

WO 2014/04824 A1



Veröffentlicht:

- mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

eine Vielzahl von Überwachungseinrichtungen, wie z.B. Überwachungskameras, um derartige Überwachungsbereiche großflächig abdecken zu können. Hierzu wird ein Endgerät 7 mit mindestens einer Funktionseinrichtung, wobei die Funktionseinrichtung als eine Sensor- und/oder Aktoreinrichtung ausgebildet ist, mit einer Steuerungseinrichtung 10, wobei die Steuerungseinrichtung 10 als eine digitale Datenverarbeitungseinrichtung ausgebildet ist, und mit mindestens einer Netzwerkschnittstelle 9 vorgeschlagen, wobei die Netzwerkschnittstelle 9 zur Kopplung der Steuerungseinrichtung 10 mit einem Netzwerk 2 ausgebildet ist, so dass Daten von der Funktionseinrichtung in das Netzwerk 2 und/oder Daten von dem Netzwerk 2 in die Funktionseinrichtung übertragbar sind, wobei das Endgerät 7 eine Client-Adresse aus einem ersten Netzwerk 2 als das Netzwerk aufweist, wobei das Endgerät 7 eine Speichereinrichtung 11 aufweist, in der eine Server-Adresse aus einem anderen Netzwerk 4 abgelegt ist, wobei die Steuerungseinrichtung 10 ausgebildet ist, bei einer Initialisierung des Endgeräts 7 über die Netzwerkschnittstelle 9 eine Nachricht an die Server-Adresse zu senden.

Beschreibung

5

Titel

**ENDGERÄT, ÜBERWACHUNGSSYSTEM MIT DEM ENDGERÄT SOWIE
VERFAHREN ZUR INITIALISIERUNG DES ENDGERÄTS**

10

Stand der Technik

15

20

25

Die Überwachung von komplexen oder weitläufigen Gebäuden oder Plätzen erfordert eine Vielzahl von Überwachungseinrichtungen, wie z.B. Überwachungskameras, um derartige Überwachungsbereiche großflächig abdecken zu können. Während bei früheren Überwachungsanlagen die Bilddatenströme von den Überwachungskameras analog in Überwachungszentralen übertragen und dort ausgewertet wurden, ist es mittlerweile bekannt, Überwachungskameras an ein Datennetzwerk anzuschließen und die Bilddatenströme digital zu übertragen. Hierzu ist es notwendig, die Überwachungskameras in dem Datennetzwerk zu integrieren und ihnen eine Netzwerkadresse (IP-Adresse) zuzuweisen. Nachfolgend muss die Überwachungskamera von der Überwachungszentrale in dem Datennetzwerk "aufgefunden" werden, um mit dieser kommunizieren zu können. Folglich benötigt die Integration einer Überwachungskamera in ein Netzwerk üblicherweise das gehobene Fachwissen eines Systemadministrators, um die Inbetriebnahme fehlerfrei durchführen zu können.

Offenbarung der Erfindung

30

35

Es wird ein Endgerät für ein Überwachungssystem sowie das Überwachungssystem mit dem Endgerät und ein Verfahren zur Initialisierung des Endgeräts in dem Überwachungssystem mit den Merkmalen der Ansprüche 1, 9 sowie 12 vorgeschlagen. Bevorzugte oder vorteilhafte Ausführungsformen der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung sowie den beigefügten Figuren.

Die Erfindung betrifft somit ein Endgerät - auch Edge-Gerät genannt -, welches für eine Integration in ein Überwachungssystem geeignet und/oder ausgebildet ist. Insbesondere bildet das Endgerät eine Schnittstelle zwischen dem Überwachungssystem und einem Überwachungsbereich.

Das Endgerät weist mindestens eine Funktionseinrichtung auf, wobei die Funktionseinrichtung als eine Sensor- und/oder Aktoreinrichtung ausgebildet ist. Die Funktionseinrichtung kann beispielsweise als ein automatischer oder manueller Brandmelder, als ein Temperatursensor, als ein Objektsensor, wie z.B. eine Lichtschranke, als ein Türöffner, als ein Drehkreuzöffner etc. ausgebildet sein.

Das Endgerät umfasst eine Steuerungseinrichtung, wobei die Steuerungseinrichtung als eine digitale Datenverarbeitungseinrichtung ausgebildet ist. Insbesondere ist die digitale Datenverarbeitungseinrichtung als ein Computer mit einem Betriebssystem realisiert.

