(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
16. März 2017 (16.03.2017)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2017/041831 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2015/070506

(22) Internationales Anmeldedatum:
8. September 2015 (08.09.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **FRANK, Reinhard**; Ebermayerstraße 10, 81369 München (DE). **ZEIGER, Florian**; Spitzwegstr. 56 a, 85521 Ottobrunn (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, 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, ST, 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).

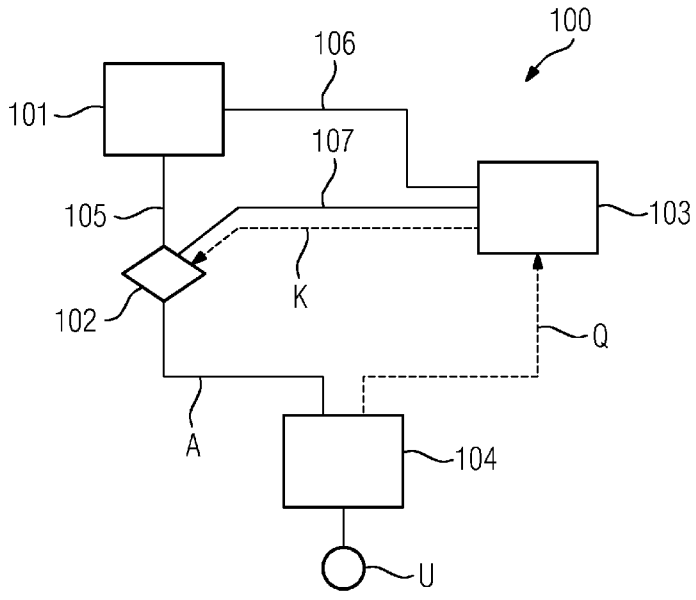
Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) **Title**: METHOD FOR OPERATING AN INDUSTRIAL NETWORK, AND INDUSTRIAL NETWORK

(54) **Bezeichnung** : VERFAHREN ZUM BETREIBEN EINES INDUSTRIENETZWERKS UND INDUSTRIENETZWERK

FIG 1



(57) **Abstract**: The invention relates to a method (300) for operating an industrial network (100). The industrial network (100) has at least one network device (101), which can be actuated by a central control device (103), and a local interface (102) for locally accessing (A) the network device (101). The method has the following steps: - transmitting (301) an access request (Q) for locally accessing (A) the network device (101) via the local interface (A) to the central control device (103); - authenticating (302) the access request (Q) by means of the central control device (103); and - setting up (304) the local interface (102) by means of the central control device in order to locally access (A) the network device (101) on the basis of the access request (Q). The invention further relates to a corresponding industrial network. By using the proposed method and the proposed industrial network, access to the network device can be configured more efficiently and without loss. Furthermore, the security of the industrial network is increased.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2017/041831 A1

Es wird ein Verfahren (300) zum Betreiben eines Industrienetzwerks (100) vorgeschlagen. Das Industrienetzwerk (100) weist mindestens eine Netzwerkeinrichtung (101), die von einer zentralen Steuereinrichtung (103) ansteuerbar ist, und eine lokale Schnittstelle (102) für einen lokalen Zugriff (A) auf die Netzwerkeinrichtung (101) auf. Das Verfahren umfasst: - Übermitteln (301) einer Zugriffsanfrage (Q) für den lokalen Zugriff (A) auf die Netzwerkeinrichtung (101) über die lokale Schnittstelle (A) an die zentrale Steuereinrichtung (103); - Authentifizieren (302) der Zugriffsanfrage (Q) durch die zentrale Steuereinrichtung (103); und - durch die zentrale Steuereinrichtung, Einrichten (304) der lokalen Schnittstelle (102) für den lokalen Zugriff (A) auf die Netzwerkeinrichtung (101) in Abhängigkeit von der Zugriffsanfrage (Q). Ferner wird ein entsprechendes Industrienetzwerk vorgeschlagen. Mit Hilfe des vorgeschlagenen Verfahrens sowie des vorgeschlagenen Industrienetzwerks kann der Zugriff auf die Netzwerkeinrichtung effizienter und verlustfreier gestaltet werden. Ferner kann die Sicherheit des Industrienetzes erhöht werden.

Beschreibung

Verfahren zum Betreiben eines Industrienetzwerks und Industrienetzwerk

Die vorliegende Erfindung betrifft ein Verfahren zum Betreiben eines Industrienetzwerks und ein Industrienetzwerk.

Für Wartungsarbeiten in industriellen Anlagen, z.B. Windparks, wird üblicherweise eine Remote-Service-Lösung angewendet. Demgemäß loggt sich ein Wartungstechniker in ein Industrienetzwerk (Industrial Control Network) der zu wartenden Anlage ein. Die Zugriffsrechte zu dem Industrienetzwerk werden von einer Steuerzentrale erteilt und überwacht. Das Einloggen des Technikers in das Industrienetzwerk, das Authentifizieren des Zugriffs des Technikers und die Überwachung des Technikers im Industrienetzwerk erfolgt durch die Steuerzentrale, was mit hohem technischem Aufwand verbunden ist.

Vor diesem Hintergrund besteht eine Aufgabe der vorliegenden Erfindung darin, ein verbessertes Verfahren zum Betreiben eines Netzwerks bereitzustellen.

Demgemäß wird ein Verfahren zum Betreiben eines Industrienetzwerks vorgeschlagen. Das Industrienetzwerk umfasst mindestens eine Netzwerkeinrichtung, die von einer zentralen Steuereinrichtung ansteuerbar ist. Das Industrienetzwerk umfasst ferner eine lokale Schnittstelle für einen lokalen Zugriff auf die Netzwerkeinrichtung. Der lokale Zugriff auf die Netzwerkeinrichtung kann über die lokale Schnittstelle realisiert werden.

Das Verfahren umfasst folgende Schritte:

Übermitteln einer Zugriffsanfrage für den lokalen Zugriff auf die Netzwerkeinrichtung über die lokale Schnittstelle an die zentrale Steuereinrichtung;

Authentifizieren der Zugriffsanfrage durch die zentrale Steuereinrichtung; und

Einrichten der lokalen Schnittstelle für den lokalen Zugriff auf die Netzwerkeinrichtung in Abhängigkeit von der Zugriffsanfrage, wobei das Einrichten der lokalen Schnittstelle durch die zentrale Steuereinrichtung erfolgt.

Das Industrienetzwerk betrifft insbesondere jede Art industrieller Kommunikationsnetze, z.B. eine Produktionsanlage mit Produktionszellen, einen Windpark oder einen Teil hiervon. Beispielsweise ist das Industrienetzwerk ein Betreibernetzwerk eines Stromversorgungsnetzes, und die Netzwerkeinrichtungen sind einzelne Generatoren, z.B. Windturbinen, in diesem Netzwerk. Das Industrienetzwerk kann ferner ein Verkehrsnetz und/oder ein Versorgungsnetz von Ressourcen, z.B. Strom, Öl, Wasser, Erdgas, Lebensmittel oder Wärme, umfassen.

Insbesondere weist das Industrienetzwerk mehrere Netzwerkeinrichtungen auf. Die Netzwerkeinrichtungen des Industrienetzwerks können einzelne Module, z.B. Produktionsmodule, Steuereinheiten oder Feldgeräte, im Straßenverkehr und/oder in einem Versorgungsnetzwerk betreffen. Insbesondere können die Netzwerkeinrichtungen zumindest teilweise automatisiert arbeiten, d.h. sie benötigen für ihren Betrieb keinen oder lediglich einen reduzierten menschlichen Eingriff. Vorzugsweise sind die Netzwerkeinrichtungen zumindest teilweise miteinander gekoppelt, so dass ein Transport von Daten, Material, Produkten und/oder Ressourcen (z.B. Strom oder Energie) von- und zueinander möglich ist.

Das Industrienetzwerk weist mindestens eine zentrale Steuereinrichtung auf, die die Netzwerkeinrichtungen des Industrienetzwerks zentral steuern kann. Insbesondere ist die zentrale Steuereinrichtung eingerichtet, mit den Netzwerkeinrichtungen zu kommunizieren und/oder zu interagieren, z.B. Daten von den Netzwerkeinrichtungen abzufragen und/oder Daten oder Befehle in die Netzwerkeinrichtungen einzugeben.

Insbesondere kann sich das Industrienetzwerk über einen derart dimensionierten Bereich erstrecken, dass geographische

Entfernungen zwischen den einzelnen Netzwerkeinrichtungen bis zu mehreren zehntausend Kilometern betragen. Das Industrienetzwerk kann eine Hauptleitung (Backbone-Leitung) aufweisen, von der mehrere Zweigverbindungen zu den einzelnen Netzwerkeinrichtungen ausgehen und sie mit dem Industrienetzwerk koppeln. Denkbar sind auch andere Netzwerktopologien, wie Bus-, Ring- oder Stern-Topologien. Alternativ oder zusätzlich kann das Netzwerk mit einem Wide Area Network (WAN) und/oder dem Internet gekoppelt sein.

Für Wartungsarbeiten an einer oder mehreren Netzwerkeinrichtungen kann einem Service-Personal (z.B. Techniker, Operator, Administrator oder Mechaniker) ein Zugriff auf die entsprechende Netzwerkeinrichtung gestattet werden. Es ist vorteilhaft, das Industrienetzwerk von einem Zugriff durch Unbefugte zu schützen. Vorzugsweise ist das Industrienetzwerk ein geschlossenes, privates Kommunikationsnetz. Zu diesem Zweck kann das Industrienetzwerk zumindest teilweise als ein Corporate Network ausgestaltet sein, das räumlich entfernte Einzelnetze eines Unternehmens miteinander vernetzt und beispielsweise über eine gemeinsame Firewall an das Internet anbindet. Der Zugriff zum Industrienetzwerk kann verschlüsselt sein und/oder eine Authentifizierung erfordern. Die zentrale Steuereinrichtung kann ferner zum Überwachen von Zugriffen auf die Netzwerkeinrichtungen eingerichtet sein. Das Service-Personal kann beispielsweise von der zentralen Steuereinrichtung einen lokalen Zugriff auf die Netzwerkeinrichtung anfordern.

Insbesondere erfolgt der lokale Zugriff auf die Netzwerkeinrichtung über die und/oder mit Hilfe der lokalen Schnittstelle, die einer oder mehreren Netzwerkeinrichtungen zugeordnet und mit diesen verbunden ist. Die lokale Schnittstelle kann über ein Local Area Network (LAN), Wireless LAN, Mobilfunk und/oder Kabelverbindungen mit der zugeordneten Netzwerkeinrichtung verbunden sein. Die lokale Schnittstelle kann eine physische und/oder virtuelle Schnittstelle, z.B. eine Maschinenschnittstelle, eine Hardwareschnittstelle, eine Netzwerk-

schnittstelle, eine Datenschnittstelle, eine Softwareschnittstelle oder eine Kombination hiervon, umfassen.

