(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
18. Januar 2018 (18.01.2018)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2018/010949 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *G05B 19/418* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/065844

(22) Internationales Anmeldedatum:
27. Juni 2017 (27.06.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
16179006.8 12. Juli 2016 (12.07.2016) EP

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Werner-von-Siemens-Straße 1, 80333 München (DE).

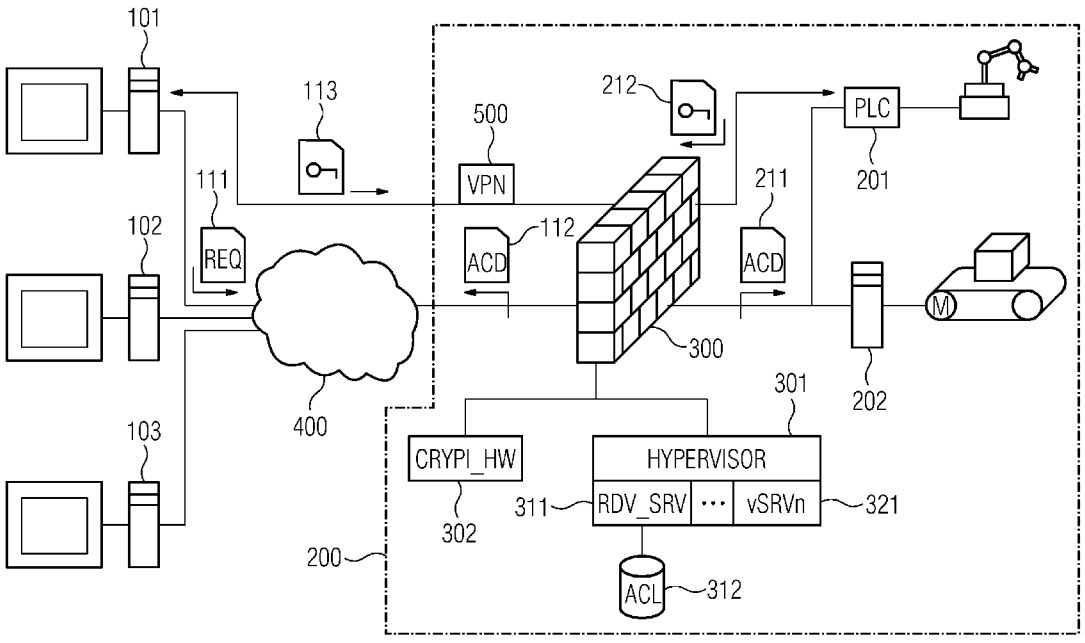
(72) Erfinder: **GLAS, Karl**; Langer Platz 9 A, 91074 Herzogenaurach (DE). **GOTTWALD, Sven**; Freystädter Str. 126, 90475 Nürnberg (DE).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) **Title:** METHOD FOR ESTABLISHING SECURED COMMUNICATIONS CONNECTIONS TO AN INDUSTRIAL AUTOMATION SYSTEM AND FIREWALL SYSTEM

(54) **Bezeichnung:** VERFAHREN ZUM AUFBAU GESICHERTER KOMMUNIKATIONSVERBINDUNGEN ZU EINEM INDUSTRIELLEN AUTOMATISIERUNGSSYSTEM UND FIREWALL-SYSTEM



(57) **Abstract:** The invention relates to a connection management device for establishing secured communications connections to an industrial automation system, said device providing, in case of a positive authorization verification outcome, access control information for establishing an encrypted communication connection between a first communication unit of a requesting user and a selected second communication unit. The connection management device is formed by a server instance running on a firewall system. Data packets transmitted via an encrypted communications connection between the first communication unit of the requesting user and the

[Fortsetzung auf der nächsten Seite]

WO 2018/010949 A1

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)*

selected second communication unit are encrypted for verification by the firewall system, based on specified security rules, and, in case of successful verification, forwarded encrypted to the first communication unit of the requesting user or to the selected second communication unit.

(57) Zusammenfassung: Zum Aufbau gesicherter Kommunikationsverbindungen zu einem industriellen Automatisierungssystem stellt eine Verbindungsverwaltungseinrichtung bei einem positiven Berechtigungsüberprüfungsergebnis Zugriffskontrollinformationen zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen einem ersten Kommunikationsgerät eines anfordernden Benutzers und einem ausgewählten zweiten Kommunikationsgerät für diese Kommunikationsgeräte bereit. Dabei wird die Verbindungsverwaltungseinrichtung durch eine auf einem Firewall-System ablaufende Server-Instanz gebildet wird. Über eine verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät übermittelte Datenpakete werden für eine auf festgelegten Sicherheitsregeln basierende Überprüfung durch das Firewall-System entschlüsselt und bei erfolgreicher Überprüfung verschlüsselt zum ersten Kommunikationsgerät des anfordernden Benutzers oder zum ausgewählten zweiten Kommunikationsgerät weitergeleitet.

