

(12)

Österreichische Patentanmeldung

(21)

Anmeldenummer:

A 51106/2018

(22)

Anmeldetag:

13.12.2018

(43)

Veröffentlicht am:

15.06.2020

(51)

Int. Cl.:

H04L 29/08

H04W 88/18

(2006.01)

(2009.01)

(56)

Entgegenhaltungen:

WO 2015089457 A1

US 2018219944 A1

WO 2005050933 A1

(71)

Patentanmelder:

AVL List GmbH

8020 Graz (AT)

(72)

Erfinder:

Aldrian Andreas Dipl.Ing. Ing. BSc

8144 Haselsdorf-Tobelbad (AT)

Wolf Christoph

8055 Graz (AT)

Ma Zhendong

1180 Wien (AT)

Maier Patrik

8010 Graz (AT)

Sprung Samuel

8020 Graz (AT)

(74)

Vertreter:

Patentanwälte Pinter & Weiss OG

1040 Wien (AT)

(54)

Kommunikationsmodul

(57)

Kommunikationsmodul (1) zur Datenübertragung zwischen zumindest einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) eingebunden ist, und einem Backend-Rechnersystem (5), welches an ein paketvermitteltes Datennetz (6) angeschlossen ist. Das Kommunikationsmodul (1) weist ein gerätenahes Gateway (7) und ein netzwerknahe Gateway (8) auf, die über eine zwischenstationsfreie Punkt-zu-Punkt-Verbindung (9) miteinander verbunden sind. Das netzwerknahe Gateway (8) stellt eine Datenübertragungsschnittstelle zwischen dem paketvermittelten Datennetz (6) und der Punkt-zu-Punkt-Verbindung (9) bereit und das gerätenahe Gateway (7) stellt eine Datenübertragungsschnittstelle zwischen der Punkt-zu-Punkt-Verbindung (9) und dem internen Netz (3) bereit.

Fig. 1

Zusammenfassung

Kommunikationsmodul (1) zur Datenübertragung zwischen zumindest einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) eingebunden ist, und einem Backend-Rechnersystem (5), welches an ein paketvermitteltes Datennetz (6) angeschlossen ist. Das Kommunikationsmodul (1) weist ein gerätenahes Gateway (7) und ein netzwerknahe Gateway (8) auf, die über eine zwischenstationsfreie Punkt-zu-Punkt-Verbindung (9) miteinander verbunden sind. Das netzwerknahe Gateway (8) stellt eine Datenübertragungsschnittstelle zwischen dem paketvermittelten Datennetz (6) und der Punkt-zu-Punkt-Verbindung (9) bereit und das gerätenahe Gateway (7) stellt eine Datenübertragungsschnittstelle zwischen der Punkt-zu-Punkt-Verbindung (9) und dem internen Netz (3) bereit.

Fig. 1

Kommunikationsmodul

Die Erfindung betrifft ein Kommunikationsmodul zur Datenübertragung zwischen zumindest einer Hardwarekomponente, die in ein internes Netz eines technischen Systems eingebunden ist, und einem Backend-Rechnersystem, welches an ein paketvermitteltes Datennetz angeschlossen ist. Weiters betrifft die Erfindung ein technisches System mit einem solchen Kommunikationsmodul und mit solchen Systemen ausführbare Verfahren.

Durch die Fortschritte in der Entwicklung „intelligenter“ Hardwaresysteme und deren Einsatz in technischen Systemen sowohl im industriellen, im professionellen als auch im privaten Umfeld hat die Sicherung von Daten gegen unberechtigten Zugriff und Manipulationen erheblich an Wichtigkeit erhalten. Dies ist unter anderem damit zu begründen, dass eine Datenmanipulation, wie etwa ein Hackerangriff auf eingebettete Hardwaresysteme, unmittelbare Auswirkungen auf das Verhalten dieser Systeme hat und nicht nur die Intaktheit und Funktion dieser Systeme beeinträchtigen kann, sondern sogar eine Gefahr für Leib und Leben der Benutzer darstellen kann. Beispielhaft seien hier Lenk- oder Bremssysteme in autonomen, teilautonomen und konventionellen Fahrzeugen, Steuereinrichtungen von Flugzeugen oder Schaltanlagen in Infrastruktureinrichtungen, wie etwa für die Stromversorgung, angeführt. Von böswilligen Manipulationen der Funktionen solcher Systeme kann nicht nur eine Gefahr für einzelne, sondern auch für die Allgemeinheit ausgehen.

Darüber hinaus erzeugen viele Hardwaresysteme zahlreiche Daten, aus denen sich beispielsweise Informationen über das Verhalten, den Aufenthaltsort, oder gar über den gesundheitlichen Zustand von Benutzern auswerten lassen (beispielsweise bei Daten von Fitness-Trackern oder ähnlichem). Zu Beispielen solcher Daten zählen auch Telemetriedaten von (autonomen) Fahrzeugen, Sensor- und Steuerungsdaten von industriellen Anlagen, Forschungsdaten, aus denen sich Informationen über Forschungsprojekte von konkurrierenden Unternehmen oder Einrichtungen ableiten lassen, Kommunikationsdaten, etc. Für alle solche Daten besteht ein berechtigtes Interesse der Inhaber, dass diese Daten von Dritten nicht unberechtigt eingesehen bzw. verwendet werden können.

Technische Systeme, wie etwa ein (gegebenenfalls autonomes) Fahrzeug, eine Maschine oder Maschinenanordnung in einer industriellen Umgebung, eine Transporteinrichtung, eine Prüf- oder Messeinrichtung, wie etwa ein (Motor-)Prüfstand oder technische Überwachungseinrichtungen beinhalten üblicherweise eine Vielzahl an Hardwarekomponenten, die über ein internes Netz (oder gegebenenfalls mehrere interne Netze) miteinander kommunizieren, um die an das technische System gestellte Aufgabe zu bewerkstelligen. Die Hardwarekomponenten umfassen üblicherweise Sensoren und Aktoren, über die das technische System mit der (realen) Umgebung in eine Wechselwirkung tritt.

Damit solche komplexen Aufgaben von den Hardwarekomponenten umgesetzt werden können, sind diese mit jeweils eigenen (Micro-)Prozessoren und Speichereinheiten ausgestattet, die die Funktionen der Hardwarekomponente gemäß einer Programmlogik steuern.

- 5 Einen wesentlichen Teil dieser Programmlogik ist üblicherweise in einem nichtflüchtigen Speicher, beispielsweise einem Flash-Speicher, abgelegt, sodass er bei jedem Start bzw. jeder Initialisierung der Hardwarekomponente zur Verfügung steht. Dieser Teil wird üblicherweise als „Firmware“ bezeichnet. Die Firmware bleibt zwar während des Betriebs der Hardware unverändert, dennoch sind Änderungen möglich, etwa wenn eine alte Version der
- 10 Firmware durch eine neue Version ersetzt wird. Die neue Version wird dabei üblicherweise vom Hersteller der Hardwarekomponente von einem Backend-Rechnersystem über ein paketvermitteltes Datennetz, insbesondere das Internet bereitgestellt. Das Aktualisieren der Firmware kann entweder aufgrund eines Benutzereingriffs erfolgen, es kann von der Hardwarekomponente oder von einer anderen Komponente des technischen Systems
- 15 ausgelöst werden, oder es kann vom Backend-Rechnersystem ausgelöst werden. Eine Angriffsstrategie liegt darin, die Firmware während der Übertragung über das Internet (oder ein anderes paketvermitteltes Datennetz) gegen eine korruptierte Version auszutauschen und dadurch einen (Fern)zugriff auf Funktionalität der Hardwarekomponente zu erhalten. Bei einer unverschlüsselten Übertragung ist dies für technisch versierte Täter mit
- 20 verhältnismäßig geringem Aufwand möglich, aber auch bei einer verschlüsselten Übertragung kann ein Angriff erfolgreich sein, etwa in Form eines Man-in-the-Middle-Angriffs oder indem eine der Übertragungskomponenten, über die die Ver- bzw. Entschlüsselung erfolgt, gehackt wird.

- Ein weiterer Sicherheitsaspekt betrifft die Übermittlung von Daten, die von einer
- 25 Hardwarekomponente erzeugt werden, an das Backend-Rechnersystem. Solche Daten können beispielsweise Telemetrie- oder Sensordaten sein, die beispielsweise zu Wartungs- oder Überwachungszwecken an das Backend-Rechnersystem übermittelt werden. Diese Übermittlung soll einerseits aus Gründen der Datensicherheit abhörsicher erfolgen, andererseits muss auch hierbei eine Manipulation der Daten ausgeschlossen werden
- 30 können. Durch eine gezielte Manipulation der Daten wäre es nämlich beispielsweise möglich, dem Backend-Rechnersystem eine falsche Gefahrensituation vorzuspielen, etwa um eine (falsche) Reaktion oder einen falschen Alarm auszulösen.

- Es ist die Aufgabe der gegenständlichen Erfindung, Vorrichtungen und Verfahren bereitzustellen, mit denen die Übertragung von Daten zwischen Hardwarekomponenten, die
- 35 in technische Systeme eingebettet sind, und einem Backend-Rechnersystem, das ans Internet oder ein anderes paketvermitteltes Datennetz angeschlossen ist, manipulations- und abhörsicher durchgeführt werden kann.

Diese und weitere Aufgaben werden erfindungsgemäß durch ein Kommunikationsmodul der eingangs genannten Art gelöst, welches ein gerätenahes Gateway und ein netzwerknahe Gateway aufweist, die über eine zwischenstationsfreie Punk-zu-Punkt-Verbindung miteinander verbunden sind, wobei das netzwerknahe Gateway eine

- 5 Datenübertragungsschnittstelle zwischen dem paketvermittelten Datennetz und der Punk-zu-Punkt-Verbindung bereitstellt und wobei das gerätenahe Gateway eine Datenübertragungsschnittstelle zwischen der Punk-zu-Punkt-Verbindung und dem internen Netz bereitstellt. Die Punk-zu-Punkt-Verbindung stellt dabei ein nicht umleitbares „Nadelöhr“ dar, das einen aus dem paketvermittelten Datennetz kommenden Angriff verhindert. Die
- 10 Kommunikation zwischen dem gerätenahen und dem netzwerknahen Gateway ist strikt definiert und ein „Ausbrechen“ daraus ist nicht möglich. Da die zwischenstationsfreie Punk-zu-Punkt-Verbindung kein Routing erlaubt, ist es einem Angreifer nicht möglich, durch ein Umleiten der Kommunikation beliebige Komponenten anzusprechen. Sogar wenn es einem Angreifer gelungen sein sollte, Sicherheitsfunktionen des netzwerknahen Gateways zu
- 15 umgehen oder auszuschalten, kann er dennoch keinen Zugriff auf das interne Netz oder die Hardwarekomponente erhalten.

- In vorteilhafter Weise kann das gerätenahe Gateway ein Gateway-Sicherheitsmodul aufweisen und/oder das netzwerknahe Gateway kann ein Gateway-Sicherheitsmodul aufweisen. Solche Gateway-Sicherheitsmodule erlauben die Umsetzung komplexer
- 20 Verschlüsselungs- und Signaturverfahren in hardwarenaher Weise.

- In einer bevorzugten Ausführungsform kann zumindest ein Gateway-Sicherheitsmodul eine Kartenschnittstelle für eine Prozessorchipkarte aufweisen. Dies erleichtert die Serienfertigung der Gateways, da die konkreten Sicherheitsmerkmale (insbesondere die Definition und/oder Erzeugung der kryptographischen Schlüssel, die Auswahl und Definition
- 25 der Sicherheitsprotokolle, etc.) in der Prozessorchipkarte gemäß einem kryptographischen System definiert sein kann. Die Prozessorchipkarte kann von dritten, auf dieses technische Gebiet spezialisierten Herstellern zugekauft werden, was die Entwicklung der Gateways erleichtert.

- Die Erfindung betrifft weiters ein technisches System mit einem entsprechenden
- 30 Kommunikationsmodul, wobei das technische System weiters zumindest eine Hardwarekomponente und zumindest ein internes Netz umfasst. Erfindungsgemäß lassen sich dadurch sehr komplexe technische Systeme, beispielsweise (autonome) Fahrzeuge, industrielle Anlagen, Transporteinrichtungen, Prüfstände oder Messeinrichtungen, gegen Datenmanipulationen und Datenspionage sichern.