Die physische Schnittstelle stellt einen physischen Anschluss zur Verfügung, an den eine Zugriffseinrichtung, z.B. ein Computer, ein Laptop oder ein sonstiges rechenfähiges Gerät, angeschlossen werden kann, um auf die Netzwerkeinrichtung zuzugreifen. Es ist denkbar, dass die lokale Schnittstelle eine Zugriffseinrichtung bereitstellt oder dass die Zugriffseinrichtung in die lokale Schnittstelle integriert vorliegt.

Ferner kann die physische Schnittstelle einen Netzwerkanschluss umfassen, über den Komponenten des Industrienetzwerks mit der Netzwerkeinrichtung verbunden werden können. Insbesondere kann die physische Schnittstelle ferner zum Konvertieren zwischen verschiedenen Kommunikationsprotokollen eingerichtet sein, um eine Kommunikation zwischen der Netzwerkeinrichtung und unterschiedlichen Netzwerkkomponenten und/oder der Zugriffseinrichtung zu ermöglichen.

Eine virtuelle Schnittstelle kann eine Schnittstelle zwischen Programmen, Applikationen und/oder Betriebssystemen sein, um eine Interaktion zwischen den Programmen, Applikationen und/oder Betriebssystemen der Netzwerkeinrichtung, der Zugriffseinrichtung und/oder Netzwerkkomponenten zu ermöglichen.

Insbesondere ermöglicht die lokale Schnittstelle eine Datenabfrage von der zugeordneten Netzwerkeinrichtung und/oder eine Eingabe von Daten oder Befehlen in die zugeordnete Netzwerkeinrichtung. Die lokale Schnittstelle kann mit einer Rechenleistung ausgestattet sein, um z.B. Daten zu verarbeiten und die zugeordnete Netzwerkeinrichtung zu betreiben. Ferner kann die lokale Schnittstelle über eine Speicherkapazität verfügen, um z.B. Zugriffskonfigurationen, Applikationen oder Benutzerspezifikationen zu speichern. Die lokale Schnittstelle kann als ein Zugriffspunkt (Access Point) angesehen werden.

Die Zugriffsanfrage für den lokalen Zugriff auf die Netzwerkeinrichtung gibt beispielsweise die Netzwerkeinrichtung, auf die zugegriffen werden soll, und/oder eine Identität des Service-Personals an, das den lokalen Zugriff auf die Netzwerkeinrichtung anfordert.

Die Zugriffsanfrage kann beispielsweise über die Leitung des Industrienetzwerks, über eine VPN-Verbindung oder über Mobilfunk an die zentrale Steuereinrichtung übermittelt werden. Die zentrale Steuereinrichtung empfängt die Zugriffsanfrage und wertet diese aus. Die Authentifizierung der Zugriffsanfrage kann von den Ergebnissen der Auswertung der Zugriffsanfrage durch die zentrale Steuereinrichtung abhängen. Falls die Zugriffsanfrage authentifiziert ist, kann die zentrale Steuereinrichtung die lokale Schnittstelle derart einrichten, dass der lokale Zugriff auf die Netzwerkeinrichtung gemäß der Zugriffsanfrage ermöglicht wird.

Vorzugsweise wird eine Vertrauensstufe der Zugriffsanfrage, insbesondere eines die Zugriffsanfrage erstellenden Service-Personals, bestimmt. Dementsprechend kann das Einrichten der lokalen Schnittstelle gemäß der von der zentralen Steuereinrichtung bestimmten Vertrauensstufe der Zugriffsanfrage erfolgen.

Durch das Einrichten der lokalen Schnittstelle für den lokalen Zugriff wird die lokale Schnittstelle aktiviert und für den lokalen Zugriff auf die Netzwerkeinrichtung durch das Service-Personal bereitgestellt. Dabei werden insbesondere die entsprechenden Zugriffsrechte berücksichtigt. Das Einrichten der lokalen Schnittstelle kann ein Aktivieren von physischen Anschlüssen, Starten einer Zugriffseinrichtung oder Herstellen einer Verbindung zwischen der lokalen Schnittstelle und/oder der Netzwerkeinrichtung umfassen. Das Einrichten der lokalen Schnittstelle kann ferner ein Konfigurieren einer virtuellen Schnittstelle an der lokalen Schnittstelle umfassen. Hierbei kann eine von der zentralen Steuer-

einrichtung erstellte Zugriffskonfiguration, z.B. ein Betriebssystem oder ein Satz von Applikationen, an der lokalen Schnittstelle instanziiert werden. Ferner können virtuelle Sensoren, z.B. zur Datenauswertung oder Datenaggregation, an der Netzwerkeinrichtung instanziiert werden. Es sei angemerkt, dass das Instanziieren von Betriebssystemen, Applikationen oder virtuellen Sensoren ein Implementieren, Installieren, Starten, Ausrollen und/oder Aktivieren derselben umfassen kann.

Vorzugsweise erfolgt die Einrichtung der lokalen Schnittstelle isoliert und derart gekapselt, dass die Schnittstelle rückstandsfrei aufgelöst werden kann.

Das Instanziieren umfasst zum Beispiel die jeweils benötigten Konfigurationen, Applikationen, und Kommunikationsverbindungen, die durch virtuelle Komponenten realisiert sind. Somit ist solch ein Zugriff für sich gekapselt. Wenn mehrere unterschiedliche Zugriffe zeitgleich aktiv sind, beeinflussen diese sich somit nicht.

Die Applikationen können z.B. zur Datenabfrage und -eingabe oder zur Steuerung der Netzwerkeinrichtung verwendet werden. Ferner können die Applikationen einen Terminal oder ein Wartungsprogramm zum Interagieren mit der Netzwerkeinrichtung umfassen.

Es ist denkbar, dass Daten (z.B. Applikationen, Programme oder Betriebssysteme) zum Einrichten der lokalen Schnittstelle an der lokalen Schnittstelle oder an der Zugriffseinrichtung gespeichert oder installiert vorliegen.

Beim Einrichten der lokalen Schnittstelle kann ein virtuelles Netzwerk erzeugt und/oder virtuelle Netzwerkfunktionen für dieses virtuelle Netzwerk instanziiert werden. Dabei können unterschiedliche Netzwerkkonfigurationstechnologien, z.B. VPN, Bildung von „Tunneln“ zwischen Netzwerkkomponenten oder Software-Defined-Networking (SDN), angewendet werden.

Das virtuelle Netzwerk ist vorzugsweise auf die Zugriffsanfrage angepasst. Ferner ist das virtuelle Netzwerk z.B. ein virtuelles Overlay-Netz, das auf ein bestehendes Netz, z.B. Industrienetzwerk, ein WAN oder das Internet, aufbaut, d.h. Teile von Strukturen dieses bestehenden Netzes benutzt, um Daten zu transportieren.

Die virtuellen Netzwerkfunktionen können z.B. eine Steuerung des Datenverkehrs (traffic shaping), eine Firewall, eine Vermittlung (switching), eine Datenverkehrslenkung (routing) oder eine Überwachung der Anschlüsse (ports monitoring) umfassen. Insbesondere kann eine virtuelle Firewall an der lokalen Schnittstelle instanziiert werden, um den lokalen Zugriff einzuschränken und/oder zu filtern. Vorzugsweise ist die virtuelle Firewall eine industrielle Firewall speziell zum Schutz von Industrienetzwerken.

Die lokale Schnittstelle kann insbesondere derart eingerichtet sein, dass der lokale Zugriff auf die Netzwerkeinrichtung bestimmten Verbindungsanforderungen, z.B. Vorschriften gemäß Quality of Service (QoS) für das Industrienetzwerk, genügt. Die QoS kann Mindestanforderungen an einer Qualität und/oder einer Güte der Verbindung sowie Datenübertragung in einem Industrienetzwerk vorgeben. Beispielsweise betrifft die QoS eine Geschwindigkeit, Latenzzeiten, einen Jitter oder eine Zuverlässigkeit der Verbindung und/oder Datenübertragung. Ferner kann die QoS eine Häufigkeit von Störungen, Übertragungsfehlern, Verbindungsfehlern und/oder Verbindungsproblemen betreffen.

Gemäß einer Ausführungsform ist der lokale Zugriff auf die Netzwerkeinrichtung zeitlich beschränkt.

Die Zugriffsanfrage kann eine zu erwartende Dauer des lokalen Zugriffs auf die Netzwerkeinrichtung enthalten. Die Zugriffsdauer kann von der zentralen Steuereinrichtung festgelegt, mit der Zugriffsanfrage angefordert, oder allgemein festge-

legt werden. Ferner kann an der zentralen Steuereinrichtung oder an der lokalen Schnittstelle eine vordefinierte Zugriffsdauer gespeichert sein, und die Zugriffsdauer automatisch festgelegt werden. Eine Angabe der Zugriffsdauer kann einen Anfangszeitpunkt, einen Endzeitpunkt und/oder ein Zeitintervall des lokalen Zugriffs auf die Netzwerkeinrichtung umfassen.
Durch die zeitliche Beschränkung des lokalen Zugriffs kann ein unerwünschter Zugriff auf das Industrienetzwerk nach dem Ablauf der Zugriffsdauer ausgeschlossen werden. Damit kann die Sicherheit des Industrienetzwerks erhöht werden.

Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner Deaktivieren der lokalen Schnittstelle, nachdem der lokale Zugriff auf die Netzwerkeinrichtung beendet ist.

Dadurch wird ein unnötiges Fortbestehen einer Zugriffsmöglichkeit auf die Netzwerkeinrichtung und/oder das Industrienetzwerk nach Beendigung des lokalen Zugriffs verhindert und ein Sicherheitsrisiko beseitigt.

Das Deaktivieren der lokalen Schnittstelle kann insbesondere ein Deaktivieren von Komponenten, die an der lokalen Schnittstelle instanziiert oder erzeugt sind, umfassen. Die Komponenten betreffen z.B. das virtuelle Netzwerk, die virtuellen Netzwerkfunktionen, die Applikationen und/oder die Betriebssysteme. Ein Deaktivieren kann ein Schließen, Löschen, Deinstallieren, Stoppen, Abbrechen, Rückabwickeln, Entfernen oder Beseitigen der entsprechenden Komponente umfassen.

Gemäß einer weiteren Ausführungsform erfolgt der lokale Zugriff auf die Netzwerkeinrichtung mit Hilfe einer Zugriffseinrichtung, die mit der lokalen Schnittstelle gekoppelt ist. Ferner wird an der Zugriffseinrichtung ein Zugriffsdatensatz zum Freischalten des lokalen Zugriffs auf die Netzwerkeinrichtung über die lokale Schnittstelle bereitgestellt, falls die Zugriffsanfrage durch die zentrale Steuereinrichtung authentifiziert ist.

