

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges
Eigentum

Internationales Büro

(43) Internationales
Veröffentlichungsdatum
12. November 2015 (12.11.2015)



(10) Internationale Veröffentlichungsnummer
WO 2015/169347 A1

(51) Internationale Patentklassifikation:

H04L 29/06 (2006.01) H04L 29/08 (2006.01)
H04L 9/08 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2014/059275

(22) Internationales Anmeldedatum:
6. Mai 2014 (06.05.2014)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder: **VEGA GRIESHABER KG** [DE/DE];
Hauptstraße 1-5, 77709 Wolfach (DE).

(72) Erfinder: **ISENMANN, Andreas**; Bohnackerstr. 13,
77716 Haslach i. K. (DE). **GAISER, Martin**; Tannenweg
5, 72275 Alpirsbach (DE). **FEHRENBACH, Josef**;
Schlattstr. 1, 77716 Haslach i. K. (DE). **DECK, Thomas**;
Siechenwaldweg 13, 77709 Wolfach (DE).

(74) Anwalt: **WESTPHAL, MUSSGNUMG & PARTNER**; Am
Riettor 5, 78048 Villingen-Schwenningen (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,

AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,
BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK,
DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ,
TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,
RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT,
LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,
SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA,
GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz
3)

(54) Title: METHOD FOR ENCRYPTED DATA TRANSFER IN PROCESS AUTOMATION TECHNOLOGY

(54) Bezeichnung : VERFAHREN ZUR VERSCHLÜSSELTEN DATENÜBERTRAGUNG IN DER
PROZESSAUTOMATISIERUNGSTECHNIK

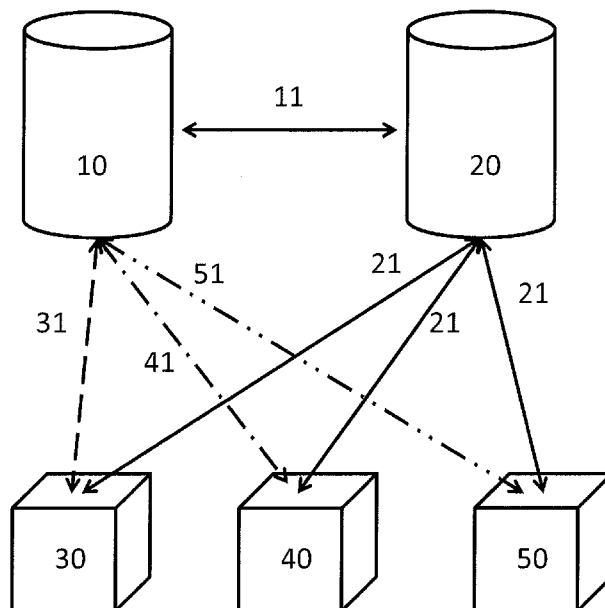


Fig.1

(57) Abstract: The invention relates to a method for encrypted data transfer in process automation technology, wherein the encrypted data transfer is carried out between at least one field device (30, 40, 50) and at least one internet server (10). The method comprises the following steps: forming an encrypted connection (21) between the field device (30, 40, 50) and a key server (20) using a key which is not device-specific and which is recorded on the key server (20) and in the field device (30, 40, 50); transferring data to record a key that is specific to the field device (30, 40, 50) on the key server (20), wherein the transfer between the field device (30, 40, 50) and the key server (20) is carried out using the non-device-specific key recorded on the key server (20); and transferring further data between the field device (30, 40, 50) and the internet server (10) using a connection (31, 41, 51) encrypted by the key specific to the field device (30, 40, 50)

(57) Zusammenfassung: Bereitgestellt wird
[Fortsetzung auf der nächsten Seite]



ein Verfahren zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik, wobei die verschlüsselte Datenübertragung zwischen mindestens einem Feldgerät (30, 40, 50) und mindestens einem Internetdienst-Server (10) erfolgt, mit den Schritten: Aufbau einer verschlüsselten Verbindung (21) zwischen dem Feldgerät (30, 40, 50) und einem Schlüssel-Server (20) unter Verwendung eines auf dem Schlüssel-Server (20) und im Feldgerät (30, 40, 50) hinterlegten, geräteunspezifischen Schlüssels, Übertragung von Daten zur Hinterlegung eines für das Feldgerät (30, 40, 50) spezifischen Schlüssels auf dem Schlüssel-Server (20), wobei die Übertragung zwischen dem Feldgerät (30, 40, 50) und dem Schlüssel-Server (20) unter Verwendung des auf dem Schlüssel-Server (20) hinterlegten, geräteunspezifischen Schlüssels erfolgt, und Übertragung weiterer Daten zwischen Feldgerät (30, 40, 50) und Internetdienst-Server (10) unter Verwendung einer mit dem für das Feldgerät (30, 40, 50) spezifischen Schlüssel verschlüsselten Verbindung (31, 41, 51).

Verfahren zur verschlüsselten Datenübertragung in der Prozess-
automatisierungstechnik

Moderne Prozessautomatisierungstechniken involvieren oftmals
5 die Kommunikation über das Internet zwischen einem gelegent-
lich auch als „Host“ bezeichneten Internetdienst-Server, z.B.
einem Web-Server, einem Email-Server, einem File-Server oder
dergleichen, und einem oder mehreren Feldgeräten, die zur Pro-
zesssteuerung bzw. Prozessregelung dienen, indem sie (mindestens)
10 eine Prozessgröße bestimmen, steuern oder regeln. Bei-
spiele für solche Feldgeräte sind z.B. Sensoren oder Aktoren.

Eine derartige Kommunikation über das Internet birgt stets das
Risiko, dass Unbefugte sich Zugang zu den Prozessdaten ver-
15 schaffen oder, schlimmer noch, die Möglichkeit erlangen, Steu-
erbefehle an die Feldgeräte zu geben. Ein bekanntes Mittel, um
dieses Risiko zumindest zu reduzieren, besteht in der Ver-
schlüsselung der übertragenen Daten. Geeignete Verschlüsse-
lungsalgorithmen, z.B. DES, 3DES, IDEA, AES oder RSA, und Mög-
20 lichkeiten zu deren Implementierung sind aus dem Stand der
Technik bekannt.