- 35 In einer vorteilhaften Ausführungsform kann die Hardwarekomponente einen Sicherheitscontroller mit einem integrierten Kryptoprozessor, einen nichtflüchtigen Speicher

und einen flüchtigen Speicher aufweisen. Dadurch lässt sich einerseits eine (zusätzliche) End-zu-End-Verschlüsselung der zwischen einem Backend-Rechnersystem bzw. einem anderen berechtigten Datensender bzw. Datenempfänger und der Hardwarekomponente (bzw. umgekehrt) übermittelten Daten erreichen, andererseits kann etwa mittels digitaler

5 Signaturen die Authentizität und Integrität der Daten sowohl durch die Hardwarekomponente selbst, als auch durch das Backend-Rechnersystem geprüft und sichergestellt werden. Indem in der Hardwarekomponente ein Sicherheitscontroller verbaut ist, können die Daten beispielsweise so verschlüsselt werden, dass nicht einmal der Hersteller des Kommunikationsmoduls oder das Backend-Rechnersystem die Daten entschlüsseln könnte.

10 Beispielsweise können die Daten für einen berechtigten Datenempfänger (etwa den Besitzer des technischen Systems oder einen anderen Berechtigten) verschlüsselt werden, der die verschlüsselten Daten von dem Backend-Rechnersystem abrufen und dann entschlüsseln kann.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung kann das technische System ein

15 autonomes, teilautonomes oder konventionelles Fahrzeug gemäß einer der Autonomiestufen 0 bis 5 sein. Die Einteilung der Autonomiestufen bezieht sich dabei auf die in diesem Bereich üblicherweise angewendete und wohlbekannte Norm SAE J3016, die der SAE International herausgegeben wird in der zum Zeitpunkt des ältesten Anmeldetags der gegenständlichen Patentfamilie geltenden Fassung. Insbesondere bei Fahrzeugen höherer Autonomiestufen

20 kann eine Datenmanipulation verheerende Folgen nach sich ziehen, sodass in diesem Bereich ein besonderer Bedarf an hochwertigen Sicherheitslösungen besteht.

In vorteilhafter Weise kann das technische System eine von einem Automatisierungssystem gesteuerte Maschinenanordnung, insbesondere ein Prüfstand sein. In zahlreichen industriellen Anwendungen, die von Automatisierungssystemen gesteuert werden, kommen

25 unterschiedliche Hardwarekomponenten zum Einsatz, die Sensoren und Aktuatoren aufweisen. Erfindungsgemäß können diese Hardwarekomponenten „ferngewartet“ werden, wobei einerseits die Firmware oder andere Anwendungssoftware sowie beispielsweise Parameterdaten von einem Backend-Rechnersystem aus aktualisiert werden können. Andererseits können auch Daten von der Hardwarekomponente zu dem Backend-

30 Rechnersystem übermittelt werden, etwa Telemetriedaten, mit denen beispielsweise Fehlfunktionen oder Wartungserfordernisse erkannt werden können.

Die Erfindung betrifft weiters ein Verfahren zur Übertragung von Gerätedaten einer Hardwarekomponente, die in ein internes Netz eines technischen Systems eingebunden ist, zu einem Backend-Rechnersystem, welches an ein paketvermitteltes Datennetz

35 angeschlossen ist, wobei das Verfahren durch die folgenden Schritte gekennzeichnet ist:

- Übermitteln der Gerätedaten von der Hardwarekomponente über das interne Netz zu dem gerätenahen Gateway,
- Übermitteln der Gerätedaten von dem gerätenahen Gateway über die Punkt-zu-Punkt-Verbindung zu dem netzwerknahen Gateway,

5 wobei von dem gerätenahen Gateway oder dem netzwerknahen Gateway die Gerätedaten in eine verschlüsselte Instanz der Gerätedaten umgewandelt wird, und

- Übermitteln der verschlüsselten Instanz der Gerätedaten von dem netzwerknahen Gateway über das paketvermittelte Datennetz zu dem Backend-Rechnersystem.

Gerätedaten können jegliche Daten sein, die von der Hardwarekomponente gemessen oder
 10 erstellt werden, bzw. in einem Gerätespeicher der Hardwarekomponente gespeichert sein können. Der Begriff „Gerätedaten“ umfasst sowohl die unverschlüsselten Gerätedaten, als auch Gerätedaten, die in verschlüsselter Form vorliegen, und die hierin auch als „verschlüsselte Instanz“ der Gerätedaten bezeichnet werden. Als „verschlüsselte Instanz“ der Gerätedaten werden somit Daten bezeichnet, aus denen sich mithilfe der jeweiligen
 15 kryptographischen Schlüssel und der entsprechenden kryptographischen Verfahren die unverschlüsselten Gerätedaten errechnen lassen. Gegebenenfalls können die Gerätedaten mehrmals überlagernd verschlüsselt werden. Beispielsweise kann die Hardwarekomponente die Gerätedaten gemäß einem eigenen Verschlüsselungsprotokoll verschlüsseln, das gegebenenfalls von der Funktionalität des Kommunikationsmoduls vollkommen getrennt und
 20 unabhängig sein kann. In dem Fall werden die Gerätedaten bereits als verschlüsselte Instanz an das gerätenahe Gateway des Kommunikationsmoduls übermittelt. Das Kommunikationsmodul erstellt dann eine weitere verschlüsselte Instanz dieser Gerätedaten.

In vorteilhafter Weise kann das Verfahren die folgenden Schritte aufweisen: Erstellen einer verschlüsselten Instanz der Gerätedaten unter Verwendung eines öffentlichen Schlüssels
 25 eines Empfängers der Daten, insbesondere des Backend-Rechnersystems, durch das gerätenahe Gateway, vorzugweise unter Verwendung des Gateway-Sicherheitsmoduls des gerätenahen Gateways, oder durch das netzwerknahen Gateway, vorzugweise unter Verwendung des Gateway-Sicherheitsmoduls des netzwerknahen Gateways. Die Verschlüsselung kann entweder von der Hardwarekomponente, von dem gerätenahen
 30 Gateway oder vom netzwerknahen Gateway durchgeführt werden, wobei die Sicherheit umso höher ist, je weniger Übermittlungsschritte unverschlüsselt erfolgen müssen.

Gegebenenfalls können auch zusätzliche Ver- und Entschlüsselungsschritte vorgesehen sein, beispielsweise kann die Übertragung zwischen dem gerätenahen Gateway und dem netzwerknahen Gateway über die Punkt-zu-Punkt-Verbindung durch eine zusätzliche
 35 Verschlüsselung geschützt sein, die zwischen dem gerätenahen Gateway und dem netzwerknahen Gateway (oder auch zwischen der Hardwarekomponente und dem

netzwerknahen Gateway) aufgebaut wird. Dies kann insbesondere dann vorteilhaft sein, wenn die Gerätedaten erst von dem netzwerknahen Gateway unter Verwendung des öffentlichen Schlüssels des Backend-Rechensystems verschlüsselt werden.

Die Begriffe „öffentlicher Schlüssel“ und „privater Schlüssel“ bezeichnen in bekannter Weise Schlüsselpaare gemäß asymmetrischer Kryptosysteme (sowohl im Zusammenhang mit Verschlüsselung/Entschlüsselung, als auch im Zusammenhang mit digitalen Signaturen).

In einer vorteilhaften Ausführungsform kann der Schritt des Übermittels der verschlüsselten Instanz über das paketvermittelte Datennetz das Übermitteln der verschlüsselten Instanz zu einem Broker umfasst, und gemäß einem Protokoll erfolgt, welches rein über Push-Mechanismen funktioniert. Dadurch lässt sich das netzwerknahe Gateway zusätzlich gegen Hackerangriffe schützen, da mit derartigen Protokollen jeglicher Inbound-Traffic (d.h. eine „von außen her“ über offene Ports eingeleitete Datenübertragung) unterbunden werden kann.

In vorteilhafter Weise kann das netzwerknahe Gateway die verschlüsselte Instanz der Gerätedaten vor der Übermittlung über das paketvermittelte Datennetz gemäß einem Netzwerk-Verschlüsselungsprotokoll verschlüsseln, wobei bewährte Protokolle verwendet werden können. Dies sperrt die Daten mit einer weiteren Sicherheitsschicht gegen einen unbefugten Zugriff. Diese Verschlüsselung kann vom Gateway-Sicherheitsmodul des netzwerknahen Gateways ausgeführt werden.

Gemäß einer weiteren vorteilhaften Ausführungsform kann die verschlüsselte Instanz der Gerätedaten Prüfdaten beinhalten, welche dem Backend-Rechensystem und/oder einem anderen berechtigten Datenempfänger eine Prüfung der Integrität und/oder Authentizität der Gerätedaten erlauben. Solche Prüfdaten können beispielsweise in an sich bekannter Weise Prüfsummen (Hashs) und digitale Signaturen verwenden, wobei diese Daten gegebenenfalls gemeinsam mit den Gerätedaten in einer Datenhülle verschlüsselt werden können.

In einem weiteren Aspekt betrifft die Erfindung ein Verfahren zum Speichern von Aktualisierungsdaten in einem Gerätespeicher einer Hardwarekomponente, die in ein internes Netz eines technischen Systems eingebunden ist, wobei die Aktualisierungsdaten für die Hardwarekomponente von einem Backend-Rechnersystem bereitgestellt werden und wobei das Verfahren die folgenden Schritte aufweist:

- Empfangen einer verschlüsselten Instanz der Aktualisierungsdaten durch das netzwerknahe Gateway über das paketvermittelte Datennetz von dem Backend-Rechnersystem,
- Übermitteln der Aktualisierungsdaten von dem netzwerknahen Gateway über die Punkt-zu-Punkt-Verbindung zu dem gerätenahen Gateway,

- Übermitteln der Aktualisierungsdaten an die Hardwarekomponente über das interne Netz,

wobei die verschlüsselte Instanz der Aktualisierungsdaten von dem gerätenahen Gateway oder dem netzwerknahen Gateway entschlüsselt wird, und

- 5 - Speichern der Aktualisierungsdaten in dem Gerätespeicher der Hardwarekomponente.

Dadurch lassen sich Aktualisierungsdaten, beispielsweise aktuelle Firmware oder Parameterdaten, in einer sicheren Weise von dem Backend-Rechnersystem zur Hardwarekomponente übermitteln. Gegebenenfalls kann wiederum zusätzlich eine weitere, 10 unabhängige Verschlüsselung der Gerätedaten zwischen einem berechtigten Datensender und der Hardwarekomponente vorgesehen sein.

Aktualisierungsdaten können jegliche Daten sein, die in einem Gerätespeicher der Hardwarekomponente gespeichert sein können. Der Begriff „Aktualisierungsdaten“ umfasst sowohl die unverschlüsselten Aktualisierungsdaten, als auch Aktualisierungsdaten, die in 15 verschlüsselter Form vorliegen, und die hierin auch als „verschlüsselte Instanz“ der Aktualisierungsdaten bezeichnet werden. Als „verschlüsselte Instanz“ der Aktualisierungsdaten werden somit jegliche Daten bezeichnet, aus denen sich mithilfe der jeweiligen kryptographischen Schlüssel und der entsprechenden kryptographischen Verfahren die unverschlüsselten Aktualisierungsdaten errechnen lassen.

20 Die Aktualisierungsdaten können entweder von einem berechtigten Datensender mit einem öffentlichen Schlüssel der Hardwarekomponente oder des gerätenahen Gateways oder des netzwerknahen Gateways verschlüsselt worden sein und bereits in verschlüsselter Form an das Backend-Rechnersystem übermittelt worden sein. In dem Fall agiert das Backend-Rechnersystem nur als Vermittler, der selbst keinen Zugriff auf die unverschlüsselten Daten 25 hat. Andererseits kann die verschlüsselte Instanz der Aktualisierungsdaten auch von dem Backend-Rechnersystem unter Verwendung eines öffentlichen Schlüssels der Hardwarekomponente, des gerätenahen Gateways, oder des netzwerknahen Gateways erstellt werden.

In vorteilhafter Weise kann das Verfahren die folgenden Schritte aufweisen: Entschlüsseln 30 der verschlüsselten Instanz der Aktualisierungsdaten durch das netzwerknahe Gateway, vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls des netzwerknahen Gateways oder durch das gerätenahe Gateway, vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls des gerätenahen Gateways.

