -systems zu steuern.

[0004] Informationen von den Feldvorrichtungen und der Steuerung werden üblicherweise über eine Datenautobahn für eine oder mehrere Hardwarevorrichtungen zugänglich gemacht, wie zum Beispiel Arbeitsstationen mit Bedienpersonal, PCs oder Rechenvorrichtungen, Datenverlaufsarchive, Reportgeneratoren, zentralisierte Datenbanken oder andere zentralisierte verwaltende Rechenvorrichtungen, die üblicherweise in Steuerräumen oder an anderen von der rauen Anlagenumgebung entfernten Orten platziert werden. Jede dieser Hardwarevorrichtungen ist üblicherweise über die Prozessanlage oder über einen Teil der Prozessanlage zentralisiert. Diese Hardwarevorrichtungen lassen Anwendungen ablaufen, die es zum Beispiel einem Betreiber ermöglichen können, Funktionen in Bezug auf die Steuerung eines Prozesses und/oder den Betrieb der Prozessanlage auszuführen, wie zum Beispiel die Änderung von Einstellungen der Prozesssteuerungsroutine, Modifizieren des Betriebs der Steuermodule in den Steuerungen oder den Feldvorrichtungen, Ansehen des derzeitigen Prozessstatus, Ansehen von mit Feldvorrichtungen und Steuerungen generierten Alarmen, Simulieren des Vorgangs des Prozesses zum Zwecke der Schulung des Personals oder zum Testen der Prozesssteuerungssoftware, Pflegen und Aktualisieren einer Konfigurationsdatenbank usw. Die von den Hardwarevorrichtungen, Steuerungen und Feldvorrichtungen verwendete Datenautobahn kann einen verdrahteten Kommunikationspfad, einen drahtlosen Kommunikationspfad oder eine Kombination aus verdrahteten und drahtlosen Kommunikationspfaden umfassen.

[0005] Als ein Beispiel umfasst das von Emerson Process Management verkaufte DeltaV™-Steuerungssystem mehrere Anwendungen, die in verschiedenen Vorrichtungen, die sich an verschiedenen Orten innerhalb einer Prozessanlage befinden, gespeichert sind und von diesen ausgeführt werden. Eine Konfigurationsanwendung, die in einer oder

mehreren Arbeitsstationen oder Rechenvorrichtungen gespeichert ist, ermöglicht es Benutzern, Prozesssteuermodule zu erstellen oder zu ändern und diese Prozesssteuermodule über eine Datenautobahn auf dedizierte verteilte Steuerungen herunterzuladen. Üblicherweise bestehen diese Steuermodule aus kommunikativ zusammengeschalteten Funktionsblöcken, die Objekte in einem objektorientierten Programmierprotokoll sind, die Funktionen innerhalb des Steuerungsschemas auf der Grundlage diesbezüglicher Eingaben ausführen und für andere Funktionsblöcke in dem Steuerungsschema Ausgaben bereitstellen. Die Konfigurationsanwendung kann es außerdem einem Konstrukteur ermöglichen, Bedienschnittstellen zu erstellen oder zu verändern, die von einer Betrachtungsanwendung verwendet werden, um Daten für einen Betreiber anzuzeigen und um dem Betreiber das Ändern von Einstellungen wie Sollwerten in den Prozesssteuerungsroutinen zu ermöglichen. Jede dedizierte Steuereinheit und, in einigen Fällen, eine oder mehrere Feldvorrichtungen speichern eine entsprechende Steueranwendung, welche die ihr zugewiesenen und darauf heruntergeladenen Steuermodule ablaufen lässt und führen diese aus, um die tatsächliche Prozesssteuerungsfunktionalität zu implementieren. Die Betrachtungsanwendungen, die an einer oder mehreren Arbeitsstationen mit Bedienpersonal (oder an einer oder mehreren entfernten Rechenvorrichtungen, die kommunikativ mit den Arbeitsstationen mit Bedienpersonal und der Datenautobahn verbunden sind) ausgeführt werden können, empfangen über die Datenautobahn Daten von der Steueranwendung und zeigen diese Daten für Konstrukteure von Prozesssteuerungssystemen, Betreiber oder Benutzer an, welche die Benutzerschnittstellen verwenden, und können eine beliebige Anzahl verschiedener Ansichten wie eine Ansicht eines Betreibers, eine Ansicht eines Ingenieurs, eine Ansicht eines Technikers usw. bereitstellen. Eine Data-Historian-Anwendung wird üblicherweise in einer Data-Historian-Vorrichtung, die einige oder alle der Daten sammelt oder speichert, die über die Datenautobahn bereitgestellt werden, gespeichert und von dieser ausgeführt, während eine Konfigurationsdatenbankanwendung in einem weiteren mit der Datenautobahn verbundenen Computer ablaufen kann, um die aktuelle Routinekonfiguration der Prozesssteuerung und damit verknüpfte Daten zu speichern. Alternativ kann sich die Konfigurationsdatenbank in der gleichen Arbeitsstation befinden wie die Konfigurationsanwendung.

[0006] Allgemein ausgedrückt, beinhaltet ein Prozesssteuerungssystem einer Prozessanlage Feldvorrichtungen, Steuerungen, Arbeitsstationen und andere Vorrichtungen, die durch einen Satz von geschichteten Netzwerken und Bussen verbunden sind. Das Prozesssteuerungssystem kann wiederum mit verschiedenen Geschäfts- und externen Netzwerken verbunden sein, um z. B. Herstellungs- und Betriebskosten zu reduzieren, die Produktivität und Effizienz zu verbessern, rechtzeitigen Zugriff aus Prozesssteuerungs- und/oder Prozessanlageninformationen bereitzustellen usw. Auf der anderen Seite erhöht die Verbindung von Prozessanlagen und/oder Prozesssteuerungssystemen mit Unternehmens- und/oder externen Netzwerken das Risiko für Cyber-Eingriffe und/oder schädliche Cyber-Attacken, die aus erwarteten Schwachstellen bei kommerziellen Systemen und Anwendungen, wie zum Beispiel jene, die in Unternehmens- und externen Netzwerken verwendet werden, entstehen können. Cyber-Eingriffe und schädliche Cyber-Attacken von Prozessanlagen, -netzwerken und/oder -steuerungssystemen können sich negativ auf die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Informationsbeständen auswirken, wobei es sich allgemein ausgedrückt um Schwachstellen handelt, die jenen von Universal-Rechennetzwerken ähneln. Im Gegensatz zu Universal-Rechennetzwerken können Cyber-Eingriffe von Prozessanlagen, -netzwerken und/oder -steuerungssystemen können jedoch ebenfalls zur Beschädigung, Zerstörung und/oder zum Verlust von nicht nur Ausrüstung, Produkten und anderen physischen Gütern, sondern auch zum Verlust eines Menschenlebens führen. Zum Beispiel kann ein Cyber-Eingriff bewirken, dass ein Prozess nicht mehr gesteuert werden kann und dadurch Explosionen, Brände, Überflutungen, Exposition gegenüber Gefahrgut usw. erzeugt werden. Somit ist das Sichern von Kommunikationen in Bezug auf Prozesssteuerungsanlagen und -systeme von großer Bedeutung.

[0007] **Fig. 1** beinhaltet ein Blockdiagramm 10 beispielhafter Sicherheitsstufen für ein Prozesssteuerungs- oder ein industrielles Prozesssystem. Das Diagramm 10 stellt Verbindungen zwischen verschiedenen Komponenten des Prozesssteuerungssystems, dem Prozesssteuerungssystem selbst und anderen Systemen und/oder Netzwerken, mit welchen das Prozesssteuerungssystem kommunikativ verbunden sein kann, sowie Schichten oder Stufen der Sicherheit in Bezug auf Kommunikationen in und zwischen dem Prozesssteuerungssystem und den anderen Systemen/Netzwerken dar. Die Sicherheitsstufen stellen einen Schichtansatz für die Sicherheit über Segmentierung oder Trennung bereit und verschiedene Stufen werden durch eine oder mehrere Firewalls 12A, 12B, 12C geschützt, um nur autorisierten Verkehr zwischen den unterschiedlichen Stufen zuzulassen. In **Fig. 1** befinden sich Sicherheitsstufen mit niedrigeren Zahlen näher am angeschlossenen, zu steuernden Prozess, während die Sicherheitsstufen mit höheren Zahlen weiter vom Ausführungsprozess entfernt sind. Dementsprechend sind Vertrauensstufen (z. B. ein relativer Grad an Vertrauen in die Sicherheit und Echtheit von Nachrichten, Paketen und andere Kommunikationen) auf der Vorrichtungsstufe (Stufe 0) am höchsten und Vertrauensstufen sind unter der Geschäftsnetzwerkstufe (Stufe

5) am niedrigsten, z. B. im öffentlichen Internet und/oder anderen öffentlichen Netzwerken. Unter Verwendung des logischen Rahmens des Purdue Model for Control Hierarchy, standardisiert durch ISA (International Society of Automation) 95.01 - IEC (International Electrotechnical Commission) 62264-1, fallen Prozesssteuerungssysteme im Allgemeinen in die Sicherheitsstufen 0-2 und Herstellungs-, Firmen- und Unternehmenssysteme fallen im Allgemeinen in die Sicherheitsstufen 3-5.

[0008] Beispiele für unterschiedliche Funktionalitäten bei jeder der unterschiedlichen Sicherheitsstufen werden in **Fig. 1** gezeigt. Stufe 0 beinhaltet typischerweise Feldvorrichtungen und andere Vorrichtungen, die innerhalb einer Prozessanlage angeordnet sind und die direkten Kontakt mit dem Prozess und/oder Prozessablauf aufweisen, zum Beispiel Sensoren, Ventile, Ventilstellungsregler, Schalter, Sender und andere Vorrichtungen, die physische und/oder Prozesssteuerungsfunktionen erfüllen, wie zum Beispiel das Öffnen oder Schließen von Ventilen, das Messen von Prozessparametern wie Druck, Temperatur usw. und dergleichen. Für eine übersichtliche Veranschaulichung werden in **Fig. 1** keine beispielhaften Feldvorrichtungen gezeigt.

[0009] Stufe 1 beinhaltet Steuerungen und andere Prozesssteuerungsvorrichtungen 15A-15D, welche die grundlegende Steuerung von Echtzeit-Vorgängen des Prozesses bereitstellen, z. B. durch Empfangen von Eingaben von Feldvorrichtungen, Verarbeiten der Eingaben unter Verwendung von Steuerschemata, -modulen oder anderer Logik und Senden resultierender Aufgaben an andere Vorrichtungen. Im Allgemeinen sind derartige Prozesssteuerungsvorrichtungen mit entsprechenden Steuerschemata programmiert und/oder konfiguriert. Zum Beispiel können die Prozesssteuerungsvorrichtungen auf Stufe 1 Prozesssteuerungen, speicherprogrammierbare Steuerungen (PLCs), Fernbedienungsterminals (RTUs) und dergleichen beinhalten. Wie in **Fig. 1** gezeigt, können die Prozesssteuerungsvorrichtungen auf Stufe 1 jene beinhalten, die Chargensteuerung 15A, diskrete Steuerung 15B, kontinuierliche Steuerung 15C, Hybridsteuerung 15D und/oder andere Steuerungsarten durchführen.

[0010] Stufe 2 beinhaltet Vorrichtungen und Ausrüstung 18A-18D, die eine Überwachungssteuerung der Produktionsfläche der Prozessanlage bereitstellen. Zum Beispiel kann Stufe 2 Alarmierungs- und/oder Benachrichtigungssysteme 18A, Arbeitsstationen mit Bedienpersonal 18C, andere Mensch-Maschine-Schnittstellen (HMIs) 18B, 18D und dergleichen beinhalten. Im Allgemeinen können Vorrichtungen und Ausrüstung der Stufe 2 mit den Vorrichtungen 15A-15D der Stufe 1 sowie mit Vorrichtungen und Ausrüstung der Stufe 3 kommunizieren, z. B. über eine oder mehrere Firewalls 12A, 12B.

[0011] Stufe 3 umfasst Anlagensysteme und/oder -netzwerke, z. B. Vorrichtungen, Ausrüstung und Systeme 20A-20D, die Standort-/Anlagenvorgänge verwalten und die Produktion oder Herstellung eines gewünschten Endprodukts steuern. Zum Beispiel kann Stufe 3 Produktionssysteme 20A, die zur Produktionssteuerung, -berichterstattung, -planung usw. verwendet werden; Optimierungssysteme 20B, die zum Verbessern der Qualität, Produktivität, Effizienz usw. verwendet werden; Historians 20C zum Archivieren von Daten, die durch die Prozessanlage erzeugt wurden und/oder auf diese hindeuten; und/oder Konstruktionsarbeitsstationen oder -rechenvorrichtungen 20D, die von Personal für die Gestaltung und Entwicklung von Steuerschemata und -modulen verwendet werden, Arbeitsstationen mit Bedienpersonal und/oder HMI-Schnittstellen usw. beinhalten.

[0012] Springt man zu Stufe 5, beinhaltet Stufe 5 im Allgemeinen Geschäfts-, Firmen- oder Unternehmenssysteme und/oder -netzwerke. Derartige Systeme und/oder Netzwerke verwalten die Verbindung mit Systemen außerhalb des Unternehmens. Zum Beispiel können ein VPN (Virtuelles Privates Netzwerk) des Unternehmens, Firmen- oder Unternehmensinternetzugriffsdienste und/oder andere IT (Informationstechnologie)-Infrastruktursysteme und -anwendungen auf Stufe 5 gefunden werden.

[0013] Stufe 4, die als eine nach innen gerichtete Erweiterung von Stufe 5 betrachtet werden kann, umfasst im Allgemeinen Firmen- oder Unternehmenssysteme, die unternehmensintern sind, zum Beispiel Firmensysteme, die E-Mail-, Intranet-, Standort-Geschäftsplanungs- und -logistik-, Bestands-, Planungs- und/oder andere Firmen-/Unternehmenssysteme und -netzwerke unterstützen.

[0014] Wie in **Fig. 1** gezeigt, verknüpfen sich die Sicherheitsstufen 3 und 4 über eine entmilitarisierte Zone (DMZ) 22 miteinander, welche Geschäfts- oder Unternehmenssysteme und/oder -netzwerke von Anlagen-/Prozesssystemen und/oder -netzwerken trennt, wodurch die Stufe des Sicherheitsrisikos, gegenüber welchem eine Prozessanlage ausgesetzt ist, minimiert wird. Die DMZ 22 kann eine oder mehrere entsprechende Firewalls 12C beinhalten und kann verschiedene Vorrichtungen, Ausrüstung, Server und/oder Anwendungen 25A-25F umfassen, die mit zur Anlage gehörenden/r Vorrichtungen, Ausrüstung und Anwendungen auf niedrigeren Sicherheitsstufen kommunizieren und/oder die mit zum Unternehmen gehörenden/r Vorrichtungen, Ausrüstung und Anwendungen auf höheren Sicherheitsstufen kommunizieren. Zum Beispiel kann die DMZ 22 Terminaldienste 25A, Patchverwaltung 25B, einen oder mehrere AV-Server 25C, einen oder mehrere Historians 25D (welche zum Beispiel Spiegel-Historians beinhalten können), Webdienstvorgänge 25E und/oder einen oder mehrere Anwendungsser-

ver 25F umfassen, um einige zu nennen. Typischerweise ist es bei den Vorrichtungen, der Ausrüstung und/oder den Anwendungen auf Sicherheitsstufen über der DMZ 22 nur jenen, die autorisiert sind, gestattet, kommunikativ auf die Prozessanlage zuzugreifen, und es ist ferner erforderlich, dass sie sich über die Vorrichtungen, Ausrüstung, Server und/oder Anwendungen 25A-25F der DMZ 22 verbinden. Die DMZ-Vorrichtungen 25A-25F halten wieder getrennte Verbindungen mit den niedrigeren Stufen, wodurch die Prozessanlage und das Steuerungssystem von Attacken von Unternehmenssystemen und/oder -netzwerken (oder höher) geschützt werden.

[0015] Nun folgt eine kurze Erörterung entfernter Dienste, entfernte Dienste werden immer häufiger durch unterschiedliche Benutzer und Systeme verwendet. Zum Beispiel ermöglicht es das Produkt Remote Desktop Services, welches durch das Microsoft-Windows®-Betriebssystem bereitgestellt wird, den Benutzern, auf sitzungsbasierte Desktops, auf Desktops auf der Grundlage von virtuellen Maschinen und/oder andere Anwendungen in einem Rechenzentrum von einem Firmennetzwerk und/oder vom Internet aus zuzugreifen. Das durch Intuit® bereitgestellte Produkt QuickBooks® Online ermöglicht es den Benutzern, Buchführungsfunktionen durchzuführen, wie zum Beispiel Kapitalflussverwaltung, Ausstellen von Rechnungen und durchführen von Zahlungen online über das Internet. Allgemein ausgedrückt werden entfernte Dienste durch eine oder mehrere Anwendungen bereitgestellt, die entfernt von dem System oder Benutzer ausgeführt werden, das/der auf den entfernten Dienst zugreift. Zum Beispiel führen die eine oder die mehreren Anwendungen Daten bei einer entfernten Serverbank, in der Cloud usw. aus und verwalten diese und auf sie wird über ein oder mehrere private und/oder öffentliche Netzwerke zugegriffen, wie zum Beispiel ein Unternehmensnetzwerk und/oder das öffentliche Internet.

KURZDARSTELLUNG

[0016] In einer Ausführungsform beinhaltet ein Verfahren zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System Folgendes: bei einem Feld-Gateway, welches ein Netzwerk der Prozessanlage und eine Datendiode verbindet, die zum Verhindern von Zweiwege-Kommunikation zwischen dem Feld-Gateway und einem Rand-Gateway konfiguriert ist, wiederkehrendes Ankündigen gegenüber dem Rand-Gateway über die Datendiode von entsprechenden Kontextinformationen, die jede von einer oder mehreren Vorrichtungen der Prozesssteuerungsanlage beschreiben; Empfangen, bei dem Feld-Gateway über das Prozessanlagennetzwerk, von Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, während die Prozessanlage arbeitet, um einen Prozess zu steuern; und Veröffentlichen, durch das Feld-Gateway gegenüber dem Rand-Gateway über die Datendiode, der Prozessanlagendaten.

[0017] In einer Ausführungsform umfasst ein System zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System ein Feld-Gateway, das kommunikativ mit einem Netzwerk der Prozessanlage gekoppelt ist; ein Rand-Gateway, das kommunikativ mit dem anderen System gekoppelt ist; und eine Datendiode, welche das Feld-Gateway und das Rand-Gateway verbindet. Die Datendiode ist konfiguriert, um zu verhindern, dass Kommunikationen, die von dem Rand-Gateway übertragen werden, in das Feld-Gateway eingelassen werden, und Daten, die durch eine oder mehrere in der Prozessanlage enthaltene Vorrichtungen erzeugt wurden, während die Prozessanlage arbeitet, um einen industriellen Prozess zu steuern, bei dem Feld-Gateway über das Prozessanlagennetzwerk empfangen werden und durch das Feld-Gateway über die Datendiode gegenüber dem Rand-Gateway veröffentlicht werden.

Figurenliste

Fig. 1 beinhaltet ein Blockdiagramm beispielhafter Sicherheitsstufen für ein Prozesssteuerungs- oder industrielles Prozesssystem, einschließlich unter anderem Verbindungen zwischen verschiedenen beispielhaften Komponenten des Prozesssteuerungssystems, dem Prozesssteuerungssystem selbst und anderen beispielhaften Systemen und/oder Netzwerken;

Fig. 2 ist ein Blockdiagramm einer beispielhaften Prozessanlage oder eines beispielhaften Prozesssteuerungssystems, welches unter anderem Verbindungen zwischen verschiedenen beispielhaften Komponenten des Prozesssteuerungssystems, dem Prozesssteuerungssystem selbst und anderen beispielhaften Systemen und/oder Netzwerken veranschaulicht;

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

Fig. 4 stellt einen beispielhaften Nachrichtenablauf dar, der zur Bereitstellung gesicherter Kommunikationen für eine Prozessanlage oder ein Prozesssteuerungssystem verwendet werden kann;

Fig. 5 stellt einen beispielhaften Nachrichtenablauf dar, der zum Zustellen von Prozessanlagendaten über die Datendiode verwendet werden kann;

Fig. 6 ist ein Ablaufdiagramm eines beispielhaften Verfahrens zum sicheren Transportieren von Kommunikationen von einer Prozessanlage oder einem Prozesssteuerungssystem; und

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

DETAILLIERTE BESCHREIBUNG

[0018] Wie vorstehend erörtert, nutzt das Sichern von Prozesssteuerungsanlagen und - systemen gegen Cyber-Eingriffe und schädliche Cyber-Attacken eine geschichtete oder stufige Sicherheitshierarchie, wobei einige der Schichten oder Stufen durch die Verwendung von Firewalls und anderen Sicherheitsmechanismen geschützt werden. Wie zum Beispiel bereits in Bezug auf **Fig. 1** erörtert, können Prozessanlagensysteme, -netzwerke und - Vorrichtungen auf den Sicherheitsstufen **0**-**3** gegen Bedrohungen von Unternehmensnetzwerken auf den Stufen **4**-**5** und/oder von beliebigen externen Netzwerken, die über Stufe **5** liegen und die Unternehmensnetzwerke ausnutzen, geschützt werden, z. B. durch die Verwendung einer DMZ **22** und einer oder mehrerer Firewalls **12A**-**12C**. Da jedoch immer mehr Dienste und Anwendungen, die mit Prozessanlagendaten arbeiten, verschoben werden, um z. B. entfernt in Netzwerken und Systemen außerhalb der Prozessanlage (z. B auf den Stufen **4** und/oder **5** innerhalb des Unternehmens oder Geschäfts) und/oder sogar in Netzwerken und Systemen außerhalb des Unternehmens oder Geschäfts (z. B. über Stufe **5**, über das Internet oder ein anderes öffentliches Netzwerk) ausgeführt zu werden, werden stärkere Techniken zum Schützen von Prozessanlagensysteme, -netzwerken und -vorrichtungen vor Schäden benötigt.

[0019] Die neuartigen hier beschriebenen Systeme, Komponenten, Einrichtungen, Verfahren und Techniken gehen diese und andere Sicherheitsprobleme in Bezug auf Prozessanlagen und deren Netzwerke an und sind insbesondere auf das Sichern von Kommunikationen zwischen Prozessanlagen/-netzwerken und anderen Netzwerken oder Systemen gerichtet.

[0020] Um dies zu veranschaulichen, ist **Fig. 2** ein Blockdiagramm einer beispielhaften Prozessanlage **100**, die zum Steuern eines industriellen Prozesses während angeschlossener Vorgänge konfiguriert ist und die unter Verwendung einer oder mehrerer der hier beschriebenen Sicherheitstechniken gesichert werden kann. Die Prozessanlage **100** (die hier austauschbar ebenfalls als ein Prozesssteuerungssystem **100** oder Prozesssteuerungsumgebung **100** bezeichnet wird) beinhaltet eine oder mehrere Prozesssteuerungen, die Signale empfangen, die auf von Feldvorrichtungen durchgeführte Prozessmessungen hindeuten, diese Informationen verarbeiten, um eine Steuerroutine umzusetzen, und Steuersignale erzeugen, die über drahtgebundene oder drahtlose Prozesssteuerungskommunikationsverbindungen oder -netzwerke an andre Feldvorrichtungen gesendet werden, um den Betrieb eines Prozesses in der Anlage **100** zu steuern. Typischerweise erfüllt mindestens eine Feldvorrichtung eine physische Funktion (z. B. Öffnen oder Schließen eines Ventils, Erhöhen oder Senken einer Temperatur, Aufnehmen eines Messwerts, Erfassen einer Bedingung usw.), um den Betrieb des Prozesses zu steuern. Einige Typen von Feldvorrichtungen kommunizieren mit Steuerungen durch E/A-Vorrichtungen. Prozesssteuerungen, Feldvorrichtungen und E/A-Vorrichtungen können drahtgebunden oder drahtlos sein und eine beliebige Anzahl und Kombination von drahtgebundenen und drahtlosen Prozesssteuerungen, Feldvorrichtungen und E/A-Vorrichtungen können in der Prozessanlagenumgebung oder dem Prozessanlagensystem **100** enthalten sein.