In der Prozesstechnik ist es aber gleichzeitig wesentlich,
dass eine exakte Zuordnung der Datenkommunikation zu einem ge-
25 gegebenen Feldgerät möglich ist, denn man möchte beispielsweise
bei der Übermittlung des von einem Sensor über das Internet an
eine zentrale Steuerung gemessenen Wertes den Sensor, von dem
dieser Wert stammt, identifizieren können.

30 Eine in der DE 10 2011 085 568 A1 offenbarte Lösung, um diese
Zuordnung unter Verwendung einer verschlüsselten Verbindung zu
gewährleisten besteht darin, einem gegebenen Feldgerät z.B.
bei der Herstellung oder während seiner Fertigstellung, jeden-

falls aber vor der Auslieferung des Feldgeräts einen spezifischen Schlüssel zuzuordnen und diesen in einem Webserver zu hinterlegen, so dass eine mit diesem spezifischen Schlüssel individuell verschlüsselte Kommunikation jederzeit die exakte Identifikation des jeweiligen Feldgeräts ermöglicht.

In der Praxis bedeutet dies aber, dass im Endeffekt bereits bei der Herstellung des Feldgeräts festgelegt werden muss, ob ein Gerät für eine Anwendung, in der eine verschlüsselte Kommunikation notwendig ist, geeignet sein soll oder nicht. Eine spätere Festlegung und eine Nachrüstung älterer Geräte bzw. ein Übergang zu einem anderen Verschlüsselungsstandard ist bei der Lösung gemäß der DE 10 2011 085 568 A1 nicht möglich. Zudem muss wegen der Zuordnung eines Schlüssels zum Feldgerät bei der Herstellung des Feldgeräts serverseitig eine Vielzahl von Schlüsseln hinterlegt und verwaltet werden, die unter Umständen nie gebraucht wird, was die Performance des Servers reduziert.

Die der Erfindung zu Grunde liegende Aufgabe besteht darin, ein Verfahren zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik bereitzustellen, bei dem auch noch nach der Herstellung ein Feldgerät zur verschlüsselten Kommunikation befähigt werden kann.

25

Diese Aufgabe wird gelöst durch ein Verfahren zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik mit den Merkmalen des Patentanspruchs 1. Vorteilhafte Weiterbildungen des Verfahrens sind Gegenstand der abhängigen Ansprüche.

30

Das erfindungsgemäße Verfahren zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik, wobei die ver-

schlüsselte Datenübertragung zwischen mindestens einem Feldgerät und mindestens einem Internetdienst-Server erfolgt, weist zumindest die folgenden Schritte auf:

- Aufbau einer verschlüsselten Verbindung zwischen dem Feldgerät und einem Schlüssel-Server unter Verwendung eines auf dem Schlüssel-Server und im Feldgerät hinterlegten, geräteunspezifischen Schlüssels,
- Übertragung von Daten zur Hinterlegung eines für das Feldgerät spezifischen Schlüssels auf dem Schlüssel-Server, wobei die Übertragung zwischen dem Feldgerät und dem Schlüssel-Server unter Verwendung des auf dem Schlüssel-Server hinterlegten, geräteunspezifischen Schlüssels erfolgt, und
- Übertragung weiterer Daten zwischen Feldgerät und Internetdienst-Server unter Verwendung einer mit dem für das Feldgerät spezifischen Schlüssel verschlüsselten Verbindung.

Mit anderen Worten wird also erfindungsgemäß ein für alle oder zumindest eine große Vielzahl von Feldgeräten identischer Schlüssel, der „geräteunspezifische Schlüssel“, im Feldgerät und in einem Schlüssel-Server hinterlegt, beispielsweise bei der Herstellung des Feldgeräts. Im Gegensatz zu einer Hinterlegung eines für das Feldgerät spezifischen Schlüssels (der nachfolgend auch als „gerätespezifischer Schlüssel“ bezeichnet wird) bei der Herstellung, müssen aber trotzdem außer einem geräteunspezifischen Schlüssel nur die gerätespezifischen Schlüssel verwaltet werden, die tatsächlich genutzt werden sollen und daher hinterlegt werden.

Über diesen geräteunspezifischen Schlüssel ist dann eine verschlüsselte Kommunikation zwischen dem Feldgerät und dem Schlüssel-Server möglich, bei der ein für unterschiedliche Feldgeräte unterschiedlicher, individueller (also nicht nur den Typ des Feldgeräts identifizierender, sondern für unter-

schiedliche Feldgeräte gleichen Typs unterschiedlicher)
Schlüssel, der „gerätespezifische Schlüssel“ zumindest auf
dem Schlüssel-Server hinterlegt wird. Der gerätespezifische
Schlüssel wird somit nur bei Bedarf erzeugt und auf dem
5 Schlüssel-Server hinterlegt, was die Menge der zu verwaltenden
Schlüssel gering hält.

Basierend auf diesem gerätespezifischen Schlüssel wird dann
die Kommunikation zwischen dem Feldgerät und dem Internet-
10 dienst-Server, der z.B. ein Web-Server, ein Email-Server, ein
File-Server oder dergleichen sein kann, verschlüsselt. Der In-
ternetdienst-Server kann dabei bevorzugt ein hardwaremäßig o-
der zumindest virtuell vom Schlüssel-Server getrennter Server
sein; er hat aber Zugriffsrechte auf die im Schlüssel-Server
15 hinterlegten Daten. Geht bei dem Internetdienst-Server eine
mit einem gerätespezifischen Schlüssel verschlüsselte Nach-
richt ein, so kann dieser den Schlüssel auf dem Schlüssel-
Server nachschlagen und mit Hilfe der erhaltenen Informationen
die Nachricht entschlüsseln.