Wenn die Hardwarekomponente mit einem Sicherheitscontroller versehen ist, kann 35 zusätzlich eine vollständige End-zu-End-Verschlüsselung umgesetzt werden. Andererseits

können die Daten auch zu Hardwarekomponenten ohne eigenen Sicherheitscontroller auf sehr sichere Weise übermittelt werden, da die unverschlüsselten Daten lediglich im internen Netz, also beispielsweise über ein internes Feldbussystem, wie etwa einen CAN-Bus, und gegebenenfalls über die Punkt-zu-Punkt-Verbindung übermittelt werden. Gegebenenfalls

5 kann die Übertragung zwischen dem netzwerknahe Gateway und dem gerätenahe Gateway über die Punkt-zu-Punkt-Verbindung wiederum durch eine zusätzliche Verschlüsselung geschützt sein, die zwischen dem gerätenahe Gateway (oder der Hardwarekomponente) und dem netzwerknahe Gateway aufgebaut wird. Die Entschlüsselung erfolgt vorzugsweise durch das gerätenahe Gateway oder die
10 Hardwarekomponente, die beide keine direkte Anbindung an ein öffentliches Netzwerk aufweisen. Das Verfahren mit gewissen Einschränkungen auch mit einem vereinfachten Kommunikationsmodul ausgeführt werden, bei dem das gerätenahe Gateway über kein eigenes Gateway-Sicherheitsmodul verfügt.

In vorteilhafter Weise können die Aktualisierungsdaten eine Firmware, eine
15 Anwendungssoftware und/oder Parameterdaten der Hardwarekomponente umfassen.

In einer weiteren vorteilhaften Ausführungsform kann der Schritt des Empfangens das Abrufen der verschlüsselten Instanz der Aktualisierungsdaten von einem Broker umfassen und gemäß einem Protokoll erfolgen, welches rein über Push-Mechanismen funktioniert.

Erfindungsgemäß kann gemäß einer weiteren Ausführungsform vorgesehen sein, dass die
20 verschlüsselte Instanz der Aktualisierungsdaten Prüfdaten beinhaltet, welche dem Gateway-Sicherheitsmodul des gerätenahe Gateways, und/oder dem Gateway-Sicherheitsmodul des netzwerknahe Gateways und/oder dem Sicherheitscontroller der Hardwarekomponente eine Prüfung der Integrität und/oder Authentizität der Aktualisierungsdaten erlauben. Mithilfe einer Prüfung der Authentizität und Integrität der erhaltenen Instanz der

25 Aktualisierungsdaten, beispielsweise mittels digitaler Signaturen gemäß dem vom Sicherheitscontroller bzw. Gateway-Sicherheitsmodul verwendeten kryptographischen System kann sichergestellt werden, dass z.B. der Austausch der Firmware (der üblicherweise durch sogenanntes "Flashen" des entsprechenden Gerätespeichers erfolgt, nur dann durchgeführt wird, wenn die Vertrauenswürdigkeit der Daten vom
30 Sicherheitscontroller (bzw. Gateway-Sicherheitsmodul) sichergestellt ist.

Definitionen:

Als „**technisches System**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Vorrichtung bezeichnet, welche zumindest ein internes Netz und zumindest eine Hardwarekomponente aufweist, die zu einer Kommunikation über dieses interne Netz
35 befähigt ist.

Als „**internes Netz**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine vorzugsweise auf das technische System begrenzte Kommunikations-Infrastruktur des technischen Systems bezeichnet, die zum Datenaustausch zwischen Hardwarekomponenten geeignet ist. Je nach Art des technischen Systems kann das interne Netz gemäß einem

5 routingfähigen Protokoll oder einem nicht routingfähigen Protokoll funktionieren.

Als „**Hardwarekomponente**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine technische Einheit angesehen, die zumindest einen Prozessor oder Microcontroller und eine Speichereinheit aufweist, und die zu einer Kommunikation über das jeweilige interne Netz befähigt ist.

10 Als „**Firmware**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine in einem Speicher der Hardwarekomponente gespeicherte Programmlogik bezeichnet, welche für den Betrieb der Hardwarekomponente erforderlich ist. Je nach Komplexität der Hardwarekomponente kann die Firmware den Betrieb der Hardwarekomponente vollständig definieren, gegebenenfalls unter Verwendung veränderbarer Parameter, oder sie kann der

15 Hardwarekomponente erlauben, Anwendungsprogramme auszuführen.

Als „**Anwendungssoftware**“ der Hardwarekomponente wird im Zusammenhang mit der gegenständlichen Offenbarung allgemein eine von der Hardwarekomponente ausführbare Programmlogik bezeichnet.

20 Als „**Parameterdaten**“ der Hardwarekomponente werden im Zusammenhang mit der gegenständlichen Offenbarung Daten bezeichnet, die Werte repräsentieren, welche den Betrieb der Hardwarekomponente beeinflussen.

Als „**Backend-Rechnersystem**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Computerinfrastruktur bezeichnet, in welcher die Hardwarekomponente betreffende Daten gespeichert sind. Das Backend-Rechnersystem ist in der Lage über das

25 paketvermittelte Datennetz zu kommunizieren, um Daten über dieses paketvermittelte Datennetz zu dem technischen System, bzw. über das Kommunikationsmodul des technischen Systems zu der Hardwarekomponente zu senden, und Daten von dieser Hardwarekomponente über das Kommunikationsmodul des technischen Systems zu empfangen.

30 Als „**Sicherheitscontroller**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Einheit bezeichnet, die vorzugsweise als Hardware, insbesondere als ein Mikrochip ausgebildet sein kann, wobei der Sicherheitscontroller eine Hardwarekomponente um grundlegende Sicherheitsfunktionen erweitert. Die grundlegenden Sicherheitsfunktionen betreffen insbesondere die Erzeugung kryptographischer Schlüssel, deren sichere

35 Verwahrung (eine Extraktion von privaten Schlüsseln soll verhindert werden), die Ver- und Entschlüsselung von Daten und die Handhabung von digitalen Signaturen. Der

Sicherheitscontroller enthält zumindest eine eindeutige Kennung, die zur Identifizierung der Hardwarekomponente genutzt werden kann. Aus Gründen der Größenoptimierung ist es bevorzugt, den Sicherheitscontroller als einen einzigen Microchip auszubilden, der in die jeweilige Hardwareeinheit eingebaut wird. Falls die Baugröße der Hardwareeinheit dies zulässt, ist es jedoch auch möglich, ein System mit einer Kartenschnittstelle und einer Prozessorchipkarte zu verwenden, wie dies für das untenstehend definierte Gateway-Sicherheitsmodul beschrieben ist.

Ein Sicherheitscontroller umfasst vorzugsweise zumindest einen Kryptoprozessor. Der Kryptoprozessor kann vorzugsweise einen Zufallszahlengenerator, zumindest einen Schlüsselgenerator (z.B. gemäß RSA), zumindest einen Hashgenerator (z.B. gemäß eines Secure Hash Algorithmus – SHA), sowie zumindest eine Verschlüsselungs-/Entschlüsselungs-/Signatureinheit aufweisen. Weiters weist der Sicherheitscontroller üblicherweise einen nichtflüchtigen und/oder einen flüchtigen Speicher auf. Im nichtflüchtigen Speicher können beispielsweise ein Endorsement-Key und ein Storage-Root-Key gespeichert sein. Als Endorsement-Key wird ein dem Sicherheitscontroller zugewiesener kryptographischer Schlüssel bezeichnet, der vorzugsweise bereits bei der Herstellung im nichtflüchtigen Speicher vorzugsweise unveränderbar abgelegt wird. Als Storage-Root-Key wird ein im geschützten, nicht flüchtigen Speicher abgelegter kryptographischer Schlüssel bezeichnet, der jedoch durch spezielle Funktionen veränderbar ist, beispielsweise wenn der Sicherheitscontroller von einem neuen Benutzer in Besitz genommen wird. Aus Sicherheitsgründen dürfen der Endorsement-Key und der Storage-Root-Key den sicheren Speicher nicht verlassen können. Deswegen muss der Kryptoprozessor diese Keys verwenden können um die kryptographische Operation ausführen zu können. Im flüchtigen Speicher des Sicherheitscontrollers können beispielsweise Plattformkonfigurationsregister, Attestation-Identity-Keys und andere gespeicherte Schlüssel abgelegt sein.

Zu Beispielen von Sicherheitscontrollern zählen Trusted-Platform-Module (TPM) gemäß der TCG-Spezifikation der Trusted Computing Group. Es wird im Zusammenhang mit der gegenständlichen Offenbarung vorausgesetzt, dass der Fachmann detaillierte Kenntnisse über die TCG-Spezifikation in der zum Zeitpunkt des ältesten Anmeldetags der gegenständlichen Patentfamilie geltenden Fassung hat.

Als „**Kryptoprozessor**“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Mikroprozessor bezeichnet, der kryptographische Grundfunktionen, insbesondere die sichere Datenkommunikation, die Ver- und Entschlüsselung, die Authentisierung und/oder die Verwaltung von Kryptologie-Schlüsseln in sich vereinigt.

Als „**Gateway-Sicherheitsmodul**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Hardwareeinheit bezeichnet, die ein Gateway um grundlegende

Sicherheitsfunktionen erweitert. Das Gateway-Sicherheitsmodul kann ähnlich aufgebaut sein, wie ein Sicherheitscontroller, oder sogar baugleich sein. Das Gateway-Sicherheitsmodul kann eine Kartenschnittstelle aufweisen, in die eine Prozessorchipkarte eingesetzt werden kann, die einen wesentlichen Teil des Gateway-Sicherheitsmoduls enthält, und in der insbesondere die grundlegenden Sicherheitsfunktionen kodiert sein können. Dadurch lässt sich etwa bei einer Serienfertigung des Gateway-Sicherheitsmoduls durch Kombination mit der jeweiligen Prozessorchipkarte ein hardwaretechnisch einzigartiges Gateway-Sicherheitsmodul erstellen.

Es ist zu beachten, dass die Unterscheidung zwischen den Begriffen „Gateway-Sicherheitsmodul“ und „Sicherheitscontroller“ weder eine funktionelle, noch eine hardwaretechnische Verschiedenheit impliziert, sondern lediglich deren Zuordnung (einmal zu einer Hardwareeinheit, das andere Mal zu einem Gateway) definiert. Insbesondere können Gateway-Sicherheitsmodul und Sicherheitscontroller funktionell und/oder hardwaretechnisch identisch oder unterschiedlich ausgebildet sein. Auch können mehrere Gateway-Sicherheitsmodule unterschiedlicher Gateways jeweils als unterschiedliche Hardware ausgebildet sein und auch die Sicherheitscontroller unterschiedlicher Hardwareeinheiten müssen nicht identisch sein, sondern können eine unterschiedliche Bauart aufweisen. Alle Merkmale, die hierin in Zusammenhang mit dem Sicherheitscontroller beschrieben werden, können somit auch auf das Gateway-Sicherheitsmodul angewendet werden und vice versa, sofern nichts anderes ausdrücklich bestimmt ist.

Als „**Prozessorchipkarte**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine in eine Kartenschnittstelle einsteck- bzw. einsetzbare Karte – üblicherweise aus Kunststoff – bezeichnet, die mit einem eingebauten integrierten Schaltkreis (Chip) versehen ist. Der integrierte Schaltkreis umfasst eine Hardware-Logik, zumindest einen Speicher und zumindest einen Mikroprozessor. Prozessorchipkarten werden durch spezielle Kartenlesegeräte angesteuert, die im Zusammenhang mit der gegenständlichen Offenbarung als „Kartenschnittstelle“ bezeichnet werden. Prozessorchipkarten werden im allgemeinen Sprachgebrauch oft auch als „Smartcard“ oder „Integrated Circuit Card (ICC)“ bezeichnet. Die Prozessorchipkarte weist häufig ein Scheckkartenformat auf, sie kann jedoch auch andere Formate aufweisen, wie etwa ein SIM-Karten-Format (z.B. Standard-SIM, Mini-SIM, Micro-SIM, Nano-SIM). Gegebenenfalls kann die Prozessorchipkarte auch in Form einer Embedded-SIM direkt im entsprechenden Gerät verbaut und nicht auswechselbar sein.

Als „**Hardware-Sicherheitsmodul**“ (im Englischen auch als „Hardware Security Module – HSM“ bezeichnet) wird im Zusammenhang mit der gegenständlichen Offenbarung allgemein ein internes oder externes Peripheriegerät bezeichnet, das in einer Computerinfrastruktur (wie etwa dem hierin beschriebenen Backend-Rechnersystem) für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen dient. Dies ermöglicht zum

Beispiel, die Vertrauenswürdigkeit und die Integrität von Daten und den damit verbundenen Informationen IT-Systemen sicherzustellen.