Vorzugsweise enthält der Zugriffsdatensatz Informationen über die Vertrauensstufe des lokalen Zugriffs und/oder des Service-Personals, dem der Zugriffsdatensatz zugeordnet ist. Der Zugriffsdatensatz kann personalisiert sein, d.h. einem die Zugriffsanfrage erstellenden Service-Personal angepasst und/oder nur für dieses Service-Personal gültig sein. Der lokale Zugriff auf die Netzwerkeinrichtung kann insbesondere durch ein Erstellen eines Kontos (Access Account), mit dem sich das Service-Personal in das Industrienetzwerk einwählen kann, bereitgestellt sein. Entsprechend kann der Zugriffsdatensatz Kontodaten, z.B. eine Benutzeridentifikation und einen Schlüssel, zum Einwählen in die Netzwerkeinrichtung und/oder das Industrienetzwerk enthalten.

Der Zugriffsdatensatz kann von der zentralen Steuereinrichtung in Abhängigkeit von Ergebnissen der Auswertung der Zugriffsanfrage erstellt werden. Der Zugriffsdatensatz kann an der zentralen Steuereinrichtung vorgespeichert vorliegen und nach einer Authentifizierung der Zugriffsanfrage ausgegeben werden. Der Zugriffsdatensatz kann eine Zeitdauer umfassen, innerhalb welcher der Zugriff auf die Netzwerkeinrichtung gewährt ist. Vorzugsweise erfolgt die Übertragung des Zugriffsdatensatzes verschlüsselt.

Es ist ferner denkbar, dass das Einrichten der lokalen Schnittstelle für den lokalen Zugriff auf die Netzwerkeinrichtung dann erfolgt, wenn das Service-Personal den Zugriffsdatensatz in die lokale Schnittstelle oder in eine Zugriffseinrichtung, die mit der lokalen Schnittstelle verbunden ist, eingibt.

Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner ein Erzeugen eines virtuellen Netzwerks. Das virtuelle Netzwerk des Industrienetzwerks ist dann Teil des Industrienetzwerks und umfasst mindestens die Netzwerkeinrichtung, auf die die Zugriffsanfrage gerichtet ist. Dabei ist die zentrale Steuereinrichtung aus dem virtuellen Netzwerk ausgegliedert,

also vorzugsweise nicht Teil des von der Zugriffseinrichtung verwendeten virtuellen Netzwerks für den lokalen Zugriff auf die mindestens eine Netzwerkwerkeinrichtung.

Als virtuelles Netzwerk kommen zu Beispiel Overlay-Netze infrage. Denkbar sind protokollbasierte Netze, wie VLANS, VPN, VPLS oder dergleichen und Software-definierte Netzte (SDN).

Dadurch kann ein gekapseltes Netzwerk erzeugt werden, in dem der Zugriff auf die lokale Schnittstelle und die zugeordnete Netzwerkeinrichtung eingeschränkt ist. Ein Sicherheitsrisiko für das Industrienetzwerk kann damit gesenkt werden.

Ferner erfolgt ein Datentransport zwischen dem Service-Personal und der Netzwerkeinrichtung nicht über die zentrale Steuereinrichtung, so dass eine verbesserte Verbindungsgüte aufgrund geringerer Latenzzeiten oder Schwankungen erzielt werden kann.

Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner ein Übermitteln von Zugriffsspezifikationen der Zugriffsanfrage an die zentrale Steuereinrichtung. Dabei umfassen die Zugriffsspezifikationen eine Kennung einer Zugriffseinrichtung, eine Identität eines Bedieners, eine Verbindungsart des lokalen Zugriffs, Verbindungsanforderungen des lokalen Zugriffs, eine Zugriffsdauer und/oder für den lokalen Zugriff vorgesehene Ressourcen. Das Verfahren umfasst weiterhin das Einrichten der Schnittstelle für den lokalen Zugriff auf die Netzwerkeinrichtung gemäß den Zugriffsspezifikationen.

Insbesondere können die Zugriffsspezifikationen eine Bandbreite und/oder eine Rechenleistung für den lokalen Zugriff auf die Netzwerkeinrichtung festlegen. Für den Fall, dass gleichzeitig mehrere lokale Zugriffe auf die Netzwerkeinrichtung stattfinden, kann es vorteilhaft sein, eine Aufteilung von Ressourcen, insbesondere der Bandbreite und der Rechenleistung an der lokalen Schnittstelle und Netzwerkeinrich-

tung, z.B. mit Hilfe von Priorisierung von Verbindungen, festzulegen und zu verwalten.

Die Verbindungsanforderungen können insbesondere durch Normen, z.B. Quality of Service oder Dienstgüte eines Kommunikationsdienstes, bestimmt sein. Die Verbindungsanforderungen können vorgegebenen Standards, z.B. IEEE 802.1p, entsprechen.

Gemäß einer weiteren Ausführungsform umfasst das Einrichten der lokalen Schnittstelle ein Instanziieren von Applikationen an der lokalen Schnittstelle.

Die Applikationen umfassen beispielsweise Anwendungen, die bei dem lokalen Zugriff auf die Netzwerkeinrichtung verwendet werden. Ferner können die Applikationen virtuelle Sensoren umfassen, die an der Netzwerkeinrichtung instanziiert werden. Ferner können die Applikationen an der Zugriffseinrichtung, die mit der lokalen Schnittstelle verbunden ist, instanziiert werden.

Gemäß einer weiteren Ausführungsform erfolgt das Einrichten der lokalen Schnittstelle mit Hilfe von Vorlagen, die an der zentralen Steuereinrichtung gespeichert vorliegen.

Die Vorlagen können Komponenten oder Bestandteile von Daten oder Informationen umfassen, die für das Einrichten der lokalen Schnittstelle für den Zugriff auf die Netzwerkeinrichtung relevant sind. Beispielsweise umfassen die Vorlagen Informationen über die Vertrauensstufe, Zugriffsart, Zugriffsdauer, Verbindungsanforderungen, Zugriffseinrichtung und/oder Ressourcenverteilung. Insbesondere können die Vorlagen zumindest teilweise Zugriffsspezifikationen für den Zugriff auf die Netzwerkeinrichtung enthalten.

Gemäß einer weiteren Ausführungsform erfolgt das Übermitteln der Zugriffsanfrage an die zentrale Steuereinrichtung verschlüsselt. Zusätzlich oder alternativ erfolgt das Einrichten

der lokalen Schnittstelle durch die zentrale Steuereinrichtung verschlüsselt.

Dadurch kann die Sicherheit des Industrienetzwerks weiter erhöht sein. Insbesondere kann ein Angriff von außen besser abgewehrt werden.

Gemäß einer weiteren Ausführungsform erfolgt der lokale Zugriff auf die Netzwerkeinrichtung zum Warten, Überprüfen, Überwachen, Modifizieren, Betreiben, Reparieren, Anschalten, Abschalten, Ansteuern der Netzwerkeinrichtung und/oder zum lokalen Abrufen von Daten von der Netzwerkeinrichtung.

Das Service-Personal kann den lokalen Zugriff zu einem der oben genannten Zwecke durchführen. Insbesondere werden technische Arbeiten an der zugeordneten Netzwerkeinrichtung ausgeführt.

Gemäß einer weiteren Ausführungsform erfolgt der lokale Zugriff auf die Netzwerkeinrichtung über ein Local Area Network (LAN) und/oder mit Hilfe von Wireless-LAN, Bluetooth, Mobilfunk-Technologien, LTE-basierten Verbindungen und/oder kabelgebunden.

Dadurch kann eine Verbindungsgüte beim lokalen Zugriff auf die Netzwerkeinrichtung verbessert werden. Zusätzlich kann eine kurze Datenübertragungsstrecke die Verbindungsgüte weiter verbessern.

Gemäß einer weiteren Ausführungsform umfasst das Industrienetzwerk mehrere Netzwerkeinrichtungen. Dabei umfasst die Zugriffsanfrage einen lokalen Zugriff auf ein Unternetz von mehreren Netzwerkeinrichtungen des Industrienetzwerks, wobei der lokale Zugriff über die lokale Schnittstelle erfolgt.

Die oben beschriebenen Merkmale des Verfahrens können auch auf einen lokalen Zugriff auf ein Unternetz des Industrienetzwerks angewendet werden. Das Unternetz von Netzwerkein-

richtungen kann ein Verband von geographisch nahe beieinander liegenden Netzwerkeinrichtungen sein. Insbesondere kann das Unternetz einem Standort von mehreren Standorten des Industrienetzwerks entsprechen. Ein Unternetz kann insbesondere durch die Funktionalitäten der Netzwerkeinrichtungen, beispielsweise Controller für Feldgeräte in Automatisierungsnetzen, festgelegt sein.

Das Unternetz kann eine definierte Teilmenge von Netzwerkeinrichtungen des Industrienetzwerks umfassen. Ferner kann das Unternetz in Form eines virtuellen Netzwerks ausgebildet sein. Eine lokale Schnittstelle eines Unternetzes kann mit jeder der Netzwerkeinrichtungen des Unternetzes verbunden sein und einen lokalen Zugriff auf jede der Netzwerkeinrichtungen ermöglichen.

Gemäß einer weiteren Ausführungsform weist der lokale Zugriff auf die Netzwerkeinrichtung eine geringere Datenübertragungsstrecke auf als eine Datenübertragungsstrecke zum Ansteuern der Netzwerkeinrichtung durch die zentrale Steuereinrichtung.

Insbesondere ist eine geographische Entfernung zwischen der Netzwerkeinrichtung und der zentralen Steuereinrichtung größer als eine geographische Entfernung zwischen der Netzwerkeinrichtung und der lokalen Schnittstelle. Eine kürzere Datenübertragungsstrecke kann Latenzzeiten bei der Datenübertragung verringern und/oder unerwünschte Schwankungen (z.B. Jitter) reduzieren. Auf diese Weise kann zum Beispiel die Verbindungsgüte verbessert werden. Das Verfahren ermöglicht insbesondere, dass die für eine jeweilige Applikation erforderlichen Garantien zur Verbindungsgüte realisiert werden können.

Vorzugsweise wird eine lokale Schnittstelle geplant zugewiesen und es werden entsprechende Ressourcen, beispielsweise einer zugrundeliegenden Netzwerkinfrastruktur, bereitgestellt. Dadurch können bestimmte Verbindungsgüten über den

Zeitraum des Bestehens der lokalen Schnittstelle auch garantiert werden.

Gemäß einem zweiten Aspekt der vorliegenden Erfindung wird ein Industrienetzwerk vorgeschlagen. Das Industrienetzwerk umfasst mindestens eine Netzwerkeinrichtung, die von einer zentralen Steuereinrichtung ansteuerbar ist. Ferner umfasst das Industrienetzwerk eine lokale Schnittstelle für den lokalen Zugriff auf die Netzwerkeinrichtung. Das Industrienetzwerk ist zum Ausführen des oben beschriebenen Verfahrens geeignet.

Insbesondere umfasst das Industrienetzwerk mehrere Netzwerkeinrichtungen. Sämtliche Merkmale, die oben für das Verfahren zum Betreiben eines Industrienetzwerks vorgeschlagen sind, können auch auf das vorgeschlagene Industrienetzwerk entsprechend angewendet werden.