20 Gemäß einer ersten Ausführungsform des Verfahrens umfassen die
Daten zur Hinterlegung eines für das Feldgerät spezifischen
Schlüssels auf dem Schlüssel-Server einen auf dem Feldgerät
erzeugten oder von einem Speichermedium auf das Feldgerät ü-
25 bertragenen spezifischen Schlüssel umfassen. Diese Vorgehens-
weise hat den Vorteil, dass der für das Feldgerät spezifische
Schlüssel auf dem Feldgerät selbst unmittelbar hinterlegt wer-
den kann und nicht durch eine Rückübertragung vom Schlüssel-
Server an das Feldgerät übermittelt und gespeichert werden
30 muss. Wenn das Feldgerät den Schlüssel selbst erzeugt, kann
dies z.B. unter Verwendung der Seriennummer und/oder von Pro-
duktionsdatum und -zeitpunkt als Eingangsdaten für den Schlüs-
selgenerierungsalgorithmus erfolgen. Entscheidend für die Er-

zeugung eines Schlüssels auf dem Feldgerät ist die Erzeugung einer Zufallszahl, die in den Schlüssel eingeht. Eine solche Zufallszahl kann über einen entsprechenden Algorithmus durch ein Softwaremodul oder durch eine speziell dafür vorhandene Hardware im Feldgerät erzeugt werden.

Alternativ können die Daten zur Hinterlegung eines für das Feldgerät spezifischen Schlüssels auf dem Schlüssel-Server für das Feldgerät spezifische Daten und Anweisungen zur Generierung des für das Feldgerät spezifischen Schlüssels durch den Schlüssel-Server umfassen. In diesem Fall würde das Feldgerät also mit dem geräteunspezifischen Schlüssel verschlüsselt gerätespezifische Daten, z.B. seine Seriennummer und/oder Produktionsdatum und -Zeitpunkt als Eingangsdaten für einen Schlüsselgenerierungsalgorithmus, der auf dem Schlüssel-Server ausgeführt wird, an den Schlüssel-Server übermitteln und diesen zur Generierung eines Schlüssels auffordern.

Diese Vorgehensweise kann unter zwei Gesichtspunkten vorteilhaft sein: Einerseits kann man dadurch verhindern, dass der gerätespezifische Schlüssel selbst über die nur geräteunspezifisch verschlüsselte Verbindung gesendet wird. Allerdings muss in diesem Fall ein nach demselben Schlüsselgenerierungsalgorithmus generierter, auf denselben gerätespezifischen Daten basierender gerätespezifischer Schlüssel auf dem Feldgerät generiert und/oder gespeichert werden.

Andererseits kann auf diese Weise der Bedarf an die Leistungsfähigkeit der Feldgeräte-Hardware reduziert werden, wenn der so erzeugte gerätespezifische Schlüssel vom Schlüssel-Server mit dem geräteunspezifischen Schlüssel verschlüsselt an das Feldgerät zurückübertragen und dort gespeichert wird.

Zweckmäßig ist insbesondere dass der gerätespezifische Schlüssel aus spezifischen Daten des Feldgeräts, wie z.B. Seriennummer oder Produktionsdatum und -Zeit, eindeutig bestimmbar ist. Auf diese Weise wird eine Doppelvergabe von Schlüsseln, die zu Mehrdeutigkeiten in der Datenkommunikation führen kann, sicher vermieden.

Besonders bevorzugt ist es, wenn die Gültigkeit des für das Feldgerät spezifischen Schlüssels durch den Internetdienst-Server mit Hilfe des Schlüssel-Servers verifizierbar ist. Dies ist insbesondere realisiert, wenn der für das Feldgerät spezifische Schlüssel auf dem Schlüssel-Server als ungültig markierbar ist. Der mit einer solchen Verifikationsmöglichkeit verbundene Vorteil besteht darin, dass über den Schlüssel-Server sichergestellt werden kann, dass nur Feldgeräte, die tatsächlich noch in einer gegebenen Produktionsanlage verwendet werden auch an der verschlüsselten Kommunikation dieser Produktionsanlage teilnehmen.

Besonders bevorzugt ist, dass der geräteunspezifische Schlüssel im Feldgerät in dessen Firmware hinterlegt ist. Diese Maßnahme hat den Vorteil, dass ein einfaches „Nachrüsten“ eines ursprünglich nicht für verschlüsselte Kommunikation ausgelegten Feldgeräts durch ein entsprechendes Firmware-Update möglich wird. Das Feldgerät wird durch die Firmware in die Lage versetzt, die verschlüsselte Kommunikation zum Schlüssel-Server aufzubauen und dann nachträglich einen gerätespezifischen Schlüssel zugewiesen zu bekommen.

Es ist möglich, dass der Schlüssel-Server eine im Feldgerät fest hinterlegte, eine auswählbare oder eine frei einstellbare Adresse hat. Es wird dadurch möglich, die Komplexität der Schlüsselmanagement in Grenzen zu halten, da nicht zwingend

alle Schlüssel von demselben Schlüsselserver verwaltet werden müssen und optional eine zentralisierte oder eine dezentrale Schlüsselverwaltung zu wählen.

5 Die Erfindung wird nachfolgend an Hand von Figuren, die spezielle Ausführungsbeispiele der Erfindung zeigen, näher erläutert. Es zeigen:

- 10 Fig.1: Den schematischen Aufbau eines Systems mit Internet-Server, Schlüssel-Server und drei Feldgeräten und dessen Kommunikationswege,
- Fig.2: ein Ablaufschema einer ersten Variante eines Verfahrens zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik,
- 15 Fig.3: ein Ablaufschema einer zweiten Variante eines Verfahrens zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik, und
- 20 Fig.4: ein Ablaufschema einer dritten Variante eines Verfahrens zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik.

Die Ablaufschemata gemäß Figuren 2 bis 4 geben die bevorzugte Reihenfolge des Verfahrensablaufs an, es sind aber Abweichungen möglich.