Das Endgerät umfasst mindestens eine Netzwerkschnittstelle, welche eine Kopplung der Steuerungseinrichtung bzw. des Endgeräts mit einem Netzwerk erlaubt. Bei dem Netzwerk handelt es sich besonders bevorzugt um ein Datennetzwerk, welches auf Basis des TCP-IP-Protokolls arbeitet. Im speziellen handelt es sich um ein Ethernet-Netzwerk. Die Netzwerkschnittstelle und/oder die Steuerungseinrichtung erlauben es, dass Daten von der Funktionseinrichtung in das Netzwerk und/oder Daten von dem Netzwerk in die Funktionseinrichtung übertragbar sind. Somit ist es beispielsweise möglich, Sensordaten der Sensoreinrichtung in das Netzwerk zu übertragen oder Befehlsdaten von dem Netzwerk in die Aktoreinrichtung zu übermitteln. Es ist beispielsweise auch möglich, dass eine bidirektionale Kommunikation zur Konfiguration der Funktionseinrichtung über die Netzwerkschnittstelle erfolgt.

Das Endgerät weist eine Client-Adresse aus einem ersten Netzwerk auf, wobei das erste Netzwerk bevorzugt als ein LAN (Local Area Network) ausgebildet ist. Insbesondere ist das erste Netzwerk als ein lokales Subnetz ausgebildet.

Im Rahmen der Erfindung wird vorgeschlagen, dass das Endgerät eine Speichereinrichtung aufweist, in der eine Server-Adresse aus einem anderen

Netzwerk abgelegt ist. Die Speichereinrichtung ist besonders bevorzugt als nicht flüchtiger Speicher ausgebildet. Insbesondere ist die Speichereinrichtung vorkonfiguriert, sodass in der Speichereinrichtung die Server-Adresse z.B. werkseitig abgelegt und damit bekannt ist. Die Steuerungseinrichtung ist
5 programmtechnisch und/oder schaltungstechnisch ausgebildet, bei einer Initialisierung des Endgeräts über die Netzwerkschnittstelle eine Nachricht an die Server-Adresse zu senden. Somit weist das Endgerät die Funktionalität auf, dass bei einer Initialisierung des Endgeräts die Nachricht vorzugsweise automatisch oder automatisiert von dem Endgerät in das erste Netzwerk und von dort in das
10 andere Netzwerk an den Server gesendet wird, wobei die Server-Adresse in dem Endgerät vorkonfiguriert ist. Das Endgerät ist somit programmtechnisch und/oder schaltungstechnisch ausgebildet, bei der Initialisierung aktiv eine Kommunikation zu dem Server an der vorkonfigurierten Serveradresse aufzubauen.

Mit der erfindungsgemäßen Ausgestaltung des Endgeräts ist es möglich, dass sich das Endgerät selbsttätig, insbesondere ohne Benutzerinteraktion, an dem Server anmeldet. Auf diese Weise wird die Installation des Endgeräts in dem ersten Netzwerk deutlich vereinfacht. Das Endgerät ist somit eine technische Lösung für das Problem, dass in einem weit verteilten Netzwerk mit mindestens
20 einem lokalen Subnetz als das erste Netzwerk und einem Hauptnetzwerk als das andere Netzwerk besteht, wenn das lokale Subnetz durch einen Router von dem Hauptnetzwerk abgeteilt ist. Durch die Trennung (NAT) sind Netzwerkteilnehmer (Clients) in dem lokalen Subnetzen für die Anwendungen und Geräte in dem Hauptnetz als das andere Netzwerk unsichtbar. Auf herkömmlichem Weg müsste man z.B. den Router des lokalen Subnetzes derart umkonfigurieren, sodass
25 einzelne Ports zu den Clients in dem lokalen Subnetz sichtbar sind. Allerdings birgt dieses Verfahren Sicherheitsrisiken, da der freigeschaltete Port auch für andere Teilnehmer im Hauptnetzwerk sichtbar ist.

Das erfindungsgemäße Endgerät nutzt dagegen den entscheidenden Vorteil, dass es die Gegenstelle, den Server als Backend, schon vorab kennt, da die Server-Adresse in der Speichereinrichtung vorkonfiguriert abgelegt ist. Damit handelt es sich bei dem Verbindungsaufbau von dem Endgerät zu dem Server um eine Kommunikation vom lokalen Subnetz als erstes Netzwerk ins Hauptnetz
30 als das andere Netzwerk und nicht umgekehrt. Herkömmliche Router oder NAT-Einrichtungen erlauben Verbindungen in diese Richtung und müssen nicht
35

aufwendig umparametriert werden. Der Server als Backend wiederum kann die aufgebaute Verbindung nutzen, um mit dem Endgerät zu kommunizieren und weitere Anfragen zu stellen. Z.B. kann das Endgerät auf diese Weise von dem Server parametrisiert werden und es können Daten, z.B. Videoscreens, angefordert oder übermittelt werden.

