(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 226 388 A1** 2016.03.24

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 226 388.3**
(22) Anmeldetag: **18.12.2014**
(43) Offenlegungstag: **24.03.2016**

(51) Int Cl.: ***H04L 12/24*** (2006.01)
H04L 9/32 (2006.01)
G06F 7/58 (2006.01)

(71) Anmelder:
Siemens Aktiengesellschaft, 80333 München, DE

(72) Erfinder:
Falk, Rainer, 85586 Poing, DE; Fries, Steffen, 85598 Baldham, DE

(56) Ermittelter Stand der Technik:

DE	**10 2012 217 743**	**A1**
US	**2006 / 0 072 747**	**A1**
US	**2009 / 0 323 967**	**A1**
WO	**2014/ 091 336**	**A1**

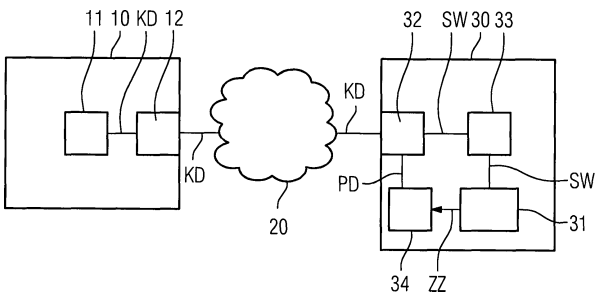
Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

Rechercheantrag gemäß § 43 Abs. 1 Satz 1 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Konfigurationsvorrichtung und Verfahren zum Konfigurieren von Feldgeräten**

(57) Zusammenfassung: Es wird eine Konfigurationsvorrichtung zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks koppelbaren Feldgeräten vorgeschlagen. Das jeweilige Feldgerät weist einen Zufallszahlengenerator zur Erzeugung einer Zufallszahl für eine Erzeugung kryptografischer Daten auf. Die Konfigurationsvorrichtung umfasst eine Bereitstellungseinheit und eine Übertragungseinheit. Die Bereitstellungseinheit ist dazu eingerichtet, Konfigurationsdaten für das jeweilige Feldgerät bereitzustellen. Die Konfigurationsdaten umfassen projektierte Daten und einen Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts. Die Übertragungseinheit ist dazu eingerichtet, die bereitgestellten Konfigurationsdaten über das Automatisierungsnetzwerk auf das Feldgerät zu übertragen.
Hierdurch ist es möglich, Feldgeräte, welche keine eigene Quelle für guten Zufall haben, mittels des Startwertes mit einer initialen Entropie zu versorgen.
Des Weiteren werden ein Verfahren zum Konfigurieren von Feldgeräten, ein solches Feldgerät und ein System mit Feldgeräten und einer Konfigurationsvorrichtung vorgeschlagen.



Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Konfigurationsvorrichtung zum Konfigurieren von Feldgeräten. Des Weiteren betrifft die vorliegende Erfindung ein Verfahren zum Konfigurieren von Feldgeräten, ein solches Feldgerät und ein System mit Feldgeräten und einer Konfigurationsvorrichtung.

[0002] Das Feldgerät umfasst einen Zufallszahlengenerator zur Erzeugung einer Zufallszahl. Die Zufallszahl wird in dem Feldgerät zur Generierung kryptographischer Daten verwendet. Beispiele für kryptographische Daten sind ein kryptografischer Schlüssel oder ein Einmalwert (Nonce).

[0003] Zufallszahlen bilden eine Grundlage in der Kryptographie, beispielsweise bei der Verwaltung von Schlüsseln (Key Management) für Sicherheitsdienste, wie den Integritätsschutz oder die Verschlüsselung von Daten. Zufallszahlen werden insbesondere benötigt, um den kryptographischen Schlüssel zu erzeugen oder um die Nonce zu ermitteln. Zufallszahlen können über logische Zufallszahlengeneratoren oder physikalische Zufallszahlengeneratoren erzeugt werden. Starke Zufallszahlen werden häufig durch oder unter Verwendung eines physikalischen Zufallszahlengenerators erzeugt.

[0004] Feldgeräte, wie Sensoren oder Aktuatoren, die über einen Zufallszahlengenerator verfügen, haben aber oftmals keine geeignete Quelle für "Zufall", um den Zufallszahlengenerator geeignet über einen Startwert zu initialisieren. Folglich besteht ein Bedarf, Feldgeräte mit geeigneten guten Startwerten, so genannten Seeds, für den lokalen Zufallszahlengenerator des Feldgeräts zu versorgen.

[0005] In dem Dokument US 20060072747 A1 ist ein geräteexterner Server zur Bereitstellung von zusätzlicher Entropie beschrieben.

[0006] Dabei wird mittels einer SSL/TLS-Verbindung unter Verwendung eines temporären Schlüsselpaares des Gerätes die Übermittlung des Startwerts zum Gerät geschützt.

[0007] Aus dem Dokument WO 2014091336 A1 ist bekannt, ein Feldgerät während des Engineerings mit Zugangsdaten zu einem externen Zufallszahlengenerator zu versorgen. Das Feldgerät kann sich mittels dieser Zugangsdaten mit der externen Quelle verbinden und auf gesicherte Art und Weise Startwerte (Seeds) abfragen.

[0008] Vor diesem Hintergrund besteht eine Aufgabe der vorliegenden Erfindung darin, das Konfigurieren von Feldgeräten zu verbessern.

[0009] Gemäß einem ersten Aspekt wird eine Konfigurationsvorrichtung zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks koppelbaren Feldgeräten vorgeschlagen. Das jeweilige Feldgerät weist einen Zufallszahlengenerator zur Erzeugung einer Zufallszahl für eine Erzeugung kryptografischer Daten auf. Die Konfigurationsvorrichtung umfasst eine Bereitstellungseinheit und eine Übertragungseinheit. Die Bereitstellungseinheit ist dazu eingerichtet, Konfigurationsdaten für das jeweilige Feldgerät bereitzustellen. Die Konfigurationsdaten umfassen projektierte Daten und einen Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts. Die Übertragungseinheit ist dazu eingerichtet, die bereitgestellten Konfigurationsdaten über das Automatisierungsnetzwerk oder über eine serielle Konfigurationsschnittstelle auf das Feldgerät zu übertragen. Auch ist es möglich, dass eine Konfigurationsinformation auf ein wechselbares Konfigurationsspeichermodul eines Feldgeräts geschrieben wird.