[0021] Zum Beispiel veranschaulicht **Fig. 2** eine Prozesssteuerung **111**, die kommunikativ mit drahtgebundenen Feldvorrichtungen **115**-**122** über Eingabe/Ausgabe(E/A)-Karten 126 und 128 verbunden ist und die kommunikativ mit drahtlosen Feldvorrichtungen **140**-**146** über ein drahtloses Gateway **135** und eine Prozesssteuerungsdatenautobahn oder ein - backbone 110 verbunden ist. Die Prozesssteuerungsdatenautobahn **110** kann eine oder mehrere drahtgebundene oder drahtlose Kommunikationsverbindungen beinhalten und kann unter Verwendung eines beliebigen gewünschten oder geeigneten Kommunikationsprotokolls, wie zum Beispiel ein Ethernet-Protokoll, umgesetzt werden. In einigen (nicht gezeigten) Konfigurationen kann die Steuerung **111** kommunikativ mit dem drahtlosen Gateway **135** unter Verwendung eines oder mehrerer Kommunikationsnetzwerke verbunden sein, die sich vom Backbone **110** unterscheiden, wie zum Beispiel durch die Verwendung einer beliebigen Anzahl drahtgebundener oder drahtloser Kommunikationsverbindungen, die ein oder mehrere Kommunikationsprotokolle unterstützen, z. B. Wi-Fi oder ein anderes mit IEEE **802.11** konformes Protokoll für drahtlose lokale Netzwerke, ein mobiles Kommunikationsprotokoll (z. B. WiMAX, LTE oder ein anderes mit ITU-R konformes Protokoll), Bluetooth®, HART®, WirelessHART®, Profibus, FOUNDATION® Fieldbus usw.

[0022] Die Steuereinheit **111**, welche beispielsweise die von Emerson Process Management verkaufte DeltaV™-Steuerung sein kann, kann betrieben werden, um einen Chargenprozess oder einen kontinuierlichen Prozess unter Verwendung von mindestens einigen der Feldvorrichtungen **115**-**122** und **140**-**146** umzusetzen. In einer Ausführungsform ist die Steuerung **111** zusätzlich zur kommunikativen Verbindung mit der Prozesssteuerungsdatenautobahn **110** ebenfalls kommunikativ mit mindestens einigen der Feldvorrichtungen **115**-**122** und **140**-**146** verbunden, und zwar unter Verwendung beliebiger Hardware und Software, die zum Beispiel mit Standard-

Vorrichtungen mit 4-20 mA, E/A-Karten 126, 128 und/oder einem beliebigen intelligenten Kommunikationsprotokoll assoziiert ist, wie zum Beispiel dem FOUNDATION®-Fieldbus-Protokoll, dem HART®-Protokoll, dem WirelessHART®-Protokoll usw. In **Fig. 2** sind die Steuerung **111**, die Feldvorrichtungen **115**-**122** und die E/A-Karten 126, 128 drahtgebundene Vorrichtungen und die Feldvorrichtungen **140**-**146** sind drahtlose Feldvorrichtungen. Natürlich können die drahtgebundenen Feldvorrichtungen **115**-**122** und die drahtlosen Feldvorrichtungen **140**-**146** (einem) beliebigen anderen gewünschten Standard(s) oder Protokollen entsprechen, wie etwa beliebigen drahtgebundenen oder drahtlosen Protokollen, einschließend beliebige in der Zukunft entwickelte Standards oder Protokolle.

[0023] Die Prozesssteuerung **111** aus **Fig. 2** umfasst einen Prozessor **130**, der eine oder mehrere Prozesssteuerungsroutinen **138** (die z. B. in einem Speicher **132** gespeichert sind) implementiert oder überwacht. Der Prozessor **130** ist zum Kommunizieren mit den Feldvorrichtungen **115**-**122** und **140**-**146** und mit anderen Knoten konfiguriert, die kommunikativ mit der Steuerung **111** verbunden sind. Es ist anzumerken, dass beliebige hier beschriebene Steuerroutinen oder -module diesbezügliche Teile aufweisen können, die, falls gewünscht, von anderen Steuerungen oder anderen Vorrichtungen umgesetzt oder ausgeführt werden. Gleichermaßen können die hier beschriebenen Steuerroutinen oder -module 138, die in dem Prozesssteuerungssystem **100** umgesetzt werden sollen, jede Form annehmen, einschließlich Software, Firmware, Hardware usw. Steuerroutinen können in jedem gewünschten Softwareformat umgesetzt werden, wie zum Beispiel unter Verwendung von objektorientierter Programmierung, Leiterlogik, sequentiellen Funktionsplänen, Funktionsblockdiagrammen oder unter Verwendung einer anderen Sprache für die Softwareprogrammierung oder eines anderen Designparadigmas. Die Steuerroutinen **138** können in jeder gewünschten Form eines Speichers **132** gespeichert werden, wie etwa einem Random Access Memory (RAM) oder einem Read Only Memory (ROM). Gleichermaßen können die Steuerroutinen **138** zum Beispiel in einem bzw. einer oder mehreren EPROMs, EEPROMs, anwendungsspezifischen integrierten Schaltungen (ASICs) oder beliebigen anderen Hardware- oder Firmware-Elementen fest kodiert werden. Demnach kann die Steuerung **111** konfiguriert werden, um eine Steuerstrategie oder eine Steuerroutine auf eine gewünschte Weise umzusetzen.

[0024] Die Steuereinheit **111** setzt eine Steuerstrategie unter Verwendung von dem, was gemeinhin als Funktionsblöcke bezeichnet wird, um, wobei jeder Funktionsblock ein Objekt oder ein anderer Teil (z. B. eine Teilroutine) einer gesamten Steuerroutine ist und zusammen mit anderen Funktionsblöcken arbeitet (über Kommunikationen, die Verbindungen genannt werden), um Prozesssteuerschleifen in dem Prozesssteuerungssystem **100** umzusetzen. Steuerungsbasierte Funktionsblöcke führen üblicherweise eine einer Eingabefunktion wie diejenige, die mit einem Transmitter, einem Sensor oder anderen Messvorrichtungen für Prozessparameter verknüpft ist; einer Steuerfunktion, wie diejenige, die mit einer Steuerroutine verknüpft ist, die eine PID-, eine Fuzzy-Logic-Steuerung usw. ausführt; oder einer Ausgabefunktion aus, welche den Betrieb von einigen Vorrichtungen wie einem Ventil steuert, um in dem Prozesssteuerungssystem **100** eine physische Funktion auszuführen. Natürlich existieren Mischformen und andere Arten von Funktionsblöcken. Funktionsblöcke können in der Steuerung **111** gespeichert und von dieser ausgeführt werden, was üblicherweise der Fall ist, wenn diese Funktionsblöcke für Standard-Vorrichtungen mit 4-20 mA und einige Arten von intelligenten Feldvorrichtungen wie HART®-Vorrichtungen verwendet werden oder mit diesen verknüpft sind oder sie können in den Feldvorrichtungen an sich gespeichert und von diesen implementiert werden, was bei FOUNDATION®-Feldbus-Vorrichtungen der Fall sein kann. Die Steuerung **111** kann eine oder mehrere Steuerroutinen **138** umfassen, die eine oder mehrere Steuerschleifen umsetzen können, die durch das Ausführen eines oder mehrerer der Funktionsblöcke durchgeführt werden.

[0025] Die drahtgebundenen Feldvorrichtungen **115**-**122** können jede Art von Vorrichtungen sein, wie etwa Sensoren, Ventile, Sender, Stellungsregler usw., während die E/A-Karten 126 und 128 jede Art von E/A-Vorrichtungen sein können, die einem gewünschten Kommunikations- oder Steuerprotokoll entsprechen. In **Fig. 2** sind die Feldvorrichtungen **115**-**118** Standard-Vorrichtungen mit 4-20 mA oder HART®-Vorrichtungen, die über analoge Leitungen oder eine Kombination aus analogen und digitalen Leitungen mit der E/A-Karte 126 kommunizieren, während die Feldvorrichtungen **119**-**122** intelligente Vorrichtungen wie FOUNDATION®-Feldbus-Feldvorrichtungen sind, die unter Verwendung eines FOUNDATION® Feldbus-Kommunikationsprotokolls über einen digitalen Bus mit der E/A-Karte 128 kommunizieren. In einigen Ausführungsformen kommunizieren jedoch mindestens einige der drahtgebundenen Feldvorrichtungen **115**, **116** und **118**-**121** und/oder mindestens einige der E/A-Karten 126, 128 zusätzlich oder alternativ mit der Steuerung **111** unter Verwendung der Prozesssteuerungsdatenautobahn **110** und/oder durch die Verwendung anderer geeigneter Steuerungssystemprotokolle (z. B. Profibus, DeviceNet, Foundation Fieldbus, ControlNet, Modbus, HART usw.).

[0026] In **Fig. 2** kommunizieren die drahtlosen Feldvorrichtungen **140**-**146** über ein Drahtlosprozesssteuerungskommunikationsnetzwerk **170** unter Verwendung eines drahtlosen Protokolls, wie dem Wire-

lessHART®-Protokoll. Derartige drahtlose Feldvorrichtungen **140**-**146** können direkt mit einer/einem oder mehreren anderen Vorrichtungen oder Knoten des Drahtlosnetzwerks **170** kommunizieren, die ebenso konfiguriert sind, um drahtlos zu kommunizieren (zum Beispiel unter Verwendung des drahtlosen Protokolls oder eines anderen drahtlosen Protokolls). Um mit anderen Knoten zu kommunizieren, die nicht konfiguriert sind, um drahtlos zu kommunizieren, können die drahtlosen Feldvorrichtungen **140**-**146** das drahtlose Gateway **135** verwenden, das mit der Prozesssteuerungsdatenautobahn **110** oder mit einem anderen Prozesssteuerungskommunikationsnetzwerk verbunden ist. Das drahtlose Gateway **135** stellt Zugriff auf die verschiedenen drahtlosen Vorrichtungen **140**-**158** des Drahtloskommunikationsnetzwerks **170** bereit. Insbesondere stellt das drahtlose Gateway **135** eine kommunikative Kopplung zwischen den drahtlosen Vorrichtungen **140**-**158**, den drahtgebundenen Vorrichtungen **115**-**128** und/oder anderen Knoten oder Vorrichtungen der Prozesssteuerungsanlage **100** bereit. Zum Beispiel kann das drahtlose Gateway **135** unter Verwendung der Prozesssteuerungsdatenautobahn **110** und/oder unter Verwendung eines oder mehrerer anderer Kommunikationsnetzwerke der Prozessanlage **100** eine kommunikative Kopplung bereitstellen.

[0027] Ähnlich wie die drahtgebundenen Feldvorrichtungen **115**-**122** führen die drahtlosen Feldvorrichtungen **140**-**146** des Drahtlosnetzwerks **170** in der Prozessanlage **100** physische Steuerfunktionen durch, z. B. Öffnen oder Schließen von Ventilen oder das Aufnehmen von Messwerten für Prozessparameter. Die drahtlosen Feldvorrichtungen **140**-**146** sind jedoch konfiguriert, um unter der Verwendung des drahtlosen Protokolls des Netzwerks **170** zu kommunizieren. Daher sind die drahtlosen Feldvorrichtungen **140**-**146**, das drahtlose Gateway **135** und die anderen drahtlosen Knoten **152**-**158** des Drahtlosnetzwerks **170** Erzeuger und Konsumenten von drahtlosen Kommunikationspaketen.

[0028] In einigen Konfigurationen der Prozessanlage **100** beinhaltet das Drahtlosnetzwerk **170** nicht drahtlose Vorrichtungen. Zum Beispiel ist in **Fig. 2** eine Feldvorrichtung **148** aus **Fig. 2** eine ältere Vorrichtung mit 4-20 mA und eine Feldvorrichtung **150** ist eine drahtgebundene HART®-Vorrichtung. Um in dem Netzwerk **170** zu kommunizieren, sind die Feldvorrichtungen **148** und **150** über einen entsprechenden Drahtlosadapter **152A**, **152B** mit dem Drahtloskommunikationsnetz **170** verbunden. Die Drahtlosadapter **152A**, **152B** unterstützen ein drahtloses Protokoll, wie zum Beispiel WirelessHART, und sie können ebenfalls ein oder mehrere andere Kommunikationsprotokolle wie Foundation® Fieldbus, PROFIBUS, DeviceNet usw. unterstützen. Außerdem beinhaltet das Drahtlosnetzwerk **170** in einigen Konfigurationen einen oder mehrere Netzwerkzugangspunkte **155A**, **155B**, bei welchen es sich um getrennte physische Vorrichtung in drahtgebundener Kommunikation mit dem drahtlosen Gateway **135** handeln kann oder die mit dem drahtlosen Gateway **135** als eine einstückige Vorrichtung bereitgestellt sein können. Das Drahtlosnetzwerk **170** kann außerdem einen oder mehrere Router **158** einschließen, um Pakete in dem Drahtloskommunikationsnetzwerk **170** von einer drahtlosen Vorrichtung zu einer anderen drahtlosen Vorrichtung weiterzuleiten. In **Fig. 2** kommunizieren die drahtlosen Vorrichtungen **140**-**146** und **152**-**158** über drahtlose Verbindungen **160** des Drahtloskommunikationsnetzwerks **170** und/oder über die Prozesssteuerungsdatenautobahn **110** miteinander und mit dem drahtlosen Gateway **135**.

[0029] In **Fig. 2** beinhaltet das Prozesssteuerungssystem **100** eine oder mehrere Arbeitsstationen mit Bedienpersonal **171**, die kommunikativ mit der Datenautobahn **110** verbunden sind. Über die Arbeitsstationen mit Bedienpersonal **171** können Bediener Laufzeitvorgänge der Prozessanlage **100** betrachten und überwachen sowie beliebige Diagnose-, Korrektur-, Wartungs- und/oder andere nötige Handlungen durchführen. Mindestens einige der Arbeitsstationen mit Bedienpersonal **171** können in verschiedenen, geschützten Bereichen oder in der Nähe der Anlage **100**, z. B. in einer Backend-Umgebung der Anlage **100**, angeordnet sein und in einigen Situationen können mindestens einige der Arbeitsstationen mit Bedienpersonal **171** entfernt, aber nichtsdestoweniger in kommunikativer Verbindung mit der Anlage **100** angeordnet sein. Die Arbeitsstationen mit Bedienpersonal **171** können drahtgebundene oder drahtlose Rechenvorrichtungen sein.

[0030] Das beispielhafte Prozesssteuerungssystem **100** beinhaltet der Veranschaulichung nach ferner eine Konfigurationsanwendung **172A** und eine Konfigurationsdatenbank **172B**, wobei jede davon ebenfalls kommunikativ mit der Datenautobahn **110** verbunden ist. Wie vorstehend erörtert, können verschiedene Instanzen der Konfigurationsanwendung **172A** auf einer oder mehreren Rechenvorrichtungen (nicht gezeigt) ausgeführt werden, um Benutzern das Erstellen oder Verändern von Prozesssteuerungsmodulen und das Herunterladen dieser Module über die Datenautobahn **110** auf die Steuerung **111** zu ermöglichen sowie den Benutzern das Erstellen und Verändern von Bedienerschnittstellen zu ermöglichen, über welche ein Bediener in der Lage ist, Daten zu betrachten und Dateneinstellungen innerhalb von Prozesssteuerungsroutinen zu verändern. Die Konfigurationsdatenbank **172B** speichert die erzeugten (z. B. konfigurierten) Module und/oder Bedienerschnittstellen. Im Allgemeinen sind die Konfigurationsanwendung **172A** und die Konfigurationsdatenbank **172B** zentralisiert und weisen eine einheitliche logische Erscheinung gegenüber dem Prozesssteuerungssystem **100** auf, obwohl mehrere Instanzen der Konfi-

gurationsanwendung **172A** gleichzeitig innerhalb des Prozesssteuerungssystems **100** ausgeführt werden können und die Konfigurationsdatenbank **172B** über mehrere physische Datenspeichervorrichtungen hinweg umgesetzt sein kann. Dementsprechend umfassen die Konfigurationsanwendung **172A**, die Konfigurationsdatenbank **172B** und zugehörige Benutzerschnittstellen (nicht gezeigt) ein Konfigurations- oder Entwicklungssystem **172** für Steuer- und/oder Anzeigemodule. Typischerweise, jedoch nicht notwendigerweise, unterschieden sich die Benutzerschnittstellen für das Konfigurationssystem **172** von den Arbeitsstationen mit Bedienpersonal **171**, da die Benutzerschnittstellen für das Konfigurationssystem **172** durch Konfigurations- und Entwicklungsingenieure unabhängig davon verwendet werden, ob die Anlage **100** in Echtzeit arbeitet oder nicht, wohingegen die Arbeitsstationen mit Bedienpersonal **171** durch Bediener während Echtzeitvorgängen der Prozessanlage **100** verwendet werden (hier ebenfalls austauschbar als „Laufzeit"-Vorgänge der Prozessanlage **100** bezeichnet).

[0031] Das beispielhafte Prozesssteuerungssystem **100** beinhaltet eine Data-Historian-Anwendung **173A** und eine Data-Historian-Datenbank **173B**, wobei jede davon ebenfalls kommunikativ mit der Datenautobahn **110** verbunden ist. Die Datenverlaufsarchivanwendung **173A** dient dazu, einige oder alle der Daten zu sammeln, die über die Datenautobahn **110** bereitgestellt werden und die Daten in der Historian-Datenbank **173B** für Langzeitspeicherung zu archivieren oder zu speichern. Ähnlich wie die Konfigurationsanwendung **172A** und die Konfigurationsdatenbank **172B** sind die Datenverlaufsarchivanwendung **173A** und die Historian-Datenbank **173B** zentralisiert und weisen eine einheitliche logische Erscheinung gegenüber dem Prozesssteuerungssystem **100** auf, obwohl mehrere Instanzen einer Datenverlaufsarchivanwendung **173A** gleichzeitig innerhalb des Prozesssteuerungssystems **100** ausgeführt werden können und das Data-Historian **173B** über mehrere physische Datenspeichervorrichtungen hinweg umgesetzt sein kann.

[0032] In einigen Konfigurationen beinhaltet das Prozesssteuerungssystem **100** einen oder mehrere andere drahtlose Zugangspunkte **174** auf, die mit anderen Vorrichtungen unter Verwendung von drahtlosen Protokolle kommunizieren, wie zum Beispiel Wi-Fi oder andere IEEE **802.11** konforme Protokoll für drahtlose lokale Netzwerke, mobile Kommunikationsprotokolle, wie zum Beispiel mit WiMAX (Worldwide Interoperability for Microwave Access), LTE (Long Term Evolution) oder anderen ITU-R (International Telecommunication Union Radiocommunication Sector) konformen Protokollen, kurzwellige Funkkommunikationen wie Nahfeldkommunikationen (NFC) und Bluetooth oder andere drahtlose Kommunikationsprotokolle. Typischerweise ermöglichen derartige drahtlose Zugriffspunkte **174**, dass Hand- oder andere tragbare Rechenvorrichtungen (z. B. Benutzerschnittstellenvorrichtungen **175**) über ein entsprechendes Drahtlosprozesssteuerungskommunikationsnetzwerk kommunizieren, das sich von dem Drahtlosnetzwerk **170** unterscheidet und ein anderes drahtloses Protokoll unterstütz als das Drahtlosnetzwerk **170**. Zum Beispiel kann eine drahtlose oder tragbare Benutzerschnittstellenvorrichtung **175** eine mobile Arbeitsstation oder Diagnosetestausrüstung sein, die durch einen Bediener innerhalb der Prozessanlage **100** verwendet wird (z. B. im Falle einer der Arbeitsstationen **171** mit Bedienpersonal). In einigen Szenarien kommunizieren zusätzlich zu tragbaren Rechenvorrichtungen außerdem eine oder mehrere Prozesssteuerungsvorrichtungen (z. B. die Steuerung **111**, die Feldvorrichtungen **115**-**122** oder die drahtlosen Vorrichtungen **135**, **140**-**158**) unter Verwendung des drahtlosen Protokolls, das von dem Zugriffspunkt **174** unterstützt wird.

[0033] In einigen Konfigurationen beinhaltet das Prozesssteuerungssystem **100** ein oder mehrere Gateways **176**, **178** zu Systemen außerhalb des unmittelbaren Prozesssteuerungssystems **100**. Typischerweise sind derartige Systeme Abnehmer oder Lieferanten von Informationen, die von dem Prozesssteuerungssystem **100** erzeugt werden oder mit denen es arbeitet. Zum Beispiel kann die Prozesssteuerungsanlage **100** einen Gateway-Knoten **176** zum kommunikativen Verbinden der unmittelbaren Prozessanlage **100** mit einer anderen Prozessanlage beinhalten. Zusätzlich oder alternativ kann die Prozessteuerungsanlage **100** einen Gateway-Knoten **178** zum kommunikativen Verbinden der unmittelbaren Prozessanlage **100** mit einem externen öffentlichen oder privaten System beinhalten, wie einem Laborsystem (z. B. Labor-Informations- und Managementsystem oder LIMS), einer Operator-Rounds-Datenbank, einem Materialhandhabungssystem, einem Wartungsmanagementsystem, einem Produktbestandssteuerungssystem, einem Produktionszeitplansystem, einem Wetterdatensystem, einem Transport- und Handhabungssystem, einem Verpackungssystem, dem Internet, dem Prozesssteuerungssystem eines anderen Providers oder anderen externen Systemen.

[0034] Es ist anzumerken, dass, obwohl **Fig. 2** nur eine einzelne Steuerung **111** mit einer begrenzten Anzahl an Feldvorrichtungen **115**-**122** und **140**-**146**, drahtlosen Gateways **35**, drahtlosen Adaptern **152**, zugangspunkten 155, Routern **1158** und Drahtlosprozesssteuerungskommunikationsnetzwerken **170**, die in der beispielhaften Prozessanlage **100** enthalten sind, veranschaulicht, handelt es sich dabei nur um eine veranschaulichende und nicht einschränkende Ausführungsform. Eine beliebige Anzahl an Steuerungen **111** kann in der Prozesssteuerungsanlage oder dem -system 100 enthalten sein und beliebige

der Steuerungen **111** können mit einer beliebigen Anzahl an drahtgebundenen oder drahtlosen Vorrichtungen und Netzwerken **115**-**122**, **140**-**146**, **135**, **152**, **155**, **158** und **170** kommunizieren, um einen Prozess in der Anlage **100** zu steuern.

[0035] **Fig. 3** veranschaulicht ein Blockdiagramm einer beispielhaften Sicherheitsarchitektur **200** für die beispielhafte Prozessanlage **100** aus **Fig. 1**. Zur Referenz werden die verschiedenen Sicherheitsstufen **0**-**5** aus **Fig. 1** über die Oberseite von **Fig. 3** hinweg dargestellt, um anzugeben, auf welchen Sicherheitsstufen verschiedene Teile der Sicherheitsarchitektur **200** enthalten sein können, diese Referenz ist jedoch lediglich eine Richtlinie, da verschiedene Teile der Sicherheitsarchitektur **200** auf anderen Sicherheitsstufen eingeschlossen sein können als jenen, die in **Fig. 3** dargestellt sind.