Somit weist das Endgerät mehrere Vorteile auf: Es ist weniger Konfigurationsaufwand notwendig, da die Überwindung einer NAT-Grenze ohne Routerkonfiguration möglich ist. Das Endgerät erlaubt eine Plug-and-Play-Einrichtung, da das Endgerät in dem ersten Netzwerk lediglich eine Netzwerkadresse erhalten muss.

Bei einer bevorzugten Realisierung der Erfindung sind die Funktionseinrichtungen und die Steuerungseinrichtung in einem Gehäuse integriert. In dieser Form ist das Endgerät besonders kompakt und kann einfach aufgestellt werden, da nur das Gehäuse montiert und der Netzwerkanschluss hergestellt werden muss.

Besonders bevorzugt ist das Endgerät als ein Embedded System und/oder als eine intelligente Funktionskomponente ausgebildet. Als Betriebssystem wird bevorzugt Linux- (Embedded Linux) NetBSD oder Windows (CE, XP Embedded, Automotive oder Embedded for PoS) eingesetzt. Durch die Ausbildung als Embedded System/intelligente Funktionskomponente kann eine große Funktionsvielfalt mit einem geringen Hardwareaufwand umgesetzt werden.

Bei einer bevorzugten Ausgestaltung der Erfindung umfasst die Nachricht eine eindeutige Geräte-ID, sodass es dem Server ermöglicht wird, das Endgerät eindeutig zu identifizieren. Die Geräte-ID - nachfolgend auch einfach ID genannt - kann beispielsweise als eine Zahlen- und/oder Ziffernfolge ausgebildet sein. Durch die ID kann der Server sowohl die Art und/oder den Funktionsumfang des Endgeräts als auch weitere Informationen, wie z.B. Befehlssätze und Kommunikationsdetails, ableiten.

Bei einer bevorzugten Weiterbildung der Erfindung ist das Endgerät ausgebildet, eine bidirektionale Kommunikation mit zertifikatsbasierter Authentifizierung mit dem Server zu etablieren. Insbesondere ist das Endgerät ausgebildet, mit dem

Server einen SSL-Handshake durchzuführen, um eine sichere Kommunikation zwischen Server und Endgerät zu ermöglichen. Besonders bevorzugt weist die Speichereinrichtung des Endgeräts ein Authentifizierungszertifikat auf. Statt einer SSL-Kommunikation kann auch ein anderes Verschlüsselungsprotokoll zur sicheren Datenübertragung, wie z.B. TLS (Transport Layer Security) eingesetzt werden. Durch die zertifikatsbasierter Authentifizierung wird ein Abhören oder ein Missbrauch des Endgeräts wirkungsvoll unterbunden.

Bei einer bevorzugten Ausgestaltung der Erfindung weist die Steuerungseinrichtung ein Verbindungsmodul auf, welches ausgebildet ist, die Nachricht mehrmals nacheinander zu senden. Insbesondere wird die Nachricht solange gesendet, bis eine Reaktion von dem Server erfolgt ist.

Besonders bevorzugt ist es, dass das Verbindungsmodul so ausgebildet ist, dass die zeitlichen Abstände zwischen dem Senden der Nachrichten in Abhängigkeit der Zeit ab der Initialisierung und/oder in Abhängigkeit der gesendeten Nachrichten vergrößert werden. Dieser Ausgestaltung liegt die Überlegung zugrunde, dass bei einem Verbindungsaufbau durchaus Fehler auftreten können, sodass es sinnvoll ist, die Nachricht wiederholt zu senden. Ist es jedoch nicht möglich, innerhalb eines definierbaren Zeitraums eine Verbindung herzustellen, so ist davon auszugehen, dass physikalische Netzwerkprobleme vorherrschen und eine sofortige Wiederholung der Nachricht sinnlos ist. Beispielsweise wird zunächst die Nachricht in einem Intervall von 10 Sekunden gesendet; wenn eine entsprechende Antwort vom Server innerhalb der ersten Stunde nicht vorliegt, wird das Intervall auf 30 Sekunden erhöht und - falls nach einem Zeitraum von z.B. sieben Tagen keine Antwort vom Server vorliegt - wird das Intervall auf 300 Sekunden erhöht. Auf diese Weise ist es möglich, zum einen regelmäßig den Verbindungsaufbau zu probieren bzw. zu prüfen und auf der anderen Seite das Endgerät energiesparend zu betreiben.

Bei einer besonders einfachen und damit bevorzugten Ausgestaltung der Erfindung wird die Initialisierung durch ein Einschalten des Endgeräts, insbesondere durch ein Verbinden des Endgeräts mit einer Spannungsversorgung, automatisch gestartet. Somit ist es bei der Inbetriebnahme ausreichend, die Netzwerkschnittstelle mit dem ersten Netzwerk zu verbinden und nachfolgend das Endgerät einzuschalten, wobei die

nachfolgende Initialisierung automatisch erfolgt. Es ist auch möglich, dass die Spannungsversorgung über das Netzwerk (POE - Power Over Ethernet) erfolgt, sodass es ausreichend ist, das Endgerät mit dem ersten Netzwerk zu verbinden, um die Initialisierung zu starten.