Beschreibung

Verfahren zum Aufbau gesicherter Kommunikationsverbindungen zu einem industriellen Automatisierungssystem und Firewall-System

Industrielle Automatisierungssysteme dienen zur Überwachung, Steuerung und Regelung von technischen Prozessen, insbesondere im Bereich Fertigungs-, Prozess- und Gebäudeautomatisierung, und ermöglichen einen Betrieb von Steuerungseinrichtungen, Sensoren, Maschinen und industriellen Anlagen, der möglichst selbständig und unabhängig von menschlichen Eingriffen erfolgen soll. Eine besondere Bedeutung hat dabei eine Bereitstellung von Überwachungs-, Steuerungs- und Regelungsfunktionen in Echtzeit. Störungen von Kommunikationsverbindungen zwischen Automatisierungsgeräten oder Rechnereinheiten eines industriellen Automatisierungssystems können zu einer nachteiligen Wiederholung einer Übermittlung einer Dienstanforderung führen. Insbesondere können nicht oder nicht vollständig übermittelte Nachrichten einen Übergang oder Verbleib eines industriellen Automatisierungssystems in einen sicheren Betriebszustand verhindern und zu einem Ausfall einer industriellen Anlage führen. Eine besondere Problematik resultiert in industriellen Automatisierungssystemen aus einem Meldungsverkehr mit verhältnismäßig vielen, aber relativ kurzen in Echtzeit zu übermittelnden Nachrichten.

Aus US8555373B2 ist eine zwischen einem Quell-Gerät und einem Ziel-Gerät vorgesehene Firewall bekannt, die eine Hardware-Sicherheitskomponente zur Prüfung von aus einem Datenpaket extrahierten Daten gegen eine zulässige Liste umfasst. Zusätzlich führt die Hardware-Sicherheitskomponente eine zustandsbasierte Prüfung hinsichtlich eines Protokolls durch. Die Firewall kann als Security-Proxy ausgestaltet sein und

mittels einer Software-Sicherheitskomponente gesicherte Sitzungen zwischen zwei Teilnehmern ermöglichen. Zur Authentifizierung bzw. Entschlüsselung zu prüfender Pakete und Verschlüsselung geprüfter Pakete greift die Software-Sicherheitskomponente auf die Hardware-Sicherheitskomponente zurück.

In US7958549B2 ist eine Firewall mit einem Verschlüsselungsprozessor und einem virtualisierten Server beschrieben. Dabei ist der Verschlüsselungsprozessor dem virtualisierten Server vorgeschaltet und entschlüsselt verschlüsselte Datenpakete, die dann an den virtualisierten Server zur Verarbeitung weitergeleitet werden. In umgekehrter Richtung empfängt der Verschlüsslungsprozessor vom virtualisierten Server verarbeitete Datenpakete, um diese Weiterleitung zu verschlüsseln.

Zum Schutz vertraulicher Informationen oder Daten werden auch in industriellen Kommunikationsnetzen VPN-Kommunikationsverbindungen (Virtual Private Network) verwendet. Bei VPN-Kommunikationsverbindungen erfolgt eine Ende-zu-Ende-Verschlüsselung für zwischen einem Sender und einem Empfänger übermittelte Daten. Dabei kann ein Sender mehrere VPN-Kommunikationsverbindungen gleichzeitig zu mehreren Empfängern aufbauen und nutzen.

Zur Verwaltung einer Vielzahl von VPN-Verbindungen eines Fernwartungssystems, bei dem von einer Vielzahl von Fernwartungsrechnern außerhalb eines industriellen Kommunikationsnetzes auf verschiedene zu steuernde Anlagen oder Anlagenkomponenten innerhalb eines industriellen Kommunikationsnetzes zugegriffen werden kann, sind Rendezvous-Server vorgesehen. Dabei melden sich Benutzer von Fernüberwachungsrechnern beispielsweiser mit ihrer jeweiligen Benutzerkennung am Rendezvous-Server an und fordern bei diesem einen Zugriff auf eine

Anlage, Anlagenkomponente oder ein Feldgerät an. Bei erfolgreicher Anmeldung und Anforderung veranlasst der Rendezvous-Server statisch oder dynamisch einen Aufbau von VPN-Kommunikationsverbindungen zwischen Kommunikationsteilnehmern eines Fernwartungsvorgangs und schaltet diese zusammen. Hierdurch wird eine verschlüsselte Ende-zu-Ende-Kommunikationsverbindung zwischen einem Fernwartungsrechner einerseits und einer Anlage, Anlagenkomponente oder einem Feldgerät andererseits aufgebaut. Eine derartige abhörsichere Ende-zu-Ende-Kommunikationsverbindung verhindert jedoch grundsätzlich eine Kontrolle über Daten oder Informationen, die zwischen den Kommunikationsteilnehmern eines Fernwartungsvorgangs ausgetauscht werden. Insbesondere kann nicht ohne weiteres geprüft werden, ob ausgehend von einem Fernwartungsrechner unzulässige Eingriffe an einer Anlage, Anlagenkomponente oder einem Feldgerät vorgenommen werden oder ob zugelassene Kommunikations- oder Automatisierungssystemprotokolle verwendet werden.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Aufbau gesicherter Kommunikationsverbindungen zu einem industriellen Kommunikationssystem anzugeben, das eine abhörsichere Datenübermittlung bei gleichzeitiger Überprüfbarkeit übermittelter Daten auf Zulässigkeit ermöglicht, sowie eine geeignete Vorrichtung zur Durchführung des Verfahrens zu schaffen.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 angegebenen Merkmalen und durch ein Firewall-System mit den in Anspruch 14 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen der vorliegenden Erfindung sind in den abhängigen Ansprüchen angegeben.