[0010] Durch die vorgeschlagene Konfigurationsvorrichtung ist es möglich, Feldgeräte, wie industrielle Feldgeräte oder Steuergeräte, welche keine eigene Quelle für guten Zufall haben, mittels des Startwertes mit einer initialen Entropie zu versorgen. Diese ermöglicht die Erzeugung von „guten" oder starken Zufallszahlen während des Betriebs des Feldgeräts ohne die Notwendigkeit einer individuellen Versorgung des Feldgeräts mit Entropie während der Produktion. Ein Startwert für einen Zufallszahlengenerator wird bei einem Konfigurationsvorgang des Feldgeräts, der z.B. zur Inbetriebnahme ohnehin erforderlich ist, automatisch eingespielt. Außerdem ist es damit nicht notwendig, einen physikalischen Zufallszahlengenerator auf dem Feldgerät vorzusehen. Das Feldgerät speichert den bereitgestellten Startwert oder eine davon abhängig bestimmte Information vorzugsweise in einem nichtflüchtigen Speicher. Der Zufallszahlengenerator des Feldgeräts kann weitere Startwerte und/oder physikalisch erzeugte Zufallszahlen verwenden, um eine Folge von Zufallszahlen mittels eines logischen Zufallszahlengenerators zu erzeugen.

[0011] Gemäß einer Ausführungsform weist die Konfigurationsvorrichtung einen Zufallszahlengenerator zur Erzeugung des Startwerts zur Initialisierung des Zufallszahlengenerators des Feldgeräts auf.

[0012] Der Startwert wird durch die Konfigurationsvorrichtung mit dem Zufallszahlengenerator erzeugt und als Teil der Konfigurationsdaten dem Feldgerät bereitgestellt. Dies hat den Vorteil, dass bei mehreren, funktional identisch zu konfigurierenden Feldgeräten nicht eine separate Konfiguration je Feldgerät durchgeführt werden muss. Der Zufallszahlengenerator der Konfigurationsvorrichtung kann den Startwert beispielsweise als einen Hash-Wert unter Verwendung einer kryptographischen Hash-Funktion wie SHA2, SHA3 oder BLAKE generieren.

[0013] Gemäß einer weiteren Ausführungsform bildet das Automatisierungsnetzwerk eine lokale Verbindung zwischen der Anzahl der Feldgeräte und der Konfigurationsvorrichtung. Alternativ kann das Automatisierungsnetzwerk auch eine Remote-Verbindung zwischen der Konfigurationsvorrichtung und der Anzahl der Feldgeräte ausbilden.

[0014] Gemäß einer weiteren Ausführungsform wird der Startwert verschlüsselt von der Konfigurationsvorrichtung zu dem Feldgerät übermittelt. Hierzu kann eine symmetrische Verschlüsselung eingesetzt werden.

[0015] Gemäß einer weiteren Ausführungsform wird der Startwert über einen authentisierten und verschlüsselten Kanal dem Feldgerät übermittelt. Die Authentisierung kann hierbei symmetrisch oder asymmetrisch erfolgen.

[0016] Gemäß einer weiteren Ausführungsform ist der Zufallszahlengenerator der Konfigurationsvorrichtung als ein physikalischer Zufallszahlengenerator ausgebildet.

[0017] Der physikalische Zufallszahlengenerator der Konfigurationsvorrichtung kann starke Zufallszahlen als Startwert bereitstellen. Der zentrale physikalische Zufallszahlengenerator der Konfigurationsvorrichtung kann für alle angeschlossenen Feldgeräte verwendet werden. Folglich ist es nicht notwendig, auf den Feldgeräten einen physikalischen Zufallszahlengenerator vorzusehen.

[0018] Gemäß einer weiteren Ausführungsform ist der Zufallszahlengenerator des Feldgeräts als ein Pseudo-Zufallszahlengenerator ausgebildet.

[0019] Der Pseudo-Zufallszahlengenerator kann die von dem physikalischen Zufallszahlengenerator der Konfigurationsvorrichtung bereitgestellte hohe Entropie für seine Initialisierung nutzen und damit Zufallszahlen höherer Qualität bereitstellen.

[0020] Gemäß einer weiteren Ausführungsform ist die Bereitstellungseinheit dazu ausgebildet, die Konfigurationsdaten aus für das Feldgerät spezifischen projektierten Daten und dem Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts zu bilden.

[0021] Die projektierten Daten können für das jeweilige Feldgerät oder für eine Gruppe von Feldgeräten spezifisch projektiert sein.

[0022] Gemäß einer weiteren Ausführungsform weist die Konfigurationsvorrichtung eine Ladeeinheit auf, welche über ein Netzwerk mit einem Server zum Bereitstellen von Zufallswerten koppelbar ist und welche dazu eingerichtet ist, einen Zufallswert von dem Server herunterzuladen. Dabei ist die Bereitstellungseinheit dazu eingerichtet, den Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts in Abhängigkeit von dem heruntergeladenen Zufallswert zu bilden.

[0023] Der Server zum Bereitstellen von Zufallswerten kann auch als Zufallsserver bezeichnet werden. Die von dem Zufallsserver bereitgestellten Zufallswerte sind insbesondere starke Zufallswerte. Damit kann ein hoher Entropieanteil bei der Generierung des Startwerts für die Initialisierung des Zufallsgenerators des Feldgeräts beigebracht werden.

[0024] Gemäß einer weiteren Ausführungsform sendet die Konfigurationsvorrichtung eine Gerätekennung des Feldgeräts an den Server (Zufallsserver), um einen gerätespezifischen Startwert zu erzeugen.

[0025] Gemäß einer weiteren Ausführungsform nutzt der Zufallszahlengenerator ein von dem Feldgerät übermitteltes Gerätezertifikat, um den Startwert zu verschlüsseln. Dieser verschlüsselte Container wird dann an die Konfigurationsvorrichtung zurückgeliefert und in die Konfigurationsdaten eingefügt. Dies hat den Vorteil, dass der Startwert auf dem kompletten Transportweg geschützt ist. Darüber hinaus kann der Zufallszahlengenerator bei Kenntnis der Gerätezertifikate die Seedcontainer schon vorberechnen.

[0026] Gemäß einer weiteren Ausführungsform ist die Bereitstellungseinheit dazu eingerichtet, den heruntergeladenen Zufallswert als Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts zu verwenden.

[0027] Diese Ausführungsform hat den Vorteil einer sehr einfachen Implementierung.

[0028] Gemäß einer weiteren Ausführungsform ist die Bereitstellungseinheit dazu eingerichtet, den Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts in Abhängigkeit von dem heruntergeladenen Zufallswert und von zumindest einem von einer Entropie-Quelle bereitgestellten Parameter zu berechnen.