5

Bei einer bevorzugten Weiterbildung der Erfindung ist das Endgerät als eine Überwachungskamera, insbesondere als eine digitale Überwachungskamera, ausgebildet. In dieser Ausgestaltung ist es möglich, dass die Überwachungskamera auch als eine so genannte PTZ- (Pan-Tilt-Zoom-) Kamera realisiert ist, welche gesteuert die Blickrichtung und den Bildausschnitt verändern kann. Die Integration der Überwachungskamera funktioniert, wie zuvor erläutert, über die Plug-and-Play-Einrichtung.

10

Einen weiteren Gegenstand der Erfindung bildet ein Überwachungssystem - auch Überwachungsanlage zu nennen - mit mindesten einem Endgerät, wie dies zuvor beschrieben wurde, bzw. nach einem der vorhergehenden Ansprüche. Das Überwachungssystem weist ferner den Server auf, wobei das Endgerät die Client-Adresse aus dem ersten Netzwerk und der Server die Server-Adresse aus dem anderen Netzwerk aufweist.

15

20

Besonders bevorzugt sind die zwei Netzwerke über mindestens eine NAT-Einrichtung (Network-Address-Translation-Einrichtung) voneinander getrennt, sodass die Nachricht von dem Endgerät über die mindestens eine NAT-Einrichtung an den Server gesendet wird. Eine derartige NAT-Einrichtung ist zwischen zwei Netzwerken datentechnisch angeordnet, um verschiedene Netzwerke miteinander zu verbinden. Besonders bevorzugt ist die NAT-Einrichtung als ein Router ausgebildet. Die NAT-Einrichtung hat die Funktion, automatisiert Adressinformationen in Datenpaketen durch andere Adressinformationen zu ersetzen. Auf diese Weise ist es beispielsweise möglich, dass der Server das Endgerät mit einer Adresse anspricht, die durch die IP-Adresse und einen Port der NAT-Einrichtung gebildet ist, ohne jedoch die tatsächliche IP-Adresse (Client-Adresse) in dem lokalen Netzwerk als erstem Netzwerk des Endgeräts zu kennen. Die NAT-Einrichtung übernimmt die Funktion, die eigene IP-Adresse sowie die Portangabe in eine IP-Adresse, also die Client-Adresse, und eine Portangabe in dem ersten Netzwerk zu übersetzen.

25

30

35

Vorzugsweise erfolgt der Ersatz der Adressinformationen in Gegenrichtung in gleicher Weise.

Bei einer bevorzugten Weiterbildung ist vorgesehen, dass das erste Netzwerk eine DHCP-Funktionalität (Dynamic Host Configuration Protocol) aufweist, wobei dadurch eine automatische Einbindung des Endgeräts in das erste Netzwerk ohne manuelle Konfiguration des Endgeräts ermöglicht wird. Insbesondere ist an dem Endgerät der automatische Bezug der IP-Adresse eingestellt. Diese Ausgestaltung vereinfacht die Installation des Endgeräts nochmals.

Ein weiterer Gegenstand der Erfindung betrifft ein Verfahren zur Initialisierung des Endgeräts, wie es zuvor beschrieben wurde, in dem Überwachungssystem, wie es ebenfalls zuvor beschrieben wurde, wobei das Endgerät bei seiner Initialisierung eine Nachricht an die Server-Adresse sendet. Insbesondere umfasst das Verfahren die bestimmungsgemäße Nutzung des Endgeräts und/oder des Überwachungssystems.

Weitere Merkmale, Vorteile und Wirkungen der Erfindung ergeben sich aus der nachfolgenden Beschreibung eines bevorzugten Ausführungsbeispiels der Erfindung sowie der beigefügten Figuren. Dabei zeigen:

Figur 1 eine schematische Blockdarstellung eines Überwachungssystems als ein Ausführungsbeispiel der Erfindung;

Figur 2 ein Flussdiagramm zur Erläuterung des Verfahrens zur Inbetriebnahme eines Endgeräts in dem Überwachungssystem der Figur 1;

Figur 3 ein schematisches Diagramm zur weiteren Erläuterung des Verfahrens der Figur 2.

Die Figur 1 zeigt in einem schematischen Blockdiagramm ein Überwachungssystem 1 als ein Ausführungsbeispiel der Erfindung. Das Überwachungssystem 1 umfasst mindestens ein lokales Überwachungsnetzwerk als ein erstes Netzwerk 2. Das erste Netzwerk 2 ist in einem Überwachungsobjekt 3, wie z.B. in einem Gebäude oder Gebäudekomplex, einem Bahnhof, einem Flughafen etc. installiert.