Entsprechend dem erfindungsgemäßen Verfahren zum Aufbau gesicherter Kommunikationsverbindungen zu einem industriellen

Automatisierungssystem werden Kommunikationsverbindungen von ersten Kommunikationsgeräten außerhalb des industriellen Automatisierungssystems zu dem industriellen Automatisierungssystem zugeordneten zweiten Kommunikationsgeräten über eine Verbindungsverwaltungseinrichtung aufgebaut. Die Verbindungsverwaltungseinrichtung kann insbesondere ein Rendezvous-Server sein. Darüber hinaus können zweite Kommunikationsgeräte beispielsweise in Automatisierungsgeräte integriert oder diesen zugeordnet sein. Bei einer Anforderung eines Verbindungsaufbaus zu einem ausgewählten zweiten Kommunikationsgerät durch einen anfordernden Benutzer eines ersten Kommunikationsgeräts führt die Verbindungsverwaltungseinrichtung anhand einer Zugriffskontrollliste eine Berechtigungsüberprüfung für den anfordernden Benutzer durch. Die Zugriffskontrollliste umfasst vorzugsweise Benutzer-individuelle Angaben zulässiger Kommunikationsverbindungen zwischen jeweils zumindest einem ersten Kommunikationsgerät und zumindest einem zweiten Kommunikationsgerät.

Erfindungsgemäß stellt die Verbindungsverwaltungseinrichtung bei einem positiven Berechtigungsüberprüfungsergebnis Zugriffskontrollinformationen zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät für diese Kommunikationsgeräte bereit. Die Verbindungsverwaltungseinrichtung wird durch eine auf einem Firewall-System ablaufende Server-Instanz gebildet. Darüber hinaus werden über eine verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät übermittelte Datenpakete für eine auf festgelegten Sicherheitsregeln basierende Überprüfung durch das Firewall-System entschlüsselt. Die festgelegten Sicherheitsregeln können insbesondere Firewall-Regeln bzw. Regeln über eine Zuläs-

sigkeit von in Datenpaketen angegebenen Steuerungsbefehlen bzw. Steuerungsparametern für Automatisierungsgeräte umfassen. Erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte Datenpakete leitet das Firewall-System verschlüsselt zum ersten Kommunikationsgerät des anfordernden Benutzers bzw. zum ausgewählten zweiten Kommunikationsgerät weiter. Damit kann Datenverkehr zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät bidirektional überprüft werden. Vorzugsweise werden zu überprüfende Datenpakete vom ersten Kommunikationsgerät des anfordernden Benutzers an das ausgewählte zweite Kommunikationsgerät durch das Firewall-System entschlüsselt, überprüft und nach erfolgreicher Überprüfung an das zweite Kommunikationsgerät weitergeleitet, während zu überprüfende Datenpakete vom ausgewählten zweiten Kommunikationsgerät an das erste Kommunikationsgerät des anfordernden Benutzers durch das Firewall-System entschlüsselt, überprüft und nach erfolgreicher Überprüfung an das erste Kommunikationsgerät weitergeleitet werden. Das Firewall-System ist vorzugsweise in einem gesicherten Kommunikationsnetz des industriellen Automatisierungssystems angeordnet und verwirft vorteilhafterweise den festgelegten Sicherheitsregeln nicht entsprechende Datenpakete. Alternativ zu einem Verwerfen den festgelegten Sicherheitsregeln nicht entsprechender Datenpakete könnte beispielsweise auch ein Sicherheitsalarm generiert werden.

Entsprechend einer besonders bevorzugten Ausgestaltung der vorliegenden Erfindung sind die über die Verbindungsverwaltungseinrichtung aufgebauten Kommunikationsverbindungen zwischen ersten Kommunikationsgeräten und zweiten Kommunikationsgeräten Virtual-Private-Network-Verbindungen. Außerdem umfasst die Berechtigungsüberprüfung eine Authentisierung des anfordernden Benutzers gegenüber der Verbindungsverwaltungs-

einrichtung. Vorteilhafterweise stellt die Verbindungsverwaltungseinrichtung nur nach einer Authentifizierung des anfordernden Benutzers Zugriffskontrollinformationen zur Nutzung einer Virtual-Private-Network-Verbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät an den anfordernden Benutzer bereit. Die Zugriffskontrollinformationen können beispielsweise kryptographische Schlüssel bzw. Passwörter für VPN-Sitzungen oder temporär gültige Passwörter umfassen. Entsprechend einer weiteren Ausgestaltung umfasst die auf den festgelegten Sicherheitsregeln basierende Überprüfung durch das Firewall-System eine Überprüfung von Passwörtern für VPN-Sitzungen oder von temporär gültigen Passwörtern auf Korrektheit, und das Firewall-System verwirft Datenpakete, für deren Übermittlung inkorrekte Passwörter angegeben worden sind.

Die Verbindungsverwaltungseinrichtung baut entsprechend einer vorteilhaften Weiterbildung des erfindungsgemäßen Verfahrens bei einem positiven Berechtigungsüberprüfungsergebnis jeweils eine verschlüsselte Kommunikationsverbindung zum ersten Kommunikationsgerät des anfordernden Benutzers und zum ausgewählten zweiten Kommunikationsgerät auf und verknüpft diese Kommunikationsverbindungen miteinander. Darüber hinaus werden die über die verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät übermittelten Datenpakete vorzugsweise durch das Firewall-System entschlüsselt und auf Basis der festgelegten Sicherheitsregeln überprüft; auch erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte weiterzuleitende Datenpakete werden durch das Firewall-System verschlüsselt. Entsprechend einer besonders bevorzugten Ausgestaltung der vorliegenden Erfindung erfolgt eine Entschlüsselung bzw. Verschlüsselung von Datenpaketen durch das Firewall-System hardwarebasiert.