[0029] Diese Ausführungsform hat den Vorteil einer Entropieerhöhung für den Startwert und damit einer Erhöhung der Qualität der von dem Zufallszahlengenerator des Feldgeräts generierten Zufallszahlen.

[0030] Gemäß einer weiteren Ausführungsform weist die Konfigurationsvorrichtung eine Kombinationseinheit auf, welche dazu eingerichtet ist, den Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts durch eine Kombination eines durch den Zufallszahlengenerator der Konfigurationsvorrichtung generierten Zufallswerts und des

von dem Server heruntergeladenen Zufallswert zu kombinieren.

[0031] Durch die Kombination werden die Entropie und damit die Qualität der zu erzeugenden Zufallszahlen erhöht.

[0032] Gemäß einer weiteren Ausführungsform ist die Bereitstellungseinheit dazu eingerichtet, bei jedem Ladevorgang von projektierten Daten die an das Feldgerät zu übertragenden Konfigurationsdaten aus den projektierten Daten und einem neuen Startwert zur Initialisierung des Zufallszahlengenerators des Feldgeräts zu bilden.

[0033] Die Konfigurationsvorrichtung erzeugt vorzugsweise bei jedem Ladevorgang bzw. bei jedem Bereitstellungsvorgang einen Startwert (Seed), der dem Feldgerät bereitgestellt wird. Das heißt, selbst wenn demselben Feldgerät mehrmals projektierte Daten bereitgestellt werden, so ist bei jedem Bereitstellungsvorgang ein neuer, im Allgemeinen unterschiedlicher Seed, in den bereitgestellten Konfigurationsdaten enthalten.

[0034] Gemäß einer weiteren Ausführungsform ist die Konfigurationsvorrichtung dazu eingerichtet, sich gegenüber dem Feldgerät zu authentisieren und das Feldgerät zu authentisieren.

[0035] Das Feldgerät und die Konfigurationsvorrichtung authentisieren sich beiderseitig. Beispielsweise wirkt dann das Feldgerät als Server und die Konfigurationsvorrichtung als Client.

[0036] Gemäß einer weiteren Ausführungsform sind die kryptografischen Daten als ein kryptografischer Schlüssel ausgebildet.

[0037] Gemäß einer weiteren Ausführungsform sind die kryptografischen Daten als ein Einmalwert (Nonce) ausgebildet.

[0038] Die jeweilige Einheit, zum Beispiel Bereitstellungseinheit oder Übertragungseinheit, kann hardwaretechnisch und/oder auch softwaretechnisch implementiert sein. Bei einer hardwaretechnischen Implementierung kann die jeweilige Einheit als Vorrichtung oder als Teil einer Vorrichtung, zum Beispiel als Computer oder als Mikroprozessor oder als integrierter Schaltkreis ausgebildet sein. Bei einer softwaretechnischen Implementierung kann die jeweilige Einheit als Computerprogrammprodukt, als eine Funktion, als eine Routine, als Teil eines Programmcodes oder als ausführbares Objekt ausgebildet sein.

[0039] Gemäß einem zweiten Aspekt wird ein Feldgerät vorgeschlagen. Das Feldgerät hat einen Zufallszahlengenerator zur Erzeugung einer Zufallszahl für eine Erzeugung kryptografischer Daten, eine Kopplungseinheit zum Koppeln des Feldgeräts mit einer Konfigurationsvorrichtung zum Konfigurieren des Feldgeräts über ein Automatisierungsnetzwerk, und eine Initialisierungseinheit zum Initialisieren des Zufallszahlengenerators mittels eines von der Konfigurationsvorrichtung gesendeten und über die Kopplungseinheit empfangenen Startwerts.

[0040] Gemäß einem dritten Aspekt wird ein System vorgeschlagen. Das System umfasst eine Anzahl, insbesondere eine Mehrzahl von Feldgeräten gemäß dem zweiten Aspekt und eine Konfigurationsvorrichtung gemäß dem ersten Aspekt.

[0041] Gemäß einem vierten Aspekt wird ein Verfahren zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks koppelbaren Feldgeräten vorgeschlagen. Das jeweilige Feldgerät umfasst einen Zufallszahlengenerator zur Erzeugung einer Zufallszahl für eine Erzeugung kryptografischer Daten. Das Verfahren weist folgende Schritte auf:
Bereitstellen eines Startwerts zur Initialisierung des Zufallszahlengenerators des Feldgeräts,
Bilden von Konfigurationsdaten aus projektierten Daten und dem bereitgestellten Startwert, und
Übertragen der gebildeten Konfigurationsdaten, beispielsweise über das Automatisierungsnetzwerk, auf das Feldgerät.

[0042] Gemäß einer Weiterbildung wird der Startwert verschlüsselt auf das Feldgerät übertragen.

[0043] Alternativ oder zusätzlich kann der Startwert über einen authentisierten und verschlüsselten Kanal auf das Feldgerät übertragen werden. Die Authentisierung kann hierbei symmetrisch oder asymmetrisch erfolgen.

[0044] Die für die vorgeschlagene Konfigurationsvorrichtung beschriebenen Ausführungsformen und Merkmale gelten für das vorgeschlagene Verfahren entsprechend.

[0045] Weitere mögliche Implementierungen der Erfindung umfassen auch nicht explizit genannte Kombinationen von zuvor oder im Folgenden bezüglich der Ausführungsbeispiele beschriebenen Merkmale oder Ausführungsformen. Dabei wird der Fachmann auch Einzelaspekte als Verbesserungen oder Ergänzungen zu der jeweiligen Grundform der Erfindung hinzufügen.

[0046] Weitere vorteilhafte Ausgestaltungen und Aspekte der Erfindung sind Gegenstand der Unteransprüche sowie der im Folgenden beschriebenen Ausführungsbeispiele der Erfindung. Im Weiteren wird die Erfindung anhand von bevorzugten Ausführungsformen unter Bezugnahme auf die beigelegten Figuren näher erläutert.