25

Figur 1 zeigt den schematischen Aufbau eines Systems zur Verwendung in der Prozessautomatisierungstechnik mit einem Internet-Server 10, einem Schlüssel-Server 20 und drei Feldgeräten 30,40,50, die optional über eine nicht dargestellte Schnittstelle für ein nicht dargestelltes Speichermedium, z.B. einen USB-Stick oder eine SD-Karte, verfügen können. Die Feldgeräte

30

30,40,50 können jeweils über eine mit einem geräteunspezifischen, d.h. für alle Feldgeräte 30,40,50 identischen, Schlüssel verschlüsselte und daher mit gleichem Bezugszeichen versehene und in gleicher Linienart dargestellte Verbindung 21 mit dem Schlüssel-Server 20 kommunizieren und auf diesem einen gerätespezifischen Schlüssel hinterlegen oder erzeugen, wobei im letzten Fall der auf dem Schlüssel-Server 20 erzeugte gerätespezifische Schlüssel über die geräteunspezifisch verschlüsselte Verbindung 21 an das jeweilige Feldgerät 30,40,50 zurückübertragen und dort gespeichert werden muss. Dies entfällt im ersten Fall, weil dann schon der gerätespezifische Schlüssel auf dem Feldgerät 30,40,50 gespeichert und hinterlegt ist.

Die Feldgeräte 30,40,50 können ferner zur Übertragung von Daten und/oder Steuerbefehlen mit dem Internet-Server 10 kommunizieren, wobei das Feldgerät 30 dazu eine mit seinem gerätespezifischen Schlüssel verschlüsselte Verbindung 31, das Feldgerät 40 eine mit seinem gerätespezifischen Schlüssel verschlüsselte Verbindung 41 und das Feldgerät 50 eine mit seinem gerätespezifischen Schlüssel verschlüsselte Verbindung 51 verwendet. Da die Verbindungen 31,41,51 jeweils mit unterschiedlichen Schlüsseln verschlüsselt sind, sind sie in Figur 1 mit unterschiedlichen Linienarten dargestellt.

Um die gerätespezifisch verschlüsselten eingehenden Signale entschlüsseln und den Feldgeräten 30,40,50 zuordnen zu können und umgekehrt Kommandos an die Feldgeräte 30,40,50 entsprechend verschlüsseln zu können, ist insbesondere vorgesehen, dass der Internet-Server 10 über eine Verbindung 11, die auch verschlüsselt sein kann mit dem Schlüssel-Server 20 kommuniziert, auf dem die entsprechenden gerätespezifischen Schlüssel hinterlegt sind. Der Schlüssel-Server 20 kann dabei die gerätespezifischen Schlüssel verwalten und z.B. Schlüssel als un-

gültig markieren, so dass Feldgeräte von der Kommunikation mit dem Internet-Server ausgeschlossen sind. Es können sowohl symmetrische, als auch asymmetrische Schlüssel verwendet werden. Bei asymmetrischen Schlüsseln wird nur der öffentliche Teil
5 vom Schlüssel auf dem Schlüssel-Server 20 gespeichert. Der private Teil des asymmetrischen Schlüssels wird ausschließlich in den Feldgeräten 30,40,50 gespeichert.

Figur 2 zeigt ein Ablaufschema einer ersten Variante eines
10 Verfahrens zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik, das insbesondere auf einem System gemäß Figur 1 ausführbar ist. In einem ersten Schritt 110 wird ein geräteunspezifischer Schlüssel, der insbesondere für alle Feldgeräte 30,40,50 identisch sein kann, im Feldgerät 30,40,50
15 hinterlegt. Dies kann insbesondere bei der Herstellung des Feldgeräts 30,40,50, aber bei Hinterlegung des geräteunspezifischen Schlüssels in der Firmware auch nachträglich durch ein einfaches Firmware-Update geschehen.

20 Im zweiten Schritt 120 wird unter Verwendung dieses geräteunspezifischen Schlüssels eine verschlüsselte Verbindung 21 zum Schlüssel-Server 20 aufgebaut, über die nachfolgend im Schritt 130 gerätespezifische Daten, z.B. die Seriennummer oder der Herstellungszeitpunkt des Feldgeräts 30,40,50 an den
25 Schlüssel-Server 20 übertragen werden, wo aus ihnen – gegebenenfalls nach Übertragung eines Steuerbefehls über die Verbindung 21– ein gerätespezifischer Schlüssel im Schritt 140 erzeugt wird, der auf dem Schlüssel-Server 20 hinterlegt und im Schritt 150 zur Hinterlegung an das zugehörige Feldgerät
30 30,40,50 über die mit dem geräteunspezifischen Schlüssel verschlüsselte Verbindung 21 übertragen wird.

Ist dies erfolgt, können im Schritt 160 mit den jeweiligen gerätespezifischen Schlüsseln der Feldgeräte 30,40,50 verschlüsselte Verbindungen 31,41,51 zum Internet-Server 10 aufgebaut werden, über die dann die als Schritt 170 genannten Kommunikation zwischen feldgerät 30,40,50 und Internet-Server 10 erfolgen kann.

Das Ablaufschema einer zweiten Variante eines Verfahrens zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik gemäß Figur 3 unterscheidet sich lediglich im Hinblick auf die Erzeugung und Hinterlegung des gerätespezifischen Schlüssels von der in Figur 2 dargestellten ersten Variante des Verfahrens. Für die Beschreibung der Schritte 210,220, 260 und 270 kann daher auf die Beschreibung der Schritte 110,120,160 und 170 zu Figur 2 verwiesen werden.

Anders als in der ersten Variante wird in der zweiten Variante gemäß Figur 3 im Schritt 230 aber der gerätespezifische Schlüssel auf dem Feldgerät 30,40,50 statt auf dem Schlüssel-Server 20 aus gerätespezifischen Daten erzeugt (und auf dem Feldgerät 30,40,50 gespeichert) und im Schritt 240 über die geräteunspezifisch verschlüsselte Verbindung 21 an den Schlüssel-Server 20 übertragen, um sie dort zu hinterlegen. Die gerätespezifischen Daten, die über die geräteunspezifisch verschlüsselte Verbindung 21 an den Schlüsselserver 20 übertragen werden sind hier also der gerätespezifische Schlüssel selbst.