Das erfindungsgemäße Firewall-System ist zur Durchführung eines Verfahrens entsprechend vorangehenden Ausführungen vorgesehen und für eine auf festgelegten Sicherheitsregeln basierende Überprüfung von Datenpaketen ausgestaltet und eingerichtet, insbesondere durch Konfiguration. Zusätzlich ist das Firewall-System für einen Ablauf zumindest einer Server-Instanz ausgestaltet und eingerichtet. Durch die Server-Instanz ist eine Verbindungsverwaltungseinrichtung gebildet, die für einen Kommunikationsverbindungsaufbau von ersten Kommunikationsgeräten außerhalb eines industriellen Automatisierungssystems zu dem industriellen Automatisierungssystem zugeordneten zweiten Kommunikationsgeräten ausgestaltet und eingerichtet ist. Die Verbindungsverwaltungseinrichtung ist zusätzlich dafür ausgestaltet und eingerichtet, bei einer Anforderung eines Verbindungsaufbaus zu einem ausgewählten zweiten Kommunikationsgerät durch einen anfordernden Benutzer eines ersten Kommunikationsgeräts anhand einer Zugriffskontrollliste eine Berechtigungsüberprüfung für den anfordernden Benutzer durchzuführen.

Darüber hinaus ist die Verbindungsverwaltungseinrichtung erfindungsgemäß zusätzlich dafür ausgestaltet und eingerichtet, bei einem positiven Berechtigungsüberprüfungsergebnis Zugriffskontrollinformationen zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät für diese Kommunikationsgeräte bereitzustellen. Des weiteren ist das Firewall-System zusätzlich dafür ausgestaltet und eingerichtet, über eine verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers bzw. dem ausgewählten zweiten Kommunikationsgerät übermittelte Datenpakete für die auf den festgelegten Sicherheitsregeln basierende Überprüfung zu

entschlüsseln. Außerdem ist das Firewall-System zusätzlich dafür ausgestaltet und eingerichtet, erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte Datenpakete verschlüsselt zum ersten Kommunikationsgerät des anfordernden Benutzers oder zum ausgewählten zweiten Kommunikationsgerät weiterzuleiten.

Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert. Es zeigt die

Figur eine Anordnung mit mehreren Fernwartungsrechnern außerhalb eines industriellen Automatisierungssystems und einem Firewall-System sowie mehreren Automatisierungsgeräten innerhalb des industriellen Automatisierungssystems.

Die in der Figur dargestellte Anordnung umfasst mehrere Fernwartungsrechner 101-103, die über ein Weitverkehrsnetz 400 mit einem Kommunikationsnetz eines industriellen Automatisierungssystems 200 verbunden sind. Die Fernwartungsrechner 101-103 können beispielsweise als PC, Laptop oder Tablet-PC ausgestaltet sein. Das industrielle Automatisierungssystem 200 umfasst zum Schutz vor unzulässigem Nachrichtenverkehr ein Firewall-System 300, das insbesondere im industriellen Automatisierungssystem 200 eingehende Datenpakete auf Basis von festgelegten Sicherheitsregeln überprüft. Diese Sicherheitsregeln umfassen im vorliegenden Ausführungsbeispiel übliche Firewall-Regeln und Regeln über eine Zulässigkeit von in Datenpaketen angegebenen Steuerungsbefehlen bzw. Steuerungsparametern für Automatisierungsgeräte 201-202 des industriellen Automatisierungssystems 200. Somit bietet das Kommunikationsnetz des industriellen Automatisierungssystems 200, in dem das Firewall-System 300 angeordnet ist, sicherheitstechnisch

kontrollierte Zugriffsmöglichkeiten auf die Automatisierungsgeräte 201-202 und ist somit gesichert. Das Weitverkehrsnetz 400 kann beispielweise ein Mobilfunknetz oder ein IP-basiertes Kommunikationsnetz sein.

Die Automatisierungsgeräte 201-202 umfassen jeweils integrierte oder zugeordnete Kommunikationsmodule bzw. -geräte und können speicherprogrammierbare oder PC-basierte Steuerungen einer Maschine oder einer technischen Anlage sein, beispielsweise eines Roboters oder einer Fördervorrichtung. Insbesondere umfassen die Automatisierungsgeräte 201-202 jeweils zumindest eine Zentraleinheit und eine Eingabe/Ausgabe-Einheit. Die Eingabe/Ausgabe-Einheiten dienen einem Austausch von Steuerungs- und Messgrößen zwischen dem jeweiligen Automatisierungsgerät 201-202 und einer durch das Automatisierungsgerät 201-202 gesteuerten Maschine oder Vorrichtung. Die Zentraleinheiten der Automatisierungsgerät 201-202 sind insbesondere für eine Ermittlung geeigneter Steuerungsgrößen aus erfassten Messgrößen vorgesehen.

Das Firewall-System 300 ist rechnerbasiert und umfasst im vorliegenden Ausführungsbeispiel einen Hypervisor 301 als Hardware-Abstraktionselement zwischen tatsächlich vorhandener Hardware des Firewall-Systems und auf dem Firewall-System 300 installierbaren, ablauffähigen Betriebssystemen. Ein solcher Hypervisor 301 ermöglicht eine Bereitstellung einer virtuellen Umgebung, die partitionierte Hardwareressourcen, wie Prozessor, Speicher oder Peripheriegeräte umfasst. Anstelle eines Hypervisors 301 können grundsätzlich auch andere bekannte Virtualisierungskonzepte als Hardware-Abstraktionsmittel zur Bereitstellung auf dem Firewall-System 300 ablaufender Server-Instanzen 311, 321 genutzt werden. Im Sinn einer besseren Übersichtlichkeit ist der Hypervisor 301 in der Figur zeichnerisch vom Firewall-System 300 abgesetzt dargestellt.