[0047] Fig. 1 zeigt ein schematisches Blockschaltbild eines ersten Ausführungsbeispiels einer Konfigurationsvorrichtung zum Konfigurieren von Feldgeräten;

[0048] Fig. 2 zeigt ein schematisches Blockschaltbild von Konfigurationsdaten zum Konfigurieren eines Feldgeräts;

[0049] Fig. 3 zeigt ein schematisches Blockschaltbild eines zweiten Ausführungsbeispiels einer Konfigurationsvorrichtung zum Konfigurieren von Feldgeräten;

[0050] Fig. 4 zeigt ein schematisches Blockschaltbild eines dritten Ausführungsbeispiels einer Konfigurationsvorrichtung zum Konfigurieren von Feldgeräten;

[0051] Fig. 5 zeigt ein schematisches Blockschaltbild eines vierten Ausführungsbeispiels einer Konfigurationsvorrichtung zum Konfigurieren von Feldgeräten; und

[0052] Fig. 6 zeigt ein schematisches Ablaufdiagramm eines Ausführungsbeispiels eines Verfahrens zum Konfigurieren von Feldgeräten.

[0053] In den Figuren sind gleiche oder funktionsgleiche Elemente mit denselben Bezugszeichen versehen worden, sofern nichts anderes angegeben ist.

[0054] Fig. 1 zeigt ein schematisches Blockschaltbild eines ersten Ausführungsbeispiels einer Konfigurationsvorrichtung **10** zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks **20** koppelbaren Feldgeräten **30**.

[0055] Ohne Beschränkung der Allgemeinheit zeigt **Fig.** 1 ein Feldgerät **30**. Es kann eine Mehrzahl von Feldgeräten **30** über das Automatisierungsnetzwerk **20** mit der Konfigurationsvorrichtung **10** gekoppelt sein.

[0056] Das Feldgerät **30** umfasst einen Zufallszahlengenerator **31** zur Erzeugung einer Zufallszahl ZZ für eine Erzeugung kryptographischer Daten. Außerdem umfasst das Feldgerät **30** eine Kopplungseinheit **32** zum Koppeln des Feldgeräts **30** mit dem Automatisierungsnetzwerk **20** und damit mit der Konfigurationsvorrichtung **10** über jenes Automatisierungsnetzwerk **20**. Außerdem weist das Feldgerät **30** eine Initialisierungseinheit **33** auf, welche dazu eingerichtet ist, den Zufallszahlengenerator **31** mittels eines von der Konfigurationsvorrichtung **10** gesendeten und über die Kopplungseinheit **32** empfangenen Startwerts SW zu initialisieren. Der Zufallszahlengenerator **31** generiert eine Zufallszahl ZZ. Des Weiteren umfasst das Feldgerät **30** eine Steuereinrichtung **34** zum Steuern desselben. Die Steuereinrichtung **34** ist dazu eingerichtet, kryptografische Daten mittels der von dem Zufallszahlengenerator **31** generierten Zufallszahl ZZ zu erzeugen. Ferner nutzt die Steuereinrichtung **34** projektierte Daten PD zur Steuerung des Feldgeräts **30** bzw. zur Ausführung dessen Funktion.

[0057] Hierzu weist die Konfigurationsvorrichtung **10** eine Bereitstellungseinheit **11** und eine Übertragungseinheit **12** auf. Die Bereitstellungseinheit **11** ist dazu eingerichtet, die Konfigurationsdaten KD für das Feldgerät **30** bereitzustellen. Die bereitgestellten Konfigurationsdaten KD umfassen projektierte Daten PD und den Startwert SW zur Initialisierung des Zufallszahlengenerators **31** des Feldgeräts **30** (siehe **Fig.** 2). Die projektierten Daten PD sind vorab von einem Projektierer oder einem Ingenieur projektiert, können auch als Projektierungsdaten bezeichnet werden und sollen auf das Feldgerät **30** aufgespielt werden.

[0058] Die Bereitstellungseinheit **11** ist insbesondere dazu eingerichtet, bei jedem Ladevorgang von projektierten Daten PD, die an das Feldgerät **30** zu übertragenden Konfigurationsdaten KD aus den projektierten Daten PD und einem neuen Startwert SW zur Initialisierung des Zufallszahlengenerators **31** des Feldgeräts **30** zu bilden. Demnach wird der Startwert SW für jeden Ladevorgang neu generiert. Die projektierten Daten PD können sich von Ladevorgang zu Ladevorgang verändern oder gleich bleiben.

[0059] Die Übertragungseinheit **12** ist dazu eingerichtet, die bereitgestellten Konfigurationsdaten KD über das Automatisierungsnetzwerk **20** oder über eine serielle Konfigurationsschnittstelle (nicht gezeigt) auf das Feldgerät **30** zu übertragen. Auch ist es möglich, dass die Konfigurationsdaten KD auf ein wechselbares Konfigurationsspeichermodul des Feldgeräts **30** geschrieben werden.

[0060] Außerdem ist die Konfigurationsvorrichtung **10** insbesondere dazu eingerichtet, sich gegenüber dem Feldgerät **30** zu authentisieren und das Feldgerät **30** zu authentisieren. Folglich können sich die beiden Geräte, nämlich die Konfigurationsvorrichtung **10** und das Feldgerät **30**, gegenseitig authentisieren und so die Sicherheit der Kommunikation erhöhen.

[0061] Die kryptographischen Daten sind beispielsweise ein kryptographischer Schlüssel oder ein Einmalwert (Nonce).

[0062] Fig. 3 zeigt ein schematisches Blockschaltbild eines zweiten Ausführungsbeispiels einer Konfigurationsvorrichtung **10**. Das zweite Ausführungsbeispiel der **Fig.** 3 umfasst alle Merkmale des ersten Ausführungsbeispiels der Konfigurationsvorrichtung **10** der **Fig.** 1 und zusätzlich einen Zufallszahlengenerator **13**. Der Zufallszahlengenerator **13** ist dazu

eingerichtet, den Startwert SW zu erzeugen und an die Bereitstellungseinheit **11** zu übertragen. Die Bereitstellungseinheit **11** fügt den von dem Zufallszahlengenerator **13** erzeugten Startwert SW den Konfigurationsdaten KD für das Feldgerät **30** bei. Der Zufallszahlengenerator **13** ist insbesondere ein physikalischer Zufallszahlengenerator und stellt starke Zufallszahlen bereit. Demgegenüber ist der Zufallszahlengenerator **31** des Feldgeräts **30** beispielsweise als ein Pseudo-Zufallszahlengenerator ausgebildet und stellt Pseudo-Zufallszahlen bereit.

[0063] **Fig.** 4 zeigt ein schematisches Blockschaltbild eines dritten Ausführungsbeispiels einer Konfigurationsvorrichtung **10** zum Konfigurieren von Feldgeräten **30**.