[0036] Wie in **Fig. 3** gezeigt, sind eine oder mehrere Vorrichtungen **202** kommunikativ mit einem oder mehreren drahtlosen Gateways **205A**, **205B** verbunden, die zum Beispiel Instanzen des drahtlosen Gateways **135** aus **Fig. 1** sein können. Wie bereits erörtert, können die drahtlosen Gateways **205A**, **205B** auf Sicherheitsstufe **1** und/oder Sicherheitsstufe **2** angeordnet sein, z. B. innerhalb der Prozessanlage **100** selbst. Die kommunikativen Verbindungen zwischen den Gateways **205A**, **205B** und den Vorrichtungen **202** werden durch die Bezugszeichen **204A**, **204B** gekennzeichnet.

[0037] Der Satz von Vorrichtungen **202** befindet sich der Veranschaulichung nach auf der Sicherheitsstufe **0** der Prozessanlage **100** und umfasst der Darstellung nach eine begrenzte Anzahl an drahtlosen Feldvorrichtungen. Es versteht sich jedoch, dass die hier in Bezug auf die Vorrichtungen **202** beschriebenen Konzepte und Merkmale leicht auf eine beliebige Anzahl an Feldvorrichtungen der Prozessanlage **100** sowie auf beliebige Typen von Feldvorrichtungen angewendet werden kann. Zum Beispiel können die Feldvorrichtungen **202** eine oder mehrere der drahtgebundenen Feldvorrichtungen **115**-**122** beinhalten, die kommunikativ mit den drahtlosen Gateways **205A**, **205B** über ein oder mehrere drahtgebundene Kommunikationsnetzwerke **110** der Prozessanlage **100** verbunden sind, und/oder die Feldvorrichtungen **202** können die drahtgebundenen Feldvorrichtungen **148**, **150** beinhalten, die mit den drahtlosen Adaptern **152A**, **152B** und dadurch mit den drahtlosen Gateways **205A**, **205B** gekoppelt sind.

[0038] Es versteht sich ferner, dass der Satz von Vorrichtungen **202** nicht auf nur Feldvorrichtungen beschränkt ist, die Prozessdaten erzeugen, sondern er kann zusätzlich oder alternativ eine beliebige Vorrichtung oder Komponente innerhalb der Prozessanlage **100** beinhalten, die Daten als ein Ergebnis der Prozessanlage **100** erzeugt, die angeschlossene Prozesse steuert. Zum Beispiel kann der Satz von Vorrichtungen **202** eine Diagnosevorrichtung oder -komponente, die Diagnosedaten erzeugt, eine Netzwerk-Routing-Vorrichtung oder -komponente, die Informationen zwischen verschiedenen Komponenten und/oder Vorrichtungen der Prozessanlage **100** überträgt, und dergleichen beinhalten. Tatsächlich kann eine beliebige/können beliebige der in **Fig. 2** gezeigten Komponenten (z. B. 111, 115-122, 126, 128, 135, 140-146, 152, 155, 158, 160, 170, 171-176, 178) und andere Komponenten, die nicht in **Fig. 2** gezeigt sind, eine Vorrichtung oder Komponente **202** sein, die Daten zur Lieferung an das entfernte System **210** erzeugt. Daher wird der Satz von Vorrichtungen **202** hier austauschbar als „Datenquellen 202“ oder „Datenquellenvorrichtungen 202“ bezeichnet.

[0039] **Fig. 3** veranschaulicht ferner einen Satz von entfernten Anwendungen oder Diensten **208**, die in Bezug auf die Prozessanlage **100** verwendet werden können und/oder die die Prozessanlage **100** verwendet. Der Satz von entfernten Anwenden oder Diensten **208** kann auf einem oder mehreren entfernten Systemen **210** ausgeführt oder gehostet werden und der Satz von entfernten Anwendungen/Diensten **208** gilt allgemein betrachtet als auf Sicherheitsstufe **5** oder darüber angeordnet. Mindestens einige der Anwendungen oder Dienste **208** arbeiten in Echtzeit mit Echtzeitdaten, da die Echtzeitdaten durch die Prozessanlage **100** erzeugt werden und von den Anwendungen oder Diensten **208** empfangen werden. Andere Anwendungen oder Dienste **208** können mit von der Prozessanlage erzeugten Daten mit weniger strikten Zeitanforderungen arbeiten oder damit ausgeführt werden. Beispiele für die Anwendungen/Dienste **208**, die auf dem entfernten System **210** ausgeführt oder gehostet werden können und die Konsumenten von Daten sind, die durch die Prozessanlage **100** erzeugt wurden, beinhalten Anwendungen, die Bedingungen und/oder Ereignisse, die in der Prozessanlage **100** stattfinden, überwachen und/oder erfassen, und/oder Anwendungen oder Dienste, die mindestens einen Teil des angeschlossenen Prozesses selbst überwachen, wenn er in der Prozessanlage **100** ausgeführt wird. Andere Beispiele für die Anwendungen/Dienste **208** beinhalten deskriptive und/oder präskriptive Analytik, die mit Daten arbeiten kann, die durch die Prozessanlage **100** erzeugt wurden, und in anderen Fällen mit Wissen arbeiten kann, welches durch das Analysieren der von der Prozessanlage erzeugten Daten gesammelt oder entdeckt wurde, sowie mit Daten, die durch andere Prozessanlagen erzeugt oder von diesen empfangen wurden. Wieder andere Beispiele für die Anwendungen/Dienste **208** beinhalten eine oder mehrere Routinen, die präskriptive Funktionen, Modifikationen von Konfigurationen und/oder anderen Daten und/oder andere präskriptive Veränderungen umsetzen, die zurück in die Prozessanlage **100** umzusetzen sind, z. B. als ein Ergebnis eines anderen Diens-

tes oder einer anderen Anwendung. Einige Beispiele für Anwendungen und Dienste **208** sind beschrieben in der US-Patentanmeldung Nr. 15/274,519, eingereicht am 23. September **2016**, mit dem Titel „Data Analytics Services for Distributed Industrial Performance Monitoring“, in der US-Patentanmeldung Nr. 15/274,233, eingereicht am 23. September **2016**, mit dem Titel „Distributed Industrial Performance Monitoring and Analytics“, und in der US-Patentanmeldung Nr. 15/332,521, eingereicht am 24. Oktober **2016**, mit dem Titel „Process Device Condition and Performance Monitoring“, wobei die gesamten Offenbarungen davon hiermit durch Bezugnahme aufgenommen werden.

[0040] Das eine oder die mehreren entfernten Systeme **210** können auf eine beliebige gewünschte Weise umgesetzt werden, wie zum Beispiel durch eine entfernte Bank vernetzter Server, ein oder mehrere Cloud-Computersysteme, ein oder mehrere Netzwerke usw. Zur einfachen Erörterung werden das eine oder die mehreren entfernten Systeme **210** hier unter Verwendung der Singularform bezeichnet, d. h. „entferntes System 210“, obwohl es sich versteht, dass sich der Begriff auf ein System, mehr als ein System oder eine beliebige Anzahl an Systemen beziehen kann.

[0041] Allgemein ausgedrückt, stellt die Sicherheitsarchitektur **200** eine Ende-zu-Ende-Sicherheit von der Feldumgebung der Prozessanlagen **100**, in welchen die Vorrichtungen **202** installiert sind und arbeiten, bis zum entfernten System **210** bereit, welches Anwendungen und/oder Dienste **208** bereitstellt, welche die Daten, die durch die Prozessanlage **100** erzeugt wurden, konsumieren und damit arbeiten. Daher sind Daten, die durch die Vorrichtungen **202** und andere Komponenten der Prozessanlage **100** erzeugt wurden, in der Lage, sicher zu dem entfernten System **210** zur Verwendung durch die entfernten Anwendungen/Dienste **208** transportiert zu werden, während die Anlage **100** vor Cyber-Angriffen, -Eingriffen und/oder anderen schädlichen Ereignissen geschützt ist. Insbesondere beinhaltet die Sicherheitsarchitektur **200** ein Feld-Gateway **212**, eine Datendiode **215** und ein Rand-Gateway **218**, die zwischen der Prozessanlage **100** (z. B zwischen den drahtlosen Gateways **205A**, **205B** der Prozessanlage **100**) und dem entfernten System **210** angeordnet sind. Typischerweise, jedoch nicht notwendigerweise, sind das Feld-Gateway **212**, die Datendiode **215** und das Rand-Gateway **218** in den Sicherheitsstufen **2**-**5** enthalten.

[0042] Die Datendiode **215** ist ein wichtiger Aspekt der Sicherheitsarchitektur **200**. Die Datendiode **215** ist eine Komponente, die in Hardware, Firmware und/oder Software umgesetzt ist, und sie ist insbesondere konfiguriert, um Zweiwege-Kommunikationen zwischen der Prozessanlage **100** und dem entfernten System **210** zu verhindern. Das heißt, die Datendiode **215** ermöglicht das Austreten von Datenverkehrt aus dem Prozesssteuerungssystem **100** hin zu dem entfernten System **210** und verhindert das Eintreten von Datenverkehr (der z. B. von dem entfernten System **210** oder einem anderen System übertragen oder gesendet wird) in das Prozesssteuerungssystem **100**.

[0043] Dementsprechend beinhaltet die Datendiode **215** mindestens einen Eingangsanschluss **220**, der kommunikativ mit dem Feld-Gateway **212** verbunden ist, und mindestens einen Ausgangsanschluss **222**, der kommunikativ mit dem Rand-Gateway **218** verbunden ist. Die Datendiode **215** beinhaltet ebenfalls eine Glasfaser- oder Kommunikationsverbindung einer beliebigen anderen geeigneten Technologie, welche deren Eingangsanschluss **222** mit deren Ausgangsanschluss **222** verbindet. Um das Strömen von Datenverkehr zu dem (z. B. Eintreten in das) Prozesssteuerungssystem **100** zu verhindern, schließt die Datendiode **215** in einer beispielhaften Umsetzung einen Eingangsanschluss zum Empfangen von Daten von dem Rand-Gateway **218** (oder einer anderen Komponente auf einer höheren Sicherheitsstufe) aus oder lässt diesen weg und/oder schließt einen Ausgangsanschluss zum Übertragen von Daten an das Feld-Gateway **212** (oder eine Komponente auf einer niedrigeren Sicherheitsstufe) aus oder lässt diesen weg. In einer zusätzlichen oder alternativen Umsetzung schließt die Datendiode **215** Sendeempfänger aus, lässt diese weg und/oder deaktiviert diese, die ansonsten das Strömen von Daten von dem Ausgangsanschluss **222** zu dem Eingangsanschluss **220** ermöglichen würden, und/oder sie schließt einen physischen Kommunikationspfad für Daten zum Strömen von dem Ausgangsanschluss **222** zu dem Eingangsanschluss **220** aus. Wieder zusätzlich oder alternativ kann die Datendiode **215** nur unidirektionale Datenströmung von dem Eingangsanschluss **220** zu dem Ausgangsanschluss **222** über Software unterstützen, z. B. durch Fallenlassen oder Blockieren beliebiger Nachrichten, die am Ausgangsanschluss **222** von dem Rand-Gateway **218** (oder einer Komponente auf einer höheren Sicherheitsstufe) empfangen wurden, und/oder durch Fallenlassen oder Blockieren beliebiger Nachrichten, die an das Feld-Gateway **212** (oder eine Komponente auf einer niedrigeren Sicherheitsstufe) adressiert ist.

[0044] Daten, welche die Prozessanlage **100** verlassen und über die Datendiode **215** von dem Eingangsanschluss **220** an den Ausgangsanschluss **222** übertragen werden, können durch Verschlüsselung über die Datendiode **215** weiter gesichert werden. In einem Beispiel verschlüsselt das Feld-Gateway **212** Daten und gibt die verschlüsselten Daten an den Eingangsanschluss **220** ab. In einem weiteren Beispiel empfängt die Datendiode **215** Datenverkehr von dem Feld-Gateway **212** und die Datendiode **215** verschlüsselt den empfangenen Datenverkehr, bevor

die Daten an den Ausgangsanschluss **222** geleitet werden. Der Datenverkehr, der über die Datendiode **215** verschlüsselt und transportiert wird, kann in einem Beispiel ein UDP(User Datagram Protocol)-Datenverkehr sein und er kann in einem anderen Beispiel ein JSON-Datenverkehr oder ein anderes Universal-Kommunikationsformat sein.

[0045] Das Feld-Gateway **212** verbindet die niedrigere Sicherheitsseite der Datendiode **215** mit der Prozesssteuerungsanlage **100** kommunikativ. Wie **Fig. 3** gezeigt, ist das Feld-Gateway **212** kommunikativ mit den drahtlosen Gateways **205A**, **205B** verbunden, die innerhalb der Feldumgebung der Prozessanlage **100** angeordnet sind und die kommunikativ mit einer oder mehreren Vorrichtungen oder Datenquellen **202** verbunden sind. Wie bereits erörtert, können die Vorrichtungen oder Datenquellen **202** und die drahtlosen Gateways **205A**, **205B** unter Verwendung des industriellen WirelessHART-Protokolls oder eines anderen geeigneten drahtlosen Protokolls kommunizieren, welches aufgebaut ist, um gesicherte Kommunikationen über einen oder mehrere Sicherheitsmechanismen bereitzustellen. Zum Beispiel stellt das WirelessHART-Protokoll 128-Bit-AES-Verschlüsselung bereit und die Kommunikationspfade **204A**, **204B** können entsprechend gesichert werden.

[0046] Außerdem ist die Kommunikationsverbindung **225** zwischen den drahtlosen Gateways **205A**, **205B** und dem Feld-Gateway **212** entsprechend unter Verwendung desselben oder eines anderen Mechanismus gesichert, wie für die kommunikativen Verbindungen **204A**, **204B** verwendet. In einem Beispiel ist die kommunikative Verbindung **225** durch einen TLS(Transport Layer Security)-Wrapper gesichert. Zum Beispiel erzeugen die drahtlosen Gateways **205A**, **205B** Pakete im HART-IP-Format, welches durch einen TLS-Wrapper zum Leiten an das Feld-Gateway **212** gesichert wird.

[0047] Wie vorstehend beschrieben, können in einer Ausführungsform somit Daten oder Pakete, die durch die Vorrichtungen **202** erzeugt wurden, zur Übertragung **204A**, **204B** an die drahtlosen Gateways **205A**, **205B** unter Verwendung eines ersten Sicherheitsmechanismus und anschließend zur Übertragung **225** von den drahtlosen Gateways **205A**, **205B** an das Feld-Gateway **212** unter Verwendung eines zweiten Sicherheitsmechanismus gesichert werden und noch immer zur Übertragung über die Datendiode **215** unter Verwendung eines dritten Sicherheitsmechanismus gesichert werden.

[0048] Unter Bezugnahme auf die Seite höherer Sicherheit der Datendiode **215** kann Datenverkehr, der aus der Datendiode **215** austritt, zur Übertragung an das Rand-Gateway **218**, wenn gewünscht, unter Verwendung eines vierten Sicherheitsmechanismus oder unter Verwendung eines der Sicherheitsmechanismen gesichert werden, die für die Seite niedrigerer Sicherheit der Datendiode **215** verwendet wurden, wie vorstehend erörtert. Zusätzlich oder alternativ und wie in **Fig. 3** dargestellt kann das Rand-Gateway **218** durch eine Firewall **228** geschützt werden, bei der es sich um die Firewall **12C** aus **Fig. 1** oder um eine andere Firewall handeln kann.

[0049] Daten, die von dem Rand-Gateway **218** an das entfernte System **210** übertragen werden, können unter Verwendung eines oder mehrerer öffentlicher und/oder privater Netzwerke abgegeben werden, wie zum Beispiel ein privates Unternehmensnetzwerk, das Internet, ein Mobilfunkrouter, ein Backhaul-Internet oder ein anderer Typ von Backhaul-Verbindungen. Es ist signifikant, dass die Daten, die von dem Rand-Gateway **218** an das entfernte System **210** übertragen werden, unter Verwendung eines fünften Sicherheitsmechanismus oder unter Verwendung eines der bereits vorstehend erörterten Sicherheitsmechanismen gesichert werden. Der Darstellung in **Fig. 3** nach ist der Datenverkehr, der von dem Rand-Gateway **218** an das entfernte System **210** abgegeben wird, über ein SAS(Shared Access Signature)-Token gesichert, das durch einen Token-Dienst **230** verwaltet werden kann, der am entfernten System **210** bereitgestellt wird. Das Rand-Gateway **218** authentifiziert sich gegenüber dem Token-Dienst **230** und fordert ein SAS-Token an, das nur für einen begrenzten Zeitraum gültig sein kann, z. B. zwei Minuten, fünf Minuten, dreißig Minuten, nicht mehr als eine Stunde usw. Das Rand-Gateway **218** empfängt und verwendet das SAS-Token zum Sichern und zum Authentifizieren einer AMQP(Advanced Message Queuing Protocol)-Verbindung mit dem entfernten System **210**, über welche Inhaltsdaten von dem Rand-Gateway **218** an das entfernte System **210** übertragen werden. Selbstverständlich ist die Verwendung von SAS-Tokens und des AMQP-Protokolls zum Sichern von Daten, die zwischen dem Rand-Gateway **218** und dem entfernten System **210** übertragen werden, nur einer von vielen möglichen Sicherheitsmechanismen. Zum Beispiel kann/können ein beliebiger oder mehrere geeignete Sicherheitsmechanismen des Internets der Dinge (IOT) zum Sichern von Daten verwendet werden, die zwischen dem Rand-Gateway **218** und dem entfernten System **210** übertragen werden, wie zum Beispiel X.509-Zertifikate, andere Token-Typen, andere IOT-Protokolle, wie zum Beispiel MQTT (MQ Telemetry Transport) oder XMPP (Extensible Messaging and Presence Protocol), und dergleichen. In diesen und anderen Ausführungsformen stellt der Dienst **230** zum Beispiel die entsprechenden Sicherheitstokens oder -zertifikate bereit oder gibt diese aus.

[0050] Am entfernten System **210** wird Benutzerauthentifizierung und/oder -autorisierung durch einen beliebigen oder mehrere geeignete Authentifi-

zierungs- und/oder Autorisierungssicherheitsmechanismen **232** bereitgestellt. Zum Beispiel kann sicherer Zugriff auf das entfernte System **210** durch einen Domain-Authentifizierungsdienst, einen API-Benutzerauthentifizierungsdienst und/oder einen beliebigen anderen geeigneten Authentifizierungs- und/oder Autorisierungsdienst **232** bereitgestellt werden. Daher sind nur Benutzer **235**, die über den Authentifizierungs- und/oder Autorisierungsdienst **232** authentifiziert und/oder autorisiert sind, in der Lage, Zugriff auf mindestens einige der Daten zu erhalten, die am entfernten System **210** bereitstehen, die unter anderem die durch die Vorrichtungen **202** erzeugten Daten beinhalten.

[0051] Somit, wie vorstehend beschrieben, stellt die Sicherheitsarchitektur **200** Ende-zu-Ende-Sicherheit für Daten bereit, die durch Vorrichtungen oder Datenquellen **202** erzeugt werden, während sie in der Prozessanlage **100** arbeiten, um einen Prozess zu steuern, z. B. von der Aufnahme der Daten durch die Datenquellen **202**, über deren Übertragung an das entfernte System **210**, bis zur Verarbeitung durch eine(n) oder mehrere entfernte Anwendungen oder Dienste **208**. Es ist wichtig, dass die Sicherheitsarchitektur **200** diese Ende-zu-Ende-Sicherheit bereitstellt, während sie verhindert, dass die Prozessanlage **100** schädliche Angriffe erleidet.

[0052] Es ist anzumerken, dass, obwohl **Fig. 3** drahtlose Gateways **205A**, **205B** als Vorrichtungen oder Datenquellen **202** mit dem feld-Gateway 212 kommunikativ verbindend darstellt, in einigen Anordnungen eins oder mehrere der drahtlosen Gateways **205A**, **205B** weggelassen werden und Quellendaten von den Datenquellen **202** direkt an das Feld-Gateway **212** übertragen werden. Zum Beispiel können die Datenquellen **202** Quellendaten über ein Big-Data-Netzwerk der Prozessanlage **100** direkt an das Feld-Gateway **212** übertragen. Allgemein ausgedrückt, ist ein Big-Data-Netzwerk der Prozessanlage **100** weder das Backbone-Anlagennetzwerk **110**, noch ist das Big-Data-Netzwerk ein industrielles Protokollnetzwerk, das zum Übertragen von Steuersignalen zwischen den Vorrichtungen unter Verwendung eines industriellen Kommunikationsprotokolls (z. B. Profibus, DeviceNet, Foundation Fieldbus, ControlNet, Modbus, HART usw.) verwendet wird. Vielmehr kann ein Big-Data-Netzwerk der Prozessanlage **100** ein Überlagerungsnetzwerk sein, welches für die P 100 umgesetzt wird und welches Daten zwischen Knoten für zum Beispiel datenverarbeitungs- und -analytikzwecke streamt. Die Knoten eines Big-Data-Netzwerks können zum Beispiel die Datenquellen **202**, die drahtlosen Gateways **205A**, **205B** und das Feld-Gateway **212** sowie eine beliebige oder mehrere beliebige der in **Fig. 2** gezeigten Komponenten **111**, **115**-**122**, **126**, **128**, **135**, **140**-**146**, **152**, **155**, **158**, **160**, **170**, **171**-**176**, **178** und andere Komponenten beinhalten. Dementsprechend beinhalten viele Knoten eines Prozessanlagendatennetzwerks jeweils eine designierte Schnittstelle für Prozessanlagenvorgänge, die typischerweise ein industrielles Kommunikationsprotokoll verwenden, und eine andere designierte Schnittstelle für Datenverarbeitungs- und -analytikvorgänge, die zum Beispiel ein Streaming-Protokoll verwenden können. Ein Beispiel für ein Big-Data-Netzwerk, welches in einer Prozessanlage **100** verwendet werden kann, ist beschrieben in der US-Patentanmeldung Nr. 14/507,188 mit dem Titel „Regional Big Data in Process Control Systems“, eingereicht am 6. Oktober **2014**, wobei die gesamte Offenbarung davon durch Bezugnahme in diese Schrift aufgenommen wird.

[0053] Es ist ferner in Bezug auf **Fig. 3** anzumerken, dass in einigen Ausführungsformen ein drahtgebundenes Gateway (nicht gezeigt) an Stelle eines der drahtlosen Gateways **205A**, **205B** verwendet werden kann. Darüber hinaus können das Feld-Gateway **212** die Datendiode **215** und das Rand-Gateway **218** physisch gemeinsam angeordnet sein, wie zum Beispiel durch den in **Fig. 3** gezeigten Kasten **235** angegeben, oder eine oder mehrere der Komponenten **212**, **215**, **218** können physisch über mehrere Standorte hinweg angeordnet sein. Zum Beispiel kann/können eins oder mehrere des Feld-Gateways **212**, der Datendiode **215** oder des Rand-Gateways **218** bei der Prozessanlage **100** angeordnet sein. Zusätzlich oder alternativ kann/können eins oder mehrere des Feld-Gateways **212**, der Datendiode **215** oder des Rand-Gateways **218** entfernt von der Prozessanlage **100** angeordnet sein.

[0054] Die Prozessanlage **100** kann, wenn gewünscht, durch mehr als ein Feld-Gateway **212** bedient werden und eine beliebige Anzahl an Feld-Gateways **210** kann durch ein einzelnes Rand-Gateway **218** bedient werden. In einigen Ausführungsform wird das entfernte System **210** durch mehr als ein Rand-Gateway **218** bedient, wenn dies gewünscht ist.