Nichtsdestotrotz stellt der Hypervisor 301 eine Komponente des Firewall-Systems 300 dar. Dies gilt auch für eine hardwareimplementierte Kryptologiekomponente 302, die in der Figur vom Firewall-System 300 abgesetzt dargestellt, jedoch vom Firewall-System 300 umfasst ist.

Durch eine solche auf dem Firewall-System 300 ablaufende Server-Instanz wird ein Rendezvous-Server 311 als Verbindungsverwaltungseinrichtung gebildet. Dabei ist der Rendezvous-Server 311 dafür vorgesehen und konfiguriert, Kommunikationsverbindungen von ersten Kommunikationsgeräten außerhalb des industriellen Automatisierungssystems 200 zu dem industriellen Automatisierungssystem 200 zugeordneten zweiten Kommunikationsgeräten aufzubauen, zu verwalten und zu steuern. Zu den ersten Kommunikationsgeräten zählen im vorliegenden Ausführungsbeispiel die Fernwartungsrechner 101-103, während zweite Kommunikationsgeräte den Automatisierungsgeräten 201-202 zugeordnete oder von diesen umfasste Kommunikationsgeräte bzw. -module sind.

Bei einer Anforderung 111 eines Verbindungsaufbaus zu einem ausgewählten Automatisierungsgerät 201 durch einen anfordernden Benutzer eines Fernwartungsrechners 101 führt der Rendezvous-Server 311 anhand einer durch den Rendezvous-Server 311 verwalteten Zugriffskontrollliste 312 eine Berechtigungsüberprüfung für den anfordernden Benutzer in Bezug auf das ausgewählte Automatisierungsgerät 201 durch. Die Zugriffskontrollliste 312 umfasst Benutzer-individuelle Angaben zulässiger Kommunikationsverbindungen zwischen jeweils zumindest einem ersten Kommunikationsgerät und zumindest einem zweiten Kommunikationsgerät.

Verläuft diese Berechtigungsüberprüfung mit einem positiven Ergebnis, stellt der Rendezvous-Server 311 Zugriffskontroll-

informationen 112, 211 zum Aufbau einer verschlüsselten Kommunikationsverbindung 500 zwischen dem Fernwartungsrechner 101 des anfordernden Benutzers und dem ausgewählten Automatisierungsgerät 201 für diese Kommunikationsteilnehmer bereit. Im vorliegenden Ausführungsbeispiel sind zwischen Fernwartungsrechnern 101-103 und Automatisierungsgeräten 201-202 aufgebaute verschlüsselte Kommunikationsverbindungen VPN-Verbindungen (Virtual Private Network). Daher umfassen die Zugriffskontrollinformationen 112, 211 vorzugsweise kryptographische Schlüssel bzw. Passwörter für VPN-Sitzungen oder temporär gültige Passwörter. Die Berechtigungsüberprüfung umfasst eine Authentisierung des anfordernden Benutzers gegenüber dem Rendezvous-Server 311, der nur nach einer Authentifizierung des anfordernden Benutzers Zugriffskontrollinformationen 112 zur Nutzung einer VPN-Verbindung zwischen dem Fernwartungsrechner 101 des anfordernden Benutzers und dem ausgewählten Automatisierungsgerät 201 an den anfordernden Benutzer bereitstellt.

Über die VPN-Verbindung 500 zwischen dem Fernwartungsrechner 101 des anfordernden Benutzers und dem ausgewählten Automatisierungsgerät 201 übermittelte Datenpakete 113, 212 werden durch das Firewall-System 300 entschlüsselt und auf Basis der festgelegten Sicherheitsregeln überprüft. Erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte Datenpakete werden durch das Firewall-System 300 wieder verschlüsselt und zum Fernwartungsrechner 101 des anfordernden Benutzers bzw. zum ausgewählten Automatisierungsgerät 201 weitergeleitet. Eine Entschlüsselung bzw. Verschlüsselung von zu prüfenden bzw. geprüften Datenpaketen erfolgt durch das Firewall-System 300 hardwarebasiert. Hierzu ist die vom das Firewall-System 300 umfasste hardwareimplementierte Kryptologiekomponente 302 vorgesehen. Den festgelegten Sicherheitsregeln nicht entspre-

chende Datenpakete werden durch das Firewall-System 300 verworfen.

Im vorliegenden Ausführungsbeispiel umfasst die auf den festgelegten Sicherheitsregeln basierende Überprüfung durch das Firewall-System 300 auch eine Überprüfung von Passwörtern für VPN-Sitzungen oder temporär gültigen Passwörtern auf Korrektheit. Dabei verwirft das Firewall-System 300 Datenpakete verwirft, für deren Übermittlung inkorrekte Passwörter angegeben worden sind.

Grundsätzlich kann die zwischen dem Fernwartungsrechner 101 des anfordernden Benutzers und dem ausgewählten Automatisierungsgerät 201 aufgebaute VPN-Verbindung 500 zwei VPN-Teil-Verbindungen umfassen, die am Rendezvous-Server 311 terminieren. Damit baut der Rendezvous-Server 311 bei einem positiven Berechtigungsüberprüfungsergebnis jeweils eine verschlüsselte Kommunikationsverbindung zum Fernwartungsrechner 101 des anfordernden Benutzers und zum ausgewählten Automatisierungsgerät 201 auf und verknüpft diese Kommunikationsverbindungen miteinander.