Gemäß einer Ausführungsform ist das Industrienetzwerk zumindest teilweise in Form eines virtuellen persönlichen Netzwerks (Virtual Personal Network, VPN) in einem Netzwerk bereitgestellt.

Insbesondere erfolgt ein Datentransport in dem Industrienetzwerk zumindest teilweise über ein Wide Area Network (WAN) oder das Internet, die als ein Übertragungsweg für das Industrienetzwerk benutzt werden. Zusätzlich oder alternativ kann das Industrienetzwerk eine Hauptleitung (Backbone-Leitung) oder Funkverbindung zum Übertragen von Daten aufweisen.

Das vorgeschlagene Verfahren sowie das vorgeschlagene Industrienetzwerk ermöglichen insbesondere einen lokalen Zugriff auf die Netzwerkeinrichtung mit Unterstützung von industriellen Dienstgüteanforderungen. Ferner ist ein aufwendiges Routing von Verbindungen über weite geographische Entfernungen nicht erforderlich. Der lokale Zugriff kann temporär bereitgestellt sein. Durch das Deaktivieren des lokalen Zugriffs

können eventuell schadhafte oder mit Sicherheitsrisiken behaftete Verbindungen und/oder Funktionen beseitigt werden. Dadurch kann eine erhöhte Sicherheit für das Industrienetzwerk erreicht werden.

Netzwerkressourcen, zum Beispiel Bandbreite oder Rechenkapazitäten, können bedarfsorientiert organisiert und angefordert werden. Ebenso kann ein Überwachungsaufwand von Zugriffen auf die Netzwerkeinrichtungen des Industrienetzwerks reduziert werden.

Die jeweilige Einheit, zum Beispiel die Zugriffseinrichtung, die lokale Schnittstelle oder die zentrale Steuereinrichtung, 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 Steuerrechner eines Fahrzeuges 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.

Weiterhin wird ein Computerprogrammprodukt vorgeschlagen, welches auf einer programmgesteuerten Einrichtung, wie zum Beispiel Elemente des Netzwerks, die Durchführung des wie oben erläuterten Verfahrens veranlasst. Eine jeweilige programmgesteuerte Einrichtung kann sowohl software- wie auch hardwarebasiert sein. Denkbar ist zum Beispiel eine Implementierung der Zugriffseinrichtung als eine herunterladbare oder kurzzeitig installier- oder aktivierbare Zugriffsapplikation auf einem Smartphone.

Ein Computerprogrammprodukt, wie z.B. ein Computerprogramm-Mittel, kann beispielsweise als Speichermedium, wie z.B. Speicherkarte, USB-Stick, CD-ROM, DVD, oder auch in Form einer herunterladbaren Datei von einem Server in einem Netzwerk bereitgestellt oder geliefert werden. Dies kann zum Beispiel

in einem drahtlosen Kommunikationsnetzwerk durch die Übertragung einer entsprechenden Datei mit dem Computerprogrammprodukt oder dem Computerprogramm-Mittel erfolgen.

Die für das vorgeschlagene Verfahren beschriebenen Ausführungsformen und Merkmale gelten für das vorgeschlagene Industrienetzwerk entsprechend.

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.

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.

Fig. 1 zeigt eine schematische Ansicht einer ersten Ausführungsform eines Industrienetzwerks mit einer Zugriffseinrichtung;

Fig. 2 zeigt eine schematische Ansicht einer zweiten Ausführungsform eines Industrienetzwerks mit der Zugriffseinrichtung;

Fig. 3 zeigt ein Sequenzdiagramm eines Verfahrens zum Betreiben eines Industrienetzwerks;

Fig. 4 zeigt eine schematische Ansicht einer dritten Ausführungsform eines Industrienetzwerks mit der Zugriffseinrichtung;

Fig. 5 zeigt eine schematische Ansicht einer vierten Ausführungsform eines Industrienetzwerks mit der Zugriffseinrichtung; und

Fig. 6 zeigt eine schematische Ansicht einer fünften Ausführungsform eines Industrienetzwerks mit der Zugriffseinrichtung.

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

Fig. 1 zeigt eine schematische Ansicht einer ersten Ausführungsform eines Industrienetzwerks 100 mit einer Zugriffseinrichtung 104.

Das Industrienetzwerk 100 umfasst eine Netzwerkeinrichtung 101 und eine lokale Schnittstelle 102. Die lokale Schnittstelle 102 ist über eine Leitung 105 mit der Netzwerkeinrichtung 101 verbunden. Die Netzwerkeinrichtung 101 und die lokale Schnittstelle 102 sind über eine jeweilige Leitung 106, 107 mit einer zentralen Steuereinrichtung 103 verbunden. Die lokale Schnittstelle 102 erlaubt einem Service-Personal U, das ein Techniker, ein Bediener, ein Mechaniker oder ein Systemadministrator ist, einen lokalen Zugriff A auf die Netzwerkeinrichtung 101.

Die lokale Schnittstelle 102 ist mit einer Zugriffseinrichtung 104 verbunden. Die Zugriffseinrichtung 104 ist mit einer Rechenleistung und einer Speicherkapazität ausgestattet. Die Zugriffseinrichtung 104 ist ein Computer, ein mobiler Rechner oder ein Terminal im Industrienetzwerk 100. Mit Hilfe der Zugriffseinrichtung 104 kann über die lokale Schnittstelle 102 auf die Netzwerkeinrichtung 101 zugegriffen werden. Die Zugriffseinrichtung 104 ist über eine physische Leitung, z.B. ein Ethernet-Kabel, oder drahtlos, z.B. über W-LAN, oder per Mobilfunk, z.B. über eine LTE-Advanced-Verbindung, mit der lokalen Schnittstelle 102 verbunden.

Das Service-Personal U sendet eine Zugriffsanfrage Q über die Zugriffseinrichtung 104 an die zentrale Steuereinrichtung 103. Die Steuereinrichtung 103 wertet diese Zugriffsanfrage Q aus, authentifiziert die Zugriffsanfrage Q und legt eine Vertrauensstufe des Service-Personals U fest. Ferner erstellt die zentrale Steuereinrichtung 103 eine Zugriffskonfiguration K, gemäß welcher die lokale Schnittstelle 102 für den lokalen Zugriff A auf die Netzwerkeinrichtung 101 durch das Service-Personal U eingerichtet wird.

Die lokale Schnittstelle 102 ist insbesondere mit einer Rechenleistung und einer Speicherkapazität ausgestattet, um die Zugriffskonfiguration K zu speichern und/oder auszuführen. Die Zugriffskonfiguration K wird an die lokale Schnittstelle 102 übermittelt und dort instanziiert. Dabei werden ein Satz von Applikationen an der lokalen Schnittstelle 102, und virtuelle Sensoren zum Erfassen und Verarbeiten von Daten an der Netzwerkeinrichtung 101 installiert und gestartet.

Folglich ist die lokale Schnittstelle 102 für den lokalen Zugriff A auf die Netzwerkeinrichtung 101 eingerichtet. Mit Hilfe der Applikationen und virtuellen Sensoren kann das Service-Personal U mit der Netzwerkeinrichtung 101 interagieren und Daten von ihr abfragen. Ferner kann der lokale Zugriff A auf die Netzwerkeinrichtung 101 zum Warten, Steuern, Betreiben, Bedienen, Reparieren, Modifizieren der Netzwerkeinrichtung 101 oder Abfragen Daten von der Netzwerkeinrichtung 101 erfolgen.

Fig. 2 zeigt eine schematische Ansicht einer zweiten Ausführungsform eines Industrienetzwerks 200 mit der Zugriffseinrichtung 104 in Fig. 1.

Das Industrienetzwerk 200 weist alle Merkmale und Elemente sowie Einrichtungen des Industrienetzwerks 100 in Fig. 1 auf. Zusätzlich ist die zentrale Steuereinrichtung 103 mit einer Datenbankeinrichtung 201 ausgestattet, an der Vorlagen für

das Einrichten der lokalen Schnittstelle 102 für den lokalen Zugriff A auf die Netzwerkeinrichtung 101 vorgespeichert vorliegen.

Die Vorlagen umfassen sowohl vorgefertigte Zugriffskonfigurationen als auch Komponenten für eine Zugriffskonfiguration. Die Vorlagen umfassen insbesondere Zugriffsspezifikationen, z.B. Verbindungsanforderungen, eine Kennung einer Zugriffseinrichtung, eine Identität oder Vertrauensstufe des Service-Personals U, eine Verbindungsart des lokalen Zugriffs A, eine Zugriffsdauer und/oder Ressourcen, die den lokalen Zugriff A auf die Netzwerkeinrichtung 101 charakterisieren.

Beispielsweise Handelt es sich bei dem Industrienetzwerk um ein Stromversorgungsnetz mit einer Windkraftanlage als Netzwerkeinrichtung 101. Das Service-Personal U, das ein Techniker des Herstellers der Windkraftanlage 101 ist, fordert von der zentralen Steuereinrichtung 103, die ein zentraler Serverrechner des Betreibers der Windkraftanlage 101 ist, einen Zugriff auf die Steuereinheit der Windkraftanlage 101 für 8 Stunden an, um eine planmäßige Untersuchung durchzuführen. Die Untersuchung betrifft unter anderem eine Laufleistung, einen Verschleiß, Fluktuationen von Kenngrößen (Spannung, Frequenz und Amplitude) und eine korrekte Ansteuerbarkeit. In einem weiteren Beispiel fordert das Service-Personal von dem zentralen Serverrechner den Zugriff auf die Windkraftanlage 101 an, um statistische Daten, z.B. erzeugte elektrische Leistung der letzten 2 Wochen, zu erfassen.

Die zentrale Steuereinrichtung 103 erstellt die Zugriffskonfiguration K für den lokalen Zugriff A auf die Netzwerkeinrichtung basierend auf den an der Datenbankeinrichtung 201 gespeicherten Vorlagen. Anschließend wird die Zugriffskonfiguration K an die lokale Schnittstelle 102 übermittelt und dort instanziiert.

Nach erfolgreicher Authentifizierung der Zugriffsanfrage Q erstellt die zentrale Steuereinrichtung 103 einen Zugriffsda-

tensatz T in Form eines Zugriffstokens gemäß der Vertrauensstufe des Service-Personals U. Das Zugriffstoken T enthält eine Benutzerkennung und ein Passwort für das Einwählen in das Industrienetzwerk 200 sowie eine Zugriffsdauer, z.B. 24 Stunden oder 7 Tage, innerhalb welcher der lokale Zugriff A gestattet ist. Die Zugriffsanfrage Q sowie das Zugriffstoken T werden in einer verschlüsselten, vorzugsweise privaten Verbindung, z.B. über das Internet als eine VPN-Verbindung, übermittelt.

Fig. 3 zeigt ein Sequenzdiagramm eines Verfahrens 300 zum Betreiben eines Industrienetzwerks. Insbesondere eignet sich das Verfahren 300 in Fig. 3 zum Betreiben der Industrienetzwerke 100, 200 in Fig. 1 und 2. Ferner eignet sich das in Fig. 3 gezeigte Verfahren 300 zum Betreiben von Industrienetzwerken, die in Fig. 4 bis 6 dargestellt sind und im Folgenden erläutert werden.