Als „**kryptographischer Schlüssel**“ wird im Zusammenhang mit der gegenständlichen Offenbarung allgemein eine Information bezeichnet, die einen kryptographischen Algorithmus parametrisiert und ihn steuert. Insbesondere wird zwischen Entschlüsselungsschlüsseln und Verschlüsselungsschlüsseln unterschieden, die jeweils miteinander verknüpft sind. Bei symmetrischen Verschlüsselungssystemen sind der Entschlüsselungsschlüssel und der Verschlüsselungsschlüssel identisch. Asymmetrische Verschlüsselungssystemen hingegen verwenden Schlüsselpaare, die aus einem öffentlichen Schlüssel („Public Key“) und einem privaten Schlüssel („Private Key“) bestehen. Asymmetrische kryptographische Schlüssel können nicht nur zum Ver- und Entschlüsseln, sondern auch zum digitalen Signieren verwendet werden.

Der Begriff „**kryptographisches System**“ oder „Kryptosystem“ wird im Zusammenhang mit der gegenständlichen Offenbarung generisch sowohl für Systeme zur Ver- und Entschlüsselung, für Schlüsselaustauschverfahren und für Verfahren zur digitalen Signatur verwendet. Ein bekanntes Beispiel für ein kryptographisches System ist das RSA-Kryptosystem, das auf einer Einwegfunktion auf Primzahlbasis funktioniert. Weitere Beispiele für kryptographische Systeme basieren auf der Ellyptischen-Kurven-Kryptographie (Elliptic Curve Cryptography - ECC). Zu Beispielen hierfür zählen Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Integrated Encryption Scheme (ECIES), auch Integrated Encryption Scheme (IES) genannt, Elliptic Curve Digital Signature Algorithm (ECDSA) und ECMQV, ein von Menezes, Qu und Vanstone vorgeschlagenes Protokoll zur Schlüsselvereinbarung.

Als „**Netzwerk-Verschlüsselungsprotokoll**“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Netzwerkprotokoll bezeichnet, das die verschlüsselte Datenübertragung über ein Rechnernetz garantieren. Ein solches Netzwerk-Verschlüsselungsprotokoll kann beispielsweise aus einem Schlüsselaustauschprotokoll und symmetrischen Verfahren bestehen, die die Vertraulichkeit und Integrität der übertragenen Nachrichten sicherstellen. Zu Beispielen von Standards für Netzwerk-Verschlüsselungsprotokolle zählen Transport-Layer-Security (TLS), Secure Shell (SSH), IPsec, WPA2.

Als „**Gateway**“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Komponente bezeichnet, die eine Verbindung zwischen zwei Kommunikationssystemen und insbesondere zwischen zwei Netzwerksystemen unterschiedlicher Protokolle (die gleichen oder unterschiedlichen Schichten im OSI-Modell zuzuordnen sind) herstellt.

Als „**Punkt-zu-Punkt-Verbindung**“ wird im Zusammenhang mit der gegenständlichen Offenbarung allgemein ein direkter Verbindungsweg ohne Zwischenstationen verstanden.

Darunter fällt beispielsweise die Kommunikation in den unteren Netzwerkschichten 1–3 im OSI-Modell. Vorzugsweise wird die Kommunikation über die Punkt-zu-Punkt-Verbindung gemäß einem nicht-routingfähigen Protokoll ausgeführt. Ein Beispiel für solch eine Verbindung ist eine Direktverbindung über ein seriellcs Bussystem, beispielsweise einen Universal Serial Bus (USB).

Als „**Verfahren, das rein über Push-Mechanismen funktioniert**“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Verfahren bezeichnet, bei dem die Kommunikation immer über einen zwischengeschalteten Broker gemäß einem Publisher-Subscriber-Modell vermittelt wird. Dabei ist es insbesondere nicht erforderlich, eine direkte End-zu-End-Verbindung herzustellen. Beispiele für solche Verfahren bieten Kommunikationsverfahren, die gemäß der MQTT-Spezifikation („Message Queuing Telemetry Transport“) aufgebaut sind, insbesondere gemäß der MQTT-Spezifikation in der zum Zeitpunkt des ältesten Anmeldetags der gegenständlichen Patentfamilie geltenden Fassung.

Als „**Broker**“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Server bezeichnet, der die Nachrichten verwaltet, die gemäß einem Publisher-Subscriber-Modell, bzw. dem Verfahren, das rein über Push-Mechanismen funktioniert, bereitgestellt bzw. abgerufen werden.

Die gegenständliche Erfindung wird nachfolgend unter Bezugnahme auf die Figuren 1 bis 3 näher erläutert, die beispielhaft, schematisch und nicht einschränkend vorteilhafte Ausgestaltungen der Erfindung zeigen. Dabei zeigt

Fig. 1 eine schematische Darstellung der an einer Datenübertragung zwischen einem Backend-Server und einer Hardwarekomponente gemäß der Erfindung beteiligten Komponenten in einer Blockdarstellung,

Fig. 2 eine vereinfachte schematische Darstellung des in Fig. 1 dargestellten Datenübertragungsweges und

Fig. 3 eine schematische Blockdarstellung eines gesicherten Kommunikationssystems zwischen mehreren Backend-Rechnersystemen und mehreren technischen Systemen.

Fig. 1 zeigt eine in einer schematischen Darstellung die wesentlichen Entitäten, die im Umfeld der erfindungsgemäßen Verfahren und Vorrichtungen vorgesehen sind. Ein technisches System 4 weist eine Kommunikationsmodul 1, ein internes Netz 3 und eine Anzahl an Hardwarekomponenten 2, 2' auf, die über das interne Netz 3 miteinander und mit dem Kommunikationsmodul 1 verbunden sind. Jede der in Fig. 1 dargestellten Hardwarekomponenten 2, 2' weist einen Sicherheitscontroller 14, 14' auf, es können jedoch

in dem technischen System 4 auch herkömmliche Hardwarekomponenten an das interne Netz 3 angeschlossen sein, die über keinen Sicherheitscontroller verfügen.

Das Kommunikationsmodul 1 umfasst ein gerätenahes Gateway 7 und ein netzwerknahe Gateway 8, die mittels einer Punkt-zu-Punkt-Verbindung 9 miteinander verbunden sind. Das gerätenahe Gateway 7 stellt eine Kommunikationsverbindung zwischen dem internen Netz 3 und der Punkt-zu-Punkt-Verbindung 9 her und das netzwerknahe Gateway 8 stellt eine Kommunikationsverbindung zwischen der Punkt-zu-Punkt-Verbindung 9 und einem paketvermittelten Datennetz 6 her. Das paketvermittelte Datennetz kann ein beliebiges Nah- oder Weitverkehrsnetz sein, insbesondere das Internet.

Die Verbindung über das paketvermittelte Datennetz 6 dient dem technischen System 4 insbesondere dazu, Daten mit einer als Backend-Rechnersystem 5 bezeichneten Rechneranordnung auszutauschen. Das Backend-Rechnersystem 5 weist eine als „Datencenter“ 21 bezeichnete Computerinfrastruktur auf, wobei es sich beispielsweise um ein serverbasierendes Computernetz eines Herstellers oder Anbieters der Hardwarekomponenten 2, 2' handeln kann. Das Backend-Rechnersystem 5 umfasst weiters eine oder mehrere Datenbanken, in denen die Hardwarekomponenten 2, 2' betreffende Daten gespeichert sind. In Fig. 1 sind ein Software-Repository 15 und ein Firmware-Repository 16 symbolisch dargestellt, in denen Software bzw. Firmware für Hardwarekomponenten verschlüsselt gespeichert sind.

Die Kommunikation zwischen dem Backend-Rechnersystem 5 und dem netzwerknahen Gateway 8 des Kommunikationsmoduls 1 des technischen Systems 4 wird über einen Broker 20 geführt und gemäß einem Protokoll durchgeführt, das rein auf Push-Mechanismen basiert. Solche Protokolle, zum Beispiel gemäß der MQTT-Spezifikation, erlauben auf Seiten des Kommunikationsmoduls 1 die Umsetzung von Firewall-Richtlinien, die Incoming Traffic sperren. Eine Manipulation des Systems über Webdienste und ein Aufbau einer End-zu-End-Verbindung bis in das Kommunikationsmodul 1 kann somit ausgeschlossen werden. Bei Protokollen, die rein über Push-Mechanismen funktionieren, wie etwa gemäß dem MQTT-Protokoll, wird bekanntermaßen keine direkte End-zu-End-Verbindung hergestellt, sondern die Kommunikation wird immer über den zwischengeschalteten Broker 20 vermittelt, der Daten von einem „Publisher“ erhält, und sie für einen oder mehrere „Subscriber“ bereitstellt, wobei vorzugsweise eine zertifikatsgestützte Identifikation von Publisher und/oder Subscriber und gegebenenfalls eine Verschlüsselung der Daten vorgesehen sein kann. Jeder Endpunkt „öffnet“ die Kommunikation zum Broker 20 von sich aus, und diese wird nicht „von außen“ eingeleitet. Da beide Kommunikationspartner sowohl als Subscriber, als auch als Publisher agieren können, ist es möglich, Daten in beiden Richtungen auszutauschen, ohne dass dazu ein potentiell angreifbarer Webdienst eingerichtet werden muss. Vom Kommunikationsmodul 1 (d.h. vom netzwerknahen Gateway 7) aus wird dazu in definierten Abständen eine

Verbindung zum Broker 20 hergestellt und es werden entweder Daten für einen Abruf durch berechnete Dritte (insbesondere vom Backend-Rechnersystem 5) bereitgestellt (d.h. das Kommunikationsmodul 1 agiert als Publisher) oder es werden Daten von Dritten abgerufen (d.h. das Kommunikationsmodul 1 agiert als Subscriber). In analoger Weise kann das Backend-Rechnersystem 5 sowohl als Publisher, als auch als Subscriber agieren um Daten von dem Kommunikationsmodul 1 (bzw. von einer „dahinterliegenden“ Hardwarekomponente 2) zu erhalten oder um Daten an das Kommunikationsmodul 1 (bzw. an die Hardwarekomponente 2) zu senden.

Die Sicherheitscontroller 14, 14' der Hardwarekomponenten 2, 2' können beispielsweise als integrierte Schaltung bzw. Hardwarechip ausgebildet sein, wodurch es möglich ist, auch verhältnismäßig kleine Hardwarekomponenten mit einem solchen Sicherheitscontroller 14, 14' auszustatten. Die Sicherheitscontroller 14, 14' erweitert die Hardwarekomponenten 2, 2' um grundlegende Sicherheitsfunktionen gemäß zumindest einem kryptographischen System. Die Sicherheitscontroller können beispielsweise einer Spezifikation der Trusted Computing Group (TCG) entsprechen und als „Trusted Platform Module“ (TPM) ausgebildet sein.

Das gerätenahe Gateway 7 weist ein Gateway-Sicherheitsmodul 10 auf, welches eine Kartenschnittstelle 13 für eine Prozessorchipkarte 12 umfasst und das netzwerknahe Gateway 8 weist ein weiteres Gateway-Sicherheitsmodul 10' mit einer Kartenschnittstelle 13' und einer Prozessorchipkarte 12' auf. Gegebenenfalls kann zur Vereinfachung des Hardwareaufwandes auf das Gateway-Sicherheitsmodul 10 des gerätenahen Gateways 7 verzichtet werden, wobei dann die entsprechenden Ver- und Entschlüsselungsfunktionen von den Sicherheitsmodulen 14, 14' der Hardwarekomponenten 2, 2' und/oder dem Gateway-Sicherheitsmodul 10' des netzwerknahen Gateways 8 übernommen werden.

Die Sicherheitscontroller 14, 14' der Hardwarekomponenten 2, 2' und die Gateway-Sicherheitsmodule 10, 10' der Gateways 7, 8 enthalten jeweils eine eindeutige Kennung, die zur Identifizierung der entsprechenden Hardwarekomponente bzw. des jeweiligen Gateways dient. Entsprechende kryptographische Systeme, die von den Sicherheitscontrollern und Gateway-Sicherheitsmodulen verwendet werden können, sind im Fachbereich bekannt.

Die Sicherheitsfunktionen im Backend-Rechnersystem 5, insbesondere die Verwaltung und Verteilung kryptographischer Schlüssel, die Verschlüsselung, Entschlüsselung und digitale Signierung können von einem Hardware-Sicherheitsmodul 11 verwaltet werden. Das Hardware-Sicherheitsmodul 11 kann auch über die öffentlichen Schlüssel der Sicherheitscontroller 14, 14' und Gateway-Sicherheitsmodule 10, 10' im System verfügen. Dies ist jedoch keine zwingende Voraussetzung, da das Backend-Rechnersystem 5 auch Daten empfangen und speichern kann, die es selbst nicht entschlüsseln darf, beispielsweise wenn diese (von der Hardwarekomponente gesammelten) Daten für einen Dritten (der hierin

als berechtigter Datenempfänger bezeichnet wird) bestimmt und mit dessen öffentlichem Schlüssel verschlüsselt sind. Andererseits können von dem Backend-Rechensystem 5 gehandhabte Aktualisierungsdaten von einem Dritten stammen (der hierin auch als berechtigter Datensender bezeichnet wird) und von diesem bereits verschlüsselt wurden.