Patentansprüche

1. Verfahren zum Aufbau gesicherter Kommunikationsverbindungen zu einem industriellen Automatisierungssystem, bei dem

- Kommunikationsverbindungen von ersten Kommunikationsgeräten (101 - 103) außerhalb des industriellen Automatisierungssystems (200) zu dem industriellen Automatisierungssystem zugeordneten zweiten Kommunikationsgeräten (201 - 202) über eine Verbindungsverwaltungseinrichtung (311) aufgebaut werden,
- die Verbindungsverwaltungseinrichtung (311) bei einer Anforderung (111) eines Verbindungsaufbaus zu einem ausgewählten zweiten Kommunikationsgerät (201) durch einen anfordernden Benutzer eines ersten Kommunikationsgeräts (101) anhand einer Zugriffskontrollliste (312) eine Berechtigungsüberprüfung für den anfordernden Benutzer durchführt,
- die Verbindungsverwaltungseinrichtung (311) bei einem positiven Berechtigungsüberprüfungsergebnis Zugriffskontrollinformationen (112, 211) zum Aufbau einer verschlüsselten Kommunikationsverbindung (500) zwischen dem ersten Kommunikationsgerät (101) des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät (201) für diese Kommunikationsgeräte bereitstellt,
- die Verbindungsverwaltungseinrichtung (311) durch eine auf einem Firewall-System (300) ablaufende Server-Instanz gebildet wird,
- über eine verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät (101) des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät (201) übermittelte Datenpakete (113, 212) für eine auf festgelegten Sicherheitsregeln basierende Überprüfung durch das Firewall-System (300) entschlüsselt werden,

– das Firewall-System (300) erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte Datenpakete verschlüsselt zum ersten Kommunikationsgerät (101) des anfordernden Benutzers und/oder zum ausgewählten zweiten Kommunikationsgerät (201) weiterleitet.

2. Verfahren nach Anspruch 1,
bei dem die über die Verbindungsverwaltungseinrichtung aufgebauten Kommunikationsverbindungen zwischen ersten Kommunikationsgeräten und zweiten Kommunikationsgeräten Virtual-Private-Network-Verbindungen sind, bei dem die Berechtigungsüberprüfung eine Authentisierung des anfordernden Benutzers gegenüber der Verbindungsverwaltungseinrichtung umfasst und bei dem die Verbindungsverwaltungseinrichtung nur nach einer Authentifizierung des anfordernden Benutzers Zugriffskontrollinformationen zur Nutzung einer Virtual-Private-Network-Verbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät an den anfordernden Benutzer bereitstellt.

3. Verfahren nach Anspruch 2,
bei dem die Zugriffskontrollinformationen kryptographische Schlüssel und/oder Passwörter für VPN-Sitzungen oder temporär gültige Passwörter umfassen.

4. Verfahren nach einem der Ansprüche 2 oder 3,
bei dem die auf den festgelegten Sicherheitsregeln basierende Überprüfung durch das Firewall-System eine Überprüfung von Passwörtern für VPN-Sitzungen oder temporär gültigen Passwörtern auf Korrektheit umfasst und bei dem das Firewall-System Datenpakete verwirft, für deren Übermittlung inkorrekte Passwörter angegeben worden sind.

5. Verfahren nach einem der Ansprüche 1 bis 4,

bei dem die Zugriffskontrollliste Benutzer-individuelle Angaben zulässiger Kommunikationsverbindungen zwischen jeweils zumindest einem ersten Kommunikationsgerät und zumindest einem zweiten Kommunikationsgerät umfasst.

6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem die Verbindungsverwaltungseinrichtung bei einem positiven Berechtigungsüberprüfungsergebnis jeweils eine verschlüsselte Kommunikationsverbindung zum ersten Kommunikationsgerät des anfordernden Benutzers und zum ausgewählten zweiten Kommunikationsgerät aufbaut und diese Kommunikationsverbindungen miteinander verknüpft.

7. Verfahren nach einem der Ansprüche 1 bis 6,
bei dem die über die verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät übermittelten Datenpakete durch das Firewall-System entschlüsselt und auf Basis der festgelegten Sicherheitsregeln überprüft werden und bei dem erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte weiterzuleitende Datenpakete durch das Firewall-System verschlüsselt werden.

8. Verfahren nach Anspruch 7,
bei dem eine Entschlüsselung und/oder Verschlüsselung von Datenpaketen durch das Firewall-System hardwarebasiert erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 8,
bei dem die festgelegten Sicherheitsregeln Firewall-Regeln und/oder Regeln über eine Zulässigkeit von in Datenpaketen angegebenen Steuerungsbefehlen und/oder Steuerungsparametern für Automatisierungsgeräte umfassen.

10. Verfahren nach einem der Ansprüche 1 bis 9,

bei dem das Firewall-System den festgelegten Sicherheitsregeln nicht entsprechende Datenpakete verwirft.

11. Verfahren nach einem der Ansprüche 1 bis 10,
bei dem das Firewall-System in einem gesicherten Kommunikationsnetz des industriellen Automatisierungssystems angeordnet ist.

12. Verfahren nach einem der Ansprüche 1 bis 11,
bei dem die Verbindungsverwaltungseinrichtung ein Rendezvous-Server ist.