In Fig. 3 ist die zentrale Steuereinrichtung 103, die Zugriffseinrichtung 104 und die lokale Schnittstelle 102 symbolisch in einer horizontalen Reihe nebeneinander dargestellt. Eine vertikale Zeitachse 310 zeigt einen zeitlichen Ablauf des Verfahrens 300.

In einem ersten Schritt 301 wird die Zugriffsanfrage Q von der Zugriffseinrichtung 104 oder dem Service-Personal U an die zentrale Steuereinrichtung 103 übermittelt. Die Zugriffsanfrage Q kann dabei die angeforderten Zugriffsspezifikationen S enthalten.

In einem nächsten Schritt 302 wird die Zugriffsanfrage Q von der zentralen Steuereinrichtung 103 authentifiziert. Insbesondere werden die Zugriffsspezifikationen S ausgewertet. Gegebenenfalls werden vorgespeicherte Vorlagen, z.B. an der Datenbank 201 in Fig. 2, ermittelt, die der Zugriffsanfrage oder den Zugriffsspezifikationen entsprechen. Optional wird ferner eine Vertrauensstufe des Service-Personals U festgelegt.

Nach einer erfolgreichen Authentifizierung der Zugriffsanfrage Q erstellt die zentrale Steuereinrichtung 103 in einem nächsten Schritt 303 die Zugriffskonfiguration K zum Einrichten der lokalen Schnittstelle 102 für den lokalen Zugriff A auf die Netzwerkeinrichtung 101. Optional erstellt die zentrale Steuereinrichtung 103 ferner den Zugriffsdatensatz T für das Service-Personal U. Ferner optional erstellt die zentrale Steuereinrichtung 103 an der lokalen Schnittstelle 102 oder an der Zugriffseinrichtung 104 ein Zugriffskonto, mit dem sich das Service-Personal U in die Netzwerkeinrichtung 101 oder das Industrienetzwerk 100, 200 einwählen kann. Die Zugriffseinrichtung ist ein Rechner oder ein Terminal, die mit der lokalen Schnittstelle 102 verbunden oder in diese integriert sind.

In einem nächsten Schritt 304 wird die Zugriffskonfiguration K von der zentralen Steuereinrichtung 103 an die lokale Schnittstelle 102 übermittelt und dort instanziiert. Auf diese Weise ist die lokale Schnittstelle 102 für einen lokalen Zugriff A auf die Netzwerkeinrichtung 101 eingerichtet. Das Übermitteln der Zugriffskonfiguration K erfolgt verschlüsselt und über eine private Verbindung, z.B. über das Internet als eine VPN-Verbindung.

In einem weiteren Schritt 305 wird der Zugriffstoken T dem Service-Personal U bereitgestellt. Der Zugriffstoken T kann dem Service-Personal direkt, z.B. über Mobilfunk oder eine VPN-Verbindung, mitgeteilt oder an der lokalen Schnittstelle 102 und/oder an der Zugriffseinrichtung 104 bereitgestellt sein. Dabei erfolgt das Übermitteln des Zugriffstoken T verschlüsselt. Ferner optional enthält der Zugriffstoken T Zugriffskontodaten, z.B. eine Benutzerkennung und ein Passwort, zum Einwählen in die Netzwerkeinrichtung 101 oder das Industrienetzwerk 100, 200 unter Verwendung des Zugriffskontos.

In einem weiteren Schritt 306 erfolgt der lokale Zugriff A auf die Netzwerkeinrichtung 101 von der Zugriffseinrichtung

104 aus über die lokale Schnittstelle 102. Der lokale Zugriff A ermöglicht insbesondere Wartungsarbeiten, Service-Dienste oder Datenabfragen an der Netzwerkeinrichtung 101.

In einem abschließenden Schritt 307 wird die lokale Schnittstelle 102 geschlossen und für den lokalen Zugriff A gesperrt. Optional wird ferner der Zugriffsdatensatz T gelöscht und deaktiviert, so dass der Zugriffsdatensatz T nicht mehr gültig ist.

Im Folgenden werden das Industrienetzwerk und das Verfahren anhand von Beispielen von Windkraftanlagen und Windparks veranschaulicht. Die in Fig. 4 bis 6 gezeigten Beispiele weisen sämtliche Merkmale des in Fig. 1 gezeigten Industrienetzwerks 100 und des mit Hilfe von Fig. 1 erläuterten Verfahrens zum Betreiben des Industrienetzwerks 100.

Fig. 4 zeigt eine schematische Ansicht einer dritten Ausführungsform eines Industrienetzwerks 400 mit der Zugriffseinrichtung 104.

Das Industrienetzwerk 400 umfasst einen Windpark mit Windkraftanlagen 101a bis 101c. Die Windkraftanlagen 101a - 101c sind mit einer jeweiligen lokalen Schnittstelle 102a - 102b verbunden, die einen lokalen Zugriff auf die zugeordnete Windkraftanlage 101a – 101c ermöglicht.

Die zentrale Steuereinrichtung 103 ist als ein Server-Rechner mit einer Rechenleistung und Speicherkapazität ausgebildet. Die Zugriffseinrichtung 104 ist ein mobiler Rechner, der mit den lokalen Schnittstellen 102a – 102c verbunden werden kann.

Fig. 4 zeigt einen lokalen Zugriff A auf die Netzwerkeinrichtung 101c von dem mobilen Rechner 104 aus über die lokale Schnittstelle 102c. Von dem mobilen Rechner 104 aus wird eine Zugriffsanfrage Q an den Server-Rechner 103 übermittelt. Der Server-Rechner 103 wertet die Zugriffsanfrage Q aus. Nach erfolgreicher Authentifizierung der Zugriffsanfrage Q wird ein

Zugriffsdatensatz T erstellt und an den mobilen Rechner 104 übermittelt. Ferner legt der Server-Rechner 103 die Zugriffskonfiguration K fest, die an die lokale Schnittstelle 102c übermittelt und dort instanziiert wird.

Das Service-Personal U verbindet den mobilen Rechner 104 mit der lokalen Schnittstelle 102c und wählt sich mit dem Zugriffsdatensatz T auf den mobilen Rechner 104 in das Industrienetzwerk 400 ein. An dem mobilen Rechner werden ein Betriebssystem und verschiedene Applikationen gestartet, die von der Zugriffskonfiguration K vorgegeben und für den lokalen Zugriff erforderlich sind. Ferner wird ein virtueller Sensor zum Erfassen von Leistungskennlinien an der Windkraftanlage 101c instanziiert.

Die Zugriffskonfiguration K ist insbesondere so ausgestaltet, dass der lokale Zugriff unter Verwendung des Zugriffsdatensatzes T auf die lokale Schnittstelle 102c und die zugeordnete Windkraftanlage 101c beschränkt ist. Zu diesem Zweck wird ein virtuelles Netzwerk 401 erzeugt, das nur einen Teil des Industrienetzwerks 400 umfasst und einen Zugriff auf weitere Netzwerkeinrichtungen 101a, 101b durch das Service-Personal verhindert.

Ferner werden an der lokalen Schnittstelle virtuelle Netzwerkfunktionen für das virtuelle Netzwerk 401 instanziiert. Zum Einrichten des virtuellen Netzwerks 401 werden Netzwerkkonfigurationstechnologien wie VPN, Bildung von „Tunneln" zwischen Netzwerkkomponenten und SDN angewendet. Eine VPN-basierte Verbindung erfolgt über ein WAN oder das Internet, ohne für Unbefugte zugänglich zu sein. Der Tunnel erlaubt zwei oder mehreren Teilnehmern des Industrienetzes, über eine Verbindung (z.B. Internet), die ein anderes Kommunikationsprotokoll verwendet als das Industrienetz, miteinander zu kommunizieren. Die SDN-Technologie ermöglicht eine softwarebasierte Konfiguration und Strukturierung des Industrienetzwerks, insbesondere von virtuellen Netzwerken innerhalb des Industrienetzwerks, durch die zentrale Steuereinrichtung.

Die virtuellen Netzwerkfunktionen umfassen eine gezielte Steuerung des Datenverkehrs zwischen dem mobilen Rechner 104 und der Windkraftanlage 101a, eine Einschränkung des Datenverkehrs zwischen dem mobilen Rechner 104 und sonstigen Windkraftanlagen 101b, 101c des Industrienetzwerks 400 und eine Sperrung der sonstigen Anschlüsse zum Verhindern von unbefugten Zugriffen auf die Netzwerkeinrichtungen 101a - 101c oder auf das Industrienetzwerk 400. Ferner wird eine virtuelle industrielle Firewall zwischen dem Internet und dem Industrienetzwerk 400 sowie dem virtuelle Netzwerk 401 instanziiert, um einen unbefugten Zugriff aus dem Internet zu verhindern.

Fig. 5 zeigt eine schematische Ansicht einer vierten Ausführungsform eines Industrienetzwerks 500 mit dem mobilen Rechner 104 als Zugriffseinrichtung.

Das Industrienetzwerk 500 umfasst mehrere Windkraftanlagen 101 als Netzwerkeinrichtungen. In Fig. 5 sind die Windkraftanlagen 101 an zwei Standorten 501, 502 gezeigt. Die Windkraftanlagen 101 an einem ersten Standort 501 sind zu einem ersten Unternetz 503 zusammengefasst. Das erste Unternetz 503 ist mit einer ersten Schnittstelle 504 verbunden, die einen Zugriff auf das erste Unternetz 503 sowie auf die Netzwerkeinrichtungen 101 des ersten Unternetzes 503 ermöglicht. Analog sind die Windkraftanlagen 101 an einem zweiten Standort 502 zu einem zweiten Unternetz 505 zusammengefasst, wobei das zweite Unternetz 505 mit einer zweiten Schnittstelle 506 verbunden ist, über die ein Zugriff auf die Windkraftanlagen 101 des Unternetzes 506 möglich ist.

Zum Einrichten der Unternetze 503, 505 innerhalb des Industrienetzwerks 500 werden insbesondere die Netzwerkkonfigurationstechnologien VPN, Tunnel und SDN angewendet.

Fig. 6 zeigt eine schematische Ansicht einer fünften Ausführungsform eines Industrienetzwerkes 600 mit dem mobilen Rechner 104 als Zugriffseinrichtung. Insbesondere umfasst das In-

dustrienetzwerk 600 die Windkraftanlagen 101 des ersten Unternetzes 503 in Fig. 5.

Fig. 6 zeigt einen lokalen Zugriff A auf das zweite Unternetz 503 von Netzwerkeinrichtungen 101 über die lokale Schnittstelle 504. Eine geographische Entfernung DA zwischen dem ersten Unternetz 503 und dem mobilen Rechner 104 beträgt einige Zentimeter bis zu mehreren Hundert Metern. Eine geographische Entfernung DC zwischen dem ersten Unternetz 503 und dem Server-Rechner 103 beträgt einige Kilometer bis zu einigen Tausend Kilometern. Der Zugriff A auf das erste Unternetz 503 erfolgt ohne ein Routing über den Server-Rechner 103, so dass Latenzzeiten bei Datenübertragung verkürzt und ein Paketverlust (paket loss) sowie Fluktuationen (jitter) verringert sind. Insgesamt wird also die Verbindungsgüte verbessert.