Das Ablaufschema einer dritten Variante eines Verfahrens zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik gemäß Figur 4 unterscheidet sich lediglich im Hinblick auf die Erzeugung und Hinterlegung des gerätespezifischen Schlüssels von der in Figur 2 dargestellten ersten Variante des Verfahrens und der in Figur 3 dargestellten zweiten

Variante des Verfahrens. Für die Beschreibung der Schritte 310, 320, 360 und 370 kann daher auf die Beschreibung der Schritte 110, 120, 160 und 170 zu Figur 2 verwiesen werden.

5 Anders als in der ersten Variante des Verfahrens gemäß Figur 2 wird in der dritten Variante des Verfahrens gemäß Figur 4 im Schritt 330 aber der gerätespezifische Schlüssel auf dem Feldgerät 30, 40, 50 eingelesen, beispielsweise von einem lokal am
10 Feldgerät angebrachten USB-Stick, im Schritt 340 auf dem Feldgerät 30, 40, 50 gespeichert und im Schritt 350 über die geräteunspezifisch verschlüsselte Verbindung 21 an den Schlüssel-Server 20 übertragen, um sie dort zu hinterlegen. Damit kann
15 in Fällen, in denen das Feldgerät 30, 40, 50 eine geeignete Schnittstelle aufweist, der Hardware-Aufwand, der zur Generierung eines gerätespezifischen Schlüssels aus gerätespezifischen Daten notwendig ist, vermieden werden.

Die gerätespezifischen Daten, die über die geräteunspezifisch verschlüsselte Verbindung 21 an den Schlüsselserver 20 übertragen werden sind bei der dritten Variante gemäß Figur 4 ebenfalls der gerätespezifische Schlüssel selbst.

Bezugszeichenliste

10	Internet-Server
11	Verbindung
20	Schlüssel-Server
21	geräteunspezifisch verschlüsselte Verbindung
30	Feldgerät
31	gerätespezifisch verschlüsselte Verbindung
40	Feldgerät
41	gerätespezifisch verschlüsselte Verbindung
50	Feldgerät
51	gerätespezifisch verschlüsselte Verbindung
110, 120, 130, 140	Verfahrensschritt
150, 160, 170, 210	Verfahrensschritt
220, 230, 240, 260	Verfahrensschritt
270, 310, 320, 330	Verfahrensschritt
340, 350, 360, 370	Verfahrensschritt

Patentansprüche

1. Verfahren zur verschlüsselten Datenübertragung in der Prozessautomatisierungstechnik, wobei die verschlüsselte Datenübertragung zwischen mindestens einem Feldgerät (30, 40, 50) und mindestens einem Internetdienst-Server (10) erfolgt, mit den Schritten

- Aufbau einer verschlüsselten Verbindung (21) zwischen dem Feldgerät (30, 40, 50) und einem Schlüssel-Server (20) unter Verwendung eines auf dem Schlüssel-Server (20) und im Feldgerät (30, 40, 50) hinterlegten, geräteunspezifischen Schlüssels,

- Übertragung von Daten zur Hinterlegung eines für das Feldgerät (30, 40, 50) spezifischen Schlüssels auf dem Schlüssel-Server (20), wobei die Übertragung zwischen dem Feldgerät (30, 40, 50) und dem Schlüssel-Server (20) unter Verwendung des auf dem Schlüssel-Server (20) hinterlegten, geräteunspezifischen Schlüssels erfolgt, und

- Übertragung weiterer Daten zwischen Feldgerät (30, 40, 50) und Internetdienst-Server (10) unter Verwendung einer mit dem für das Feldgerät (30, 40, 50) spezifischen Schlüssel verschlüsselten Verbindung (31, 41, 51).

2. Verfahren nach Anspruch 1,

d a d u r c h g e k e n n z e i c h n e t, dass die Daten zur Hinterlegung eines für das Feldgerät (30, 40, 50) spezifischen Schlüssels auf dem Schlüssel-Server (20) einen auf dem Feldgerät (30, 40, 50) erzeugten oder von einem Speichermedium auf das Feldgerät (30, 40, 50) übertragenen spezifischen Schlüssel umfassen.

3. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t, dass die Da-
ten zur Hinterlegung eines für das Feldgerät (30,40,50)
spezifischen Schlüssels auf dem Schlüssel-Server (20) für
5 das Feldgerät (30,40,50) spezifische Daten und/oder Anwei-
sungen zur Generierung des für das Feldgerät (30,40,50)
spezifischen Schlüssels durch den Schlüssel-Server (20)
umfassen.
- 10 4. Verfahren nach Anspruch 3,
d a d u r c h g e k e n n z e i c h n e t, dass der
durch den Schlüssel-Server (20) generierte, für das Feld-
gerät (30,40,50) spezifische Schlüssel über die unter Ver-
wendung des geräteunspezifischen Schlüssels verschlüsselte
15 Verbindung (21) an das Feldgerät (30,40,50) übertragen und
dort gespeichert wird.
5. Verfahren nach einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t, dass der spe-
20 zifische Schlüssel aus spezifischen Daten des Feldgeräts
(30,40,50) eindeutig bestimmbar ist.
6. Verfahren nach einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t, dass die Gül-
25 tigkeit des für das Feldgerät (30,40,50) spezifischen
Schlüssels durch den Internetdienst-Server (10) mit Hilfe
des Schlüssel-Servers (20) verifizierbar ist.
7. Verfahren nach einem der vorstehenden Ansprüche,
30 d a d u r c h g e k e n n z e i c h n e t, dass der für
das Feldgerät (30,40,50) spezifische Schlüssel auf dem
Schlüssel-Server (20) als ungültig markierbar ist.

8. Verfahren nach einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t, dass der ge-
räteunspezifische Schlüssel im Feldgerät (30,40,50) in
dessen Firmware hinterlegt ist.

5

9. Verfahren nach einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t, dass der
Schlüsselserver (20) eine im Feldgerät (30,40,50) fest
hinterlegte, eine auswählbare oder eine frei einstellbare
Adresse hat.