- 5 Die für die kryptographischen Verfahren vorgesehenen Einheiten, insbesondere die Gateway-Sicherheitsmodule 10, die Sicherheitscontroller 14 und die Hardware-Sicherheitsmodule 11 können gegebenenfalls mehrere unterschiedliche kryptographische Systeme unterstützen.

Die oben beschriebene Anordnung erlaubt eine überaus wirkungsvolle und starke Sicherung
10 von Kommunikationsverbindungen zwischen den Hardwarekomponenten 2, 2' und dem Backend-Rechnersystem 5 (bzw. einem Dritten berechtigten Datenempfänger und/oder Datensender). Eine beispielhafte Kommunikation von Daten von der Hardwareeinheit 2 zu dem Backend-Rechnersystem 5 und von dem Backend-Rechnersystem 5 zu der Hardwareeinheit 2 wird im Folgenden unter Bezugnahme auf die schematische Darstellung
15 in Fig. 2 beschrieben.

Das Gateway-Sicherheitsmodul 10 des gerätenahen Gateways 7, das Gateway-Sicherheitsmodul 10' des netzwerknahen Gateways 8, das Hardware-Sicherheitsmodul 11 des Backend-Rechnersystems 5 und gegebenenfalls der Sicherheitscontroller 14 des Hardwaresystems 2 sind in der Lage, ihre Sicherheitsfunktionalitäten gemäß zumindest
20 einem gemeinsamen kryptographischen System abzuarbeiten.

Um Daten von der Hardwarekomponente 2 zu dem Backend-Rechensystem 5 zu übermitteln, wird zuerst eine Initialisierung durchgeführt, wobei der Sicherheitscontroller 14, die beiden Gateway-Sicherheitsmodule 10, 10' und das Hardware-Sicherheitsmodul 11 (bzw. ein entsprechendes Sicherheitsmodul eines Dritten, der als Datenempfänger oder -sender
25 agieren soll) jeweils Schlüsselpaare (bestehend aus einem öffentlichen und einem privaten Schlüssel) erzeugen und die öffentlichen Schlüssel untereinander in gesicherter Weise austauschen. Diese Initialisierungsphase kann bei der „Inbetriebnahme“ bzw.

Personalisierung des Kommunikationsmoduls 1 gegebenenfalls bereits vor der Auslieferung des Kommunikationsmoduls 1 durch den Hersteller erfolgen. Das Kommunikationsmodul 1
30 ist nach dieser Initialisierungsphase unmittelbar einsatzbereit und verfügt über alle Daten und Voraussetzungen, die zum Ausführen der erfindungsgemäßen Verfahren erforderlich sind. Üblicherweise sind die Kommunikationswege, für die das Kommunikationsmodul 1 vorgesehen sind, nach der Initialisierungsphase festgelegt und ändern sich in weiterer Folge nicht, bzw. können nur durch ein Löschen und ein neuerliches Initialisieren geändert werden.

35 Daten, die während des Betriebs des technischen Systems 4 über das interne Netz 3 (z.B. einen CAN-Bus eines Fahrzeugs) übermittelt werden, können vom gerätenahen Gateway 7

erfasst, von dem gerätenahen Gateway 7 oder dem netzwerknahe Gateway 8 entsprechend den erfindungsgemäßen Verfahren verschlüsselt und zu dem Backend-Rechnersystem 5 übermittelt werden. In diesem Fall ist im Grunde das gerätenahe Gateway 7 (bzw. das netzwerknahe Gateway) als Endpunkt der gesicherten Übertragungskette anzusehen. Das Verfahren kann dabei in Verbindung mit Hardwarekomponenten ausgeführt werden, die keinen eigenen Sicherheitscontroller 14 haben. Dieses Verfahren wird in der untenstehenden Beschreibung als Variante A bezeichnet. Der Fall, bei dem das netzwerknahe Gateway die Verschlüsselung vornimmt, wird in der Fig. als Variante A' bezeichnet. Auf eine detaillierte Beschreibung dieser Variante A' wird jedoch der Übersichtlichkeit halber verzichtet, da die Umsetzung dieser Variante im Können des Durchschnittsfachmanns, der Kenntnis von der gegenständlichen Offenbarung hat, liegt.

Zusätzlich ist es gemäß der Erfindung auch möglich, eine gesicherte Verbindung von der Hardwarekomponente 2 zu dem Backend-Rechnersystem 5 (bzw. zu einem diesem Backend-Rechnersystem 5 nachgelagerten dritten Datenempfänger bzw. Datensender) umzusetzen, sofern die entsprechende Hardwarekomponente 2 über einen entsprechenden Sicherheitscontroller 14 verfügt. Diese Möglichkeit wird in der untenstehenden Beschreibung als Variante B bezeichnet.

Gemäß Variante A erzeugt das gerätenahe Gateway 7 unter Verwendung des Gateway-Sicherheitsmoduls 10 einen geheimen Einmal-Schlüssel und verwendet eine authentifizierte Verschlüsselungsfunktion, um die zu übermittelnden Daten mit dem Einmal-Schlüssel zu verschlüsseln. Dann erstellt das Gateway-Sicherheitsmodul 10 einen Parametersatz für einen One-Pass-Schlüsselaustausch, wobei diese Parameter einen öffentlichen Schlüssel des Backend-Rechnersystems 5 (bzw. einer darin enthaltenen Einheit) umfassen. Das Gateway-Sicherheitsmodul 10 verschlüsselt den Einmal-Schlüssel unter Verwendung eines Key-Wrapping-Schemas und erzeugt ein Datenhüllpaket („Data-Envelope“), das alle diese Daten enthält.

Gemäß Variante B kann bereits von dem Sicherheitscontroller 14 der Hardwarekomponente 2 eine unabhängige Verschlüsselung der Gerätedaten durchgeführt werden, wobei die entsprechenden Gerätedaten über das interne Netz 3 bereits in einer gesicherten Weise von der Hardwarekomponente 2 zu der gerätenahen Gateway 7 übermittelt werden (Schritt 100). Die von der Hardwarekomponente 2 angewendete Verschlüsselung kann unabhängig von dem kryptographischen System sein, das von dem Kommunikationsmodul 1 angewendet wird. In dem Fall wendet das Kommunikationsmodul 1 die erfindungsgemäße Verschlüsselung auf bereits verschlüsselte Gerätedaten an.

Das gerätenahe Gateway 7 übermittelt das Datenhüllpaket über die (vorzugsweise nicht routingfähige) Punkt-zu-Punkt-Verbindung 9 an das netzwerknahe Gateway 8 (Schritt 101).

Das netzwerknahe Gateway 8 agiert als Publisher und baut eine gemäß einem Netzwerk-Verschlüsselungsprotokoll (z.B. TLS) gesicherte Verbindung mit dem Broker 20 auf, wobei sowohl eine Client-Authentifizierung, als auch eine Server-Authentifizierung erfolgt. Dann überträgt das netzwerknahe Gateway als Publisher das Datenhüllpaket an einen Kanal
 5 (dieser wird auch als Thema oder Topic bezeichnet, z.B. MQTT-Topic) des Brokers (Schritt 102).

Auch das Backend-Rechnersystem 5 baut eine gemäß einem Netzwerk-Verschlüsselungsprotokoll (z.B. TLS) gesicherte Verbindung mit dem Broker 20 auf, agiert als Subscriber des Kanals, und empfängt das Datenhüllpaket (Schritt 103). Gegebenenfalls
 10 übermittelt das Backend-Rechnersystem 5 das Datenhüllpaket an einen Empfänger im Backend-Rechnersystem 5.

Unabhängig von der Richtung der Datenübertragung kann der Verbindungsaufbau mit dem Broker 20 sowohl vom jeweiligen Publisher, als auch vom jeweiligen Subscriber jeweils gemäß einem definierten Zeitschema und/oder Anlassbezogen erfolgen, wobei für jeden
 15 Publisher/Subscriber entsprechende Rollen definiert sein können.

Am Zielpunkt im Backend-Rechnersystem 5 werden die relevanten Daten aus dem Datenhüllpaket extrahiert, der Key-Wrapping-Schlüssel wird unter Verwendung des One-Pass-Schlüsselaustausch-Schemas errechnet und der geheime Schlüssel wird unter Verwendung des Key-Wrapping-Schlüssels entschlüsselt. Dann werden die Integrität und die
 20 Authentizität der Daten verifiziert und die Daten selbst entschlüsselt. Das Backend-Rechnersystem 5 kann auf diese Weise entweder die unverschlüsselten Gerätedaten erzeugen, oder die Gerätedaten in der von Hardwarekomponente 2 verschlüsselten Form.

In der umgekehrten Richtung kann die Kommunikation von Daten von dem Backend-Rechnersystem 5 zu der Hardwarekomponente 2 in einer beispielhaften Ausführungsform gemäß der im Folgenden beschriebenen Schritten ausgeführt werden. Auch bei dieser Datenübermittlung werden zwei Varianten beschrieben, die hierin als Variante C und Variante C' bezeichnet werden. Bei Variante C erstreckt sich die Verschlüsselung von dem Backend-Rechnersystem 5 zu dem gerätenahen Gateway 7 und bei Variante C' erstreckt sich die gesicherte Verbindung von dem Backend-Rechnersystem 5 zu dem netzwerknahen
 30 Gateway 8. Zusätzlich können die gemäß dem erfindungsgemäßen Verfahren übermittelten Daten für die Hardwarekomponente 2 gemäß einem eigenen kryptographischen System verschlüsselt sein (wobei solche eine Verschlüsselung entweder vom Backend-Rechnersystem 5 oder von einem berechtigten Datensender erstellt wird). Eine solche zusätzliche Verschlüsselung ist in Fig. 2 als Variante D eingezeichnet.

35 Die betreffende Einheit im Backend-Rechnersystem, beispielsweise das Software-Repository 15 oder das Firmware-Repository 16, in der die Daten für die Übermittlung abgelegt sind,

verwendet den privaten Schlüssel in dem entsprechenden Hardware-Sicherheitsmodul 11, um eine digitale Signatur für die zu übermittelnden Daten zu erstellen, die zu der Hardwarekomponente 2 übermittelt werden sollen. Die Daten können beispielsweise eine Anwendungssoftware, eine Firmware oder Parameterdaten für die Hardwarekomponente 2 umfassen. Gegebenenfalls können diese Daten bereits verschlüsselt in dem Backend-Rechnersystem 5 hinterlegt worden sein, wobei die Verschlüsselung beispielsweise von einem Hersteller der Hardwarekomponente vorgenommen worden sein kann, der aber nicht der Besitzer und Verwalter des Backend-Rechnersystems ist. In dem Fall kann das Backend-Rechnersystem 5 in Verbindung mit dem Kommunikationsmodul 1 lediglich eine stark gesicherte Übertragungsfunktionalität für Dritte anbieten, bei der die ohnehin vorgesehene Verschlüsselung durch eine weitere, hochsichere Verschlüsselung „überlagert“ wird.

Die Daten, einschließlich der digitalen Signatur(en), werden im Backend-Rechnersystem 5 verschlüsselt, vorzugsweise noch bevor sie die betreffende Einheit verlassen. Unter Verwendung des Hardware-Sicherheitsmoduls 11 wird ein geheimer Einmal-Schlüssel erstellt und es wird eine authentifizierte Verschlüsselungsfunktion verwendet, um die zu signierten Daten mit dem Einmal-Schlüssel zu verschlüsseln. Dann wird in dem Hardware-Sicherheitsmodul 11 ein Parametersatz für einen One-Pass-Schlüsselaustausch erstellt, wobei diese Parameter entweder den öffentlichen Schlüssel des gerätenahen Gateways 7 (Variante C) oder den öffentlichen Schlüssel des netzwerknahe Gateways 8 (Variante C') umfassen. Der Einmal-Schlüssel wird unter Verwendung eines Key-Wrapping-Schemas verschlüsselt und es wird ein Datenhüllpaket („Data-Envelope“) erzeugt, das alle diese Daten enthält. Die obigen Schritte können alternativ nicht von dem Hardware-Sicherheitsmodul 11 des Backend-Rechnersystems 5 vorgenommen werden, sondern beispielsweise auch von einem berechtigten Datensender. Auch kann anstelle des Hardware-Sicherheitsmoduls 11 auch eine softwaretechnische Lösung verwendet werden, etwa in Form eines Soft-HSMs oder eines ähnlichen Systems.