Der Server-Rechner ist über eine Verbindung 601 mit dem mobilen Rechner 104 und über eine Verbindung 602 mit dem ersten Unternetz 503 verbunden. Die Verbindungen 601, 602 sind dabei teilweise über das Internet hergestellt. Insbesondere stellt die Verbindung 601 eine durch eine Authentifizierung gebildete Kopplung dar, und die Verbindung 602 kann eine geschützte Verbindung, zum Beispiel in der Art einer Standleitung, sein. Alternativ oder zusätzlich können die Verbindungen 601, 602 zumindest teilweise eine elektrische, optische oder elektromagnetische Leitung umfassen. Auch die Verbindung über die Schnittstelle 504 kann als VPN-Verbindung ist möglich. Der zentrale Server-Rechner 103 ist in das Netzwerk so eingebunden, dass eine Einrichtung der Schnittstelle 504 möglich ist.

Die oben beschriebenen Industrienetzwerke 100, 200, 400, 500, 600 sind vorzugsweise so eingerichtet, dass eine Verbindung und Datenübertragung innerhalb des Industrienetzwerks vordefinierten Anforderungen, z.B. einer Quality of Service oder Normen wie IEEE 802.1p, genügen. Durch den direkten und lokalen Zugriff auf die Netzwerkeinrichtungen kann die Verbin-

dungsqualität gegenüber einem Routing über die zentrale Steuereinrichtung des Industrienetzwerks verbessert werden.

Die Kapselung des lokalen Zugriffs durch das Service-Personal U erhöht die Sicherheit des jeweiligen Industrienetzwerks. Zudem kann der lokale Zugriff zeitlich beschränkt werden, um unnötige Zugriffsmöglichkeiten auf das Industrienetzwerk auszuschließen.

Obwohl die vorliegende Erfindung anhand von Windparks beschrieben wurde, ist sie vielfältig anwendbar, z.B. auf Produktionsanlagen, sonstige Versorgungsnetze (z.B. Strom-, Wärme-, Wasser-, Öl- oder Gasversorgungsnetze), Verkehrsnetze oder Kommunikationsnetze.

Bezugszeichenliste

100	Industrienetzwerk
101, 101a - 101c	Netzwerkeinrichtung
102, 102a - 102c	lokale Schnittstelle
103	zentrale Steuereinrichtung
104	Zugriffseinrichtung
105 - 107	Verbindung
200	Industrienetzwerk
201	Datenbankeinrichtung
300	Verfahren
301 - 307	Verfahrensschritte
400	Industrienetzwerk
401	virtuelles Netzwerk
500	Industrienetzwerk
501, 502	Standort
503, 505	Unternetz
504, 506	Schnittstelle
600	Industrienetzwerk
601, 602	Verbindung
A	lokaler Zugriff
DA, DC	Entfernung
K	Zugriffskonfiguration
S	Zugriffsspezifikationen
T	Zugriffsdatensatz
Q	Zugriffsanfrage
U	Service-Personal

Patentansprüche

1. Verfahren (300) zum Betreiben eines Industrienetzwerks (100) mit mindestens einer Netzwerkeinrichtung (101), die von einer zentralen Steuereinrichtung (103) ansteuerbar ist, und mit einer lokalen Schnittstelle (102) für einen lokalen Zugriff (A) auf die Netzwerkeinrichtung (101), umfassend:

Übermitteln (301) einer Zugriffsanfrage (Q) für den lokalen Zugriff (A) auf die Netzwerkeinrichtung (101) über die lokale Schnittstelle (102) an die zentrale Steuereinrichtung (103);

Authentifizieren (302) der Zugriffsanfrage (Q) durch die zentrale Steuereinrichtung (103); und

durch die zentrale Steuereinrichtung, Einrichten (304) der lokalen Schnittstelle (102) für den lokalen Zugriff (A) auf die Netzwerkeinrichtung (101) in Abhängigkeit von der Zugriffsanfrage (Q).

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass der lokale Zugriff (A) auf die Netzwerkeinrichtung (101) zeitlich beschränkt ist.

3. Verfahren nach Anspruch 1 oder 2,
gekennzeichnet durch:

Deaktivieren (307) der lokalen Schnittstelle (102), nachdem der lokale Zugriff (A) auf die Netzwerkeinrichtung (101) beendet ist.

4. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass der lokale Zugriff (A) auf die Netzwerkeinrichtung (101) mit Hilfe einer Zugriffseinrichtung (104) erfolgt, die mit der lokalen Schnittstelle (102) gekoppelt ist, und
dass an der Zugriffseinrichtung (104) ein Zugriffsdatensatz (T) zum Freischalten des lokalen Zugriffs (A) auf die Netzwerkeinrichtung (101) über die lokale Schnittstelle (102) bereitgestellt wird, falls die Zugriffsanfrage (Q) authentifiziert ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch:

Erzeugen eines virtuellen Netzwerks (400), das Teil des Industrienetzwerks (100) ist und mindestens die Netzwerkeinrichtung (101), auf die die Zugriffsanfrage (Q) gerichtet ist, umfasst,

wobei die zentrale Steuereinrichtung (103) nicht Teil des virtuellen Netzwerks (100) ist.

6. Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch:

Übermitteln von Zugriffsspezifikationen (S) der Zugriffsanfrage (Q) an die zentrale Steuereinrichtung (103),

wobei die Zugriffsspezifikationen (S) eine Kennung einer Zugriffseinrichtung, eine Identität eines Service-Personals, eine Verbindungsart des lokalen Zugriffs, Verbindungsanforderungen des lokalen Zugriffs, eine Zugriffsdauer und/oder für den lokalen Zugriff vorgesehene Ressourcen umfassen; und

Einrichten der lokalen Schnittstelle (102) für den lokalen Zugriff (A) auf die Netzwerkeinrichtung (101) gemäß den Zugriffsspezifikationen (S).

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Einrichten (304) der lokalen Schnittstelle (102) Instanziieren von Applikationen an der lokalen Schnittstelle (102) umfasst.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Einrichten (304) der lokalen Schnittstelle (102) mit Hilfe von an der zentralen Steuereinrichtung (103) gespeicherten Vorlagen erfolgt.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Übermitteln (301) der Zugriffsanfrage (Q) an die zentrale Steuereinrichtung (103) und/oder das Einrichten (304) der lokalen Schnittstelle (102)

durch die zentrale Steuereinrichtung (103) verschlüsselt erfolgt.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der lokale Zugriff (A) auf die Netzwerkeinrichtung (101) zum Warten, Überprüfen, Überwachen, Modifizieren, Betreiben, Reparieren, Anschalten, Abschalten, Ansteuern der Netzwerkeinrichtung (101) und/oder zum lokalen Abrufen von Daten von der Netzwerkeinrichtung (101) erfolgt.

11. Verfahren nach einem der vorhergehenden Ansprüche, dass der lokale Zugriff (A) auf die Netzwerkeinrichtung (101) über ein Local Area Network und/oder mit Hilfe von Wireless-LAN, Bluetooth, Mobilfunk-Technologien, LTE-basierten Verbindungen und/oder kabelgebunden erfolgt.

12. Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet dadurch, dass das Industrienetzwerk (100) mehrere Netzwerkeinrichtungen (101) umfasst, und die Zugriffsanfrage (Q) einen lokalen Zugriff (A) auf ein Unternetz (503, 505) von mehreren Netzwerkeinrichtungen (101) über die jeweilige lokale Schnittstelle (504, 506) umfasst.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der lokale Zugriff (A) auf die Netzwerkeinrichtung (101) eine geringere Datenübertragungsstrecke (DA) aufweist als eine Datenübertragungsstrecke (DC) zum Ansteuern der Netzwerkeinrichtung (101) durch die zentrale Steuereinrichtung (103).

14. Industrienetzwerk (100) mit mindestens einer Netzwerkeinrichtung (101), die von einer zentralen Steuereinrichtung (103) ansteuerbar ist, und einer lokalen Schnittstelle (102) für den lokalen Zugriff (A) auf die Netzwerkeinrichtung (101), wobei das Industrienetzwerk (100) zum Ausführen des Verfahrens nach einem der Ansprüche 1 - 13 geeignet ist.

15. Industrienetzwerk nach Anspruch 14,

dadurch gekennzeichnet, dass das Industrienetzwerk (100) zumindest teilweise in Form eines virtuellen Netzwerks in einem Netzwerk (600) bereitgestellt ist.