[0055] Wie bereits erörtert, ist Datenverkehr, der über die Datendiode **215** transportiert wird, gesichert. Ein derartiger Datenverkehr kann zum Beispiel unter Verwendung von serieller Kommunikation oder UDP-Kommunikation über die Datendiode **215** kommuniziert werden. Das sicher derartiger Kommunikationen ohne Zweiwege-Kommunikationen ist jedoch schwierig und umständlich, da typischerweise sowohl UDP- als auch serielle Kommunikationen erfordern, dass beide Seiten nicht nur bidirektional kommunizieren (was unter Verwendung der Datendiode **215** nicht möglich ist), sondern sich auch lange Schlüsselsequenzen merken und eingeben. Statt traditionelle Zweiwege-Kommunikationen zum Sichern von Daten zu verwenden, die über die unidirektionale Datendiode **215** transportiert werden, werden die transportierten Daten über einen Sicherheitsbereitstellungs-

prozess gesichert, der zwischen dem Rand-Gateway **218** und dem Feld-Gateway **212** verwendet wird. Der Sicherheitsbereitstellungsprozess etabliert einen einzigartigen anfänglichen Schlüssel oder ein geheimes Material, welches zwischen dem Rand-Gateway **218** und dem Feld-Gateway **212** geteilt wird (z. B. ein symmetrischer Schlüssel oder ein symmetrisches Material), wie zum Beispiel ein Verknüpfungsschlüssel. Unter Verwendung des Verknüpfungsschlüssels etablieren das Rand-Gateway **218** und das Feld-Gateway **212** eine sichere Verbindung, die zum Austauschen von weiterem Schlüssel- oder geheimen Material verwendet wird, welches wiederum zum Sicheren Transportieren von Datenverkehr über die Datendiode **215** verwendet wird.

[0056] Fig. 4 stellt einen beispielhaften Nachrichtenablauf **250** dar, der für den Sicherheitsbereitstellungsprozess verwendet werden kann. In **Fig. 4** sind sowohl das Feld-Gateway **212** als auch das Rand-Gateway **218** in einem Bereitstellungsnetzwerk (z. B. dasselbe Teilnetzwerk, nicht gezeigt) enthalten, wie auch ein Bereitstellungsserver oder eine - rechenvorrichtung 252, der/die durch einen Benutzer betrieben wird, um das Feld-Gateway **212** an das Rand-Gateway **218** bereitzustellen. In einer Ausführungsform sind das Feld-Gateway **212** und das Rand-Gateway **218** über das Bereitstellungsnetzwerk in der Lage, vorrübergehend bidirektional miteinander zu kommunizieren, das Bereitstellen z. B. unter Verwendung einer Kommunikation von TCP-Typ einzustellen.

[0057] Zum Beispiel meldet sich bei Referenz **255** ein Benutzer über die Bereitstellungsvorrichtung **252** in der Benutzerschnittstelle (UI) des Rand-Gateways **218** an und ist diesbezüglich authentifiziert. Zum Beispiel kann die UI des Rand-Gateways **218** eine Webschnittstelle oder eine andere geeignete UI sein. Über die Bereitstellungsseiten- oder - anzeigeansicht des Rand-Gateways **218** gibt der Benutzer die Adresse des Feld-Gateways **212** (Referenz **258**) ein (die in einem Beispiel eine IP-Adresse sein kann), wodurch bewirkt wird, dass das Rand-Gateway **218** einen Eintrag in der weißen Liste für das Feld-Gateway **212** (Referenz **260**) anlegt. Anschließend fordert das Rand-Gateway **218** von der Bereitstellungsvorrichtung **252** die Berechtigungen des Feld-Gateways **212** an, die bei der Datenübertragung zu verwenden sind (Referenz **262**).

[0058] Als Reaktion auf die Anforderung des Rand-Gateways stellt der Benutzer über die Bereitstellungsvorrichtung **252** Autorisierungs- und Sicherheitsinformationen für das Feld-Gateway **212** bereit (Referenz **265**). Diese Autorisierungs- und Sicherheitsinformationen beinhalten typischerweise (jedoch nicht notwendigerweise) anfängliches Schlüsselmaterial, welches mit dem Feld-Gateway **212** zu teilen ist. In einem Beispiel beinhaltet das anfängliche Schlüsselmaterial einen 128-Bit-, 192-Bit- oder 256-Bit-Verknüpfungsschlüssel und beinhaltet einen 32-Bit- oder 64-Bit-Paketzähler, der als ein Teil einer Nonce für Paketverschlüsselung/-entschlüsselung und in einigen Fällen für MIC(Message Integrity Check)-Berechnungen verwendet wird, die mit den Paketen durchgeführt werden. Zum Beispiel wird ein Wert des Paketzählers in der Nonce jeder Übertragung erhöht, verändert oder aktualisiert, um bei der Verteidigung gegen Netzwerk-Replay-Angriffe zu helfen. Das Rand-Gateway **218** verschlüsselt eine lokale Kopie des anfänglichen Schlüsselmaterials bei einer beliebigen Geschwindigkeit und speichert diese und sendet das anfängliche Schlüsselmaterial sowie eine oder mehrere Adressen des Rand-Gateways **218** (z. B. die IP-Adresse und/oder die MAC-Adresse des Rand-Gateways **218**) an das Feld-Gateway **212** (Referenz **268**). Bei dem Feld-Gateway **212** entschlüsselt und speichert das Feld-Gateway **212** eine lokale Kopie des anfänglichen Schlüsselmaterials sowie die Adressen des Rand-Gateways **218** und bestätigt den Empfang gegenüber dem Rand-Gateway **218** (Referenz **270**).

[0059] Anschließend leitet das Feld-Gateway **212** unidirektionale Kommunikationen mit dem Rand-Gateway **218** über die Datendiode **215** z. B. unter Verwendung von UDP ein. Insbesondere überträgt das Feld-Gateway **212** eine anfängliche Nachricht an das Rand-Gateway **218**, welche einen neuen zufällig erzeugten Netzwerkschlüssel und einen zufällig erzeugten Paketzähler (der z. B. in der Nonce und für MIC-Berechnungen zu verwenden ist) enthält, die zum Verschlüsseln und zum Überprüfen der Integrität anschließender Nachrichten zu verwenden sind. Der neue Netzwerkschlüssel und der entsprechende Paketzähler werden unter Verwendung des anfänglichen Schlüsselmaterials, z. B. dem Verknüpfungsschlüssel, und dessen entsprechenden Paketzählers verschlüsselt (Referenz **272**). Das Rand-Gateway **218** entschlüsselt die empfangene anfängliche Nachricht unter Verwendung seines lokal gespeicherten anfänglichen Schlüsselmaterials, speichert den neuen Netzwerkschlüssel und Paketzähler (Referenz **275**) und verwendet den gespeicherten Netzwerkschlüssel im Paketzähler zum Entschlüsseln von Nachrichten oder Paketen, die anschließend von dem Feld-Gateway **212** empfangen werden.

[0060] Es ist anzumerken, dass, wie in **Fig. 4** veranschaulicht, beim Empfangen durch das Rand-Gateway **218** der ersten Nachricht von dem Feld-Gateway **212**, die unter Verwendung des neuen Netzwerkschlüssels verschlüsselt wurde und den neuen Paketzähler beinhaltet (Referenzen **278**, **280**), der gesicherte Bereitstellungsprozess als abgeschlossen betrachtet werden kann und die Bereitstellungsvorrichtung **252** nicht länger am Nachrichtenablauf **250** beteiligt ist. Folglich wird in einer Ausführungsform ein vorübergehender Kommunikationskanal, der zur Kommunikation von dem Rand-Gateway **218** an das

Feld-Gateway **212** verwendet wurde (der z. B. bei Referenz **268** verwendet wurde), unterbrochen, deaktiviert oder anderweitig nicht zur Verfügung stehen kann. Das Feld-Gateway **212** sendet jedoch weiterhin Daten über die unidirektionale Datendiode **215** an das Rand-Gateway **218** unter Verwendung des gespeicherten Netzwerkschlüssels und Paketzählers (Referenz **282**) und das Rand-Gateway **218** entschlüsselt weiterhin empfangene Nachrichten unter Verwendung seines gespeicherten Netzwerkschlüssels und Paketzählers (Referenz **285**).

[0061] In einigen Ausführungsformen kehren das Feld-Gateway **212** und das Rand-Gateway **218** jedoch zu unidirektionalen Kommunikationen über die Datendiode **215** zurück, wenn die Bereitstellungsvorrichtung **252** von Netzwerk getrennt wird oder früher während des Nachrichtenablaufs **250**. Zum Beispiel kann das Rand-Gateway **218** beim Übertragen des anfänglichen Verknüpfungsschlüsselmaterials an das Feld-Gateway **212** zu unidirektionalen Kommunikationen zurückkehren (Referenz **268**) und das Feld-Gateway **212** kann beim Übertragen der Empfangsbestätigung des anfänglichen Schlüsselmaterials zu unidirektionalen Kommunikationen zurückkehren (Referenz **270**).

[0062] Für die Robustheit und Zuverlässigkeit der Datenübertragung über die unidirektionale Datendiode **215** erzeugt das Feld-Gateway **212** eine weitere Initialisierungsnachricht und einen entsprechenden zufälligen Paketzähler, um ein neues oder aktualisiertes Schlüsselmaterial mit dem Rand-Gateway **218** zu etablieren. Zum Beispiel überträgt das Feld-Gateway **212** eine weitere Initialisierungsnachricht, die unter Verwendung des anfänglichen Verknüpfungsschlüsselmaterials verschlüsselt wurde und die einen neuen oder aktualisierten Netzwerkschlüssel und einen entsprechenden neuen oder aktualisierten Paketzähler beinhaltet (Referenz **288**). Das anfängliche Verknüpfungsschlüsselmaterial wurde zuvor bei dem Feld-Gateway **212** und dem Rand-Gateway **218** gespeichert (siehe Referenzen **265**, **268**, **270**) und der aktualisierte Netzwerkschlüssel und der zufällige Paketzähler werden zum Beispiel bei dem Feld-Gateway **212** zufällig erzeugt.

[0063] Bei Referenz **290** verifiziert das Rand-Gateway **218** die empfangene Initialisierungsnachricht z. B. durch das Überprüfen der weißen Liste und/oder der Adressen, von welchen die neue Initialisierungsnachricht empfangen wurde. Wenn das Randgateway **218** bestimmt, dass die empfangene neue Initialisierungsnachricht gültig ist, entschlüsselt das Rand-Gateway **218** die Initialisierungsnachricht unter Verwendung seines lokal gespeicherten anfänglichen Verknüpfungsschlüsselmaterials und speichert den neuen/aktualisierten Netzwerkschlüssel und den zufälligen Paketzähler, die darin enthalten sind, zur Verwendung bei der Verarbeitung zukünftiger Nachrichten, die von dem Feld-Gateway **212** empfangen werden. Zum Beispiel kann das Feld-Gateway **212** anschließende Nachrichten (Referenzen **292**, **295**) senden, die unter Verwendung des neuen/aktualisierten Netzwerkschlüsseln und des zufälligen Paketzählers verschlüsselt werden, und das Rand-Gateway **218** entschlüsselt die empfangenen Nachrichten unten Verwendung des gespeicherten neuen/aktualisierten Netzwerkschlüssels und des zufälligen Paketzählers (Referenzen **298**, **300**).

[0064] Das Feld-Gateway **212** wiederholt das Senden neuer oder aktualisierter Initialisierungsnachrichten (z. B. Referenzen **275**, **288** und so weiter) zum Etablieren eines aktualisierten oder neuen Netzwerkschlüssels und es entsprechenden zufälligen Paketzählers wiederkehrend, periodisch oder, wenn gewünscht, z. B. als eine Folge eines Benutzerbefehls oder des Eintretens eines anderen Ereignisses. Da Kommunikationen zwischen dem Feld-Gateway **212** und dem Rand-Gateway **218** über die Datendiode **215** unidirektional sind, weist das Feld-Gateway **212** keine explizite Bestätigung dafür auf, dass das Rand-Gateway **218** tatsächlich die durch das Feld-Gateway **212** übertragenen Daten empfängt. Dadurch, dass das Feld-Gateway **212** wiederkehrend eine neue/aktualisierte Initialisierungsnachricht sendet, die einen neuen/aktualisierten Netzwerkschlüssel und einen entsprechenden zufälligen Paketzähler enthält, ist das Netzwerkschlüsselmaterial, das zwischen dem Feld-Gateway **212** und dem Rand-Gateway **218** geteilt wird, in der Lage, neu synchronisiert zu werden. Diese Neusynchronisationstechnik ermöglicht dir Wiederherstellung während Fehler- oder Ausfallbedingungen, wie zum Beispiel dann, wenn das Rand-Gateway ausfällt, und ersetzt oder neu gestartet wird, und/oder wenn ein Paket fehlt. Die Länge des Zeitraums für die Neusynchronisation des Netzwerkschlüsselmaterials kann von der anwendungsabhängig sein, kann z. B. durch eine Toleranz einer Anwendung (z. B. von einer der Anwendungen oder Dienste **208**) für verlorene Pakete oder Daten geregelt werden, und er kann konfigurierbar sein.

[0065] Dementsprechend, wie vorstehend beschrieben, kann der anfänglich bereitgestellte Verknüpfungsschlüssel und der zufällige Paketzähler oder das Nonce-Material, die bei dem Rand-Gateway **218** (Referenz **268**) und bei dem Feld-Gateway **212** (Referenz **270**) gespeichert werden, zum Verschlüsseln/Entschlüsseln der anfänglichen Initialisierungsnachricht verwendet, die den anfänglichen zufälligen Netzwerkschlüssel und den zufälligen Paketstartzähler bereitstellt (Referenz **275**), und anschließende Kommunikationen nutzen den zufälligen Netzwerkschlüssel und Paketzähler, die in der Initialisierungsnachricht enthalten sind, zum Verschlüsseln/Entschlüsseln der darin übertragenen Daten. Das Feld-Gateway **212** erzeugt wiederkehrend, periodisch oder

wie gewünscht a neue oder aktualisierte Initialisierungsnachricht, die unter Verwendung des anfänglichen Verknüpfungsschlüsselmaterials verschlüsselt/entschlüsselt wird und die einen neuen/aktualisierten zufälligen Netzwerkschlüssel und einen zufälligen Paketstartzähler bereitstellt (Referenz **288**). Kommunikationen, die nach der neuen/aktualisierten Initialisierungsnachricht gesendet werden, unterliegen dem neuen/aktualisierten zufälligen Netzwerkschlüssel und dem Paketzähler, um die darin übertragenen Daten zu entschlüsseln/verschlüsseln. Somit kann das Rand-Gateway **218** gleichzeitig bereits verwendete Netzwerkschlüsselinformationen und neue Netzwerkschlüsselinformationen für einen begrenzten Zeitraum speichern, um in der Lage zu sein, Pakete zu verarbeiten, die beim Übergang zu den neuen Netzwerkschlüsselinformationen außerhalb der Reihenfolgen ankommen.

[0066] Wie in **Fig. 4** veranschaulicht, verwendet der Nachrichtenablauf **250** ein Bereitstellungsnetzwerk und eine Bereitstellungsvorrichtung **252** zum Durchführen des sicheren Bereitstellungsprozesses zwischen dem Feld-Gateway **212** und dem Rand-Gateway **218**. Diese ist jedoch nur eine von vielen möglichen Ausführungsformen.

[0067] Zum Beispiel befinden sich das Feld-Gateway **212** und das Rand-Gateway **218** in einer weiteren Ausführungsform nicht in einem Bereitstellungsnetzwerk und können sich sogar nicht im selben Netzwerk befinden. In dieser Ausführungsform authentifiziert sich ein Benutzer direkt gegenüber dem Rand-Gateway **218** und stellt Sicherheitsinformationen oder - daten bereit, welche das Feld-Gateway **212** beschrieben, bereit, um das Feld-Gateway **212** und das Rand-Gateway **218** sicher bereitzustellen. Zum Beispiel stellt der Benutzer die IP-Adresse des Feld-Gateways **212** für deren Eintrag in der weißen Liste am Rand-Gateway **218** bereit und der Benutzer stellt die Sicherheitsinformationen oder das anfängliche Schlüsselmaterial z. B. auf eine ähnliche Weise wie jene bereit, die vorstehend mit Referenz **265** in **Fig. 4** erörtert wurde. Die Sicherheitsinformationen werden verschlüsselt und bei dem Rand-Gateway **218** zur Verwendung bei Kommunikationen mit dem Feld-Gateway **212** gespeichert. Außerdem werden die verschlüsselten Sicherheitsinformationen in einer separaten Datei gespeichert, die ebenfalls entsprechend verschlüsselt werden kann. Die separate Datei wird z. B. durch den Benutzer zu dem Feld-Gateway **212** transportiert. Der Benutzer authentifiziert sich direkt gegenüber dem Feld-Gateway **212** und stellt die separate Datei zur Verwendung beim Feld-Gateway **212** bereit. Das Feld-Gateway **212** verifiziert die separate Datei (und entschlüsselt die Datei, sollte dies notwendig sein), erhält die darin gespeicherten Sicherheitsinformationen (z.B. das anfängliche Schlüsselmaterial), verschlüsselt die erhaltenen Sicherheitsinformationen und speichert die verschlüsselten Sicherheitsinformationen zur Verwendung in zukünftigen Kommunikationen mit dem Rand-Gateway **218** über die Datendiode **215**.

[0068] In einer weiteren Ausführungsform werden Daten anstelle von UDP unter Verwendung von seriellen Kommunikationen über die Datendiode **215** transportiert. In dieser Ausführungsform kann der gesicherte Bereitstellungsprozess jenem ähnlich sein, der vorstehend für das Bereitstellen des Feld-Gateways **212** und des Rand-Gateways **218** beschrieben wurden, während sich die Gateways **212**, **218** nicht in einem Bereitstellungsnetzwerk befinden oder sich in separaten Netzwerken befinden.

[0069] In einigen Umsetzungen, unter den gesicherten TCP-, UDP- und/oder seriellen Kommunikationen über die Datendiode **215**, kann das für das Übertragen von prozessanlagenerzeugten Daten über die Datendiode **215** verwendete Kommunikationsprotokoll ein modifiziertes HART-IP-Protokoll sein oder kann eine Modifikation eines beliebigen bekannten industriellen Kommunikationsprotokolls wie zum Beispiel Feldbus sein.

[0070] Um das HART-IP-Protokoll als ein veranschaulichendes, aber nicht einschränkendes Beispiel zu verwenden, kann das HART-IP-Protokoll genutzt werden, um ferner zusätzliche Sicherheit für Ende-zu-Ende-Kommunikationen von den Vorrichtungen **102**, die in der Prozessanlage **100** arbeiten, zu dem entfernten System **210** bereitzustellen. Insbesondere werden der in HART-IP enthaltene Veröffentlichungsmechanismus und HART auf eine einzigartige Weise genutzt, um die unidirektionalen Kommunikationen über die Datendiode **215** zu unterstützen, sodass Daten, die in der Prozessanlage **100** erzeugt werden, über Nachrichten oder Pakete, die zwischen dem Feld-Gateway **212** und dem Rand-Gateway **218** über die Datendiode **215** übertragen werden (z. B. durch die Referenzen **278**, **282**, **292**, **295** in **Fig. 4** angegeben), an die entfernten Anwendungen **208** abgegeben werden können.

[0071] Die modifizierten HART-IP-Protokollpakete können ein Token-Passing-Data-Link-Layer-Frame-Format aufweisen und/oder sie können ein Direct/Wireless-Packet-Format aufweisen. Zum Beispiel kann der HART-IP-Header so modifiziert sein, dass er Sicherheitsinformationen beinhaltet, wie zum Beispiel eine Angabe eines Sicherheitstyps (z. B. als ein Wert im Feld Nachrichtenart des Headers), die HART-IP-Sitzungsinitialisierungsnachricht kann so modifiziert sein, dass sie die anfänglichen Sicherheitsschlüsselmaterialinformationen beinhaltet, und/oder andere HAR-Nachrichtentypen (z. B. Anforderung, Antwort usw.) können so modifiziert sein, dass sie ein Netzwerksicherheitsschlüsselfeld und ein Netzwerksicherheitszählerfeld beinhalten.

[0072] Eine beispielhafte Verwendung des modifizierten HART-IP-Protokolls zum Sichern von Kommunikationen über die Datendiode **215** ist in **Fig. 5** gezeigt. **Fig. 5** stellt einen beispielhaften Nachrichtenablauf **400** dar, der zum Abgeben von Prozessanlagendaten, die durch eine oder mehrere Sendevorrichtungen **402** erzeugt wurden, über die Datendiode **215** an eine oder mehrere Empfangsvorrichtungen **405** verwendet werden kann. Allgemein ausgedrückt stellt eine Sendevorrichtung **402** zuerst einer Empfangsvorrichtung **405** Feststellungsinformationen bereit, um den Kontext für Inhalts- oder Nutzdaten einzustellen, die über die Datendiode **215** zu übertragen sind. Die Feststellungsinformationen ermöglichen es der Empfangsvorrichtung **405** zu wissen, welche Datenerzeugungskomponenten oder -vorrichtungen sich auf der Prozessanlagenseite der Datendiode **215** befinden, die Typen und/oder Identitäten der Daten zu wissen, die durch die Komponenten auf der Prozessanlagenseite erzeugt werden, die Geschwindigkeiten zu wissen, mit welchen erwartet wird, dass die erzeugten Daten bei der Empfangsvorrichtung **405** ankommen, die Zustände der verschiedenen Datenerzeugungskomponenten oder - Vorrichtungen zu wissen usw. Es ist wichtig, dass die Feststellungsdaten es der Empfangsvorrichtung **405** ermöglichen, dieses Wissen zu erhalten, ohne dass die Empfangsvorrichtung **405** Komponentenvorrichtungen auf der Prozessanlagenseite der Datendiode **215** befragen oder abfragen muss, wozu die Empfangsvorrichtung **405** aufgrund des unidirektionalen Wesens der Datendiode **215** nicht in der Lage ist.

[0073] Nach die Feststellungsinformation der Empfangsvorrichtung **405** durch die Sendevorrichtung **402** bereitgestellt worden sind, veröffentlicht die Sendevorrichtung **402** unter Verwendung des modifizierten HART-IP-Protokolls die Inhalts- oder Nutzdaten über die Datendiode **215** gemäß dem in den Feststellungsinformationen bereitgestellten Kontext in Echtzeit, z. B. wenn die Sendevorrichtung **402** die Quellendaten erzeugt und/oder wenn die Sendevorrichtung **402** Quellendaten von einer oder mehreren anderen Komponenten innerhalb der Prozessanlage **100** empfängt. Daher kann die Empfangsvorrichtung **405** ein Abonnent der Daten sein, die durch die Sendevorrichtung **402** veröffentlicht werden.

[0074] Außerdem, ebenfalls aufgrund des unidirektionalen Wesens der Datendiode **215**, ist die Sendevorrichtung **402** nicht in der Lage, den Zustand der Empfangsvorrichtung **405** zu erkennen (z. B. ob die Empfangsvorrichtung **405** betriebsfähig, aus- und wieder eingeschaltet wird, getrennt ist usw. oder nicht), und ist nicht in der Lage, explizit zu bestimmen, ob die Empfangsvorrichtung **405** die gesendeten Daten empfangen hat oder nicht. Dementsprechend stellt die Sendevorrichtung **402** wiederkehrend (z. B. periodisch und/oder wie gewünscht) Feststellungsinformationen an die Empfangsvorrichtung **405** bereit, sendet oder kündigt diese an, sodass, wenn die Empfangsvorrichtung **405** nicht erreichbar ist, die Empfangsvorrichtung **405** bei der Wiederherstellung in der Lage ist, den Kontext der Inhalts- oder Nutzdaten, die durch die Sendevorrichtung **402** gesendet wurden, schnell (erneut) zu verstehen. Die Länge des Zeitraums zwischen dem Senden der Feststellungsinformationen kann von der Toleranz einer Client-Anwendung (z. B. eine/r der entfernten Anwendungen oder Dienste **208**) auf der Empfangsvorrichtungsseite der Datendiode **215** für verlorene Pakete oder Daten abhängig sein und kann konfigurierbar sein. Die Feststellungsinformationen können ebenfalls gesendet werden, wenn eine Veränderung auf der Seite der Sendevorrichtung **402** stattfindet, wie zum Beispiel wenn die Datenquellen **202** und/oder die drahtlosen Gateways **205** zu der Prozessanlage **100** hinzugefügt oder daraus entfernt werden.