Das Backend-Rechnersystem 5 agiert als Publisher und baut eine gemäß einem Netzwerk-Verschlüsselungsprotokoll gesicherte Verbindung mit dem Broker 20 auf, wobei sowohl eine Client-Authentifizierung, als auch eine Server-Authentifizierung erfolgt. Dann überträgt das Backend-Rechnersystem 5 als Publisher das Datenhüllpaket an einen Kanal des Brokers (Schritt 201).

Auch das netzwerknahe Gateway 8 baut eine gemäß einem Netzwerk-Verschlüsselungsprotokoll gesicherte Verbindung mit dem Broker 20 auf, agiert als Subscriber des Kanals, und empfängt das Datenhüllpaket (Schritt 202), wobei sowohl eine Client-Authentifizierung, als auch eine Server-Authentifizierung erfolgt.

Gemäß Variante C' extrahiert zuvor das netzwerknahe Gateway 8 unter Verwendung des Gateway-Sicherheitsmoduls 10' die relevanten Daten aus dem Datenhüllpaket. Der Key-Wrapping-Schlüssel wird unter Verwendung des One-Pass-Schlüsselaustausch-Schemas errechnet und der geheime Schlüssel wird unter Verwendung des Key-Wrapping-Schlüssels
 5 entschlüsselt. Die Integrität und die Authentizität der Daten werden unter Verwendung eines öffentlichen Schlüssels des Backend-Rechnersystems 5 (der im Gateway-Sicherheitsmodul 10' gespeichert ist) verifiziert und die Daten selbst werden entschlüsselt und über die Punkt-zu-Punkt-Verbindung 9 an das gerätenahe Gateway 7 übermittelt.

Gemäß Variante C wird das Datenhüllpaket von dem netzwerknahe Gateway 8 über die
 10 Punkt-zu-Punkt-Verbindung 9 an das gerätenahe Gateway 7 übermittelt (Schritt 203). Das gerätenahe Gateway 7 extrahiert die relevanten Daten aus dem Datenhüllpaket, berechnet den Key-Wrapping-Schlüssel unter Verwendung des One-Pass-Schlüsselaustausch-Schemas und entschlüsselt den geheimen Schlüssel unter Verwendung des Key-Wrapping-Schlüssels. Die Integrität und die Authentizität der Daten werden verifiziert und die Daten
 15 werden entschlüsselt. Gegebenenfalls kann die Sicherstellung der Integrität und Authentizität der Daten bereits in das kryptographische System integriert sein oder auch auf eine andere geeignete Weise implementiert werden.

Dann übermittelt (204) das gerätenahe Gateway 7 die Daten an die Hardwarekomponente 2. Falls die Hardwarekomponente 2 über einen Sicherheitscontroller 14 verfügt, kann
 20 gegebenenfalls die Integrität und die Authentizität der Daten auch von dem Sicherheitscontroller 14 überprüft werden, beispielsweise unter Verwendung eines öffentlichen Schlüssels des Backend-Rechnersystems 5 bzw. eines öffentlichen Schlüssels der Stelle, an der die Daten erstellt bzw. verschlüsselt wurden. Gegebenenfalls kann der Sicherheitscontroller 14 der Hardwarekomponente 2 auch gemäß Variante D die
 25 Entschlüsselung der zusätzlichen Verschlüsselungsebene vornehmen.

Als „öffentlicher Schlüssel des Backend-Rechnersystems“ werden im Zusammenhang mit der gegenständlichen Offenbarung alle öffentlichen Schlüssel von Schlüsselpaaren bezeichnet, deren privater Schlüssel einer Komponente des Backend-Rechnersystems 5 zugeordnet bzw. darin gespeichert ist. Insbesondere kann ein solcher öffentlicher Schlüssel
 30 des Backend-Rechnersystems 5 beispielsweise dem Software-Repository 15 oder dem Firmware-Repository 16 zugeordnet sein.

Mithilfe des oben beschriebenen Verfahrens lassen sich sehr komplexe Kommunikationsstrukturen schaffen, über die zahlreiche technische Systeme 4 unterschiedlicher Art mit einem oder mehreren Backend-Rechnersystemen 5 gesichert
 35 kommunizieren können. Fig. 3 zeigt beispielsweise eine erweiterte Kommunikationsstruktur mit einem ersten technischen System 4 und einem zweiten technischen System 4'. Das erste

technische System 4 kann beispielsweise eine industrielle Einrichtung 18 repräsentieren, beispielsweise einen Prüfstand oder eine Maschinenanordnung, in dem zumindest eine Hardwarekomponente 2, beispielsweise eine Sensoreinheit, vorgesehen ist. Üblicherweise umfasst eine industrielle Einrichtung eine Vielzahl an Hardwarekomponenten 2, die in Verbindung mit den erfindungsgemäßen Lehren verwendet werden können. Das zweite dargestellte technische System 4' kann beispielsweise ein autonomes Fahrzeug 17 repräsentieren, in dem zumindest eine Hardwarekomponente 2 enthalten ist. Üblicherweise enthält ein solches Fahrzeug eine Vielzahl an Hardwarekomponenten 2, für die jeweils die erfindungsgemäßen Lehren genutzt werden können.

In Fig. 3 sind lediglich zwei technische Systeme 4, 4' repräsentativ dargestellt, es ist jedoch klar, dass die Kommunikationsinfrastruktur eine Vielzahl unterschiedlicher und/oder gleichartiger technischer Systeme unterstützen kann.

Zu Beispielen für technische Systeme, die im Zusammenhang mit der gegenständlichen Erfindung vorteilhaft betrieben werden können, zählen Anlagen von Kraftwerksbetreibern, Anlagen von Schiffsschleusenbetreibern, autonome, teilautonome und konventionelle Fahrzeuge und Schiffe, medizinische Untersuchungsanlagen, wie etwa MRT-Geräte und dergleichen, Flugzeuge, Produktionsanlagen, etc.

Zu Beispielen von Hardwarekomponenten, die in solchen technischen Systemen vorgesehen sein können, zählen portable Abgasanlagen (PEMS), Steuergeräte von Fahrzeugen, Haushaltsgeräte, SPS Systeme, allgemein Sensoren und Aktoren, etc.

Jedes technische System umfasst (zumindest) ein Kommunikationsmodul 1, 1'. Jedes Kommunikationsmodul 1, 1' weist im Wesentlichen denselben grundlegenden Aufbau mit einem gerätenahen Gateway 7, einer Punkt-zu-Punkt-Verbindung 9 und einem netzwerknahen Gateway 8 auf, wie er in Verbindung mit Fig. 1 bereits beschrieben wurde.

In der Kommunikationsinfrastruktur können ein oder mehrere Backend-Rechnersysteme 5, 5' vorhanden sein. Beispielsweise kann die Kommunikation mit Hardwarekomponenten 2 über ein Kommunikationsmodul 1 von mehreren Hardwareanbietern genutzt werden, und/oder es können mehrere Backend-Rechnersysteme 5 für unterschiedliche Gruppen an technischen Systemen und/oder Hardwarekomponenten vorgesehen sein. Die Kommunikation über das paketvermittelte Datennetz 6 kann dabei beispielsweise über denselben Broker 20 geführt werden, es können aber auch mehrere Broker für jeweils unterschiedliche Kommunikationswege vorgesehen sein.

Die in Fig. 3 beispielhaft dargestellte Kommunikationsinfrastruktur erlaubt es, für jede unterstützte Hardwarekomponente 2, 2' eine vollständige End-zu-End-Verschlüsselung zwischen einer Komponente eines Backend-Rechnersystems 5, 5' und dem Kommunikationsmodul 1 bzw. der Hardwarekomponente 2 herzustellen. Dadurch lassen sich

beispielsweise Hackerangriffe, die darauf abzielen, eine Software oder Firmware einer Hardwarekomponente im Zuge der Übertragung über das paketvermittelte Datennetz 6 gegen eine korruptierte Version auszutauschen, verhindern. Auch zahlreiche Ansätze, die einen hardwarebasierten Angriff (etwa durch eine Seitenkanalattacke) auf das

- 5 Kommunikationsmodul 1, das interne Netz 3 oder die Hardwarekomponente 2 zum Ziel haben, werden durch die erfindungsgemäßen Vorrichtungen und Verfahren vereitelt.

Bezugszeichen:

- 10 Kommunikationsmodul 1
Hardwarekomponente 2
internes Netz 3
technisches System 4
Backend-Rechnersystem 5
15 paketvermitteltes Datennetz 6
gerätenahes Gateway 7
netzwerknahe Gateway 8
Punk-zu-Punkt-Verbindung 9
Gateway-Sicherheitsmodul 10
20 Hardware-Sicherheitsmodul 11
Prozessorchipkarte 12
Kartenschnittstelle 13
Sicherheitscontroller 14
Software-Repository 15
25 Firmware-Repository 16
Fahrzeug 17
industrielle Einrichtung 18
Gerätespeicher 19
Broker 20
30 Datencenter 21

Patentansprüche

1. Kommunikationsmodul (1) zur Datenübertragung zwischen zumindest einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) eingebunden ist, und einem Backend-Rechnersystem (5), welches an ein paketvermitteltes Datennetz (6) angeschlossen ist, **dadurch gekennzeichnet, dass** das Kommunikationsmodul (1) ein gerätenahes Gateway (7) und ein netzwerknahe Gateway (8) aufweist, die über eine zwischenstationsfreie Punkt-zu-Punkt-Verbindung (9) miteinander verbunden sind, wobei das netzwerknahe Gateway (8) eine Datenübertragungsschnittstelle zwischen dem paketvermittelten Datennetz (6) und der Punkt-zu-Punkt-Verbindung (9) bereitstellt und wobei das gerätenahe Gateway (7) eine Datenübertragungsschnittstelle zwischen der Punkt-zu-Punkt-Verbindung (9) und dem internen Netz (3) bereitstellt.
2. Kommunikationsmodul (1) nach Anspruch 1, dadurch gekennzeichnet, dass das gerätenahe Gateway (7) ein Gateway-Sicherheitsmodul (10) aufweist und/oder dass das netzwerknahe Gateway (8) ein Gateway-Sicherheitsmodul (10') aufweist.
3. Kommunikationsmodul (1) nach Anspruch 2, dadurch gekennzeichnet, dass zumindest ein Gateway-Sicherheitsmodul (10) eine Kartenschnittstelle (13) für eine Prozessorchipkarte (12) aufweist.
4. Technisches System (4) mit einem Kommunikationsmodul (1) nach einem der Ansprüche 1 bis 3, wobei das technische System (4) weiters zumindest eine Hardwarekomponente (2) und zumindest ein internes Netz (3) umfasst.
5. Technisches System (4) nach Anspruch 4, dadurch gekennzeichnet, dass die Hardwarekomponente (2) einen Sicherheitscontroller (14) mit einem integrierten Kryptoprozessor, einen nichtflüchtigen Speicher und einen flüchtigen Speicher aufweist.
6. Technisches System (4) nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass das technische System ein Fahrzeug (17) gemäß einer der Autonomiestufen 1 bis 5 ist.
7. Technisches System (4) nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass das technische System (4) eine von einem Automatisierungssystem gesteuerte Maschinenanordnung (18), insbesondere ein Prüfstand ist.
8. Verfahren zur Übertragung von Gerätedaten einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) gemäß einem der Ansprüche 4 bis 7 eingebunden ist, zu einem Backend-Rechnersystem (5), welches an ein paketvermitteltes Datennetz (6) angeschlossen ist, wobei das Verfahren durch die folgenden Schritte gekennzeichnet ist:

- Übermitteln (100) der Gerätedaten von der Hardwarekomponente (2) über das interne Netz (3) zu dem gerätenahen Gateway (7),
- Übermitteln (101) der Gerätedaten von dem gerätenahen Gateway (7) über die Punkt-zu-Punkt-Verbindung (9) zu dem netzwerknahen Gateway (8),

5 wobei von dem gerätenahen Gateway (7) oder dem netzwerknahen Gateway (8) die Gerätedaten in eine verschlüsselte Instanz der Gerätedaten umgewandelt wird, und

- Übermitteln (102,103) der verschlüsselten Instanz der Gerätedaten von dem netzwerknahen Gateway (8) über das paketvermittelte Datennetz (6) zu dem Backend-Rechnersystem (5).