FIG 1

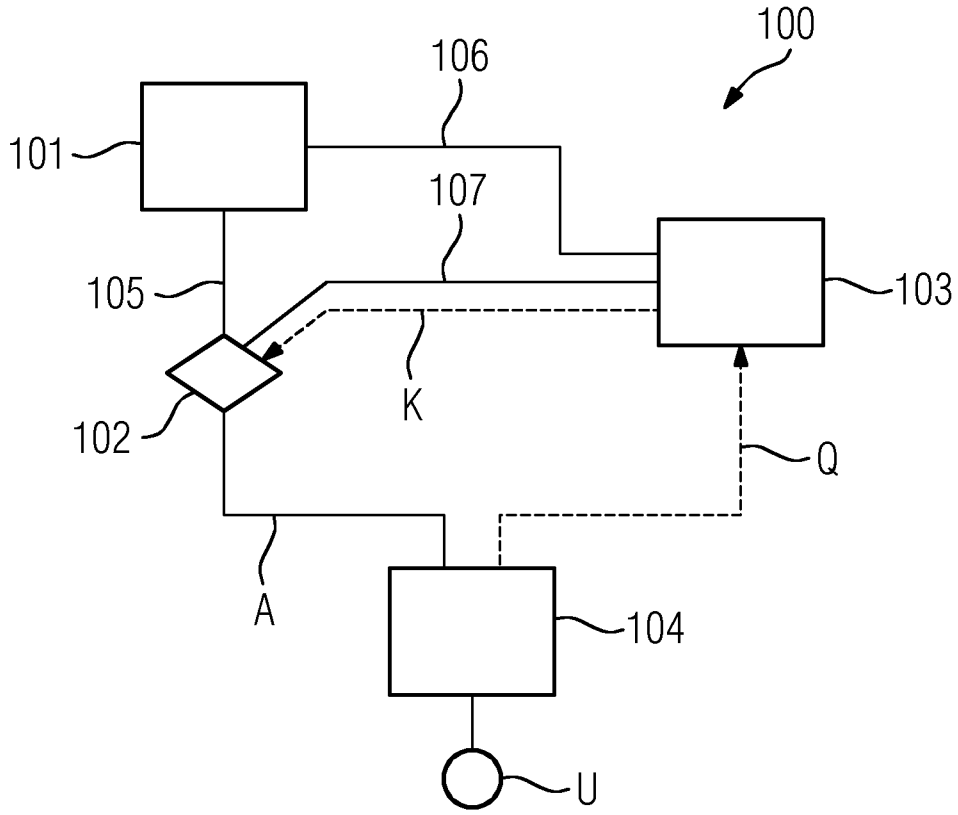

100
106
101
107
105
103
K
102
Q
A
104
U

FIG 2

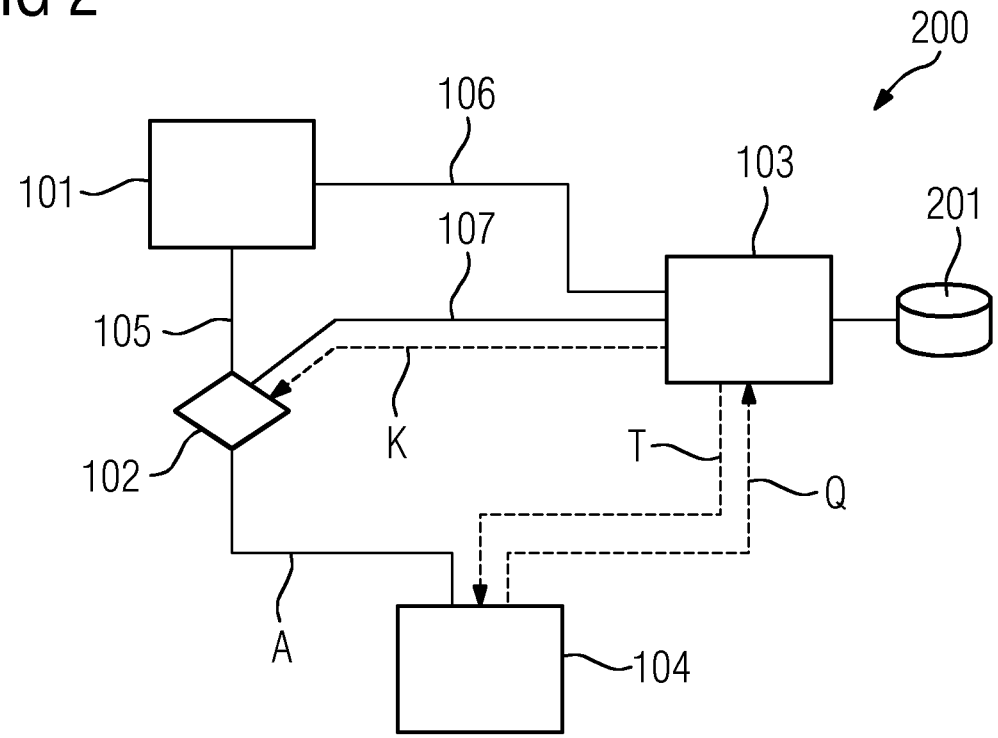

200
106
101
103
201
107
105
K
T
102
Q
A
104

FIG 3

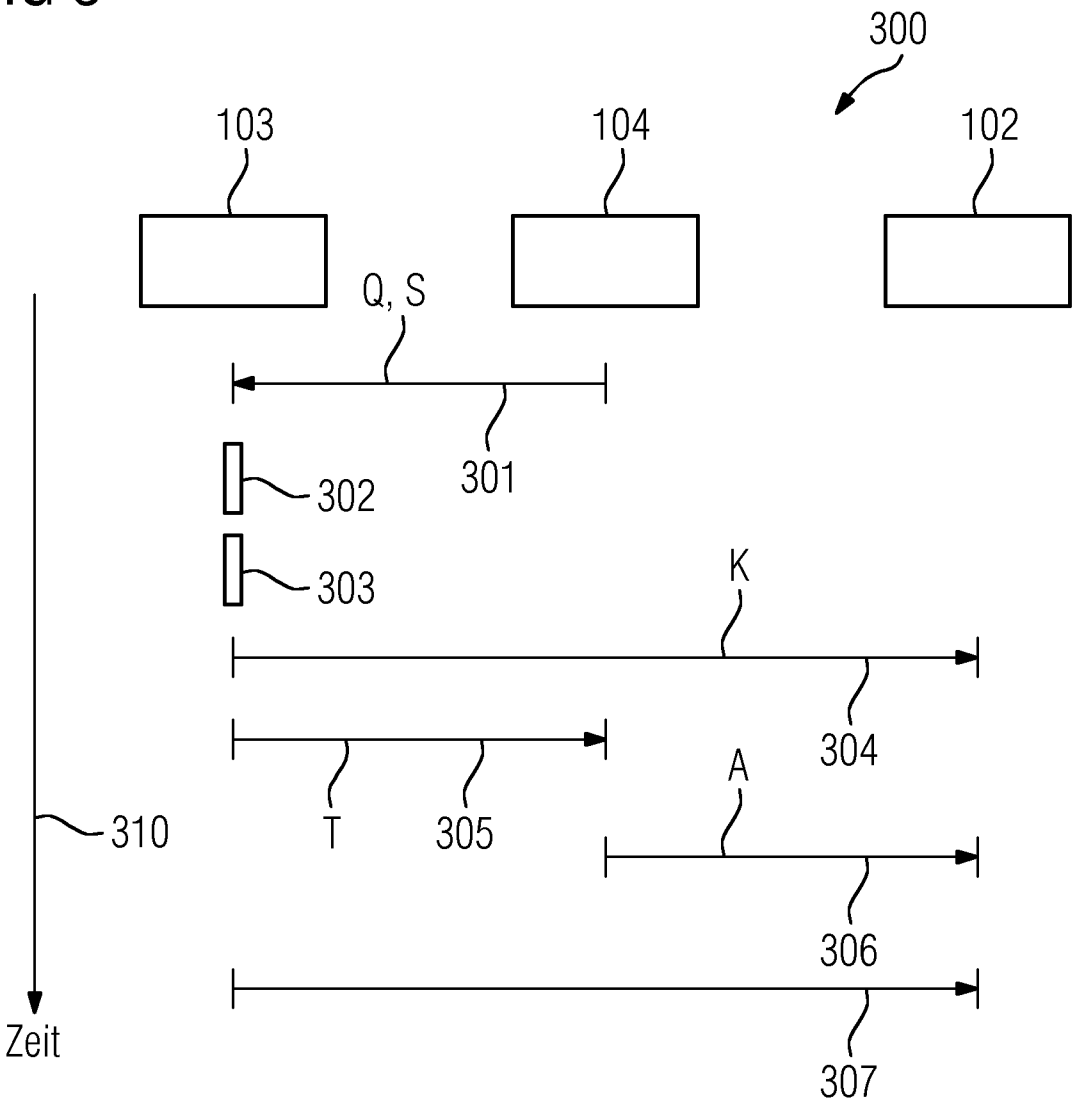


FIG 4

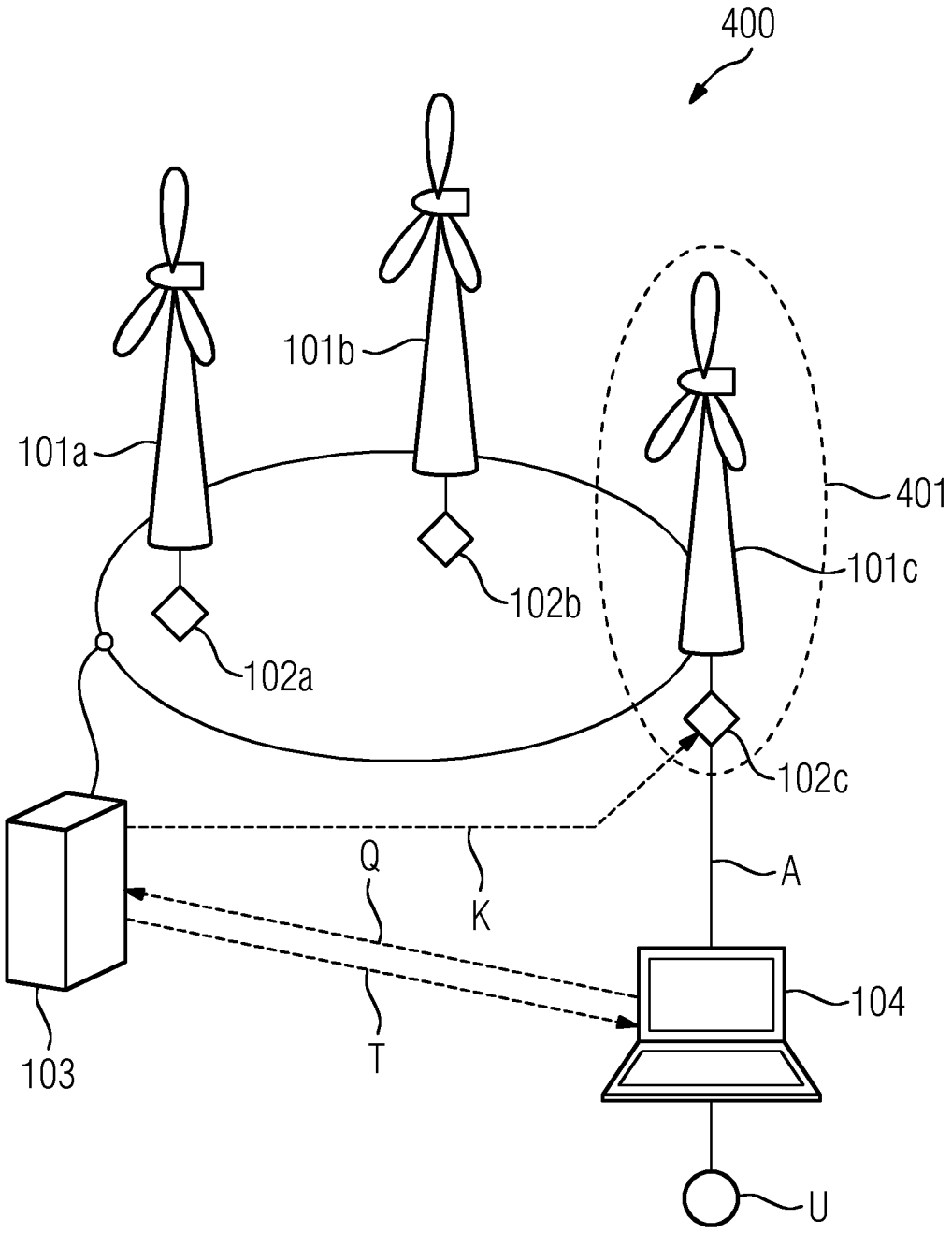


FIG 5

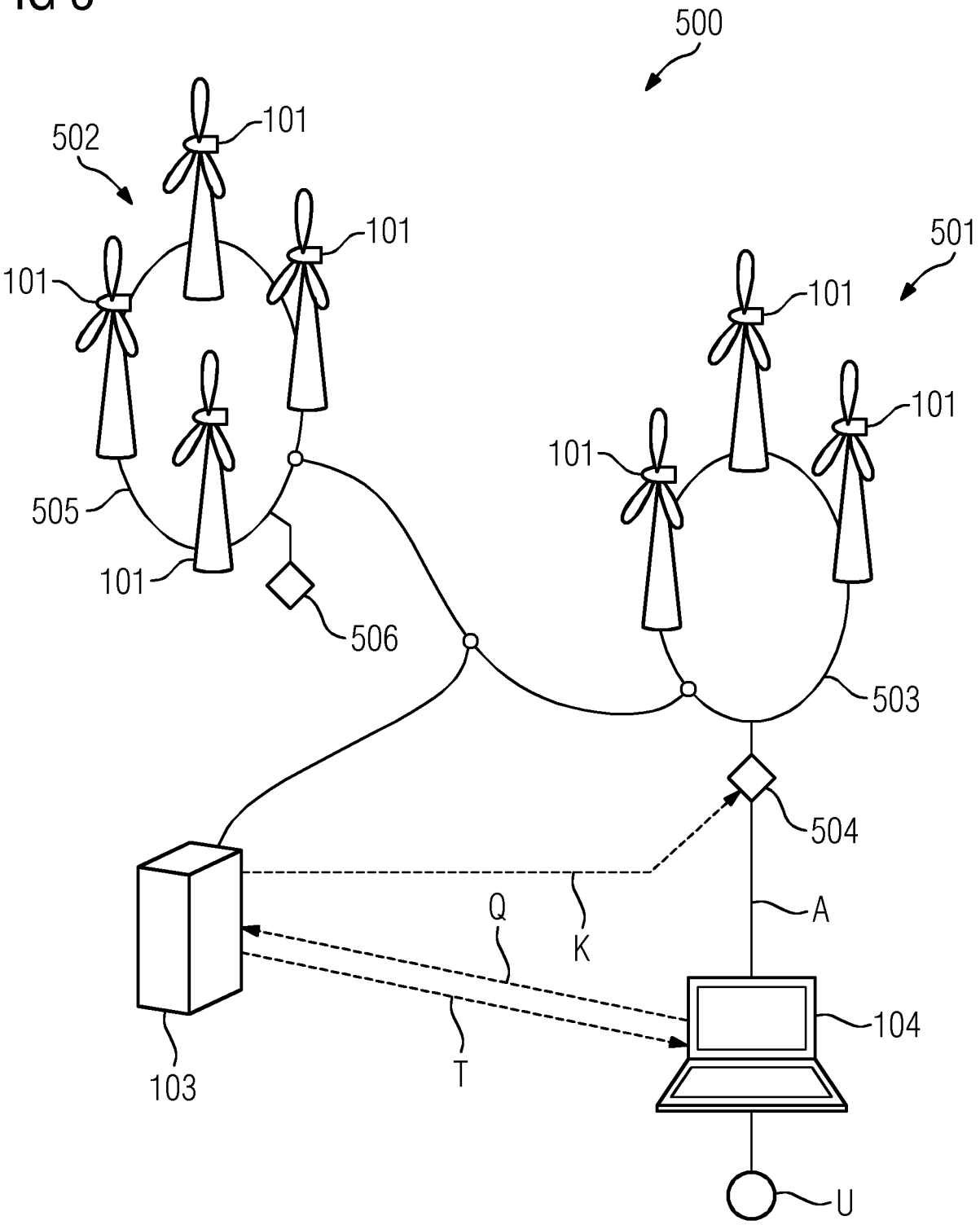
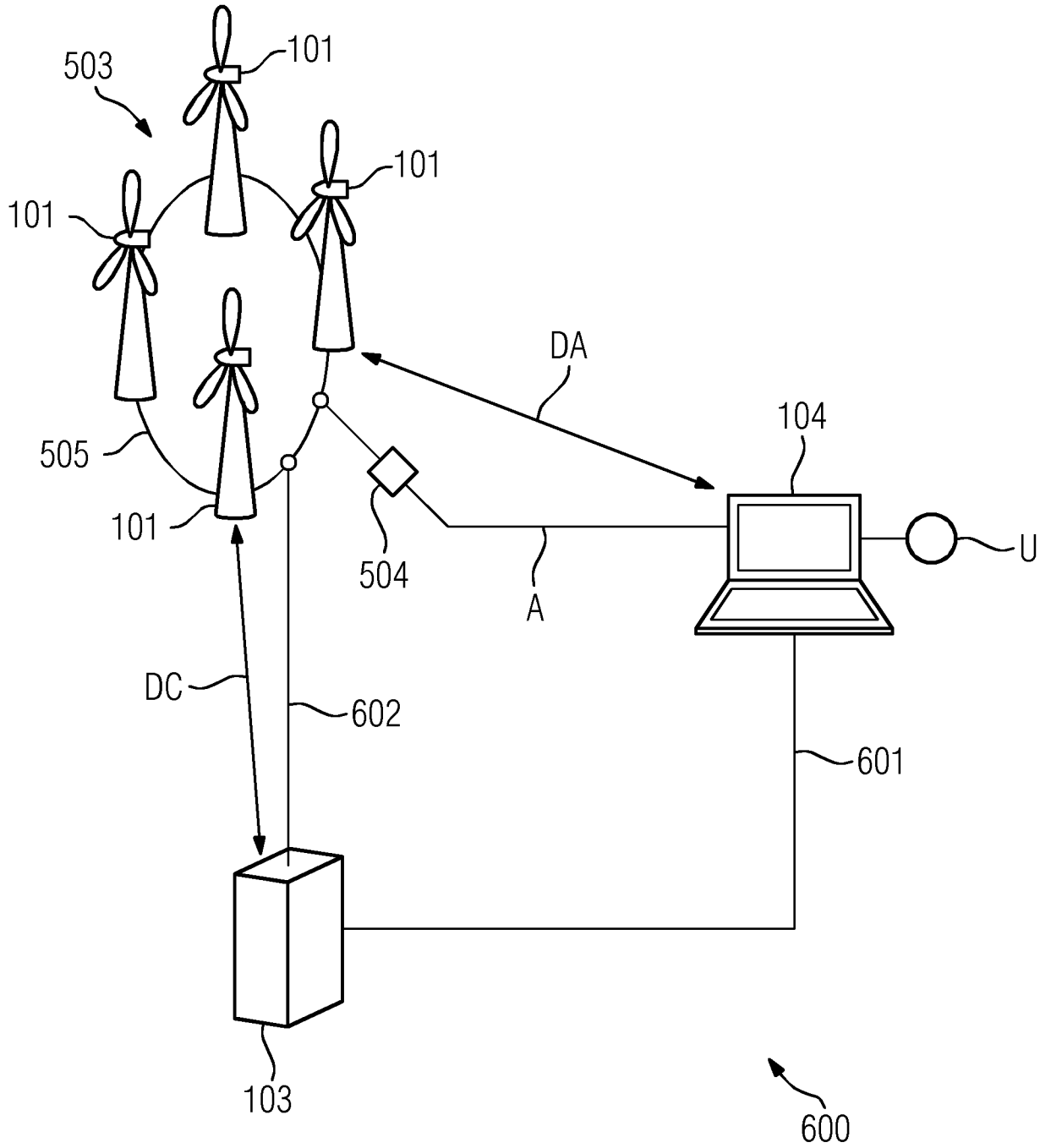

500
502
101
101
101
101
505
101
506
501
101
101
101
503
504
Q
K
A
104
103
T
U

FIG 6



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/070506

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013/128338 A1 (KONINKL PHILIPS NV [NL]) 6 September 2013 (2013-09-06)	1-3,6, 8-14
A	page 3, line 15 - page 4, line 30; figures 3,4 page 8, line 10 - page 12, line 13	4,5,7,15

X	WO 2013/106688 A2 (TELECOMM SYSTEMS INC [US]) 18 July 2013 (2013-07-18)	1-4,6,8, 9,11,12, 14
A	page 8, line 6 - page 10, line 12; figures 1-6 page 13, line 3 - page 13, line 24	5,7,10, 13,15

X	US 9 038 151 B1 (CHUA ROY LIANG [US] ET AL) 19 May 2015 (2015-05-19)	1-3,5-15
A	figures 1,9 column 5, line 31 - column 6, line 35 column 9, line 63 - column 10, line 63 column 30, line 53 - column 31, line 59	4

☐ 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	Date of mailing of the international search report
19 May 2016	30/05/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dingel, Janis

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/070506

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013128338 A1	06-09-2013	CN 104137007 A	05-11-2014
		EP 2820584 A1	07-01-2015
		JP 5702900 B1	15-04-2015
		JP 2015516610 A	11-06-2015
		WO 2013128338 A1	06-09-2013
WO 2013106688 A2	18-07-2013	CA 2861264 A1	18-07-2013
		EP 2805264 A2	26-11-2014