Das erste Netzwerk 2 ist als ein lokales Netzwerk ausgebildet und definiert eine oder mindestens eine lokale Domäne. Das erste Netzwerk 2 ist z.B. als ein LAN realisiert. Jeder der Netzwerkteilnehmer in dem ersten Netzwerk 2 weist eine lokale IP-Adresse auf.

Das erste Netzwerk 2 weist als eine Schnittstelle zu einem anderen Netzwerk 4 einen Router 5 auf, welcher eine NAT-Einrichtung 6 umfasst. Die NAT-Einrichtung 6 ist ausgebildet, Netzwerkadressen zwischen dem ersten Netzwerk 2 und dem anderen Netzwerk 4 zu übersetzen. Insbesondere handelt es sich bei dem ersten Netzwerk 2 um ein ausschließlich privates Netzwerk und bei dem anderen Netzwerk 4 um das Internet oder ein Tier-3- oder Tier-2- oder Tier-1-Netzwerk.

In dem ersten Netzwerk 2 ist mindestens ein Endgerät 7 mit einer Funktionseinrichtung 12 angeordnet. In der dargestellten Ausbildung des Endgeräts 7 als Überwachungskamera umfasst dieses eine Kameraeinrichtung als die Funktionseinrichtung 12, welche ausgebildet ist, einen Überwachungsbereich 8 in dem Überwachungsobjekt 3 zu überwachen. Die Endgeräte 7 weisen jeweils eine Netzwerkschnittstelle 9 auf, über die die Endgeräte 7 in dem ersten Netzwerk 2 kommunizieren können. Die Endgeräte 7 sind als intelligente Endgeräte 7 ausgebildet, welche jeweils eine Steuerungseinrichtung 10 sowie eine lokale Speichereinrichtung 11 umfassen.

Das andere Netzwerk 4 basiert auf dem Internetprotokoll und kann bei einer ersten Ausführungsalternative als ein öffentliches Internet ausgebildet sein. Alternativ hierzu ist das andere Netzwerk 4 als ein privates IP-Netz ausgebildet, wobei sämtliche Schnittstellen des anderen Netzwerks 4 dem privaten IP-Netz exklusiv zugeordnet sind und das private IP-Netz insbesondere von dem öffentlichen Internet datentechnisch getrennt ist. Alternativ kann das andere Netzwerk 4 auch als ein LAN (Local Area Network) oder als ein WAN (Wide Area Network) ausgebildet sein. Insbesondere setzt das andere Netzwerk 4 eine TCP-Verbindung um.

Das Überwachungssystem 1 umfasst eine insbesondere zentrale oder globale Sicherheitssteuerungseinrichtung, welche als ein Server 13 ausgebildet ist. Der

Server 13 ist über eine Schnittstelle mit dem anderen Netzwerk 4 und somit mittelbar mit dem ersten Netzwerk 2 datentechnisch verbunden.

Im Betrieb des Überwachungssystems 1 können Überwachungsdaten der Endgeräte 7 von dem ersten Netzwerk 2 über den Router 5 bzw. die NAT-Einrichtung 6 an den als Sicherheitssteuerungseinrichtung ausgebildeten Server 13 weitergeleitet werden. Der Server 13 kann nachfolgend - abhängig von seiner Ausbildung - die Überwachungsdaten auswerten und automatisiert einen Alarm auslösen oder die Überwachungsdaten an ein Überwachungspersonal weiterleiten. In Gegenrichtung kann der Server 13 Konfigurationsdaten oder Datenabfragen über das andere Netzwerk 4, den Router/die NAT-Einrichtung 5/6 an die Endgeräte 7 übermitteln. Sind die Endgeräte 7 als Überwachungskameras ausgebildet, so werden in Richtung der Server 13 Bilder des Überwachungsbereichs 8 übertragen.

Ausgebildet als intelligente Überwachungskameras können die Endgeräte 7 auch autarke Auswertungen der Überwachungsdaten mit der Steuerungseinrichtung 10 durchführen. In dem ersten Netzwerk 2 können auch andersartige Endgeräte 7, wie z.B. Türöffner, Brandmelder etc. alternativ oder ergänzend zu den Überwachungskameras integriert sein.

Den Endgeräten 7 sind in dem ersten Netzwerk 2 jeweils lokale IP-Adressen als Client-Adressen zugeordnet. Dem Server 13 ist in dem anderen Netzwerk 4 eine IP-Adresse als Server-Adresse zugeordnet. Es kann optional vorgesehen sein, dass der Server 13 wiederum in einem lokalen Netzwerk angeordnet ist, wobei der Server trotzdem über die Server-Adresse über das andere Netzwerk 4 erreichbar ist.