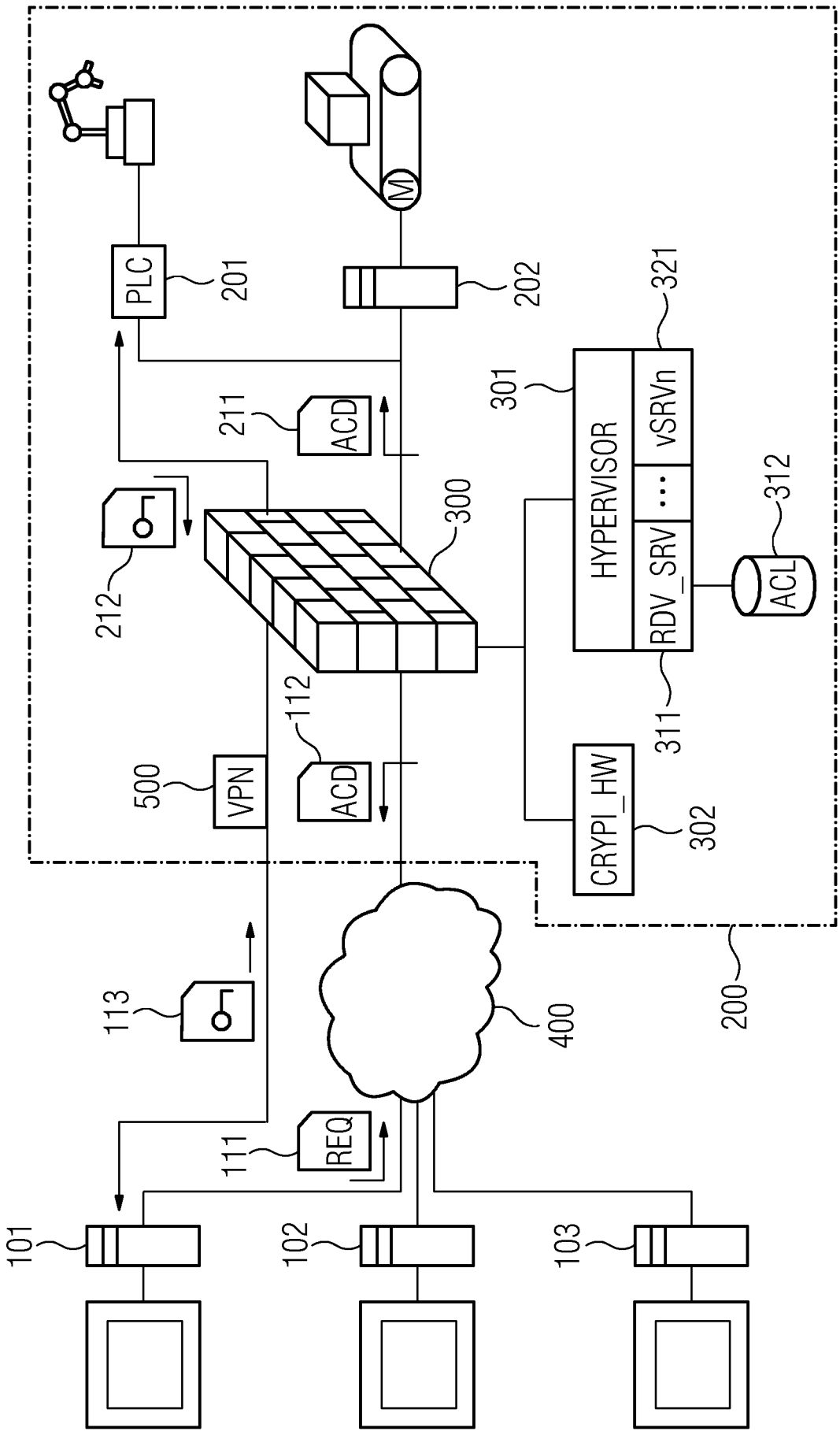
13. Verfahren nach einem der Ansprüche 1 bis 12,
bei dem zweite Kommunikationsgeräte in Automatisierungsgeräte integriert oder diesen zugeordnet sind.

14. Firewall-System zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 13, bei dem

- das Firewall-System für eine auf festgelegten Sicherheitsregeln basierende Überprüfung von Datenpaketen ausgestaltet und eingerichtet ist,
- das Firewall-System zusätzlich für einen Ablauf zumindest einer Server-Instanz ausgestaltet und eingerichtet ist,
- durch die Server-Instanz eine Verbindungsverwaltungseinrichtung gebildet ist, die für einen Kommunikationsverbindungsaufbau von ersten Kommunikationsgeräten außerhalb eines industriellen Automatisierungssystems zu dem industriellen Automatisierungssystem zugeordneten zweiten Kommunikationsgeräten ausgestaltet und eingerichtet ist,
- die Verbindungsverwaltungseinrichtung zusätzlich dafür ausgestaltet und eingerichtet ist, bei einer Anforderung eines Verbindungsaufbaus zu einem ausgewählten zweiten Kommunikationsgerät durch einen anfordernden Benutzer eines ersten

Kommunikationsgeräts anhand einer Zugriffskontrollliste eine Berechtigungsüberprüfung für den anfordernden Benutzer durchzuführen,

- die Verbindungsverwaltungseinrichtung zusätzlich dafür ausgestaltet und eingerichtet ist, bei einem positiven Berechtigungsüberprüfungsergebnis Zugriffskontrollinformationen zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät für diese Kommunikationsgeräte bereitzustellen,
- das Firewall-System zusätzlich dafür ausgestaltet und eingerichtet ist, über eine verschlüsselte Kommunikationsverbindung zwischen dem ersten Kommunikationsgerät des anfordernden Benutzers und dem ausgewählten zweiten Kommunikationsgerät übermittelte Datenpakete für die auf den festgelegten Sicherheitsregeln basierende Überprüfung zu entschlüsseln,
- das Firewall-System zusätzlich dafür ausgestaltet und eingerichtet ist, erfolgreich auf Basis der festgelegten Sicherheitsregeln überprüfte Datenpakete verschlüsselt zum ersten Kommunikationsgerät des anfordernden Benutzers oder zum ausgewählten zweiten Kommunikationsgerät weiterzuleiten.