10

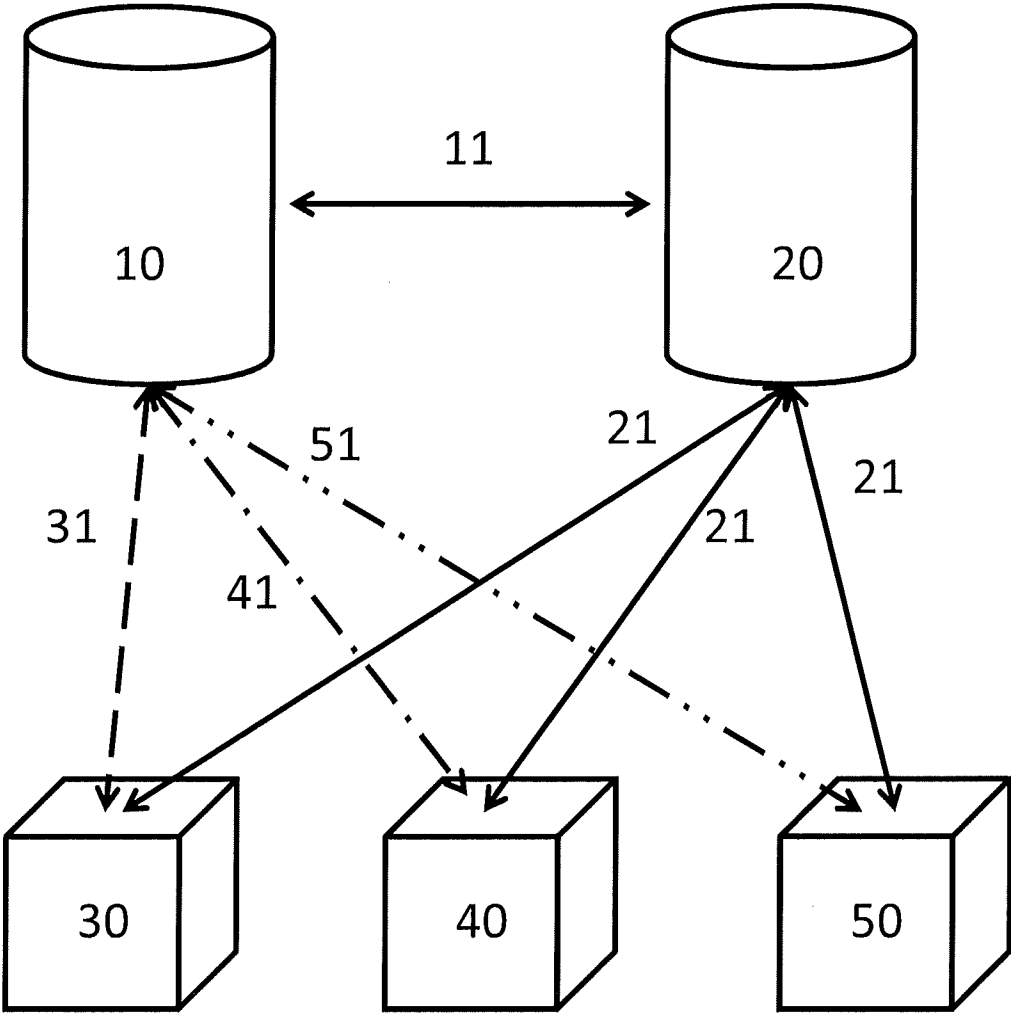


Fig.1

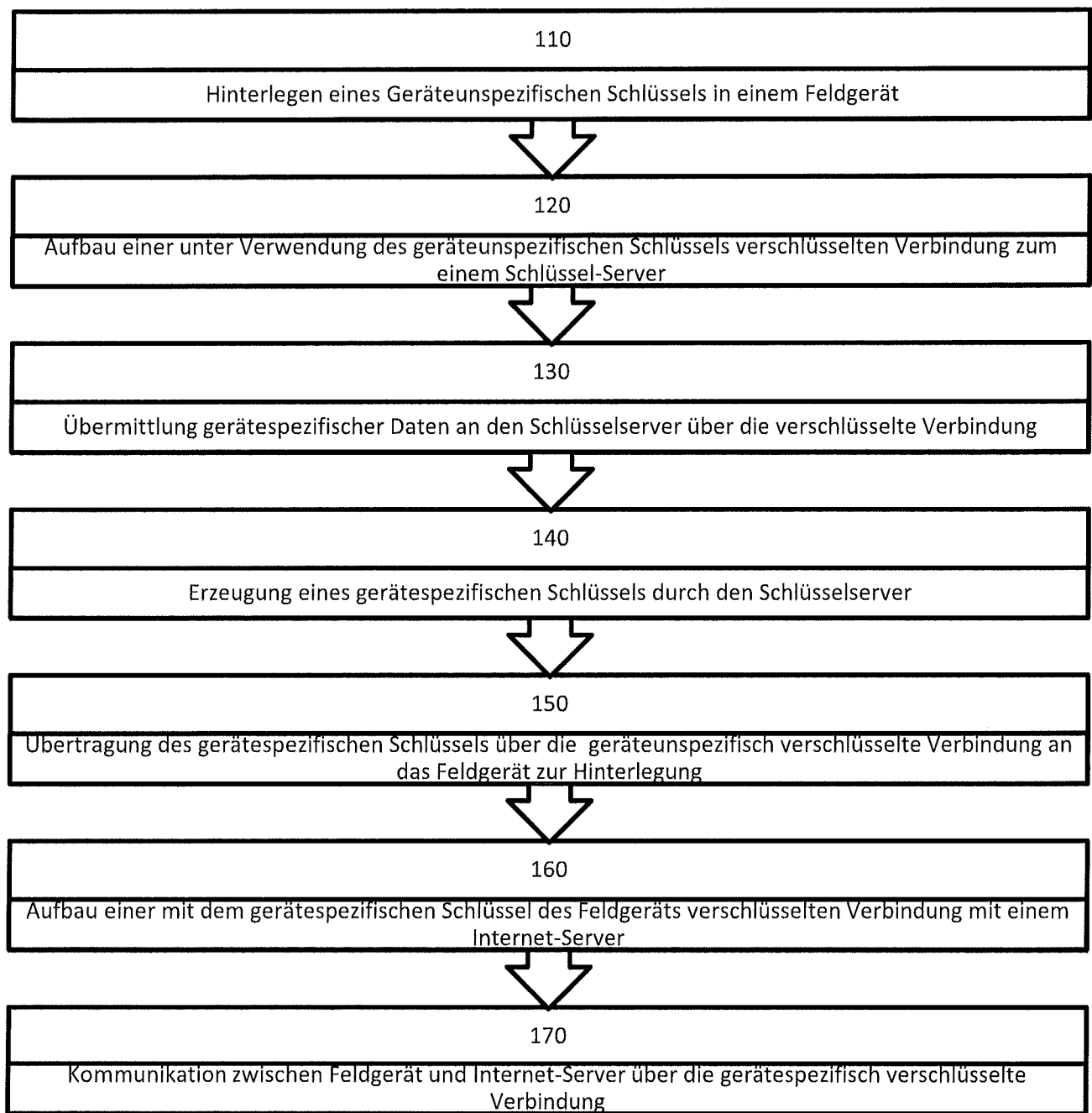


Fig.2

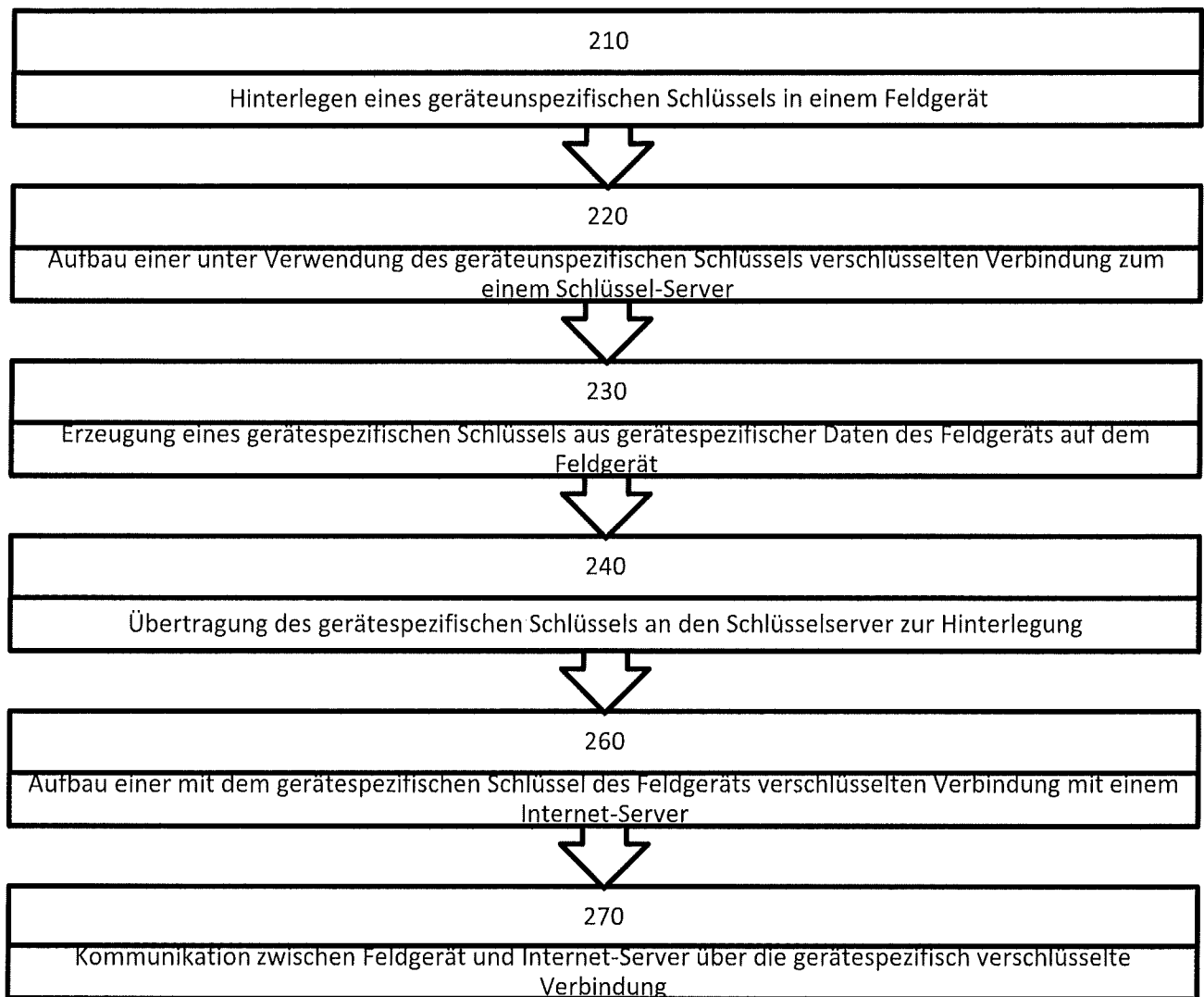


Fig.3

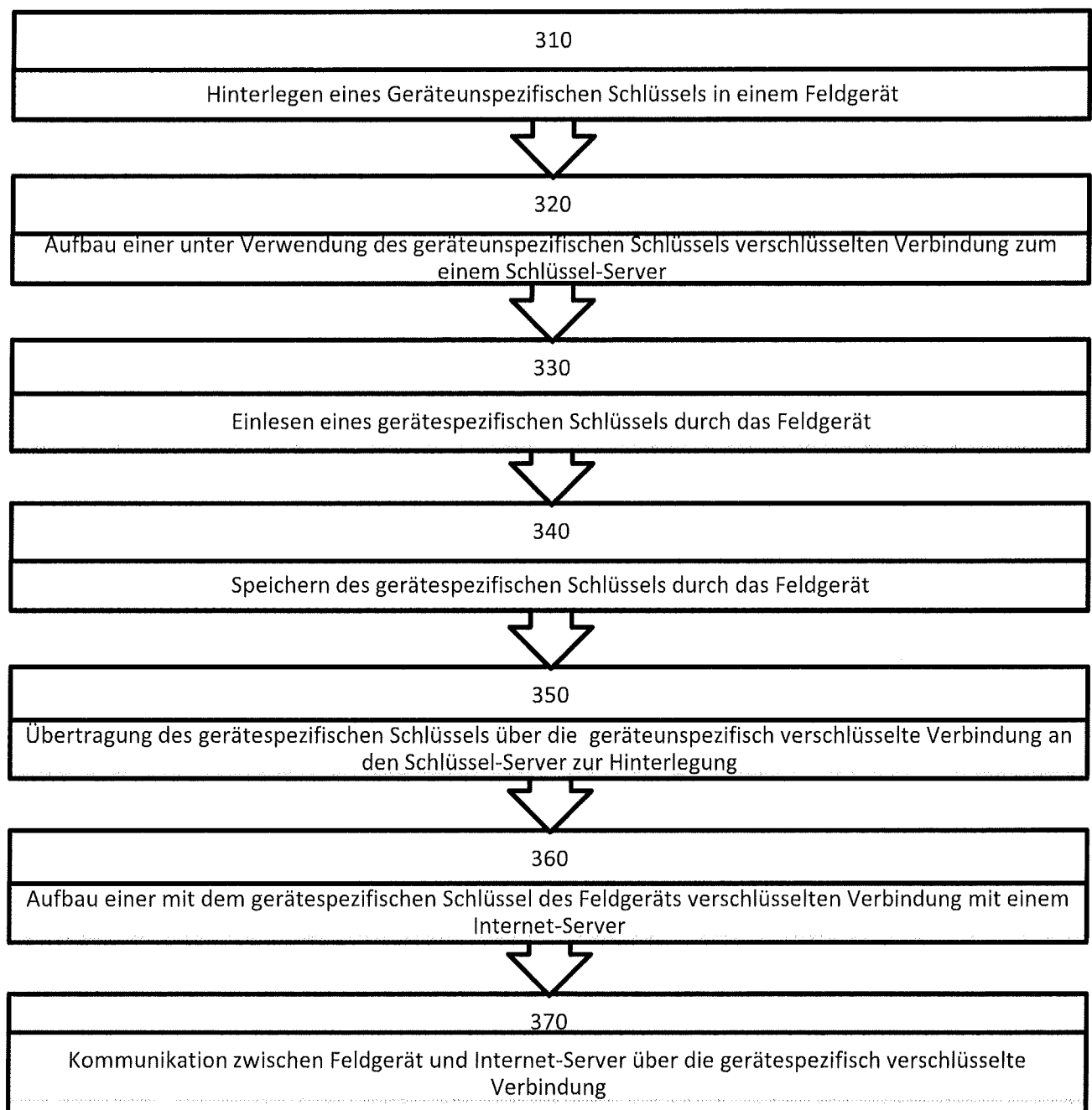


Fig.4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/059275

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/08 H04L29/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2011 085568 A1 (ENDRESS & HAUSER PROCESS SOLUT [CH]) 2 May 2013 (2013-05-02) abstract; figures 1, 2 paragraphs [0001], [0003], [0004] paragraphs [0021] - [0024], [0028] -----	1-9
X	DE 10 2010 011656 A1 (SIEMENS AG [DE]) 22 September 2011 (2011-09-22) abstract; figures 1, 2, 4, 6, 7 paragraphs [0038] - [0040], [0042] paragraphs [0043], [0048], [0049] paragraphs [0050], [0059], [0060] -----	1-9
A	DE 10 2010 010760 A1 (SIEMENS AG [DE]) 15 September 2011 (2011-09-15) abstract; figures 1, 2 paragraphs [0013] - [0024] ----- -/-	1-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

23 January 2015

Date of mailing of the international search report