Bei der Installation der Endgeräte 7 stellt sich nun das Problem, dass die Endgeräte 7 in dem ersten Netzwerk 2 datentechnisch betrachtet für den Server 13 "unsichtbar" sind, da diese hinter der NAT-Einrichtung 6 angeordnet sind.

Um anwenderfreundlich eine Kommunikation zwischen Server 13 und Endgeräten 7 zu etablieren, weisen die Endgeräte 7 jeweils eine Socket-Knocker-Senderfunktionalität und der Server 13 eine Socket-Knocker-Empfängerfunktionalität auf. Zur Umsetzung ist in der Speichereinrichtung 11 des

Endgeräts 7 die Server-Adresse des Servers 13 fest hinterlegt. Dies kann beispielsweise über eine Vorkonfiguration der Endgeräte 7 erfolgen. Ferner ist in der Speichereinrichtung 11 eine eindeutige ID des Endgeräts 7 abgespeichert. Optional ist in der Speichereinrichtung 11 auch ein Zertifikat für eine gegenseitige Authentifizierung von Endgerät 7 und Server 13 abgelegt. Zur Umsetzung der Socket-Knocker-Empfängerfunktionalität weist der Server 13 einen Gerätemanager 14 auf, welcher z.B. als ein Programm oder ein Dienst in dem Server 13 ausgebildet ist.

Zur Erläuterung des Verbindungsaufbaus zwischen Endgerät 7 und Gerätemanager 14 wird auf die Figur 2 verwiesen.

In einem Schritt 100 wird das Endgerät 7 eingeschaltet, mit einer Spannungsversorgung verbunden oder mit dem ersten Netzwerk 2 verschaltet, sodass ein Start-Up des Endgeräts 7 abläuft.

In einem Schritt 200 wird eine Nachricht N von dem Endgerät 7 an den Server 13, insbesondere an den Gerätemanager 14, als Knock gesendet. Die Versendung kann durch ein Verbindungsmodul (nicht dargestellt) der Steuereinrichtung 10 umgesetzt werden, welche ebenfalls als ein Programm oder ein Dienst ausgebildet ist. Die Nachricht N umfasst die eindeutige ID des Endgeräts 7.

Durch die Übersendung der Nachricht N an den Server 13 wird in der NAT-Einrichtung 6 eine NAT-Session gestartet, wobei die zugehörigen Verbindungsinformationen, insbesondere die IP-Adressen, Ports und gegebenenfalls Time-outs in einer NAT-Tabelle gespeichert werden. Anhand der gespeicherten Informationen kann die NAT-Einrichtung 6 ein Antwort-Datenpaket von dem Gerätemanager 14 bzw. dem Server 13 dem jeweiligen Endgerät 7 korrekt zuordnen. Durch das Absenden der Nachricht N an den Server 13 wird somit eine bidirektionale Verbindung eingeleitet.

Erhält der Server 13, insbesondere der Gerätemanager 14, die Nachricht N, fügt der Gerätemanager 14 das Endgerät 7 anhand der eindeutigen ID zu einer Geräteliste hinzu, die er dem Server 13 zur Verfügung stellt. Weiterhin initiiert der Gerätemanager 14 einen SSL-Handshake mit dem Endgerät 7.

In einem Schritt 300 wartet das Endgerät 7, ob es ein Antwort-Datenpaket von dem Gerätemanager 14 erhält. Ist dies nicht der Fall, wird das Absenden der Nachricht N wiederholt. Ist dies der Fall, wird der SSL-Handshake angenommen und in einem Schritt 400 eine sichere Verbindung zu dem Gerätemanager 14 und damit zu dem Server 13 etabliert.

Zur Sicherheit wird in einem Schritt 500 geprüft, ob das Zertifikat des Gerätemanagers 14 mit dem in der Speichereinrichtung 11 hinterlegten Zertifikat übereinstimmt.

In einem Schritt 600 wird die etablierte Verbindung offengehalten, um eingehende Anfragen des Gerätemanagers 14 oder des Servers 13 erhalten zu können. Für den Fall, dass die Verbindung verlorengeht oder ein Time-out in einem Schritt 700 erfolgt, wird die Prozedur neu gestartet.