[0064] Das dritte Ausführungsbeispiel der **Fig.** 4 umfasst sämtliche Merkmale des zweiten Ausführungsbeispiels der **Fig.** 3. Ferner umfasst die Konfigurationsvorrichtung **10** der **Fig.** 4 eine Ladeeinheit **14** sowie eine Entropie-Quelle **15**. Die Entropie-Quelle **15** kann auch außerhalb der Konfigurationsvorrichtung **10** angeordnet sein. Die Entropie-Quelle **15** stellt einen quasizufälligen Parameter P bereit. Dieser quasizufällige Parameter P ist beispielsweise von der aktuellen Temperatur der Umgebung der Konfigurationsvorrichtung **10** abgeleitet. Der quasizufällige Parameter P kann auch von dem Datenverkehr der Konfigurationsvorrichtung **10** oder dergleichen abgeleitet sein.

[0065] Die Ladeeinheit **14** ist über ein Netzwerk **40** mit einem Server **50** gekoppelt. Das Netzwerk **40** kann ein lokales Netzwerk oder auch das Internet sein. Der Server **50** ist zum Bereitstellen von Zufallswerten ZW eingerichtet. Die Ladeeinheit **14** lädt einen Zufallswert ZW von dem Server **50** über das Netzwerk **40** herunter und stellt den heruntergeladenen Zufallswert ZW der Bereitstellungseinheit **11** bereit. Die Bereitstellungseinheit **11** ist dazu eingerichtet, den Startwert SW zur Initialisierung des Zufallszahlengenerators **31** des Feldgeräts **30** in Abhängigkeit von dem heruntergeladenen Zufallswert ZW zu bilden. Beispielsweise verwendet die Bereitstellungseinheit **11** den heruntergeladenen Zufallswert ZW als den Startwert SW und fügt diesen Zufallswert ZW den Konfigurationsdaten KD bei.

[0066] Alternativ kann die Bereitstellungseinheit **11** auch dazu eingerichtet werden, den Startwert SW zur Initialisierung des Zufallszahlengenerators **31** in Abhängigkeit von dem heruntergeladenen Zufallswert ZW und in Abhängigkeit von dem von der Entropie-Quelle **15** bereitgestellten Parameter P zu bilden.

[0067] In **Fig.** 5 ist ein schematisches Blockschaltbild eines vierten Ausführungsbeispiels einer Konfigurationsvorrichtung **10** zum Konfigurieren von Feldgeräten **30** dargestellt. Das vierte Ausführungsbeispiel der **Fig.** 5 basiert auf dem dritten Ausführungsbeispiel der **Fig.** 4. Ferner hat die Konfigurationsvorrichtung **10** der **Fig.** 5 eine Kombinationseinheit **16**, welche beispielsweise in der Bereitstellungseinheit **11** integriert ist. Die Kombinationseinheit **16** ist dazu eingerichtet, den Startwert SW zur Initialisierung des Zufallszahlengenerators **31** des Feldgeräts **30** durch eine Kombination eines durch den Zufallszahlengenerator **13** der Konfigurationsvorrichtung **10** generierten Zufallswerts ZW1 und eines von dem Server **50** heruntergeladenen Zufallswerts ZW2 zu kombinieren.

[0068] **Fig.** 6 zeigt ein schematisches Ablaufdiagramm eines Ausführungsbeispiels eines Verfahrens zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks **20** koppelbaren Feldgeräten **30**. Das Feldgerät **30** ist beispielsweise wie in einer der **Fig.** 1, **Fig.** 2 oder **Fig.** 4 ausgebildet.

[0069] Das Verfahren der **Fig.** 6 umfasst die folgenden Verfahrensschritte **601**–**603**:

[0070] In Schritt **601** wird ein Startwert SW zur Initialisierung des Zufallszahlengenerators **31** des Feldgeräts **30** bereitgestellt.

[0071] In Schritt **602** werden Konfigurationsdaten KD für das Feldgerät **30** aus projektierten Daten PD und dem bereitgestellten Startwert SW gebildet.

[0072] In Schritt **603** werden die gebildeten Konfigurationsdaten KD, beispielsweise über das Automatisierungsnetzwerk **20**, auf das Feldgerät **30** übertragen.

[0073] Die Schritte **601**–**603** werden beispielsweise von einer Konfigurationsvorrichtung **10** der **Fig.** 1, **Fig.** 3 oder **Fig.** 4 ausgeführt.

[0074] Obwohl die vorliegende Erfindung anhand von Ausführungsbeispielen beschrieben wurde, ist sie vielfältig modifizierbar.

Bezugszeichenliste

10	Vorrichtung
11	Bereitstellungseinheit
12	Übertragungseinheit
13	Zufallszahlengenerator
14	Ladeeinheit
15	Entropiequelle
16	Kombinationseinheit
20	Automatisierungsnetzwerk
30	Feldgerät
31	Zufallszahlengenerator
32	Kopplungseinheit
33	Initialisierungseinheit
34	Steuereinrichtung
40	Netzwerk

50	Server
KD	Konfigurationsdaten
P	Parameter
PD	projektierte Daten
SW	Startwert
ZW	Zufallswert
ZZ	Zufallszahl

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Patentliteratur

- US 20060072747 A1 [0005]
- WO 2014091336 A1 [0007]

Patentansprüche

1. Konfigurationsvorrichtung (**10**) zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks (**20**) koppelbaren Feldgeräten (**30**), wobei das jeweilige Feldgerät (**30**) einen Zufallszahlengenerator (**31**) zur Erzeugung einer Zufallszahl (ZZ) für eine Erzeugung kryptografischer Daten umfasst, mit:
einer Bereitstellungseinheit (**11**) zum Bereitstellen von Konfigurationsdaten (KD) für das jeweilige Feldgerät (**30**), wobei die Konfigurationsdaten (KD) projektierte Daten (PD) und einen Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) umfassen, und
einer Übertragungseinheit (**12**) zum Übertragen der bereitgestellten Konfigurationsdaten (KD) auf das Feldgerät (**30**).

2. Konfigurationsvorrichtung nach Anspruch 1, gekennzeichnet durch einen Zufallszahlengenerator (**13**) zur Erzeugung des Startwerts (SW).

3. Konfigurationsvorrichtung nach Anspruch 2, **dadurch gekennzeichnet,** dass der Zufallszahlengenerator (**13**) der Konfigurationsvorrichtung (**10**) als ein physikalischer Zufallszahlengenerator ausgebildet ist und/oder der Zufallszahlengenerator (**31**) des Feldgeräts (**30**) als ein Pseudo-Zufallszahlengenerator ausgebildet ist.