10 9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass das Verfahren die folgenden Schritte aufweist:

- Erstellen einer verschlüsselten Instanz der Gerätedaten unter Verwendung eines öffentlichen Schlüssels eines Empfängers der Daten, insbesondere des Backend-Rechnersystems (5), durch

- 15 ○ das gerätenahe Gateway (7), vorzugweise unter Verwendung des Gateway-Sicherheitsmoduls (10) des gerätenahen Gateways (7), oder
- durch das netzwerknahe Gateway (8), vorzugweise unter Verwendung des Gateway-Sicherheitsmoduls (10') des netzwerknahen Gateways (7).

20 10. Verfahren nach Anspruch 8 oder 9, dadurch gekennzeichnet, dass der Schritt des Übermittels (102, 103) der verschlüsselten Instanz über das paketvermittelte Datennetz (6) das Übermitteln (102) der verschlüsselten Instanz zu einem Broker (20) umfasst, und gemäß einem Protokoll erfolgt, welches rein über Push-Mechanismen funktioniert.

25 11. Verfahren nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass das netzwerknahe Gateway (8) die verschlüsselte Instanz der Gerätedaten vor der Übermittlung über das paketvermittelte Datennetz (6) gemäß einem Netzwerk-Verschlüsselungsprotokoll verschlüsselt.

30 12. Verfahren nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass die verschlüsselte Instanz der Gerätedaten Prüfdaten beinhaltet, welche dem Backend-Rechnersystem (5) und/oder einem anderen berechtigten Datenempfänger eine Prüfung der Integrität und/oder Authentizität der Gerätedaten erlauben.

13. Verfahren zum Speichern von Aktualisierungsdaten in einem Gerätespeicher (19) einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) gemäß einem der Ansprüche 4 bis 7 eingebunden ist, wobei die Aktualisierungsdaten für die

Hardwarekomponente (2) von einem Backend-Rechnersystem (5) bereitgestellt werden und wobei das Verfahren durch die folgenden Schritte gekennzeichnet ist:

- Empfangen (202) einer verschlüsselten Instanz der Aktualisierungsdaten durch das netzwerknahe Gateway (8) über das paketvermittelte Datennetz (6) von dem Backend-Rechnersystem (5),
- Übermitteln (203) der Aktualisierungsdaten von dem netzwerknahe Gateway (8) über die Punkt-zu-Punkt-Verbindung (9) zu dem gerätenahen Gateway (7),
- Übermitteln der Aktualisierungsdaten an die Hardwarekomponente (2) über das interne Netz (3),

wobei verschlüsselten Instanz der Aktualisierungsdaten von dem gerätenahen Gateway (7) oder dem netzwerknahe Gateway (8) entschlüsselt wird, und

- Speichern der Aktualisierungsdaten in dem Gerätespeicher (19) der Hardwarekomponente.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die verschlüsselte Instanz der Aktualisierungsdaten von dem Backend-Rechnersystem (5) und/oder einem berechtigten Datensender unter Verwendung eines öffentlichen Schlüssels der Hardwarekomponente (2), und/oder des gerätenahen Gateways (7) und/oder des netzwerknahe Gateways (8) erstellt wird.

15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass das Verfahren die folgenden Schritte aufweist:

- Entschlüsseln der verschlüsselten Instanz der Aktualisierungsdaten
 - o durch das netzwerknahe Gateway (8), vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls (10') des netzwerknahe Gateways (8) oder
 - o durch das gerätenahe Gateway (7), vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls (10) des gerätenahen Gateways (7).

16. Verfahren nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, dass die Aktualisierungsdaten eine Firmware, eine Anwendungssoftware und/oder Parameterdaten der Hardwarekomponente (2) umfassen.

17. Verfahren nach einem der Ansprüche 13 bis 16, dadurch gekennzeichnet, dass der Schritt des Empfangens (202) das Abrufen der verschlüsselten Instanz der Aktualisierungsdaten von einem Broker (20) umfasst und gemäß einem Protokoll erfolgt, welches rein über Push-Mechanismen funktioniert.

18. Verfahren nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, dass die verschlüsselte Instanz der Aktualisierungsdaten Prüfdaten beinhaltet, welche dem Gateway-Sicherheitsmodul (10) des gerätenahen Gateways (7) und/oder dem Gateway-Sicherheitsmodul (10') des netzwerknahen Gateways (8) und/oder dem Sicherheitscontroller (14) der Hardwarekomponente (2) eine Prüfung der Integrität und/oder Authentizität der Aktualisierungsdaten erlauben.