Die Zuweisung der Client-Adresse in dem ersten Netzwerk 2 kann zum einen manuell erfolgen, es ist jedoch einfacher, dass das Endgerät 7 die Client-Adresse automatisch über eine DHCP-Funktionalität in einem Schritt 150 (Figur 3) erhält. In der Figur 3 ist das Verfahren nochmals in einer anderen Darstellung gezeigt:

In dem Schritt 100 wird das Endgerät 7 eingeschaltet. In dem Schritt 150 erhält das Endgerät 7 über DHCP die Clientadresse. In dem Schritt 200 wird die Nachricht N an den Gerätemanager 14 übermittelt. In dem Schritt 400 wird das Endgerät 7 der Geräteliste hinzugefügt und der SSL-Handshake vorbereitet. In dem Schritt 500 wird die Identität des Gerätemanagers 14 durch das Endgerät 7 validiert. Optional ist es möglich, dass in einem Schritt 800 von extern abgefragt wird, ob dem Server 13 oder dem Gerätemanager 14 neue Endgeräte 7 bekannt sind. In diesem Fall wird in einem Schritt 850 von dem Server 13 eine Anfrage an den Gerätemanager 14 nach neuen Geräten gerichtet und in einem Schritt 900 die Geräteliste mit den Endgeräten 7 an den Server 13 übermittelt.

Optional kann vorgesehen sein, dass das Absenden der Nachricht N wiederholt wird, wenn in dem Schritt 300 festgestellt wurde, dass keine Antwort von dem Gerätemanager 14 oder dem Server 13 eingegangen ist und somit der Knock

nicht erfolgreich war. In diesem Fall wird in einem Schritt 210 die zeitliche Länge eines Sendeintervalls bestimmt. Beispielsweise wird das Sendeintervall verlängert, wenn nach einigen Versuchen keine Antwort eingegangen ist. In einem Schritt 220 wird die zeitliche Länge des Knock-Intervalls abgewartet und in einem Schritt 230 die Nachricht N nochmals gesendet.

Ansprüche

1. Endgerät (7)

mit mindestens einer Funktionseinrichtung (12), wobei die Funktionseinrichtung (12) als eine Sensor- und/oder Aktoreinrichtung ausgebildet ist,

mit einer Steuerungseinrichtung (10), wobei die Steuerungseinrichtung (10) als eine digitale Datenverarbeitungseinrichtung ausgebildet ist,

mit mindestens einer Netzwerkschnittstelle (9), wobei die Netzwerkschnittstelle (9) zur Kopplung der Steuerungseinrichtung (10) mit einem Netzwerk (2) ausgebildet ist, so dass Daten von der Funktionseinrichtung in das Netzwerk (2) und/oder Daten von dem Netzwerk (2) in die Funktionseinrichtung übertragbar sind,

wobei das Endgerät (7) eine Client-Adresse aus einem ersten Netzwerk (2) als das Netzwerk aufweist

dadurch gekennzeichnet, dass

das Endgerät (7) eine Speichereinrichtung (11) aufweist, in der eine Server-Adresse aus einem anderen Netzwerk (4) abgelegt ist, wobei die Steuerungseinrichtung (10) ausgebildet ist, bei einer Initialisierung des Endgeräts (7) über die Netzwerkschnittstelle (9) eine Nachricht (N) an die Server-Adresse zu senden.

2. Endgerät (7) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionseinrichtung (12) und die Steuerungseinrichtung (10) in einem Gehäuse integriert sind und/oder dass das Endgerät (7) als ein Embedded System und/oder als eine intelligente Funktionskomponente ausgebildet ist.

3. Endgerät (7) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Nachricht (N) eine Geräte-ID des Endgeräts (7) umfasst.

4. Endgerät (7) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Endgerät (7) ausgebildet ist, eine bidirektionale Kommunikation mit zertifikatsbasierter Authentifizierung zu etablieren.
- 5 5. Endgerät nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Steuerungseinrichtung (10) ein Verbindungsmodul aufweist, welches ausgebildet ist, die Nachricht mehrmals nacheinander zu senden.
- 10 6. Endgerät (7) nach Anspruch 5, dadurch gekennzeichnet, dass das Verbindungsmodul ausgebildet ist, die zeitlichen Abstände zwischen dem Senden der Nachricht in Abhängigkeit der Zeit ab der Initialisierung und/oder in Abhängigkeit der Anzahl der gesendeten Nachrichten zu vergrößern.
- 15 7. Endgerät (7) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Initialisierung durch ein Einschalten des Endgeräts (7) automatisch gestartet wird.
- 20 8. Endgerät (7) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Endgerät (7) als eine Überwachungskamera ausgebildet ist.
- 25 9. Überwachungssystem (1) mit mindestens einem Endgerät (7) nach einem der vorhergehenden Ansprüche, wobei das Endgerät (7) die Client-Adresse aus dem ersten Netzwerk (2) aufweist und dem Server (13), wobei der Server (13) die Server-Adresse aus dem anderen Netzwerk (4) aufweist.
- 30 10. Überwachungssystem (1) nach Anspruch 9, gekennzeichnet durch mindestens eine NAT-Einrichtung (6), wobei das erste Netzwerk (2) und das andere Netzwerk (4) über die NAT-Einrichtung (6) datentechnisch miteinander verbunden sind und wobei die Nachricht von dem Endgerät (7) über die mindestens eine NAT-Einrichtung (6) an den Server (13) gesendet wird.