PLC
201
202
321
301
211
ACD
HYPERVISOR
vSRVn
300
312
212
RDV_SRV
ACL
311
112
500
VPN
ACD
CRYPT_HW
302
113
400
200
111
REQ
101
102
103

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/065844

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. G05B19/418

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 G05B

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	EP 2 461 538 A2 (SIEMENS CORP [US]) 6 June 2012 (2012-06-06)	1-5, 7-11,13, 14
A	abstract; figures 1,3,4-7 paragraphs [0004], [0009] - paragraph [0012] paragraph [0014] - paragraph [0018] paragraph [0030] - paragraph [0052] -----	6,12
X	US 2008/126794 A1 (WANG JIANXIN [US] ET AL) 29 May 2008 (2008-05-29)	1,6,7, 10,12,14
A	abstract; figures 1,2,4,6,7 paragraph [0019] - paragraph [0020] paragraph [0023] - paragraph [0024] paragraph [0038] - paragraph [0041] claims 6-8 ----- -/--	2-5,8,9, 11,13

[X] Further documents are listed in the continuation of Box C.

[X] 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
1 August 2017	09/08/2017

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	Barla Harter, I

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Anonymous: "DNP3 - Wikipedia", , 20 June 2016 (2016-06-20), XP055320228, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=DNP3&oldid=727297197 [retrieved on 2016-11-16] page 2	1-14
A	US 2015/113264 A1 (WANG WEI DAVID [CA] ET AL) 23 April 2015 (2015-04-23) paragraph [0003] paragraph [0006] - paragraph [0007] paragraph [0012] - paragraph [0014] paragraph [0024] - paragraph [0025] paragraph [0045] - paragraph [0051] paragraph [0071] - paragraph [0074] paragraph [0110] - paragraph [0116]	1-14
A	US 2006/053290 A1 (RANDLE WILLIAM M [US] ET AL) 9 March 2006 (2006-03-09) paragraph [0009] - paragraph [0012] paragraph [0014] paragraph [0040] - paragraph [0043] paragraph [0047] - paragraph [0049] claim 1	1-14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/065844

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2461538 A2	06-06-2012	EP 2461538 A2	06-06-2012
		US 2012144187 A1	07-06-2012
US 2008126794 A1	29-05-2008	US 2008126794 A1	29-05-2008
		US 2012272058 A1	25-10-2012
US 2015113264 A1	23-04-2015	US 2015113264 A1	23-04-2015
		US 2017093796 A1	30-03-2017
US 2006053290 A1	09-03-2006	US 2006053290 A1	09-03-2006
		US 2006107036 A1	18-05-2006

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/065844

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06
ADD. G05B19/418

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G05B

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	EP 2 461 538 A2 (SIEMENS CORP [US]) 6. Juni 2012 (2012-06-06)	1-5, 7-11,13, 14
A	Zusammenfassung; Abbildungen 1,3,4-7 Absätze [0004], [0009] - Absatz [0012] Absatz [0014] - Absatz [0018] Absatz [0030] - Absatz [0052]	6,12

X	US 2008/126794 A1 (WANG JIANXIN [US] ET AL) 29. Mai 2008 (2008-05-29)	1,6,7, 10,12,14
A	Zusammenfassung; Abbildungen 1,2,4,6,7 Absatz [0019] - Absatz [0020] Absatz [0023] - Absatz [0024] Absatz [0038] - Absatz [0041] Ansprüche 6-8	2-5,8,9, 11,13

	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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
1. August 2017	09/08/2017

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	Barla Harter, I

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	Anonymous: "DNP3 - Wikipedia", , 20. Juni 2016 (2016-06-20), XP055320228, Gefunden im Internet: URL:https://en.wikipedia.org/w/index.php?title=DNP3&oldid=727297197 [gefunden am 2016-11-16] Seite 2 -----	1-14
A	US 2015/113264 A1 (WANG WEI DAVID [CA] ET AL) 23. April 2015 (2015-04-23) Absatz [0003] Absatz [0006] - Absatz [0007] Absatz [0012] - Absatz [0014] Absatz [0024] - Absatz [0025] Absatz [0045] - Absatz [0051] Absatz [0071] - Absatz [0074] Absatz [0110] - Absatz [0116] -----	1-14
A	US 2006/053290 A1 (RANDLE WILLIAM M [US] ET AL) 9. März 2006 (2006-03-09) Absatz [0009] - Absatz [0012] Absatz [0014] Absatz [0040] - Absatz [0043] Absatz [0047] - Absatz [0049] Anspruch 1 -----	1-14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/065844

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2461538 A2	06-06-2012	EP 2461538 A2	06-06-2012
		US 2012144187 A1	07-06-2012
US 2008126794 A1	29-05-2008	US 2008126794 A1	29-05-2008
		US 2012272058 A1	25-10-2012
US 2015113264 A1	23-04-2015	US 2015113264 A1	23-04-2015
		US 2017093796 A1	30-03-2017
US 2006053290 A1	09-03-2006	US 2006053290 A1	09-03-2006
		US 2006107036 A1	18-05-2006