4. Konfigurationsvorrichtung nach einem der Ansprüche 1–3, **dadurch gekennzeichnet,** dass die Bereitstellungseinheit (**11**) dazu ausgebildet ist, die Konfigurationsdaten (KD) aus für das Feldgerät (**30**) spezifischen projektierten Daten (PD) und dem Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) zu bilden.

5. Konfigurationsvorrichtung nach einem der Ansprüche 1–4, gekennzeichnet durch eine Ladeeinheit (**14**), welche über ein Netzwerk (**40**) mit einem Server (**50**) zum Bereitstellen von Zufallswerten (ZW) koppelbar ist und welche dazu eingerichtet ist, einen Zufallswert (ZW) von dem Server (**50**) herunterzuladen, wobei die Bereitstellungseinheit (**11**) dazu eingerichtet ist, den Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) in Abhängigkeit von dem heruntergeladenen Zufallswert (ZW) zu bilden.

6. Konfigurationsvorrichtung nach Anspruch 5, **dadurch gekennzeichnet,** dass die Bereitstellungseinheit (**11**) dazu eingerichtet ist, den heruntergeladenen Zufallswert (ZW) als Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) zu verwenden.

7. Konfigurationsvorrichtung nach Anspruch 5, **dadurch gekennzeichnet,** dass die Bereitstellungseinheit (**11**) dazu eingerichtet ist, den Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) in Abhängigkeit von dem heruntergeladenen Zufallswert (ZW) und von zumindest einem von einer Entropie-Quelle (**15**) bereitgestellten Parameter (P) zu berechnen.

8. Konfigurationsvorrichtung nach einem der Ansprüche 5–7, gekennzeichnet durch eine Kombinationseinheit (**16**), welche dazu eingerichtet ist, den Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) durch eine Kombination eines durch den Zufallszahlengenerator (**13**) der Konfigurationsvorrichtung (**10**) generierten Zufallswerts (ZW1) und des von dem Server (**50**) heruntergeladenen Zufallswert (ZW2) zu kombinieren.

9. Konfigurationsvorrichtung nach einem der Ansprüche 1–8, **dadurch gekennzeichnet,** dass die Bereitstellungseinheit (**11**) dazu eingerichtet ist, bei jedem Ladevorgang von projektierten Daten (PD) die an das Feldgerät (**30**) zu übertragenden Konfigurationsdaten (KD) aus den projektierten Daten (PD) und einem neuen Startwert (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**) zu bilden.

10. Konfigurationsvorrichtung nach einem der Ansprüche 1–9, **dadurch gekennzeichnet,** dass die Konfigurationsvorrichtung (**10**) dazu eingerichtet ist, sich gegenüber dem Feldgerät (**30**) zu authentisieren und das Feldgerät (**30**) zu authentisieren.

11. Konfigurationsvorrichtung nach einem der Ansprüche 1–10, **dadurch gekennzeichnet,** dass die kryptografischen Daten als ein kryptografischer Schlüssel oder als ein Einmalwert ausgebildet sind.

12. Feldgerät (**30**), mit:
einem Zufallszahlengenerator (**31**) zur Erzeugung einer Zufallszahl für eine Erzeugung kryptografischer Daten,
einer Kopplungseinheit (**32**) zum Koppeln des Feldgeräts (**30**) mit einer Konfigurationsvorrichtung (**10**) zum Konfigurieren des Feldgeräts (**30**) über ein Automatisierungsnetzwerk (**20**), und
einer Initialisierungseinheit (**33**) zum Initialisieren des Zufallszahlengenerators (**31**) mittels eines von der Konfigurationsvorrichtung (**10**) gesendeten und über die Kopplungseinheit (**32**) empfangenen Startwerts (SW).

13. System, mit:
einer Anzahl von Feldgeräten (**30**) nach Anspruch 12, und
einer Konfigurationsvorrichtung (**10**) zum Konfigurieren der Anzahl der Feldgeräte (**30**) nach einem der Ansprüche 1–11.

14. Verfahren zum Konfigurieren einer Anzahl von mittels eines Automatisierungsnetzwerks (**20**) kop-

pelbaren Feldgeräten (**30**), wobei das jeweilige Feldgerät (**30**) einen Zufallszahlengenerator (**31**) zur Erzeugung einer Zufallszahl (ZZ) für eine Erzeugung kryptografischer Daten umfasst, mit den Schritten:
Bereitstellen (**601**) eines Startwerts (SW) zur Initialisierung des Zufallszahlengenerators (**31**) des Feldgeräts (**30**),
Bilden (**602**) von Konfigurationsdaten (KD) aus projektierten Daten (PD) und dem bereitgestellten Startwert (SW), und
Übertragen (**603**) der gebildeten Konfigurationsdaten (KD) auf das Feldgerät (**30**).

15. Verfahren nach Anspruch 14, **dadurch gekennzeichnet,** dass der Startwert (SW) verschlüsselt auf das Feldgerät (**30**) übertragen wird und/oder der Startwert (SW) über einen authentisierten und verschlüsselten Kanal auf das Feldgerät (**30**) übertragen wird.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