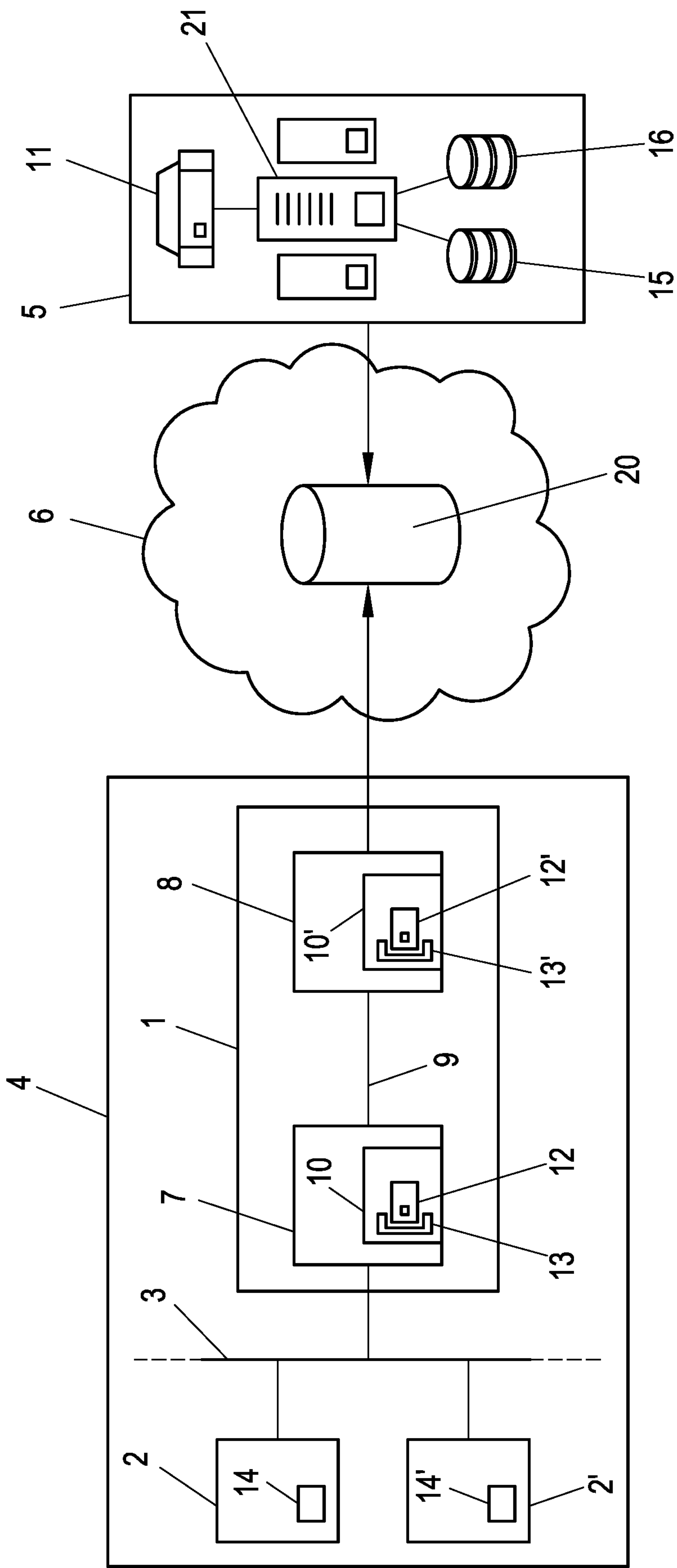


Fig. 1

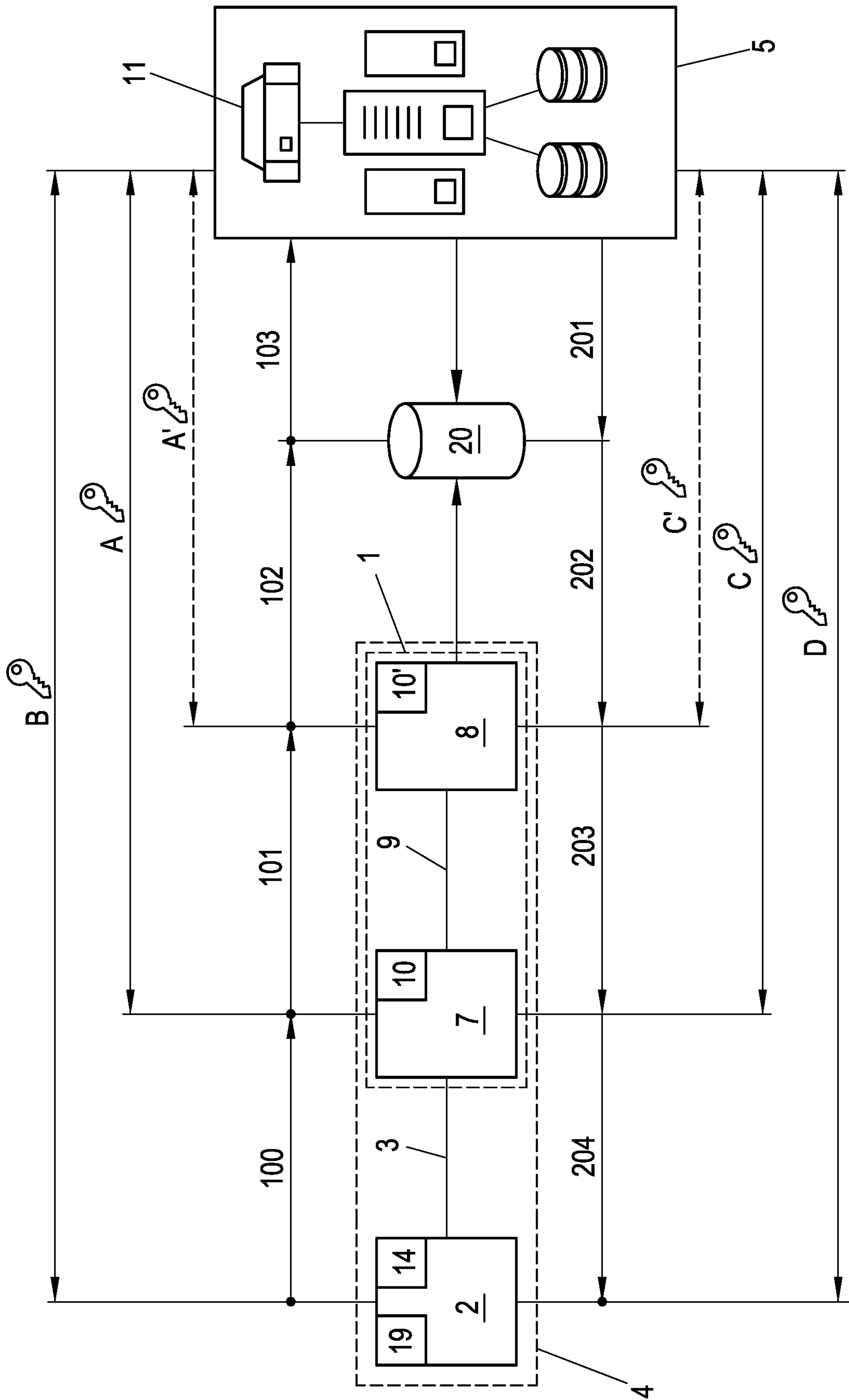


Fig. 2

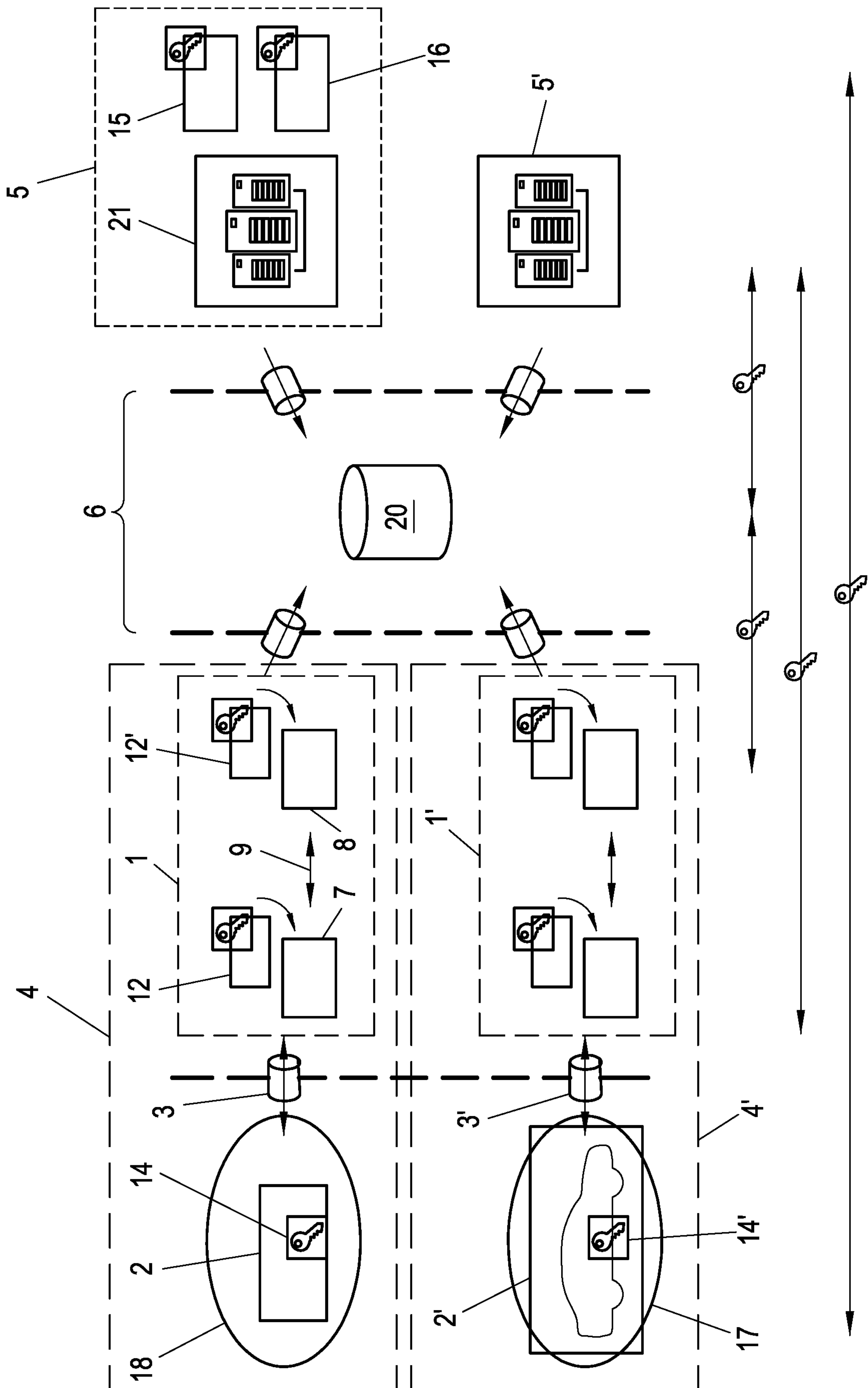


Fig. 3

Klassifikation des Anmeldungsgegenstands gemäß IPC:
H04L 29/08 (2006.01); **H04W 88/18** (2009.01)

Klassifikation des Anmeldungsgegenstands gemäß CPC:
H04L 67/104 (2019.01); **H04L 67/34** (2017.05); **H04W 88/18** (2019.01)

Recherchierter Prüfstoff (Klassifikation):
 H04L, H04W

Konsultierte Online-Datenbank:
 WPIAP, EPODOC, PATENW, PATDEW, IEEEExplore, ScienceDirect

Dieser Recherchenbericht wurde zu den am 13.12.2018 eingereichten Ansprüchen 1-18 erstellt.

Kategorie ^{*)}	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	WO 2015089457 A1 (M87) 18. Juni 2015 (18.06.2015) Figuren; Zusammenfassung; Paragrafen 067, 079, 080, 089, 090, 095, 096.	1-12, 14-18
X	US 2018219944 A1 (KWON et al.) 02. August 2018 (02.08.2018) Figuren; Zusammenfassung; Paragraf 0051.	1-12, 14-18
A	WO 2005050933 A1 (SPRINT COMMUNICATIONS) 02. Juni 2005 (02.06.2005) Figuren; Zusammenfassung.	1-18

Datum der Beendigung der Recherche:
 12.09.2019

Seite 1 von 1

Prüfer(in):

MESA PASCASIO Johannes

^{*)} Kategorien der angeführten Dokumente:

X Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
Y Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.

A Veröffentlichung, die den allgemeinen **Stand der Technik** definiert.
P Dokument, das von **Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung veröffentlicht wurde.
E Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein „**älteres Recht**“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
& Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.

Patentansprüche

1. Kommunikationsmodul (1) zur Datenübertragung zwischen zumindest einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) eingebunden ist, und einem Backend-Rechnersystem (5), welches an ein paketvermitteltes Datennetz (6) angeschlossen ist, **dadurch gekennzeichnet, dass** das Kommunikationsmodul (1) ein gerätenahes Gateway (7) und ein netzwerknahe Gateway (8) aufweist, die über eine zwischenstationsfreie Punkt-zu-Punkt-Verbindung (9) miteinander verbunden sind, wobei das netzwerknahe Gateway (8) eine Datenübertragungsschnittstelle zwischen dem paketvermittelten Datennetz (6) und der Punkt-zu-Punkt-Verbindung (9) bereitstellt, wobei das gerätenahe Gateway (7) eine Datenübertragungsschnittstelle zwischen der Punkt-zu-Punkt-Verbindung (9) und dem internen Netz (3) bereitstellt und wobei die Kommunikation über die Punkt-zu-Punkt-Verbindung (9) gemäß einem nicht-routingfähigen Protokoll ausgeführt wird.
2. Kommunikationsmodul (1) nach Anspruch 1, dadurch gekennzeichnet, dass das gerätenahe Gateway (7) ein Gateway-Sicherheitsmodul (10) aufweist und/oder dass das netzwerknahe Gateway (8) ein Gateway-Sicherheitsmodul (10') aufweist.
3. Kommunikationsmodul (1) nach Anspruch 2, dadurch gekennzeichnet, dass zumindest ein Gateway-Sicherheitsmodul (10) eine Kartenschnittstelle (13) für eine Prozessorchipkarte (12) aufweist.
4. Technisches System (4) mit einem Kommunikationsmodul (1) nach einem der Ansprüche 1 bis 3, wobei das technische System (4) weiters zumindest eine Hardwarekomponente (2) und zumindest ein internes Netz (3) umfasst.
5. Technisches System (4) nach Anspruch 4, dadurch gekennzeichnet, dass die Hardwarekomponente (2) einen Sicherheitscontroller (14) mit einem integrierten Kryptoprozessor, einen nichtflüchtigen Speicher und einen flüchtigen Speicher aufweist.
6. Technisches System (4) nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass das technische System ein Fahrzeug (17) gemäß einer der Autonomiestufen 1 bis 5 ist.
7. Technisches System (4) nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass das technische System (4) eine von einem Automatisierungssystem gesteuerte Maschinenanordnung (18), insbesondere ein Prüfstand ist.
8. Verfahren zur Übertragung von Gerätedaten einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) gemäß einem der Ansprüche 4 bis 7 eingebunden ist, zu einem Backend-Rechnersystem (5), welches an ein paketvermitteltes

Datennetz (6) angeschlossen ist, wobei das Verfahren durch die folgenden Schritte gekennzeichnet ist:

- Übermitteln (100) der Gerätedaten von der Hardwarekomponente (2) über das interne Netz (3) zu dem gerätenahen Gateway (7),
- Übermitteln (101) der Gerätedaten von dem gerätenahen Gateway (7) über die Punkt-zu-Punkt-Verbindung (9) zu dem netzwerknahe Gateway (8),

wobei von dem gerätenahen Gateway (7) oder dem netzwerknahe Gateway (8) die Gerätedaten in eine verschlüsselte Instanz der Gerätedaten umgewandelt wird und wobei die Kommunikation über die Punkt-zu-Punkt-Verbindung (9) gemäß einem nicht-routingfähigen Protokoll ausgeführt wird, und

- Übermitteln (102,103) der verschlüsselten Instanz der Gerätedaten von dem netzwerknahe Gateway (8) über das paketvermittelte Datennetz (6) zu dem Backend-Rechnersystem (5).

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass das Verfahren die folgenden Schritte aufweist:

- Erstellen einer verschlüsselten Instanz der Gerätedaten unter Verwendung eines öffentlichen Schlüssels eines Empfängers der Daten, insbesondere des Backend-Rechnersystems (5), durch
 - o das gerätenahe Gateway (7), vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls (10) des gerätenahen Gateways (7), oder
 - o durch das netzwerknahe Gateway (8), vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls (10') des netzwerknahe Gateways (7).

10. Verfahren nach Anspruch 8 oder 9, dadurch gekennzeichnet, dass der Schritt des Übermittels (102, 103) der verschlüsselten Instanz über das paketvermittelte Datennetz (6) das Übermitteln (102) der verschlüsselten Instanz zu einem Broker (20) umfasst, und gemäß einem Protokoll erfolgt, welches rein über Push-Mechanismen funktioniert.

11. Verfahren nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass das netzwerknahe Gateway (8) die verschlüsselte Instanz der Gerätedaten vor der Übermittlung über das paketvermittelte Datennetz (6) gemäß einem Netzwerk-Verschlüsselungsprotokoll verschlüsselt.

12. Verfahren nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass die verschlüsselte Instanz der Gerätedaten Prüfdaten beinhaltet, welche dem Backend-Rechnersystem (5) und/oder einem anderen berechtigten Datenempfänger eine Prüfung der Integrität und/oder Authentizität der Gerätedaten erlauben.

13. Verfahren zum Speichern von Aktualisierungsdaten in einem Gerätespeicher (19) einer Hardwarekomponente (2), die in ein internes Netz (3) eines technischen Systems (4) gemäß einem der Ansprüche 4 bis 7 eingebunden ist, wobei die Aktualisierungsdaten für die Hardwarekomponente (2) von einem Backend-Rechnersystem (5) bereitgestellt werden und wobei das Verfahren durch die folgenden Schritte gekennzeichnet ist:

- Empfangen (202) einer verschlüsselten Instanz der Aktualisierungsdaten durch das netzwerknahe Gateway (8) über das paketvermittelte Datennetz (6) von dem Backend-Rechnersystem (5),
- Übermitteln (203) der Aktualisierungsdaten von dem netzwerknahe Gateway (8) über die Punkt-zu-Punkt-Verbindung (9) zu dem gerätenahen Gateway (7),
- Übermitteln der Aktualisierungsdaten an die Hardwarekomponente (2) über das interne Netz (3),

wobei verschlüsselten Instanz der Aktualisierungsdaten von dem gerätenahen Gateway (7) oder dem netzwerknahe Gateway (8) entschlüsselt wird und wobei die Kommunikation über die Punkt-zu-Punkt-Verbindung (9) gemäß einem nicht-routingfähigen Protokoll ausgeführt wird, und

- Speichern der Aktualisierungsdaten in dem Gerätespeicher (19) der Hardwarekomponente.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die verschlüsselte Instanz der Aktualisierungsdaten von dem Backend-Rechnersystem (5) und/oder einem berechtigten Datensender unter Verwendung eines öffentlichen Schlüssels der Hardwarekomponente (2), und/oder des gerätenahen Gateways (7) und/oder des netzwerknahe Gateways (8) erstellt wird.

15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass das Verfahren die folgenden Schritte aufweist:

- Entschlüsseln der verschlüsselten Instanz der Aktualisierungsdaten
 - o durch das netzwerknahe Gateway (8), vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls (10') des netzwerknahe Gateways (8) oder
 - o durch das gerätenahe Gateway (7), vorzugsweise unter Verwendung des Gateway-Sicherheitsmoduls (10) des gerätenahen Gateways (7).

16. Verfahren nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, dass die Aktualisierungsdaten eine Firmware, eine Anwendungssoftware und/oder Parameterdaten der Hardwarekomponente (2) umfassen.

17. Verfahren nach einem der Ansprüche 13 bis 16, dadurch gekennzeichnet, dass der Schritt des Empfangens (202) das Abrufen der verschlüsselten Instanz der Aktualisierungsdaten von einem Broker (20) umfasst und gemäß einem Protokoll erfolgt, welches rein über Push-Mechanismen funktioniert.

18. Verfahren nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, dass die verschlüsselte Instanz der Aktualisierungsdaten Prüfdaten beinhaltet, welche dem Gateway-Sicherheitsmodul (10) des gerätenahen Gateways (7) und/oder dem Gateway-Sicherheitsmodul (10') des netzwerknahen Gateways (8) und/oder dem Sicherheitscontroller (14) der Hardwarekomponente (2) eine Prüfung der Integrität und/oder Authentizität der Aktualisierungsdaten erlauben.