02/02/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/059275

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 103 14 721 A1 (ENDRESS & HAUSER GMBH & CO KG [DE]) 11 November 2004 (2004-11-11) abstract; figure 1 paragraphs [0002] - [0017] -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/059275

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102011085568 A1	02-05-2013	NONE	
DE 102010011656 A1	22-09-2011	NONE	
DE 102010010760 A1	15-09-2011	DE 102010010760 A1	15-09-2011
		WO 2011110603 A1	15-09-2011
DE 10314721 A1	11-11-2004	DE 10314721 A1	11-11-2004
		WO 2004114621 A1	29-12-2004

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. H04L29/06 H04L9/08 H04L29/08
 ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 H04L H04W G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2011 085568 A1 (ENDRESS & HAUSER PROCESS SOLUT [CH]) 2. Mai 2013 (2013-05-02) Zusammenfassung; Abbildungen 1, 2 Absätze [0001], [0003], [0004] Absätze [0021] - [0024], [0028] -----	1-9
X	DE 10 2010 011656 A1 (SIEMENS AG [DE]) 22. September 2011 (2011-09-22) Zusammenfassung; Abbildungen 1, 2, 4, 6, 7 Absätze [0038] - [0040], [0042] Absätze [0043], [0048], [0049] Absätze [0050], [0059], [0060] -----	1-9
A	DE 10 2010 010760 A1 (SIEMENS AG [DE]) 15. September 2011 (2011-09-15) Zusammenfassung; Abbildungen 1, 2 Absätze [0013] - [0024] ----- -/-	1-9

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

23. Januar 2015

Absendedatum des internationalen Recherchenberichts

02/02/2015

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Schossmaier, Klaus

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 103 14 721 A1 (ENDRESS & HAUSER GMBH & CO KG [DE]) 11. November 2004 (2004-11-11) Zusammenfassung; Abbildung 1 Absätze [0002] - [0017] -----	1-9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2014/059275

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102011085568 A1	02-05-2013	KEINE	
DE 102010011656 A1	22-09-2011	KEINE	
DE 102010010760 A1	15-09-2011	DE 102010010760 A1	15-09-2011
		WO 2011110603 A1	15-09-2011
DE 10314721 A1	11-11-2004	DE 10314721 A1	11-11-2004
		WO 2004114621 A1	29-12-2004