		US 2013269020 A1	10-10-2013
		WO 2013106688 A2	18-07-2013
US 9038151 B1	19-05-2015	US 9038151 B1	19-05-2015
		US 9178807 B1	03-11-2015
		US 9264301 B1	16-02-2016
		US 9276877 B1	01-03-2016

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2015/070506

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

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2013/128338 A1 (KONINKL PHILIPS NV [NL]) 6. September 2013 (2013-09-06)	1-3,6, 8-14
A	Seite 3, Zeile 15 - Seite 4, Zeile 30; Abbildungen 3,4 Seite 8, Zeile 10 - Seite 12, Zeile 13	4,5,7,15

X	WO 2013/106688 A2 (TELECOMM SYSTEMS INC [US]) 18. Juli 2013 (2013-07-18)	1-4,6,8, 9,11,12, 14
A	Seite 8, Zeile 6 - Seite 10, Zeile 12; Abbildungen 1-6 Seite 13, Zeile 3 - Seite 13, Zeile 24	5,7,10, 13,15

X	US 9 038 151 B1 (CHUA ROY LIANG [US] ET AL) 19. Mai 2015 (2015-05-19)	1-3,5-15
A	Abbildungen 1,9 Spalte 5, Zeile 31 - Spalte 6, Zeile 35 Spalte 9, Zeile 63 - Spalte 10, Zeile 63 Spalte 30, Zeile 53 - Spalte 31, Zeile 59	4

☐ 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	Absendedatum des internationalen Recherchenberichts
19. Mai 2016	30/05/2016

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dingel, Janis

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2015/070506

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2013128338 A1	06-09-2013	CN 104137007 A	05-11-2014
		EP 2820584 A1	07-01-2015
		JP 5702900 B1	15-04-2015
		JP 2015516610 A	11-06-2015
		WO 2013128338 A1	06-09-2013
WO 2013106688 A2	18-07-2013	CA 2861264 A1	18-07-2013
		EP 2805264 A2	26-11-2014
		US 2013269020 A1	10-10-2013
		WO 2013106688 A2	18-07-2013
US 9038151 B1	19-05-2015	US 9038151 B1	19-05-2015
		US 9178807 B1	03-11-2015
		US 9264301 B1	16-02-2016
		US 9276877 B1	01-03-2016