[0075] Die Sendevorrichtung **402** kann ein Feld-Gateway **212**, ein drahtloses Gateway **205**, eine Datenquellenvorrichtung **202** und/oder eine beliebige andere Komponente sein, die Daten bereitstellt, die durch eine oder mehrere Komponenten oder Vorrichtungen erzeugt wurden, die innerhalb der Prozessanlage **100** arbeiten. Die Empfangsvorrichtung **405** kann ein Rand-Gateway **218**, eine oder mehrere der Vorrichtungen, die das entfernte System **210** umfassen, und/oder eine Client-Anwendung sein, die ein Konsument von Quellendaten ist (z. B. eine/r der entfernten Anwendungen oder Dienste **208**). In **Fig. 5** wird der Nachrichtenablauf **400** jedoch zur einfachen Erörterung so erörtert, als wäre die Sendevorrichtung **402** das Feld-Gateway **212** aus **Fig. 3** und die Empfangsvorrichtung **405** das Rand-Gateway **218** aus **Fig. 3**, obwohl es sich versteht, dass diese nur eine von zahlreichen möglichen Ausführungsformen ist.

[0076] Während der Kontexteinstellungsphase **408** überträgt die Sendevorrichtung **402** entsprechende Informationen, die jede Datenquelle der Prozessanlage **100** beschreiben, deren Daten über die Datendiode **215** zu übertragen sind. Die deskriptiven Datenquelleninformationen beinhalten zum Beispiel eine Identität der Datenquelle (z. B. eine einzigartige Kennung, eine Vorrichtungsmarkierung usw.); eine Identität der Daten (die zum Beispiel Zuordnungsinformationen zu einer oder mehreren ihrer dynamischen Variablen beinhalten können, wie zum Beispiel primäre Variable (PV), sekundäre Variable (SV), tertiäre Variable (TV), quaternäre Variable (QV) usw.); eine Angabe der Geschwindigkeit, mit welcher erwartet wird, dass die identifizierten Daten ankommen (z. B. Burst-Konfigurationsinformationen); und/oder andere Informationen, welche die Daten und/oder Datenquellen beschrieben, wie zum Beispiel Daten, die das bestimmte Gateway angeben, mit welcher die Datenquelle kommunikativ verbunden ist, der Zustand der Datenquellen, der Zustand ihres Gateways usw.

Wie in **Fig. 5** veranschaulicht, iteriert die Sendevorrichtung **402** in einer Ausführungsform auf einer Basis pro drahtlosem Gateway **205** und pro Datenquellenvorrichtung **202** während der Kontexteinstellphase **408**. Zum Beispiel sendet die Sendevorrichtung **402** deskriptive Informationen für das drahtlose Gateway **0** (Referenz **410**), bei welchem es sich zum Beispiel um eines der drahtlosen Gateways **205A**, **205B** handeln kann. Die Sendevorrichtung **402** kann deskriptive Informationen des drahtlosen Gateways **0** zum Beispiel unter Verwendung eines modifizierten HART-IP-Befehls **0**, **20** oder **74** senden. Anschließend sendet die Sendevorrichtung **402** entsprechende deskriptive Informationen für jede der N Vorrichtungen, die kommunikativ mit Gateway **0** verbunden ist (Referenz **412**), zum Beispiel unter Verwendung des/der modifizierten HART-IP-Befehls/Befehle 0, 20, 50, 105(n) und optional der Befehle **74** und **101** für Teilvorrichtungs-Burst-Zuordnung. Diese Sequenz wird für jedes der M Gateways wiederholt und die Kontexteinstellungsphase **408** endet, nachdem die deskriptiven Informationen für Gateway M und dessen entsprechende N Vorrichtungen an die Empfangsvorrichtung **405** gesendet worden sind (Referenz **415**, **418**).

[0077] Während der Veröffentlichungsphase **420** veröffentlicht die Sendevorrichtung **402** Quellendaten über die Datendiode **215** für beliebige der Datenquellenvorrichtungen **202** deren Kontext während der Kontexteinstellungsphase **408** eingestellt wurde. In einem Beispiel veröffentlicht die Sendevorrichtung **402** die Quellendaten über die Datendiode **215** unter Verwendung des modifizierten HART-IP-Befehls **48** oder eines anderen geeigneten Hart-IP-Befehls. Besondere Quellendaten werden mit der Geschwindigkeit veröffentlicht, mit der die Quellendaten bei der Sendevorrichtung **402** empfangen werden, z. B. von der Vorrichtung **202** über deren entsprechendes drahtloses Gateway **205**. Das heißt, dass während angeschlossener Vorgänge der Prozessanlage **100** Quellendaten, die durch die Prozessanlage **100** erzeugt wurden, über die Datendiode **215** in Echtzeit veröffentlicht werden, wenn die durch die Sendevorrichtung **402** empfangen werden. Es ist anzumerken, dass einige Datenerzeugungskomponenten der Prozessanlage **100** (z. B. einige der Datenquellenvorrichtungen **202** und/oder einige der drahtlosen Gateways **205**) Daten direkt gegenüber des Feld-Gateways **212** zur Abgabe über die Datendiode **215** veröffentlichen können. Andere Datenerzeugungskomponenten der Prozessanlage **100** (z. B. andere der Datenquellenvorrichtungen **202** und/oder der drahtlosen Gateways **205**) können die Veröffentlichung nicht unterstützen und das Feld-Gateway **212** kann diese Typen von Vorrichtungen/Gateways befragen, um deren entsprechende Quellendaten zu empfangen. Zum Beispiel kann das Feld-Gateway **212** auf der Grundlage einer Burst-Konfiguration der Vorrichtung/des Gateways befragen, die das Veröffentlichen nicht unterstützt, z. B. unter Verwendung der HART-IP-Befehle **3** oder **9**.

[0078] Wie bereits erörtert, werden nach dem Verstreichen eines vordefinierten Zeitraums, oder wie gewünscht, mindestens einige der Kontextinformationen **410**-**418** durch die Sendevorrichtung **402** erneut an die Empfangsvorrichtung **405** gesendet oder aktualisiert. In einer Ausführungsform wird die Gesamtheit der Kontextdaten **410**-**418** der Gateways **0-M** und der entsprechenden Vorrichtungen **1-N** erneut gesendet oder aktualisiert. In einer weiteren Ausführungsform werden bestimmte Kontextdaten für bestimmte Vorrichtungen bei verschiedenen unterschiedlichen Zeitpunkten erneut gesendet oder aktualisiert, wie es für einen bestimmten Konsumenten der Daten erforderlich ist, z. B. auf der Grundlage einer Toleranz des bestimmten Konsumenten für verlorene Daten oder Pakete. In diesen Ausführungsformen können unterschiedliche Vorrichtungen unterschiedliche Periodizitäten oder Intervalle aufweisen, bei welchen deren entsprechende Kontextdaten erneut gesendet oder aktualisiert werden.

[0079] Außerdem ist anzumerken, dass der vorstehende Nachrichtenstrom **400** in einer Ausführungsform beschrieben ist, in welcher die Datendiode **215** eine Ethernet-verbundene Datendiode ist. Ist dies gewünscht, können ähnliche Techniken jedoch leicht auf eine seriell verbundene Datendiode angewendet werden. Ferner, obwohl der vorstehende Nachrichtenablauf **400** unter Verwendung des HART-IP-Protokolls beschrieben wurde, können andere Kommunikationsprotokolle während der Kontextphase **408** und der Datenabgabephase **420** des Nachrichtenablaufs **400** verwendet werden. In einigen beispielhaften Konfigurationen können andere industrielle Kommunikationsprotokolle eingesetzt werden (z. B. Profibus, DeviceNet, Foundation Fieldbus, ControlNet, Modbus, HART usw.). In anderen beispielhaften Konfigurationen können andere Protokolle, die nicht spezifisch für industrielle Kommunikationen gestaltet wurden, während der Kontextphase **408** und der Datenabgabephase **420** des Nachrichtenablaufs **400** eingesetzt werden.

[0080] Zum Beispiel können in einer Ausführungsform Pakete unter Verwendung eines JSON(JavaScript Object Notation)-Formats anstelle der Verwendung von HART-IP über die Datendiode **215** übertragen werden. In dieser Ausführungsform wandelt das Feld-Gateway **212** Daten, die von verschiedenen Vorrichtungen und Komponenten innerhalb der Prozessanlage **100** empfangen wurden, in ein JSON-Format zur Abgabe über die Datendiode **215** um. Wenn gewünscht, können Erweiterungen der JSON-Paketdaten hinzugefügt werden, wie zum Beispiel Bereitstellen von Markierungen mit einer zusätzlichen Bedeutung (z. B. „DRUCK“ anstelle von „PV“,

vorrichtungsspezifische Markierungen für verschiedene Datenwerte und dergleichen).

[0081] Ferner, obwohl die vorstehende Erörterung von **Fig. 5** den stattfindenden Nachrichtenablauf **400** so beschreibt, als wäre das Sende-Gateway **402** das Feld-Gateway **212** und die Empfangsvorrichtung **405** das Rand-Gateway **218**, ist diese nur eine von vielen Ausführungsformen. Zum Beispiel kann die Sendevorrichtung **402** in anderen Ausführungsformen des Nachrichtenablaufs **400** ein Feld-Gateway **212**, ein drahtloses Gateway **205**, eine Datenquellevorrichtung **202** und/oder eine beliebige andere Komponente sein, die Daten bereitstellt, die durch eine oder mehrere Komponenten oder Vorrichtungen erzeugt wurden, die innerhalb der Prozessanlage **100** arbeiten, und die Empfangsvorrichtung **405** kann ein Rand-Gateway **218**, eine oder mehrere der Vorrichtungen, die das entfernte System **210** umfassen, und/oder eine Client-Anwendung sein, die ein Konsument von Quellendaten ist (z. B. eine/r der entfernten Anwendungen oder Dienste **208**). Zum Beispiel kann eine erste der Client-Anwendungen **208** Daten abonnieren, die durch eine bestimmte Vorrichtung **202** erzeugt wurden und die über die Datendiode **215** veröffentlicht werden, und eine zweite der Client-Anwendungen **28** kann Daten abonnieren, die durch eine andere bestimmte Vorrichtung **202** erzeugt wurden. In diesem Beispiel kann das Rand-Gateway **218** als ein Router zum Verteilen empfangener Daten an entsprechende Datenabonnenten dienen. In einem anderen Beispiel veröffentlicht das Rand-Gateway **218** alle Daten, dies es empfängt, über die Datendiode **215** und verschiedene Anwendungen **208** abonnieren spezifische Daten, die durch das Rand-Gateway **218** veröffentlicht werden. Andere Veröffentlicher/Abonnent-Beziehungen sind möglich und können durch eine beliebige oder mehrere der hier beschriebenen gesicherten Kommunikationstechniken unterstützt werden.

[0082] Darüber hinaus kann/können eine beliebige oder mehrere der gesicherten Kommunikationstechniken leicht auf das Sichern von Daten angewendet werden, die an Systeme und/oder Vorrichtungen gesendet werden, die lokal gegenüber der Prozessanlage **100** sind. Zum Beispiel kann eine entsprechende Datendiode **215** und/oder Instanz der Sicherheitsarchitektur **200** zum Veröffentlichen ausgewählter (oder sogar aller) Daten über die DMZ **22** der Prozessanlage **100** verwendet werden, sodass die Daten, die auf den Sicherheitsstufen **0**-**3** der Prozessanlage **100** erzeugt wurden, sicher über die DMZ **22** an Unternehmenssysteme auf den Stufen **4**-**5** über eine entsprechende Datendiode abgegeben werden. In einem anderen Beispiel kann eine entsprechende Datendiode **215** und/oder Instanz der Sicherheitsarchitektur **200** zum Veröffentlichen ausgewählter (oder sogar aller) Daten von einer oder mehreren Datenquellen **202**, die in der Prozessanlage **100** angeordnet sind, gegenüber einem oder mehreren lokalen Servern verwendet werden, die ebenfalls in oder lokal gegenüber der Prozessanlage **100** angeordnet sind und die lokale Dienste und Anwendungen hosten oder bereitstellen. Eine derartige Konfiguration ist vorteilhaft, wenn zum Beispiel lokale Dienste und Anwendungen lokale präskriptive Veränderungen erzeugen, die herunterzuladen sind oder anderweitig in die angeschlossene Prozessanlage **100** zu implementieren sind, obwohl im Allgemeinen präskriptive Funktionen, Modifikationen an den Konfigurationen und/oder anderen Daten und/oder andere Veränderungen durch entfernt angeordnete Anwendungen und Dienste **208** in der Prozessanlage **100** umgesetzt werden können.

[0083] Es ist jedoch anzumerken, dass beliebige präskriptive Änderungen, die durch die Anwendungen/Dienste **208** bestimmt werden, typischerweise über einen anderen Kommunikationsmechanismus als die Datendiode **215** in der Prozessanlage **100** umgesetzt werden, da die Datendiode **215** in der Ausgangsrichtung in Bezug auf die Prozessanlage **100** unidirektional ist. Um zum Beispiel eine präskriptive Veränderung an der Prozessanlage **100** umzusetzen, kann eine/ein entfernte/r Anwendung/Dienst **208** eine andere sichere Kommunikationsverbindung als über die Datendiode **215** mit einer oder mehreren administrativen oder Backend-Komponenten der Prozessanlage **100** herstellen, wie zum Beispiel die Arbeitsstation mit Bedienpersonal **171**, die Konfigurationsanwendungen **172A**, die Konfigurationsdatenbank **173B** usw., und die präskriptive Veränderung kann heruntergeladen werden oder anderweitig an die Prozessanlage **100** abgegeben werden. Tatsächlich kann in einer Ausführungsform eine andere Instanz der Datendiode **215** und/oder der Sicherheitsarchitektur **200** in der Eingangsrichtung etabliert werden, um beliebige präskriptive Veränderungen von der/dem entfernten Anwendung/Dienst **208** an die Prozessanlage **100** abzugeben.

[0084] Allgemein ausgedrückt verwenden beliebige Eingangskommunikationen von dem entfernten System **210** an die Prozessanlage **210** typischerweise ferner einen anderen Kommunikationsmechanismus als die Ausgangsdatendiode **215** und/oder die Ausgangssicherheitsarchitektur **200**. Zum Beispiel kann das entfernte System **210** eine andere Instanz der Datendiode **215** und/oder der Sicherheitsarchitektur **200** verwenden, die in der Eingangsrichtung angewendet ist, oder einen anderen geeigneten gesicherten Verbindungs- oder Kommunikationspfad.

[0085] Unter erneuter Bezugnahme auf die gesicherten Ausgangskommunikationen von der Prozessanlage **100** stellt **Fig. 6** ein Ablaufdiagramm eines beispielhaften Verfahrens **450** zum sicheren Transportieren von Kommunikationen von einer Prozessanlage, wie zum Beispiel der Prozessanlage **100**

aus **Fig. 2**, dar. In einigen Ausführungsformen wird zumindest ein Teil des Verfahrens **450** durch das Ausführen eines Satzes von computerausführbaren oder computerlesbaren Anweisungen umgesetzt, die zum Beispiel auf einem oder mehreren nichttransitorischen computerlesbaren Speichern gespeichert sind und durch einen oder mehrere Prozessoren z. B. des Systems **200** ausgeführt werden. Zum Beispiel kann mindestens ein Teil des Verfahrens **450** durch eine oder mehrere Komponenten des in den **Fig. 1**-**Fig. 5** dargestellten Systems **200** durchgeführt werden, wie zum Beispiel das Feld-Gateway **212** oder die Sendevorrichtung **402**. Dementsprechend wird das Verfahren **450** nachstehend mit gleichzeitiger Bezugnahme auf die **Fig. 1**-**Fig. 5** beschrieben, dies dient jedoch nur der einfachen Erläuterung und nicht zum Zwecke der Einschränkung.

[0086] Bei Block **452** beinhaltet das Verfahren **450** das Bereitstellen einer Sendevorrichtung einer Prozessanlage mit einer Empfangsvorrichtung. Zum Beispiel ist die Sendevorrichtung kommunikativ mit der Prozessanlage verbunden (z. B. über ein oder mehrere geeignete Netzwerke) und die Empfangsvorrichtung ist kommunikativ mit einem anderen System verbunden (z. B. über ein oder mehrere geeignete Netzwerke). Das andere System hostet eine/n oder mehrere Anwendungen oder Dienste, die konfiguriert sind, um mit Daten, die durch die Prozessanlage während ihrer Laufzeitvorgänge erzeugt wurden, und optional mit anderen Daten, die durch die Prozessanlage erzeugt wurden, zu arbeiten. Die Sendevorrichtung kann zum Beispiel die Sendevorrichtung **402** sein und die Empfangsvorrichtung kann zum Beispiel die Empfangsvorrichtung **405** sein, wie in **Fig. 5** veranschaulicht. Daher kann die Sendevorrichtung **402** das Feld-Gateway **212**, eine Datenquellenvorrichtung **202**, ein drahtloses Gateway **205** oder eine andere Komponente der Prozessanlage **100** sein und die Empfangsvorrichtung kann das Rand-Gateway **218**, eine in dem entfernten System **210** enthaltene Rechenvorrichtung oder eine Anwendung oder ein Dienst **208** sein, die/der in dem entfernten System **210** ausgeführt wird. Selbstverständlich sind andere Ausführungsformen der Sendevorrichtung und/oder der Empfangsvorrichtung möglich, wie zum Beispiel beliebige der bereits vorstehend erörterten.

[0087] Die Sendevorrichtung und die Empfangsvorrichtung sind über eine Datendiode, wie zum Beispiel die Datendiode **215** aus **Fig. 3**, miteinander verbunden. Die Datendiode ist konfiguriert, um unidirektionale Kommunikationen zu ermöglichen, die von der Sendevorrichtung an die Empfangsvorrichtung zu übertragen sind, und um beliebige Kommunikationen zu verhindern, die von der Empfangsvorrichtung an die Sendevorrichtung übertragen werden (abgesehen von anfänglichen Bereitstellungsnachrichten in einer Ausführungsform).

[0088] Das Bereitstellen der Sendevorrichtung gegenüber der Empfangsvorrichtung (Block **452**) wird unter Verwendung eines ersten Schlüssels durchgeführt, der ebenfalls ein Verknüpfungsschlüssel bezeichnet wird. Der Verknüpfungsschlüssel kann ein geheimer Schlüssel oder ein geteiltes Geheimnis sein und kann durch einen Benutzer z. B. über eine Bereitstellungsvorrichtung bereitgestellt werden, die kommunikativ mit der Sendevorrichtung und/oder der Empfangsvorrichtung verbunden ist, oder über eine manuelle Datenübertragung. In einigen Anordnungen wird ein erster Paketzähler (ebenfalls bezeichnet als ein Verknüpfungspaketzähler) oder ein anderen entsprechendes Nonce-Material in Verbindung mit dem Verknüpfungsschlüssel bereitgestellt. Der Verknüpfungsschlüssel und/oder der Verknüpfungspaketzähler können zufällig erzeugt werden, wenn dies gewünscht ist.

[0089] In einigen Ausführungsformen beinhaltet das Bereitstellen der Sendevorrichtung, der Empfangsvorrichtung (Block **452**) das Etablieren eines vorübergehenden Kommunikationskanals, um Kommunikationen von der Empfangsvorrichtung an die Sendevorrichtung zum Übertragen und/oder Verifizieren des Verknüpfungsschlüssels zu ermöglichen. Der vorübergehende Kommunikationskanal kann über die Datendiode etabliert werden oder er kann über eine andere kommunikative Verbindung etabliert werden, wie zum Beispiel eine externe drahtgebundene oder drahtlose Verbindung, eine manuelle Übertragung über eine tragbare Speichervorrichtung oder dergleichen. In diesen Ausführungsformen kann der vorübergehende Kommunikationskanal bei der Übertragung des Verknüpfungsschlüssels durch die Empfangsvorrichtung und/oder dem Empfang des Verknüpfungsschlüssels bei der Sendevorrichtung abgeschafft, abgebrochen oder anderweitig deaktiviert werden. Allgemein ausgedrückt, dient der vorübergehende Kommunikationskanal nur zum Teilen des ersten oder Verknüpfungsschlüssels zwischen der Sende- und der Empfangsvorrichtung. Nachdem das anfängliche Schlüsselmaterial (z. B. der Verknüpfungsschlüssel und dessen entsprechender Paketzähler oder ein anderes Nonce-Material) geteilt wurde, wird das anfängliche Schlüsselmaterial lokal verschlüsselt und entsprechend bei sowohl der Sendevorrichtung als auch der Empfangsvorrichtung gespeichert.

[0090] Das Verfahren **450** beinhaltet das Verschlüsseln z. B. durch die Sendevorrichtung einer Initialisierungsnachricht unter Verwendung des ersten oder Verknüpfungsschlüssels (Block **455**) und das Bereitstellen der verschlüsselten Initialisierungsnachricht über die Datendiode an die Empfangsvorrichtung (Block **458**). Die Initialisierungsnachricht beinhaltet darin einen zweiten Schlüssel, hier ebenfalls bezeichnet als ein Netzwerkschlüssel, der durch die Sende- und Empfangsvorrichtung zum Verarbeiten anschließender Nachrichten oder Pakete zu verwenden

ist, die über die Datendiode von der Sendevorrichtung an die Empfangsvorrichtung übertragen werden. Der zweite Schlüssel kann zum Beispiel ein anderer geheimer Schlüssel oder ein geteiltes Geheimnis sein. Mindestens einige der anschließenden Nachrichten oder Pakete, die unter Verwendung des zweiten oder Netzwerkschlüssels verarbeitet werden, beinhalten Inhalt oder Nutzdaten, der/die Daten umfassen, die durch die Prozessanlage erzeugt wurden, während sie in Echtzeit arbeitet, um einen Prozess zu steuern, wie zum Beispiel erzeugte Prozessdaten, Diagnosedaten oder andere Datentypen. In einigen Anordnungen wird ein zweiter Paketzähler (hier ebenfalls als ein Netzwerkpaketzähler bezeichnet) oder ein anderes entsprechendes Nonce-Material verschlüsselt und in Verbindung mit dem Netzwerkschlüssel bereitgestellt, um bei der Verarbeitung anschließender Nachrichten/Pakete verwendet zu werden. Der Netzwerkschlüssel und/oder der Netzwerkpaketzähler können zufällig erzeugt werden, wenn dies gewünscht ist.