FIG 1

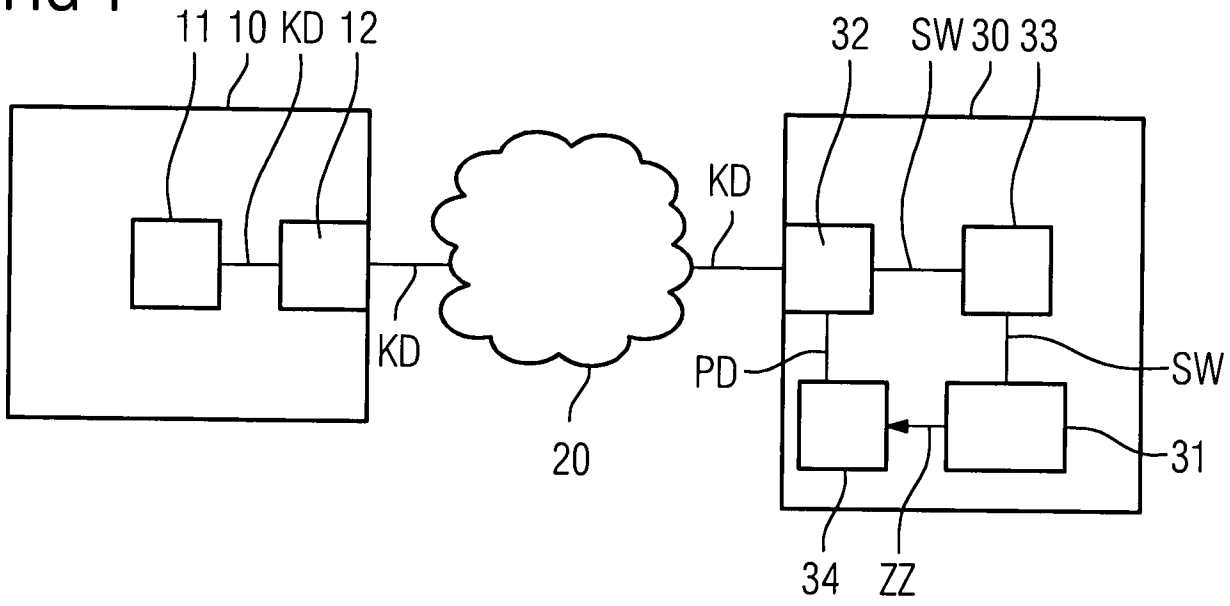


FIG 2

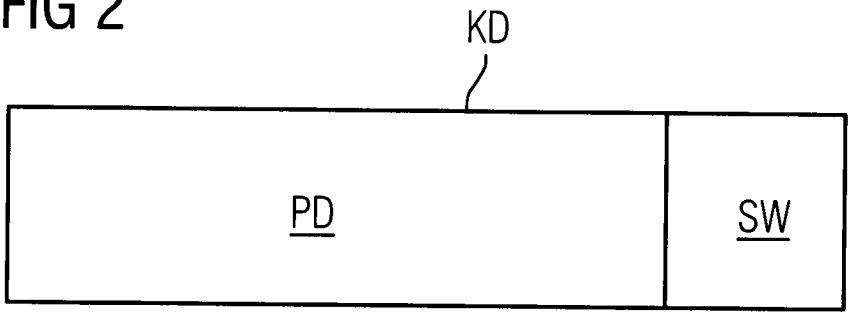


FIG 3

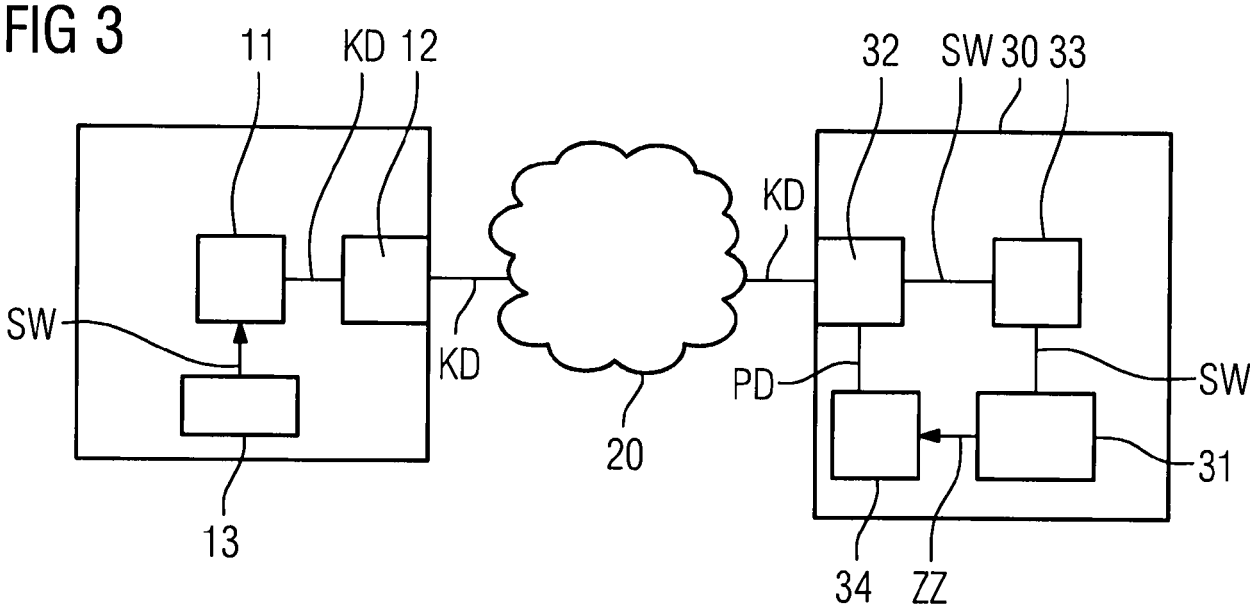

11
KD
12
32
SW
30
33
SW
KD
KD
PD
SW
20
31
13
34
ZZ

FIG 4

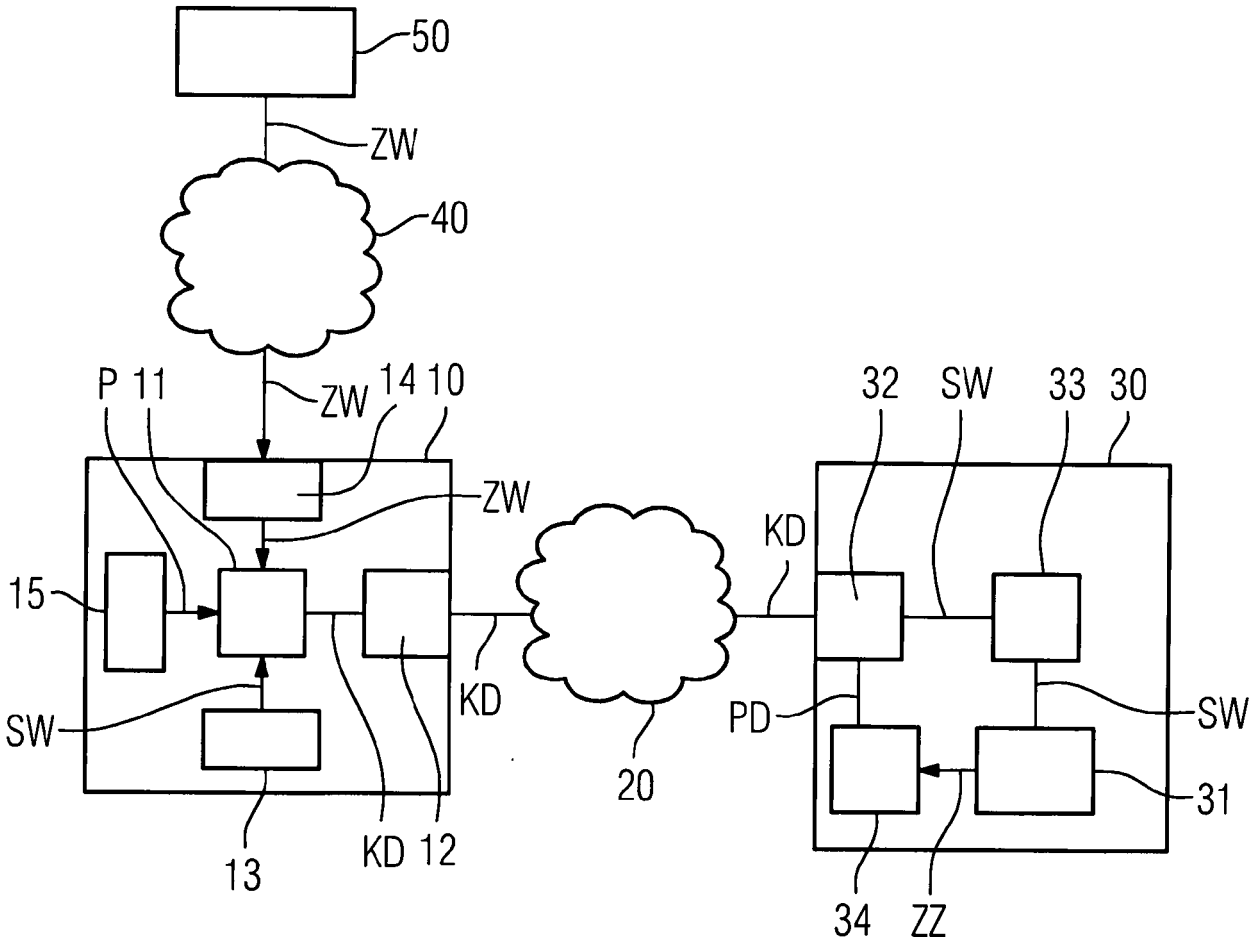

50
ZW
40
P