[0091] Dementsprechend beinhaltet das Verfahren **450** ferner das Empfangen, bei der Sendevorrichtung, von Daten, die durch die Prozessanlage erzeugt wurden, während sie in Echtzeit arbeitet, um den Prozess zu steuern (Block **460**); das Verschlüsseln, durch die Sendevorrichtung und unter Verwendung des Netzwerkschlüssels und optional des Netzwerkpaketzählers, anschließender Nachrichten/Pakete, welche die durch die Prozessanlage erzeugten Daten als Nutzdaten beinhalten (Block **462**); und das Bereitstellen der verschlüsselten anschließenden Nachrichten/Pakete über die Datendiode an die Empfangsvorrichtung (Block **465**). Bei den Blöcken **462**, **465** werden daher die anschließenden Nachrichten/Pakete, von welchen mindestens einige Daten beinhalten, die durch die Prozessanlage erzeugt werden, für den Transport über die Datendiode unter Verwendung des geteilten geheimen Netzwerkschlüssels gesichert. In einigen Ausführungsformen werden die anschließenden Nachrichten/Pakete ferner für den Transport über die Datendiode durch zusätzliche Verschlüsselung gesichert, falls dies gewünscht ist (nicht gezeigt).

[0092] Das Empfangen der Daten, die durch die Prozessanlage während Echtzeit- oder angeschlossenen Vorgängen zum Steuern des Prozesses erzeugt wurden (Block **460**), kann das Empfangen von Daten direkt von der Datenerzeugungsquelle (z. B. eine Vorrichtung oder Komponente **202**) beinhalten und/oder kann das Empfangen, von einem Gateway (z. B. ein drahtloses Gateway **205**) von Daten beinhalten, die von einer Datenerzeugungsquelle (z. B. eine Vorrichtung oder Komponente **202**) an das Gateway übertragen wurden. Die von der Prozessanlage erzeugten Daten, die bei der Sendevorrichtung empfangen werden, können verschlüsselt, umhüllt und/oder anderweitig durch die Datenerzeugungsquelle (z. B. die Vorrichtung oder Komponente **202**) und/oder durch das Gateway (z. B. das drahtlose Gateway **205**) gesichert worden sein, zum Beispiel auf eine Weise wie bereits beschrieben.

[0093] Die von der Prozessanlage erzeugten, empfangenen Daten (Block **460**) können veröffentlichte Daten beinhalten, da einige Datenerzeugungsquellenvorrichtungen ihre entsprechenden erzeugten Daten z. B. gegenüber dem drahtlosen Gateway **205** und/oder gegenüber der Sendevorrichtung **402** veröffentlichen können. Andere Datenerzeugungsquellenvorrichtungen können abgefragt werden (z. B. durch das drahtlose Gateway **205** und/oder durch die Sendevorrichtung **402**), sodass deren entsprechenden erzeugten Daten bei der Sendevorrichtung empfangen werden können (Block **460**). Ferner können die von der Prozessanlage erzeugten Daten, egal ob veröffentlicht, abgefragt oder anderweitig empfangen (Block **460**), in einem HART-kompatiblen Format, in einem JSON-kompatiblen Format oder einem anderen geeigneten Format in Übereinstimmung mit einem beliebigen geeigneten industriellen Kommunikationsprotokoll oder Universal-Kommunikationsprotokoll vorhanden sein.

[0094] Wie bereits erörtert, beinhaltet das Verschlüsseln von Nachrichten/Pakten, die von der Prozessanlage erzeugte Daten als Nutzdaten beinhalten (Block **462**), das Verschlüsseln der Nachrichten/Pakete unter Verwendung des Netzwerkschlüssels und optional des Netzwerkpaketzählers, z. B. als Nonce-Material, und der Transport der Nachrichten/Pakete über die Datendiode wird durch die unidirektionale Kommunikationskonfiguration der Datendiode weiter gesichert.

[0095] Außerdem kann das Bereitstellen oder Senden der verschlüsselten anschließenden Nachrichten über die Datendiode an die Empfangsvorrichtung (Block **465**) zum Beispiel das wiederkehrende Ankündigen oder Senden entsprechender Kontextinformationen, die jede der einen oder der mehreren Datenerzeugungsvorrichtungen der Prozessanlage beschrieben, über die Datendiode an die Empfangsvorrichtung beinhalten. Die entsprechenden Kontextinformationen können eine Kennung der vorliegenden Datenerzeugungsvorrichtung, eine entsprechende Geschwindigkeit, bei welcher Daten, die durch die vorliegende Vorrichtung erzeugt wurden, zu übertragen oder zu veröffentlichen sind, eine Angabe eines aktuellen Zustands der vorliegenden Datenerzeugungsvorrichtung und/oder andere Informationen beinhalten, welche die vorliegende Datenerzeugungsvorrichtung beschreiben, wie zum Beispiel vorstehend in Bezug auf **Fig. 5** erörtert.

[0096] Das wiederkehrende Ankündigen von Kontextinformationen kann in einem Beispiel das periodische Senden von Kontextinformationen über die

Datendiode an die Empfangsvorrichtung beinhalten. Die Dauer der Periodizität kann sich für unterschiedliche Typen von Inhaltsdaten, für unterschiedliche Datenerzeugungsquellen der Prozessanlage und/oder für unterschiedliche Konsumenten der Inhaltsdaten (z. B. eine entfernte Anwendung **208**) unterscheiden. Zum Beispiel kann eine Dauer der Periodizität für bestimmten Typen von Inhaltsdaten auf einer Toleranz eines Konsumenten der Daten für verlorene Pakete und/oder Verzögerung beruhen. Selbstverständlich können die Kontextinformationen gegenüber der Empfangsvorrichtung über die Datendiode bei oder nach Bedarf angekündigt werden, wie zum Beispiel nachdem die Sendevorrichtung neu gestartet wurde, wenn eine neue Datenerzeugungsvorrichtung zu der Prozessanlage hinzugefügt wird, wenn es ein Benutzer angibt usw.

[0097] Ferner kann das Ankündigen von Kontextinformationen in einer Ausführungsform das Verwenden eines oder mehrerer Nachrichtentypen eines industriellen Kommunikationsprotokolls beinhalten. Wenn zum Beispiel ein Typ des HART-Kommunikationsprotokolls über die Datendiode verwendet wird, kann das Ankündigen der Kontextinformationen das Verwenden der HART-Befehle **0**, **20**, **50**, **74**, **105** und optional der Befehle **74** und **101** beinhalten. In einer weiteren Ausführungsform kann das Ankündigen der Kontextinformationen unter Verwendung eines Universal-Kommunikationsprotokolls umgesetzt werden, wie zum Beispiel JSON oder ein anderes geeignetes Universal-Kommunikationsprotokoll. Verschiedene Nachrichtentypen verschiedener industrieller Kommunikationsprotokolle können in einem Beispiel modifiziert werden, um die Ankündigungen zu beherbergen.

[0098] Das Bereitstellen der verschlüsselten anschließenden Nachrichten über die Datendiode an die Empfangsvorrichtung (Block **465**) beinhaltet ebenfalls das Übertragen oder Transportieren von Inhaltsdaten über die Datendiode in Übereinstimmung mit zuvor gesendeten Kontextinformationen. Wie bereits erörtert, beinhalten die Inhaltsdaten dynamische Daten, die durch die Prozessanlage erzeugt wurden, während sie angeschlossen arbeitet, um den Prozess zusteuern, wie zum Beispiel Prozessdaten, Diagnosedaten und dergleichen. In einer Ausführungsform beinhaltet das Bereitstellen der verschlüsselten anschließenden Nachrichten über die Datendiode das Veröffentlichen der Inhaltsdaten über die Datendiode, z. B. auf eine wie vorstehend beschriebene Weise.

[0099] Das Verfahren **450** beinhaltet ferner das Verschlüsseln einer zweiten (z. B. einer anschließenden) Initialisierungsnachricht unter Verwendung des ersten oder Verknüpfungsschlüssels (Block **468**) und das Bereitstellen der verschlüsselten, zweiten Initialisierungsnachricht über die Datendiode an die Empfangsvorrichtung (Block **470**). Die zweite Initialisierungsnachricht beinhaltet einen aktualisierten oder neuen Netzwerkschlüssel, der durch die Sende- und Empfangsvorrichtung zum Verarbeiten anschließender Nachrichten oder Pakete zu verwenden ist, die über die Datendiode von der Sendevorrichtung an die Empfangsvorrichtung übertragen werden. Der aktualisierte oder neue Netzwerkschlüssel kann ein anderer geteilter Schlüssel oder ein geteiltes Geheimnis sein, der/das sich von dem in Bezug auf Block **452** erörterten Verknüpfungsschlüssel unterscheidet und sich von dem in Bezug auf die Blöcke **455**, **458** erörterten Netzwerkschlüssel unterscheidet. Ein aktualisierter Netzwerkpaketzähler, der ebenfalls zur Verwendung beim Verarbeiten anschließender Nachrichten/Pakete dient, kann erzeugt werden und in Verbindung mit dem aktualisierten oder neuen Netzwerkschlüssel über die Datendiode transportiert werden. Der neue oder aktualisierte Netzwerkschlüssel und/oder -paketzähler können zufällig erzeugt werden, falls dies gewünscht ist.

[0100] Dementsprechend wird der Netzwerkschlüssel, der durch die Sendevorrichtung und die Empfangsvorrichtung zum Verarbeiten von Nachrichten/Paketen verwendet wird, bei den Blöcken **468**, **470** neusynchronisiert. Diese Neusynchronisation ist mindestens wichtig, da die Datendiode unidirektional ist, und somit ist die Empfangsvorrichtung nicht in der Lage, beliebige Rückkopplung über ihren Betriebszustand, erfolgreichen oder nicht erfolgreichen Empfang von Nachrichten usw. gegenüber der Sendevorrichtung bereitzustellen. Über die Blöcke **468**, **470** ist das Verfahren **450** in der Lage, kommunikative Unterbrechungen zwischen der Sendevorrichtung und der Empfangsvorrichtung durch das Neusynchronisieren des Netzwerkschlüsselmaterials anzugehen. Tatsächlich werden die Blöcke **468**, **470** in einigen Ausführungsformen wiederkehrend, periodisch und/oder auf der Grundlage des Stattfindens bestimmter Ereignisse (z. B. ein Neustart der Sendevorrichtung, wenn ein Benutzer dies angibt, wenn gewünscht usw.) wiederholt. Die Dauer der Periodizität kann zum Beispiel auf einer Toleranz einer oder mehrerer Konsumenten der Inhaltsdaten für verlorene Pakete und/oder Verzögerungen beruhen.

[0101] Es ist anzumerken, dass die Empfangsvorrichtung in Bezug auf die Blöcke **468**, **470** sowohl den ersten Netzwerkschlüssel/-paketzähler als auch den zweiten Netzwerkschlüssel/-paketzähler für einen begrenzten Zeitraum behalten muss, zum Beispiel zum Verarbeiten von Paketen, die über die Datendiode in einer anderen Reihenfolge ankommen, als sie gesendet wurden.

[0102] **Fig. 7** stellt ein Ablaufdiagramm eines beispielhaften Verfahrens **500** zum sicheren Transportieren von Kommunikationen von einer Prozessanlage, wie zum Beispiel der Prozessanlage **100** aus

Fig. 2, dar. In einigen Ausführungsformen wird zumindest ein Teil des Verfahrens **500** durch das Ausführen eines Satzes von computerausführbaren oder computerlesbaren Anweisungen umgesetzt, die zum Beispiel auf einem oder mehreren nichttransitorischen computerlesbaren Speichern gespeichert sind und durch einen oder mehrere Prozessoren z. B. des Systems **200** ausgeführt werden. Zum Beispiel kann mindestens ein Teil des Verfahrens **500** durch eine oder mehrere Komponenten des in den **Fig. 1**-**Fig. 5** dargestellten Systems **200** durchgeführt werden, wie zum Beispiel das Rand-Gateway **218** oder die Empfangsvorrichtung **405**. Dementsprechend wird das Verfahren **500** nachstehend mit gleichzeitiger Bezugnahme auf die **Fig. 1**-**Fig. 5** beschrieben, dies dient jedoch nur der einfachen Erläuterung und nicht zum Zwecke der Einschränkung.

[0103] Bei Block **502** beinhaltet das Verfahren **500** das Empfangen, über die Datendiode, von Daten, die durch die Prozessanlage erzeugt wurden, während sie in Echtzeit arbeitet, um den Prozess zu steuern. Die Datendiode ist konfiguriert, um unidirektionale Kommunikationen zu ermöglichen, die von einer Sendevorrichtung an die Empfangsvorrichtung zu übertragen sind, während beliebige Kommunikationen verhindert werden, die von der Empfangsvorrichtung an die Sendevorrichtung übertragen werden. Die von der Prozessanlage erzeugten Daten, die über die Datendiode empfangen werden (Block **502**), können erzeugte Prozessdaten, Diagnosedaten und andere Datentypen beinhalten und können bei einer Empfangsvorrichtung, wie zum Beispiel dem Rand-Gateway **218** oder der Empfangsvorrichtung **405**, empfangen werden. Die von der Prozessanlage erzeugten empfangenen Daten können gesicherte Daten sein, z. B. Daten, die durch die vorstehend erörterten Verschlüsselungstechniken oder durch einen anderen Sicherheitsmechanismus gesichert wurden.

[0104] Bei Block **505** beinhaltet das Verfahren **500** das Sichern von empfangenen, durch die Prozessanlage erzeugten Daten unter Verwendung eines oder mehrerer Sicherheitsmechanismen, die denselben Sicherheitsmechanismus beinhalten können, der über die Datendiode verwendet wurde, oder einen oder mehrere andere Sicherheitsmechanismen beinhalten können. Bei Block **508** beinhaltet das Verfahren **500** das Übertragen der durch die Prozessanlage erzeugten Daten, die bei Block **505** gesichert wurden, an ein anderes System, das kommunikativ mit der Empfangsvorrichtung verbunden ist. Zum Beispiel werden die gesicherten, durch die Prozessanlage erzeugten Daten an ein oder mehrere entfernte System **210** übertragen, bei welchen ein/e oder mehrere Anwendungen, Dienste oder andere Konsumenten der durch die Prozessanlage erzeugten Daten **208** liegen und ausgeführt werden. Diese Anwendungen, Dienste oder anderen Konsumenten können mindestens mit einigen der durch die Prozessanlage erzeugten Daten arbeiten.

[0105] In einer Ausführungsform beinhaltet das Sichern der empfangenen durch die Prozessanlage erzeugten Daten (Block **505**) und das Übertragen der gesicherten, durch die Prozessanlage erzeugten Daten an das andere System (Block **508**) das Etablieren einer gesicherten Verbindung zwischen der Empfangsvorrichtung und dem anderen System. Das Übertragen der gesicherten, durch die Prozessanlage erzeugen Daten an das andere System (Block **508**) kann das Übertragen der Daten über ein oder mehrere öffentliche und/oder private Netzwerke, wie zum Beispiel das öffentliche Internet, ein privates Unternehmensnetzwerk usw., beinhalten. Daher beinhaltet das Etablieren der gesicherten Verbindung zwischen der Empfangsvorrichtung und dem anderen System das Etablieren einer gesicherten Verbindung durch ein oder mehrere öffentliche und/oder private Netzwerke. Unterschiedliche gesicherte Verbindungen können für unterschiedliche Typen von Inhaltsdaten, für unterschiedliche Datenerzeugungsquellen der Prozessanlage und/oder für unterschiedliche Konsumenten der Inhaltsdaten etabliert werden, wenn gewünscht.

[0106] In einem Beispiel wird die Verbindung zwischen der Empfangsvorrichtung und dem anderen System unter Verwendung eines Token-Dienstes gesichert. Die Empfangsvorrichtung authentifiziert sich gegenüber einem Token-System, das durch das andere System bereitgestellt wird, und als Reaktion auf die Authentifizierung empfängt die Empfangsvorrichtung einen Shared-Access-Signature(SAS)-Token von dem anderen System. Die Empfangsvorrichtung verwendet das SAS-Token dann während der Übertragung von Inhaltsdaten (z. B. durch die Prozessanlage erzeugte Daten) an das andere System. Zum Beispiel verwendet die Empfangsvorrichtung das SAS-Token zum Sichern und Authentifizieren einer Verbindung mit dem anderen System, z. B über eine AMQP(Advanced Message Queuing Protocol)-Verbindung. Außerdem können die Inhaltsdaten und das SAS-Token vor der Übertragung an das andere System verschlüsselt werden, falls dies gewünscht ist.

[0107] Das Verfahren **500** kann ebenfalls das erneute Sichern einer Verbindung zwischen der Empfangsvorrichtung und dem anderen System beinhalten (Block **510**). Das erneute Sichern einer Verbindung zwischen der Empfangsvorrichtung und dem anderen System **510** beinhaltet zum Beispiel das Empfangen eines aktualisierten oder anderen SAS-Tokens von dem anderen System (z. B. von dem Token-Dienst bei dem anderen System) zur Verwendung für das Übertragen anschließender Inhaltsdaten. Ein bestimmter SAS-Token kann einen vordefinierten Ablaufzeitraum beinhalten (z. B. fünf Minu-

ten, zehn Minuten, weniger als eine Stunde oder einen anderen Ablaufzeitraum, der konfigurierbar sein kann). Nach dem Ablauf des Tokens kann die Empfangsvorrichtung das neue SAS-Token zur Verwendung für anschließende Nachrichten anfordern oder abrufen. Alternativ kann das andere System automatisch ein aktualisiertes oder neues SAS-Token für die Empfangsvorrichtung zur Verwendung nach dem Ablauf des vorherigen Tokens senden.

[0108] Obwohl das Sichern und das erneute Sichern von Verbindungen zwischen der Empfangsvorrichtung und dem, anderen System (z. B. Blöcke **505**, **508**, **510**) vorstehend als SAS-Tokens und das AMQP-Protokoll verwendend beschrieben wurden, ist diese selbstverständlich nur eine von vielen möglichen Ausführungsformen des Verfahrens **500**. Ein beliebiger oder mehrere geeignete IOT-Sicherheitsmechanismen können durch das Verfahren **500** verwendet werden, wie zum Beispiel X.509-Zertifikate, andere Token-Typen, andere IOT-Protokolle wie MQTT oder XMPP usw.

[0109] Ausführungsformen der in der vorliegenden Offenbarung beschriebenen Verfahren können eine beliebige Anzahl der folgenden Aspekte, entweder allein oder in Kombination, umfassen:

[0110] 1. Verfahren zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System, wobei das Verfahren Folgendes umfasst: bei einem Feld-Gateway, welches ein Netzwerk der Prozessanlage und eine Datendiode verbindet, die zum Verhindern von Zweiwege-Kommunikation zwischen dem Feld-Gateway und einem Rand-Gateway konfiguriert ist, wiederkehrendes Ankündigen gegenüber dem Rand-Gateway über die Datendiode von entsprechenden Kontextinformationen, die jede von einer oder mehreren Vorrichtungen der Prozesssteuerungsanlage beschreiben; Empfangen, bei dem Feld-Gateway über das Prozessanlagennetzwerk, von Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, während die Prozessanlage arbeitet, um einen Prozess zu steuern; und Veröffentlichen, durch das Feld-Gateway gegenüber dem Rand-Gateway über die Datendiode, der Prozessanlagendaten.

[0111] 2. Verfahren nach dem vorhergehenden Aspekt, wobei wiederkehrendes Ankündigen der entsprechenden Kontextinformationen, die eine bestimmte Vorrichtung beschreiben, periodisches Senden der entsprechenden Kontextinformationen, welche die bestimmte Vorrichtung beschrieben, umfasst, wobei die Periodizität auf einer Toleranz einer Anwendung für verlorene Daten beruht, die Anwendung ein Konsument der Daten ist, die durch die bestimmte Vorrichtung erzeugt wurden, und die Anwendung kommunikativ mit dem Rand-Gateway verbunden ist.

[0112] 3. Verfahren nach einem der vorhergehenden Aspekte, wobei Empfangen, bei dem Feld-Gateway, der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, Empfangen, bei dem Feld-Gateway, von mindestens einem Teil der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, über das HART-IP®-Protokoll umfasst.

[0113] 4. Verfahren nach einem der vorhergehenden Aspekte, wobei Empfangen von mindestens einem Teil der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, über das HART-IP-Protokoll Empfangen der Daten, die durch jede der einen oder der mehreren Vorrichtungen veröffentlicht wurden, umfasst.

[0114] 5. Verfahren nach einem der vorhergehenden Aspekte, ferner umfassend Übertragen, durch das Feld-Gateway, einer Befragung an die bestimmte Vorrichtung; und wobei Empfangen, bei dem Feld-Gateway, der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, Empfangen, bei dem Feld-Gateway, von Daten, die durch die bestimmte Vorrichtung als Reaktion auf die Befragung erzeugt wurden, umfasst.

[0115] 6. Verfahren nach einem der vorhergehenden Aspekte, wobei Empfangen der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt werden, Empfangen von Daten, die ein Diagnoseergebnis angeben, umfasst.

[0116] 7. Verfahren nach einem der vorhergehenden Aspekte, wobei wiederkehrendes Ankündigen der entsprechenden Kontextinformationen jeder der einen oder der mehreren Vorrichtungen wiederkehrendes Senden der entsprechenden Kontextinformationen für jede der einen oder der mehreren Vorrichtungen unter Verwendung von mindestens einem HART-Protokollbefehl aus einer Gruppe von HART-Protokollbefehlen, einschließlich Befehl **0**, Befehl **20**, Befehl **50**, Befehl **74** oder Befehl **105**, umfasst.

[0117] 8. Verfahren nach einem der vorhergehenden Aspekte, wobei wiederkehrendes Ankündigen der entsprechenden Kontextinformationen jeder der einen oder der mehreren Vorrichtungen wiederkehrendes Senden einer Angabe einer Kennung jeder der einen oder der mehreren Vorrichtungen und einer Angabe einer entsprechenden Rate, bei welcher Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt werden, bereitzustellen sind, umfasst.

[0118] 9. Verfahren nach einem der vorhergehenden Aspekte, wobei Veröffentlichen der Prozessanlagendaten über die Datendiode Veröffentlichen der Prozessanlagendaten über die Datendiode unter Verwendung des HART-IP®-Protokolls umfasst.

[0119] 10. Verfahren nach einem der vorhergehenden Aspekte, wobei Veröffentlichen der Prozessanlagendaten über die Datendiode Veröffentlichen der Prozessanlagendaten über die Datendiode unter Verwendung eines JSON-Formats umfasst.

[0120] 11. System zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System, wobei das System Folgendes umfasst: ein Feld-Gateway, das kommunikativ mit einem Netzwerk der Prozessanlage gekoppelt ist; ein Rand-Gateway, das kommunikativ mit dem anderen System gekoppelt ist; eine Datendiode, welche das Feld-Gateway und das Rand-Gateway verbindet, wobei die Datendiode konfiguriert ist, um zu verhindern, dass Kommunikationen, die von dem Rand-Gateway übertragen werden, in das Feld-Gateway eingelassen werden, wobei Daten, die durch eine oder mehrere in der Prozessanlage enthaltene Vorrichtungen erzeugt wurden, während die Prozessanlage arbeitet, um einen industriellen Prozess zu steuern, bei dem Feld-Gateway über das Prozessanlagennetzwerk empfangen werden und durch das Feld-Gateway über die Datendiode gegenüber dem Rand-Gateway veröffentlicht werden.

[0121] 12. System nach dem vorhergehenden Aspekt, das ferner konfiguriert ist, um mindestens einen Teil des Verfahrens nach einem der Aspekt **1**-**10** durchzuführen.

[0122] 13. System nach einem der Aspekte **11**-**12**, wobei die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, über die Datendiode unter Verwendung des HART-IP®-Protokolls veröffentlicht werden.

[0123] 14. System nach einem der Aspekte **11**-**13**, wobei die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, über die Datendiode unter Verwendung eines JSON-Formats veröffentlicht werden.

[0124] 15. System nach einem der Aspekt **11**-**14**, ferner beinhaltend ein drahtloses Gateway, bei welchem die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, empfangen und dem Feld-Gateway bereitgestellt werden.

[0125] 16. System nach einem der Aspekte **11**-**15**, wobei das drahtlose Gateway ein WirelessHART®-Gateway ist.