11
ZW
14
10
32
SW
33
30
ZW
KD
15
SW
KD
PD
SW
20
31
13
KD
12
34
ZZ

FIG 5

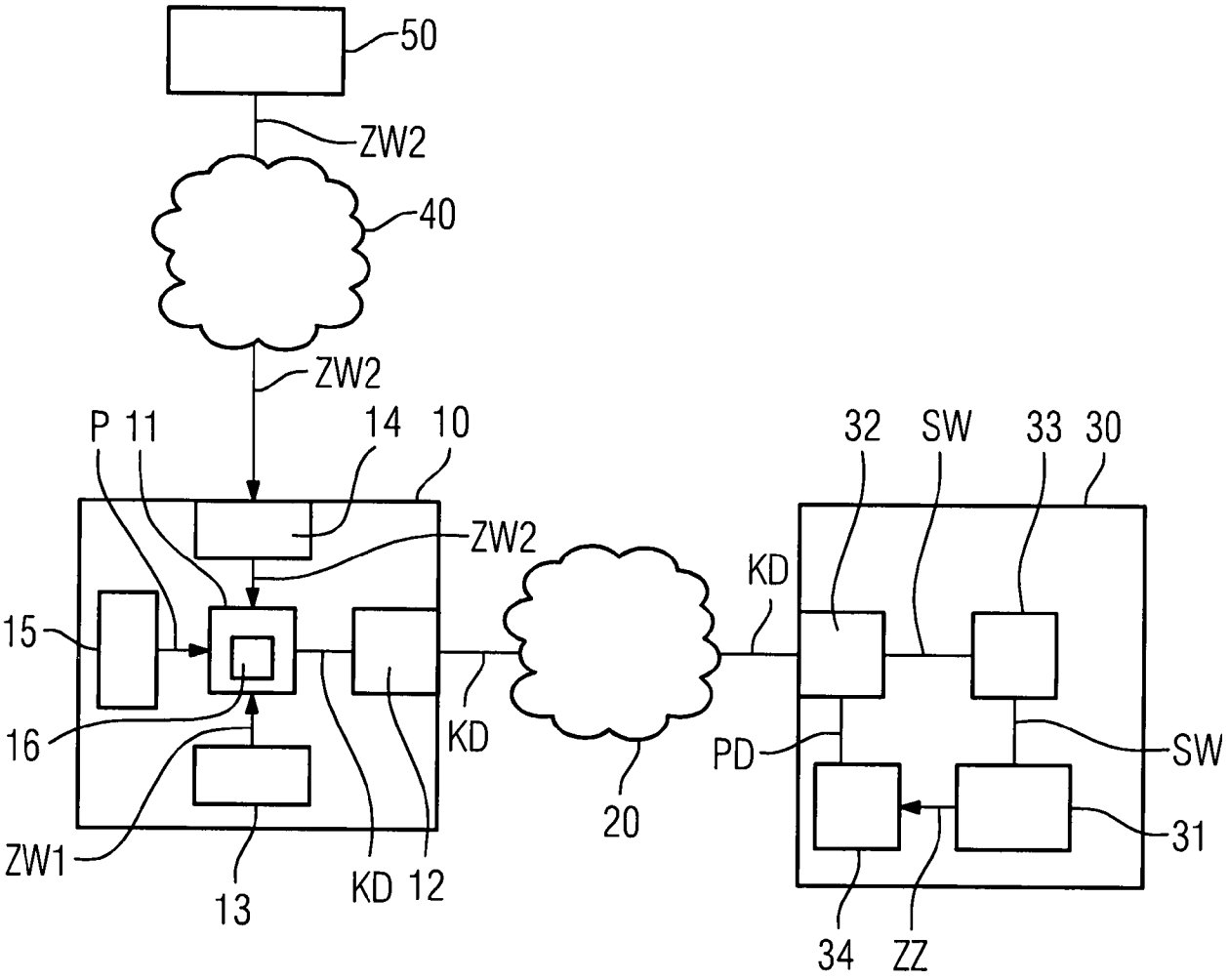
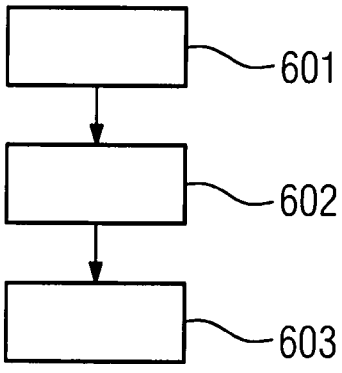

50
ZW2
40
ZW2
P
11
14
10
ZW2
15
16
ZW1
13
KD
12
KD
20
KD
32
SW
33
30
PD
SW
31
34
ZZ

FIG 6


601
602
603