[0126] 17. System nach einem der Aspekte **11**-**16**, wobei das drahtlose Gateway die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, dem Feld-Gateway unter Verwendung des HART-IP-Protokolls bereitstellt.

[0127] 18. System nach einem der Aspekte **11**-**17**, wobei mindestens eine der einen oder der mehreren Vorrichtungen entsprechende erzeugte Daten gegenüber dem drahtlosen Gateway veröffentlicht.

[0128] 19. System nach einem der Aspekte **11**-**18**, wobei das drahtlose Gateway, gegenüber welchem die entsprechenden erzeugten Daten veröffentlicht werden, ein Abonnent der entsprechenden erzeugten Daten ist.

[0129] 20. System nach einem der Aspekt **11**-**19**, wobei das drahtlose Gateway mindestens eine der einen oder der mehreren Vorrichtungen befragt, um entsprechende erzeugte Daten zu erhalten.

[0130] 21. System nach einem der Aspekte **11**-**20**, wobei eine Anwendung, die bei dem anderen System ausgeführt wird, ein Konsument von mindestens einem Teil der Daten ist, die durch die eine oder die mehreren in der Prozessanlage enthaltenen Vorrichtungen erzeugt wurden.

[0131] 22. System nach einem der Aspekte **11**-**21**, wobei das Rand-Gateway mindestens den Teil der Daten, die durch die eine oder die mehreren in der Prozessanlage enthaltenen Vorrichtungen erzeugt wurden, veröffentlicht und die Anwendung, die bei dem anderen System ausgeführt wird, ein Abonnent der durch das Rand-Gateway veröffentlichten Daten ist.

[0132] 23. System nach einem der Aspekte **11**-**22**, wobei die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt werden, während die Prozessanlage arbeitet, um einen industriellen Prozess zu steuern, mindestens eins von dynamischen Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, oder Diagnosedaten, die als ein Ergebnis einer Diagnose oder eines Tests der einen oder der mehreren Vorrichtungen erzeugt wurden, umfassen.

[0133] 24. System nach einem der Aspekte **11**-**23**, wobei die Datendiode Ethernetverbunden ist.

[0134] 25. System nach einem der Aspekte **11**-**24**, wobei die Datendiode seriell verbunden ist.

[0135] 26. System nach einem der Aspekte **11**-**25**, wobei das Feld-Gateway ferner entsprechende Informationen, die jede der einen oder der mehreren Vorrichtungen beschreiben, über die Datendiode gegenüber dem Rand-Gateway veröffentlicht.

[0136] 27. System nach einem der Aspekt **11**-**26**, wobei die entsprechenden Informationen, die jede der einen oder der mehreren Vorrichtungen beschreiben, eine Angabe einer entsprechenden Kennung jeder der einen oder der mehreren Vorrichtungen und

eine entsprechende Rate, bei welcher Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, zu veröffentlichen sind, beinhalten.

[0137] 28. System nach einem der Aspekte **11**-**27**, wobei die entsprechenden Informationen, die jede der einen oder der mehreren Vorrichtungen beschreiben, ferner eine Angabe eines Zustands jeder der einen oder der mehreren Vorrichtungen beinhalten.

[0138] 29. System nach einem der Aspekte **11**-**28**, wobei das andere System für mindestens eins des Folgenden konfiguriert ist: Überwachen von Bedingungen und/oder Ereignissen, die in der Prozessanlage auftreten;

[0139] Erfassen der Bedingungen und/oder Ereignisse, die in der Prozessanlage auftreten; Überwachen von mindestens einem Teil des Prozesses, der durch die Prozessanlage gesteuert wird; Durchführen deskriptiver Analytik unter Verwendung der erzeugten Daten; Durchführen präskriptiver Analytik unter Verwendung der erzeugten Daten; oder Erzeugen, auf der Grundlage der erzeugten Daten, einer präskriptiven Funktion zum Modifizieren von mindestens einem Teil der Prozessanlage.

[0140] 30. System nach einem der Aspekte **11**-**29**, wobei das andere System mindestens teilweise in einem oder mehreren Cloud-Computersystemen umgesetzt ist.

[0141] 31. Einer der vorhergehenden Ansprüche in Kombination mit einem anderen der vorhergehenden Aspekte.

[0142] Wenn sie in einer Software umgesetzt werden, können beliebige der hierin beschriebenen Anwendungen, Dienste und Maschinen in einem greifbaren, nicht transitorischen computerlesbaren Speicher gespeichert werden, wie auf einer Magnet-Disk, einer Laserdisk, einer Solid-State-Speichervorrichtung, einer molekularen Speichervorrichtung oder einem anderen Speichermedium, in einem RAM oder ROM eines Computers oder Prozessors usw. Obwohl die hierin offenbarten exemplarischen Systeme als, neben anderen Komponenten, Software und/oder Firmware umfassend, die auf Hardware ausgeführt wird, dargestellt werden, wird vermerkt, dass solche Systeme lediglich der Veranschaulichung dienen und nicht als einschränkend erachtet werden sollen. Es wird zum Beispiel erwogen, dass beliebige oder alle dieser Hardware-, Software- und Firmwarekomponenten ausschließlich als Hardware, ausschließlich als Software oder als eine Kombination von Hardware und Software ausgeführt werden könnten. Dementsprechend, während die hierin beschriebenen exemplarischen Systeme als in einer Software ausgeführt beschrieben werden, die an einem Prozessor von einer oder mehreren Computervorrichtungen ausgeführt wird, wird es ein gewöhnlicher Fachmann bereitwillig würdigen, dass die gelieferten Beispiele nicht die einzige Möglichkeit sind, um solche Systeme zu implementieren.

[0143] Demnach, während die vorliegende Erfindung in Bezug auf spezifische Beispiele beschrieben wurde, die lediglich der Veranschaulichung dienen und die Erfindung nicht einschränken sollen, wird es für einen gewöhnlichen Fachmann deutlich, dass an den offenbarten Ausführungsformen Veränderungen, Hinzufügungen und Streichungen vorgenommen werden können, ohne dass von dem Geist und dem Umfang der Erfindung abgewichen wird.

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 14507188 [0001, 0052]
- US 15/274519 [0001]
- US 15/274233 [0001, 0039]
- US 15332521 [0001, 0039]
- US 15274519 [0039]

Patentansprüche

1. Verfahren zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System, wobei das Verfahren Folgendes umfasst:
bei einem Feld-Gateway, welches ein Netzwerk der Prozessanlage und eine Datendiode verbindet, die zum Verhindern von Zweiwege-Kommunikation zwischen dem Feld-Gateway und einem Rand-Gateway konfiguriert ist, wiederkehrendes Ankündigen gegenüber dem Rand-Gateway über die Datendiode von entsprechenden Kontextinformationen, die jede von einer oder mehreren Vorrichtungen der Prozesssteuerungsanlage beschreiben;
Empfangen, bei dem Feld-Gateway über das Prozessanlagennetzwerk, von Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, während die Prozessanlage arbeitet, um einen Prozess zu steuern; und
Veröffentlichen, durch das Feld-Gateway gegenüber dem Rand-Gateway über die Datendiode, der Prozessanlagendaten.

2. Verfahren nach Anspruch 1, wobei wiederkehrendes Ankündigen der entsprechenden Kontextinformationen, die eine bestimmte Vorrichtung beschreiben, periodisches Senden der entsprechenden Kontextinformationen, welche die bestimmte Vorrichtung beschrieben, umfasst, wobei die Periodizität auf einer Toleranz einer Anwendung für verlorene Daten beruht, die Anwendung ein Konsument der Daten ist, die durch die bestimmte Vorrichtung erzeugt wurden, und die Anwendung kommunikativ mit dem Rand-Gateway verbunden ist.

3. Verfahren nach einem der Ansprüche 1 oder 2, insbesondere nach Anspruch 1, wobei Empfangen, bei dem Feld-Gateway, der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, Empfangen, bei dem Feld-Gateway, von mindestens einem Teil der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, über das HART-IP®-Protokoll umfasst, und/oder wobei Empfangen von mindestens einem Teil der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, über das HART-IP-Protokoll Empfangen der Daten, die durch jede der einen oder der mehreren Vorrichtungen veröffentlicht wurden, umfasst.

4. Verfahren nach einem der Ansprüche 1 bis 3, insbesondere nach Anspruch 1, ferner umfassend Übertragen, durch das Feld-Gateway, einer Befragung an die bestimmte Vorrichtung; und
wobei Empfangen, bei dem Feld-Gateway, der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, Empfangen, bei dem Feld-Gateway, von Daten, die durch die bestimmte Vorrichtung als Reaktion auf die Befragung erzeugt wurden, umfasst, und/oder
wobei Empfangen der Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt werden, Empfangen von Daten, die ein Diagnoseergebnis angeben, umfasst.

5. Verfahren nach einem der Ansprüche 1 bis 4, insbesondere nach Anspruch 1. wobei wiederkehrendes Ankündigen der entsprechenden Kontextinformationen jeder der einen oder der mehreren Vorrichtungen wiederkehrendes Senden der entsprechenden Kontextinformationen für jede der einen oder der mehreren Vorrichtungen unter Verwendung von mindestens einem HART-Protokollbefehl aus einer Gruppe von HART-Protokollbefehlen, einschließlich Befehl 0, Befehl 20, Befehl 50, Befehl 74 oder Befehl 105, umfasst.

6. Verfahren nach einem der Ansprüche 1 bis 5, insbesondere nach Anspruch 1, wobei wiederkehrendes Ankündigen der entsprechenden Kontextinformationen jeder der einen oder der mehreren Vorrichtungen wiederkehrendes Senden einer Angabe einer Kennung jeder der einen oder der mehreren Vorrichtungen und einer Angabe einer entsprechenden Rate, bei welcher Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt werden, bereitzustellen sind, umfasst.

7. Verfahren nach einem der Ansprüche 1 bis 6, insbesondere nach Anspruch 1,
wobei Veröffentlichen der Prozessanlagendaten über die Datendiode Veröffentlichen der Prozessanlagendaten über die Datendiode unter Verwendung des HART-IP®-Protokolls umfasst, und/oder
wobei Veröffentlichen der Prozessanlagendaten über die Datendiode Veröffentlichen der Prozessanlagendaten über die Datendiode unter Verwendung eines JSON-Formats umfasst.

8. System zum sicheren Transportieren von Kommunikationen von einer Prozessanlage zu einem anderen System, wobei das System Folgendes umfasst:
ein Feld-Gateway, das kommunikativ mit einem Netzwerk der Prozessanlage gekoppelt ist;
ein Rand-Gateway, das kommunikativ mit dem anderen System gekoppelt ist; und
eine Datendiode, die das Feld-Gateway und das Rand-Gateway verbindet, wobei die Datendiode konfiguriert ist, um zu verhindern, dass Kommunikationen, die von dem Rand-Gateway übertragen werden, in das Feld-Gateway eingelassen werden,
wobei Daten, die durch eine oder mehrere in der Prozessanlage enthaltene Vorrichtungen erzeugt wurden, während die Prozessanlage arbeitet, um einen industriellen Prozess zu steuern, bei dem Feld-Gateway über das Prozessanlagennetzwerk empfangen werden und durch das Feld-Gateway über die Daten-

diode gegenüber dem Rand-Gateway veröffentlicht werden.

9. System nach Anspruch 8, wobei die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, über die Datendiode unter Verwendung des HART-IP®-Protokolls veröffentlicht werden, und/oder wobei die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, über die Datendiode unter Verwendung eines JSON-Formats veröffentlicht werden.

10. System nach einem der Ansprüche 8 oder 9, insbesondere nach Anspruch 8, ferner beinhaltend ein drahtloses Gateway, bei welchem die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, empfangen und dem Feld-Gateway bereitgestellt werden, und/oder
wobei das drahtlose Gateway ein WirelessHART®-Gateway ist, und/oder
wobei das drahtlose Gateway die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, dem Feld-Gateway unter Verwendung des HART-IP-Protokolls bereitstellt, und/oder
wobei mindestens eine der einen oder der mehreren Vorrichtungen entsprechende erzeugte Daten gegenüber dem drahtlosen Gateway veröffentlicht, und/oder
wobei das drahtlose Gateway, gegenüber welchem die entsprechenden erzeugten Daten veröffentlicht werden, ein Abonnent der entsprechenden erzeugten Daten ist, und/oder
wobei das drahtlose Gateway mindestens eine der einen oder der mehreren Vorrichtungen befragt, um entsprechende erzeugte Daten zu erhalten.

11. System nach einem der Ansprüche 8 bis 10, insbesondere nach Anspruch 8, wobei eine Anwendung, die bei dem anderen System ausgeführt wird, ein Konsument von mindestens einem Teil der Daten ist, die durch die eine oder die mehreren in der Prozessanlage enthaltenen Vorrichtungen erzeugt wurden, und/oder wobei das Rand-Gateway mindestens den Teil der Daten, die durch die eine oder die mehreren in der Prozessanlage enthaltenen Vorrichtungen erzeugt wurden, veröffentlicht und die Anwendung, die bei dem anderen System ausgeführt wird, ein Abonnent der durch das Rand-Gateway veröffentlichten Daten ist.

12. System nach einem der Ansprüche 8 bis 11, insbesondere nach Anspruch 8, wobei die Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt werden, während die Prozessanlage arbeitet, um einen industriellen Prozess zu steuern, mindestens eins von dynamischen Daten, die durch die eine oder die mehreren Vorrichtungen erzeugt wurden, oder Diagnosedaten, die als ein Ergebnis einer Diagnose oder eines Tests der einen oder der mehreren Vorrichtungen erzeugt wurden, umfassen, und/oder
wobei die Datendiode Ethernet-verbunden ist, und/oder
wobei die Datendiode seriell verbunden ist.

13. System nach einem der Ansprüche 8 bis 12, insbesondere nach Anspruch 8, wobei das Feld-Gateway ferner entsprechende Informationen, die jede der einen oder der mehreren Vorrichtungen beschreiben, über die Datendiode gegenüber dem Rand-Gateway veröffentlicht, und/oder
wobei die entsprechenden Informationen, die jede der einen oder der mehreren Vorrichtungen beschreiben, eine Angabe einer entsprechenden Kennung jeder der einen oder der mehreren Vorrichtungen und eine entsprechende Rate, bei welcher Daten, die durch jede der einen oder der mehreren Vorrichtungen erzeugt wurden, zu veröffentlichen sind, beinhalten, und/oder
wobei die entsprechenden Informationen, die jede der einen oder der mehreren Vorrichtungen beschreiben, ferner eine Angabe eines Zustands jeder der einen oder der mehreren Vorrichtungen beinhalten.

14. System nach einem der Ansprüche 8 bis 13, insbesondere nach Anspruch 8, wobei das andere System für mindestens eins des Folgenden konfiguriert ist:
Überwachen von Bedingungen und/oder Ereignissen, die in der Prozessanlage auftreten;
Erfassen der Bedingungen und/oder Ereignisse, die in der Prozessanlage auftreten;
Überwachen von mindestens einem Teil des Prozesses, der durch die Prozessanlage gesteuert wird;
Durchführen deskriptiver Analytik unter Verwendung der erzeugten Daten;
Durchführen präskriptiver Analytik unter Verwendung der erzeugten Daten; oder
Erzeugen, auf der Grundlage der erzeugten Daten, einer präskriptiven Funktion zum Modifizieren von mindestens einem Teil der Prozessanlage, und/oder wobei das andere System mindestens teilweise in einem oder mehreren Cloud-Computersystemen umgesetzt ist.

15. Computerlesbares Speichermedium, welches Instruktionen enthält, die mindestens einen Prozessor dazu veranlassen, ein Verfahren nach einem der Ansprüche 1 bis 7 zu implementieren, wenn die Instruktionen durch mindestens einen Prozessor ausgeführt werden.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

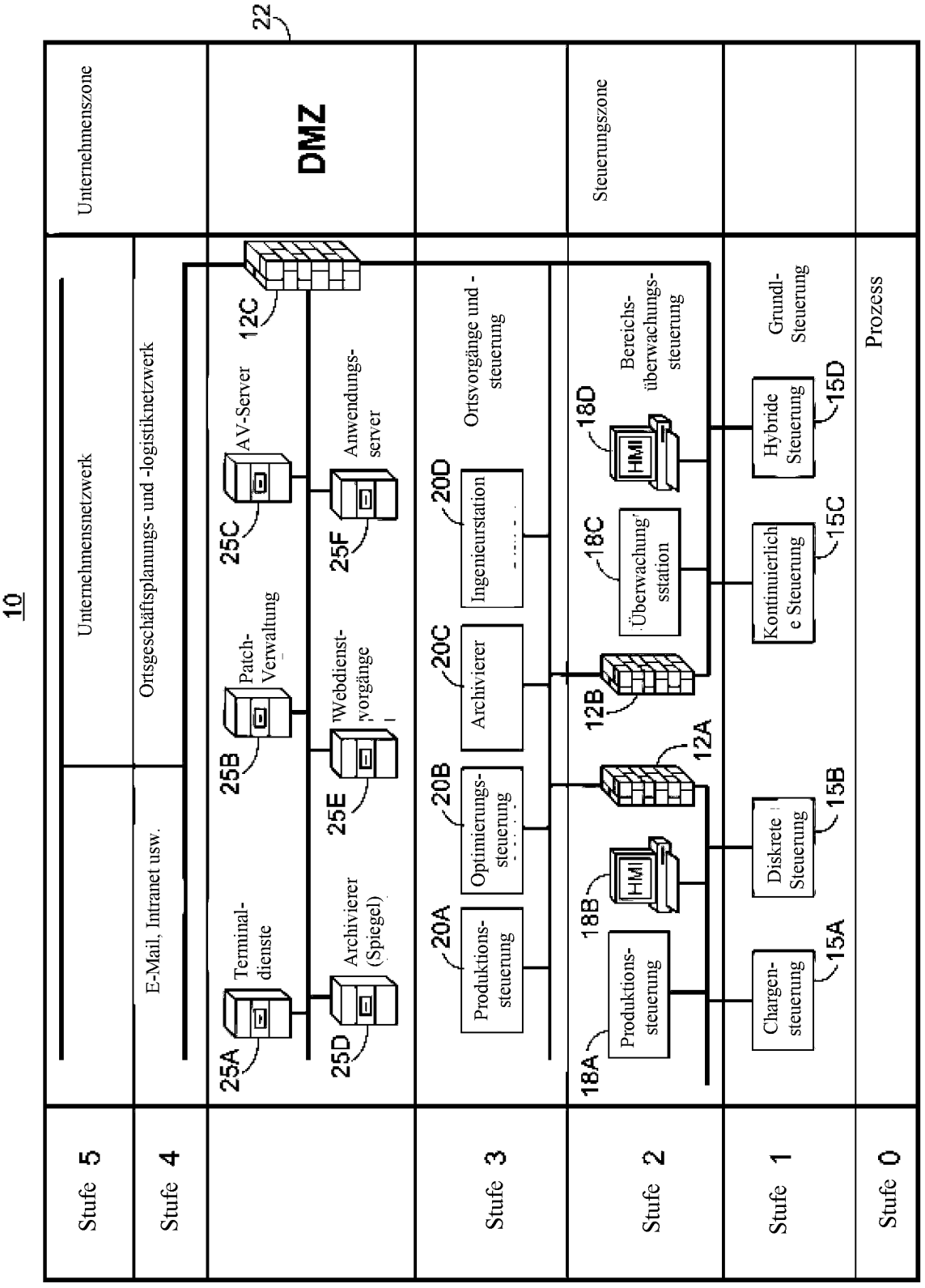


FIG. 1

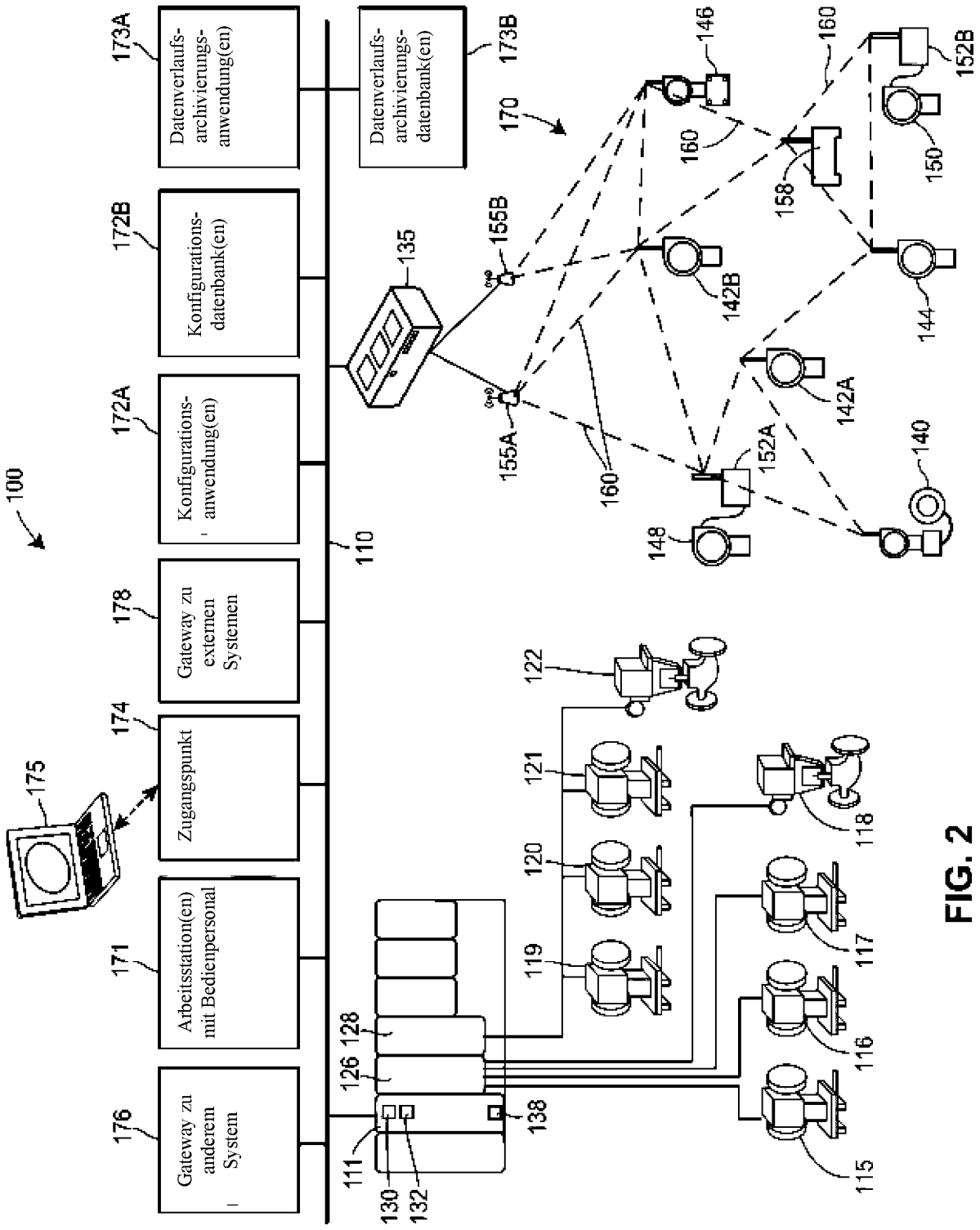

100
110
Gateway zu anderem System
176
Arbeitsstation(en) mit Bedienpersonal
171
Zugangspunkt
174
Gateway zu externen Systemen
178
Konfigurations-anwendung(en)
172A
Konfigurations-datenbank(en)
172B
Datenverlaufs-archivierungs-anwendung(en)
173A
Datenverlaufs-archivierungs-datenbank(en)
173B
170
135
155A
155B
160
142A
142B
144
146
148
150
152A
152B
158
140
111
130
132
126
128
138
115
116
117
118
119
120
121
122
175

FIG. 2

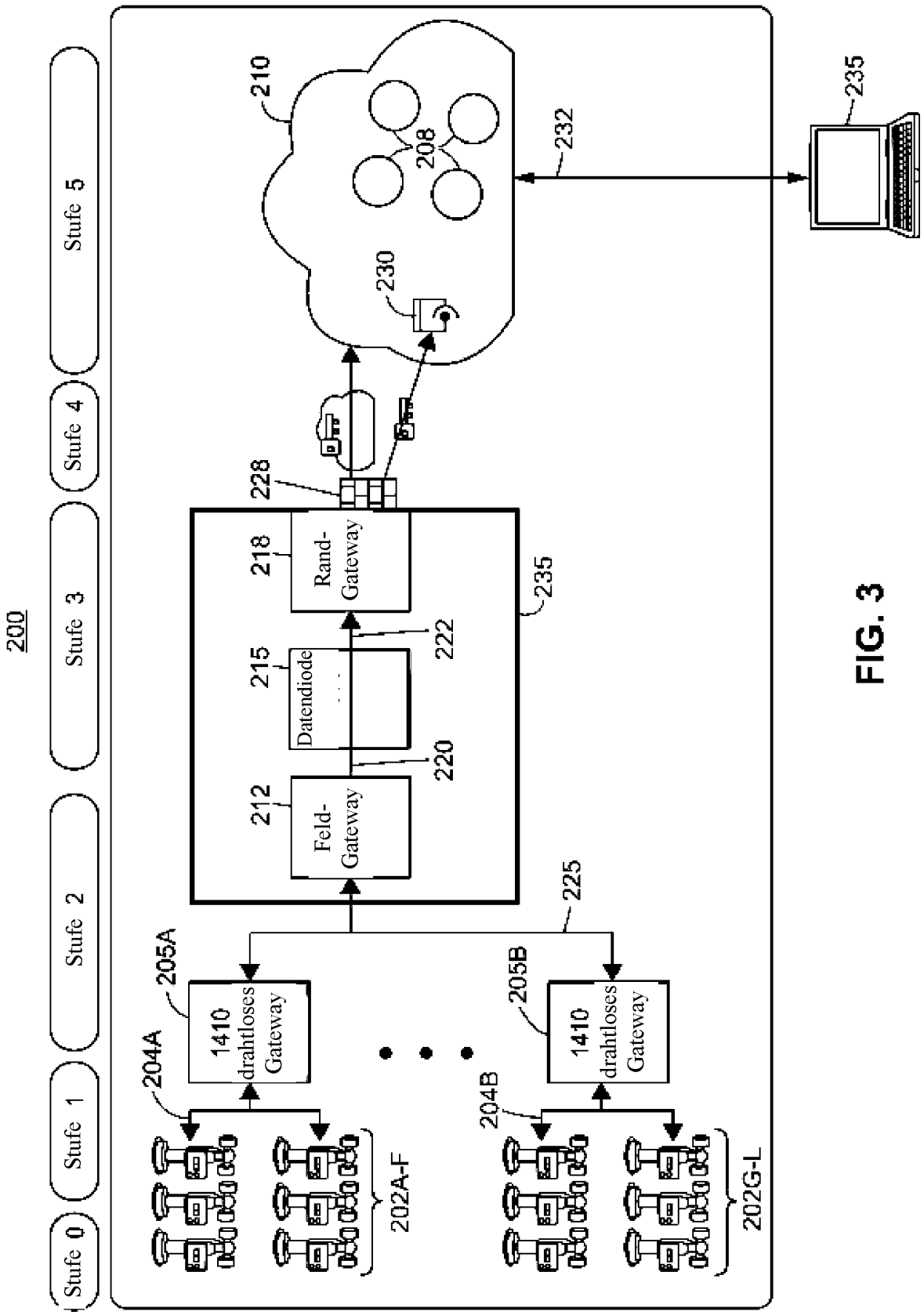

200
Stufe 0
Stufe 1
Stufe 2
Stufe 3
Stufe 4
Stufe 5
210
208
232
235
230
228
218
Rand-Gateway
215
Datendiode
222
220
212
Feld-Gateway
235
225
205A
1410 drahtloses Gateway
204A
202A-F
205B
1410 drahtloses Gateway
204B
202G-L

FIG. 3

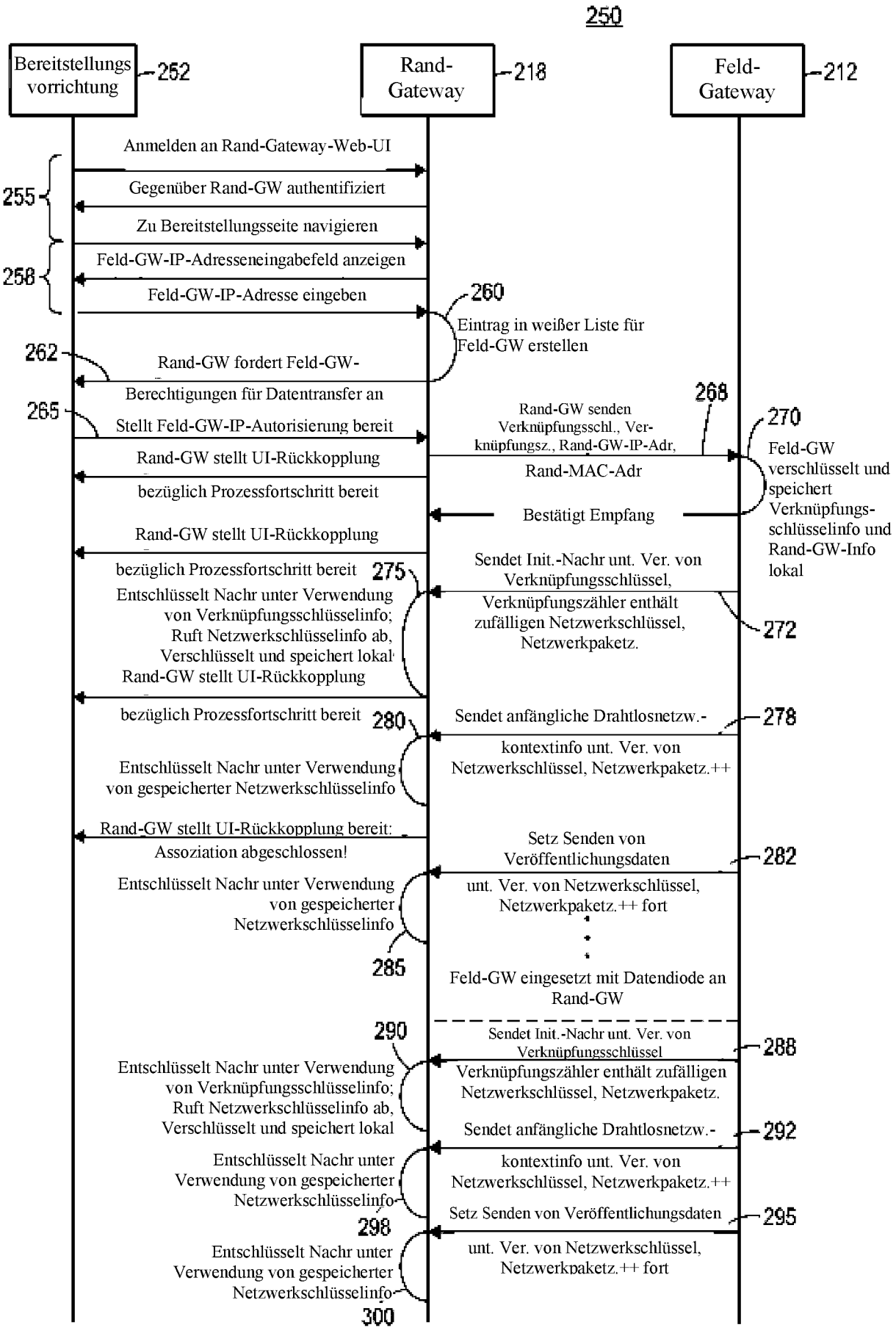

250
Bereitstellungsvorrichtung
252
Rand-Gateway
218
Feld-Gateway
212
Anmelden an Rand-Gateway-Web-UI
255
Gegenüber Rand-GW authentifiziert
Zu Bereitstellungsseite navigieren
258
Feld-GW-IP-Adresseneingabefeld anzeigen
Feld-GW-IP-Adresse eingeben
260
Eintrag in weißer Liste für Feld-GW erstellen
262
Rand-GW fordert Feld-GW-Berechtigungen für Datentransfer an
265
Stellt Feld-GW-IP-Autorisierung bereit
Rand-GW stellt UI-Rückkopplung bezüglich Prozessfortschritt bereit
268
Rand-GW senden Verknüpfungsschl., Verknüpfungsz., Rand-GW-IP-Adr, Rand-MAC-Adr
270
Feld-GW verschlüsselt und speichert Verknüpfungsschlüsselinfo und Rand-GW-Info lokal
Bestätigt Empfang
Rand-GW stellt UI-Rückkopplung bezüglich Prozessfortschritt bereit
275
Entschlüsselt Nachr unter Verwendung von Verknüpfungsschlüsselinfo; Ruft Netzwerkschlüsselinfo ab, Verschlüsselt und speichert lokal
Sendet Init.-Nachr unt. Ver. von Verknüpfungsschlüssel, Verknüpfungszähler enthält zufälligen Netzwerkschlüssel, Netzwerkpaketz.
272
Rand-GW stellt UI-Rückkopplung bezüglich Prozessfortschritt bereit
280
Entschlüsselt Nachr unter Verwendung von gespeicherter Netzwerkschlüsselinfo
Sendet anfängliche Drahtlosnetzw.-kontextinfo unt. Ver. von Netzwerkschlüssel, Netzwerkpaketz.++
278
Rand-GW stellt UI-Rückkopplung bereit: Assoziation abgeschlossen!
Setz Senden von Veröffentlichungsdaten unt. Ver. von Netzwerkschlüssel, Netzwerkpaketz.++ fort
282
Entschlüsselt Nachr unter Verwendung von gespeicherter Netzwerkschlüsselinfo
285
Feld-GW eingesetzt mit Datendiode an Rand-GW
290
Sendet Init.-Nachr unt. Ver. von Verknüpfungsschlüssel Verknüpfungszähler enthält zufälligen Netzwerkschlüssel, Netzwerkpaketz.
288
Entschlüsselt Nachr unter Verwendung von Verknüpfungsschlüsselinfo; Ruft Netzwerkschlüsselinfo ab, Verschlüsselt und speichert lokal
Sendet anfängliche Drahtlosnetzw.-kontextinfo unt. Ver. von Netzwerkschlüssel, Netzwerkpaketz.++
292
Entschlüsselt Nachr unter Verwendung von gespeicherter Netzwerkschlüsselinfo
Setz Senden von Veröffentlichungsdaten unt. Ver. von Netzwerkschlüssel, Netzwerkpaketz.++ fort
295
298
Entschlüsselt Nachr unter Verwendung von gespeicherter Netzwerkschlüsselinfo
300

FIG. 4

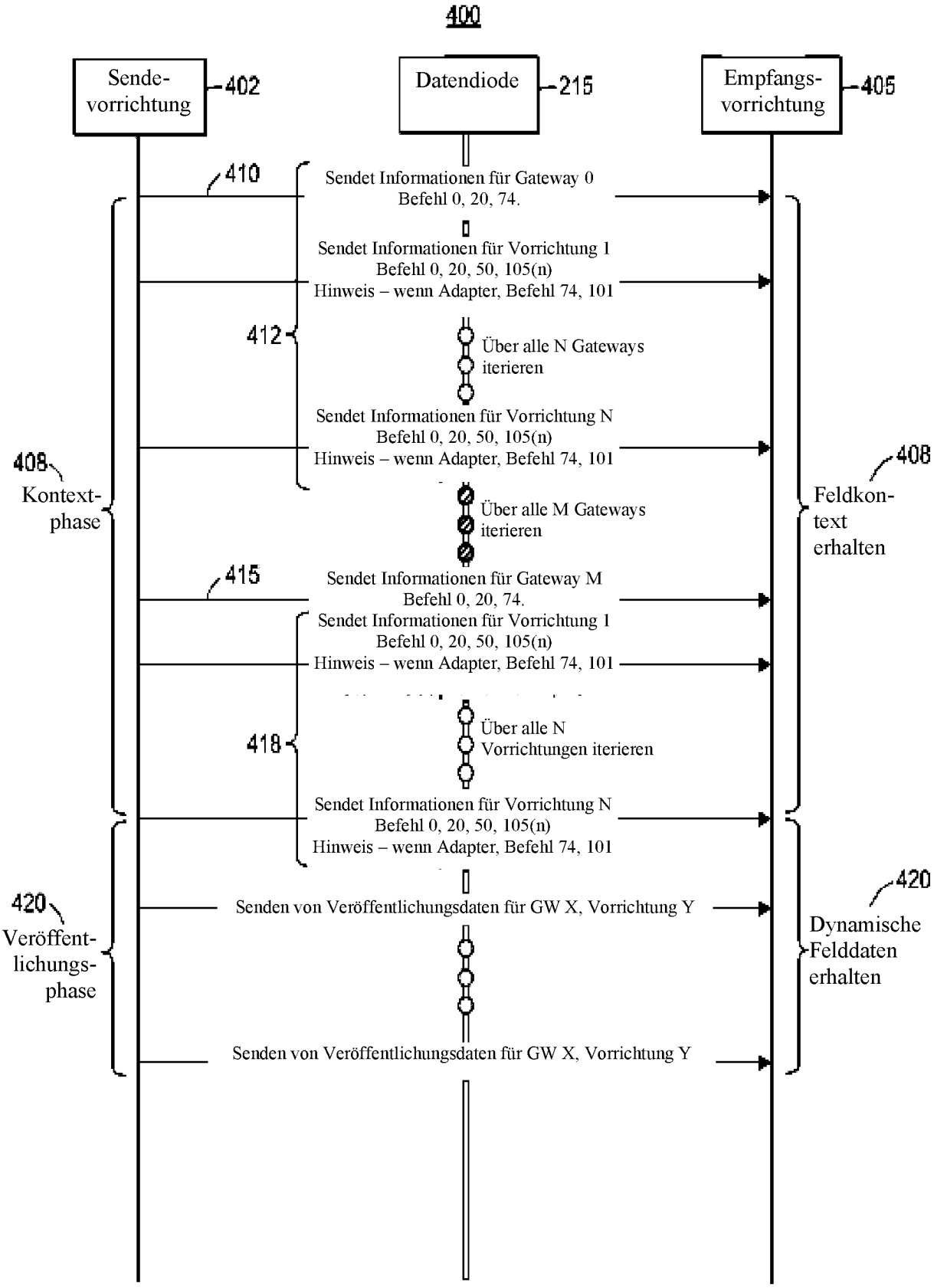

400
Sende-vorrichtung
402
Datendiode
215
Empfangs-vorrichtung
405
410
Sendet Informationen für Gateway 0
Befehl 0, 20, 74.
Sendet Informationen für Vorrichtung 1
Befehl 0, 20, 50, 105(n)
Hinweis – wenn Adapter, Befehl 74, 101
412
Über alle N Gateways iterieren
Sendet Informationen für Vorrichtung N
Befehl 0, 20, 50, 105(n)
Hinweis – wenn Adapter, Befehl 74, 101
408
Kontext-phase
Über alle M Gateways iterieren
408
Feldkon-text erhalten
415
Sendet Informationen für Gateway M
Befehl 0, 20, 74.
Sendet Informationen für Vorrichtung 1
Befehl 0, 20, 50, 105(n)
Hinweis – wenn Adapter, Befehl 74, 101
418
Über alle N Vorrichtungen iterieren
Sendet Informationen für Vorrichtung N
Befehl 0, 20, 50, 105(n)
Hinweis – wenn Adapter, Befehl 74, 101
420
Veröffent-lichungs-phase
Senden von Veröffentlichungsdaten für GW X, Vorrichtung Y
420
Dynamische Felddaten erhalten
Senden von Veröffentlichungsdaten für GW X, Vorrichtung Y

FIG. 5

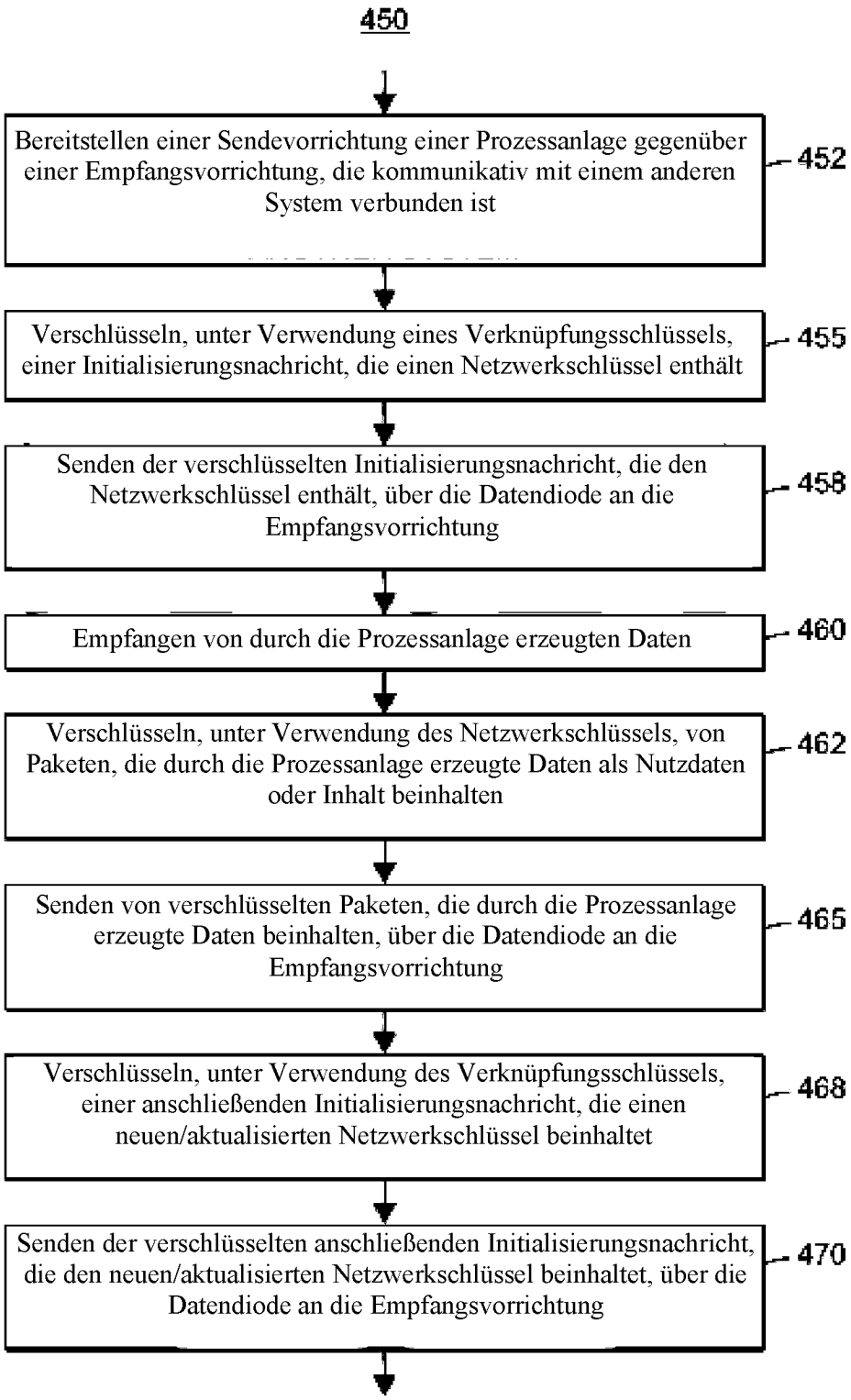

450
Bereitstellen einer Sendevorrichtung einer Prozessanlage gegenüber einer Empfangsvorrichtung, die kommunikativ mit einem anderen System verbunden ist
452
Verschlüsseln, unter Verwendung eines Verknüpfungsschlüssels, einer Initialisierungsnachricht, die einen Netzwerkschlüssel enthält
455
Senden der verschlüsselten Initialisierungsnachricht, die den Netzwerkschlüssel enthält, über die Datendiode an die Empfangsvorrichtung
458
Empfangen von durch die Prozessanlage erzeugten Daten
460
Verschlüsseln, unter Verwendung des Netzwerkschlüssels, von Paketen, die durch die Prozessanlage erzeugte Daten als Nutzdaten oder Inhalt beinhalten
462
Senden von verschlüsselten Paketen, die durch die Prozessanlage erzeugte Daten beinhalten, über die Datendiode an die Empfangsvorrichtung
465
Verschlüsseln, unter Verwendung des Verknüpfungsschlüssels, einer anschließenden Initialisierungsnachricht, die einen neuen/aktualisierten Netzwerkschlüssel beinhaltet
468
Senden der verschlüsselten anschließenden Initialisierungsnachricht, die den neuen/aktualisierten Netzwerkschlüssel beinhaltet, über die Datendiode an die Empfangsvorrichtung
470

FIG. 6

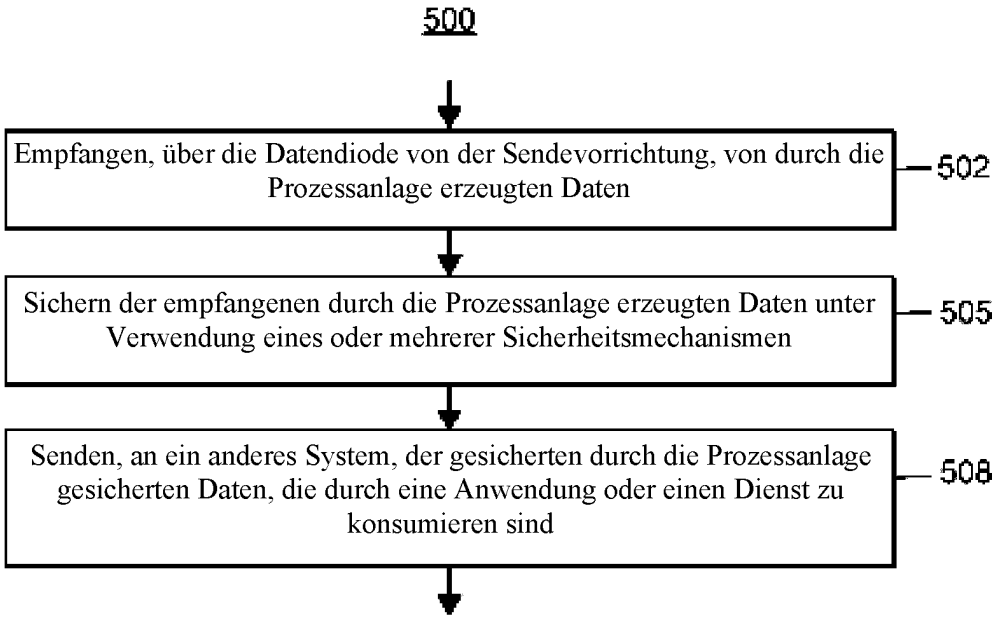

500
Empfangen, über die Datendiode von der Sendevorrichtung, von durch die Prozessanlage erzeugten Daten
502
Sichern der empfangenen durch die Prozessanlage erzeugten Daten unter Verwendung eines oder mehrerer Sicherheitsmechanismen
505
Senden, an ein anderes System, der gesicherten durch die Prozessanlage gesicherten Daten, die durch eine Anwendung oder einen Dienst zu konsumieren sind
508

FIG. 7