11. Überwachungssystem nach Anspruch 9 oder 10, dadurch gekennzeichnet,
dass das erste Netzwerk (2) eine DHCP-Funktionalität aufweist.
12. Verfahren zur Initialisierung des Endgeräts (7) nach einem der Ansprüche 1
bis 8 in einem Überwachungssystem nach einem der Ansprüche 9 bis 11,
dadurch gekennzeichnet, dass das Endgerät (7) bei seiner Initialisierung
eine Nachricht (N) an die Server-Adresse sendet.

5

10

1 / 3

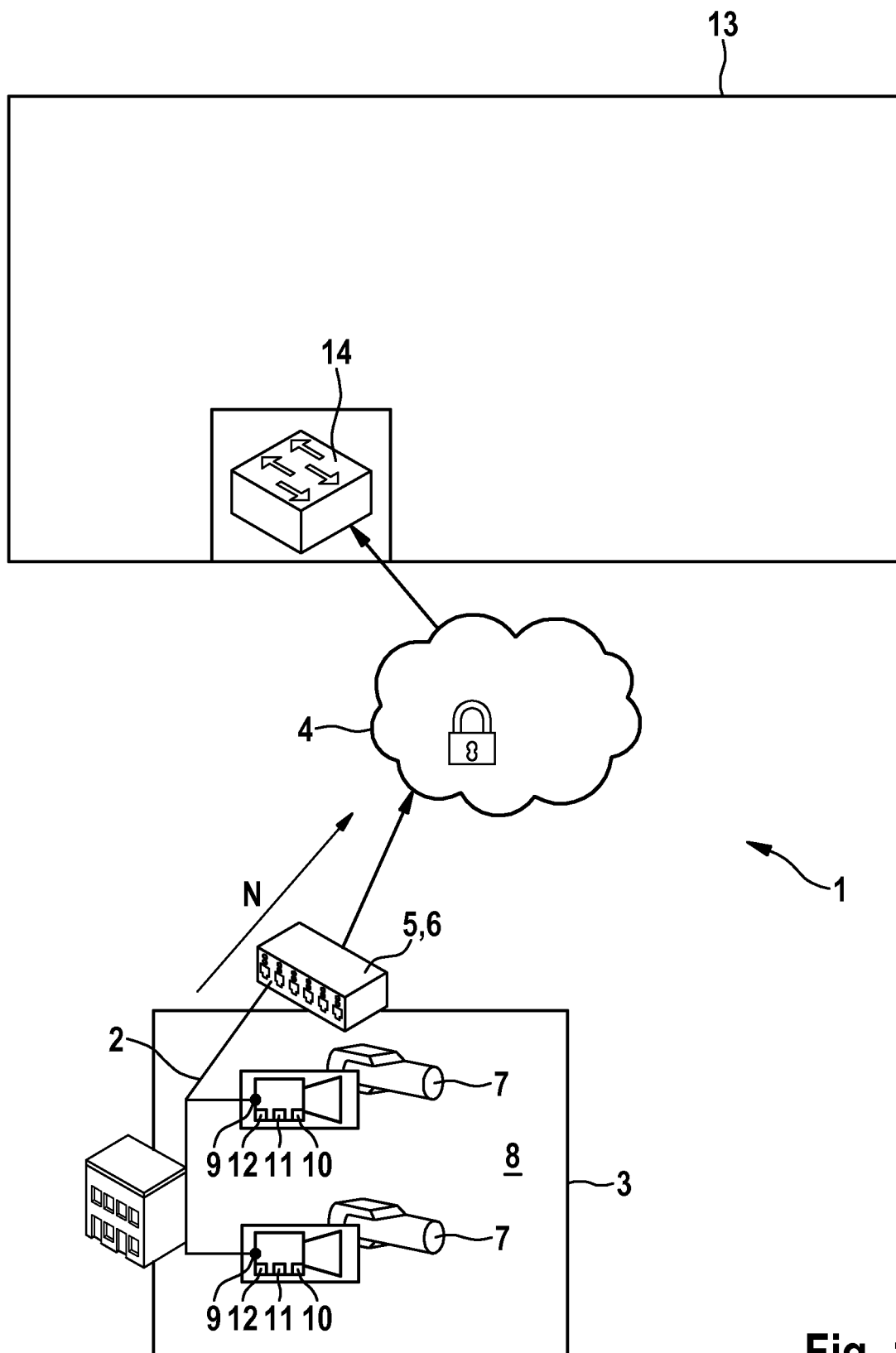


Fig. 1

2 / 3

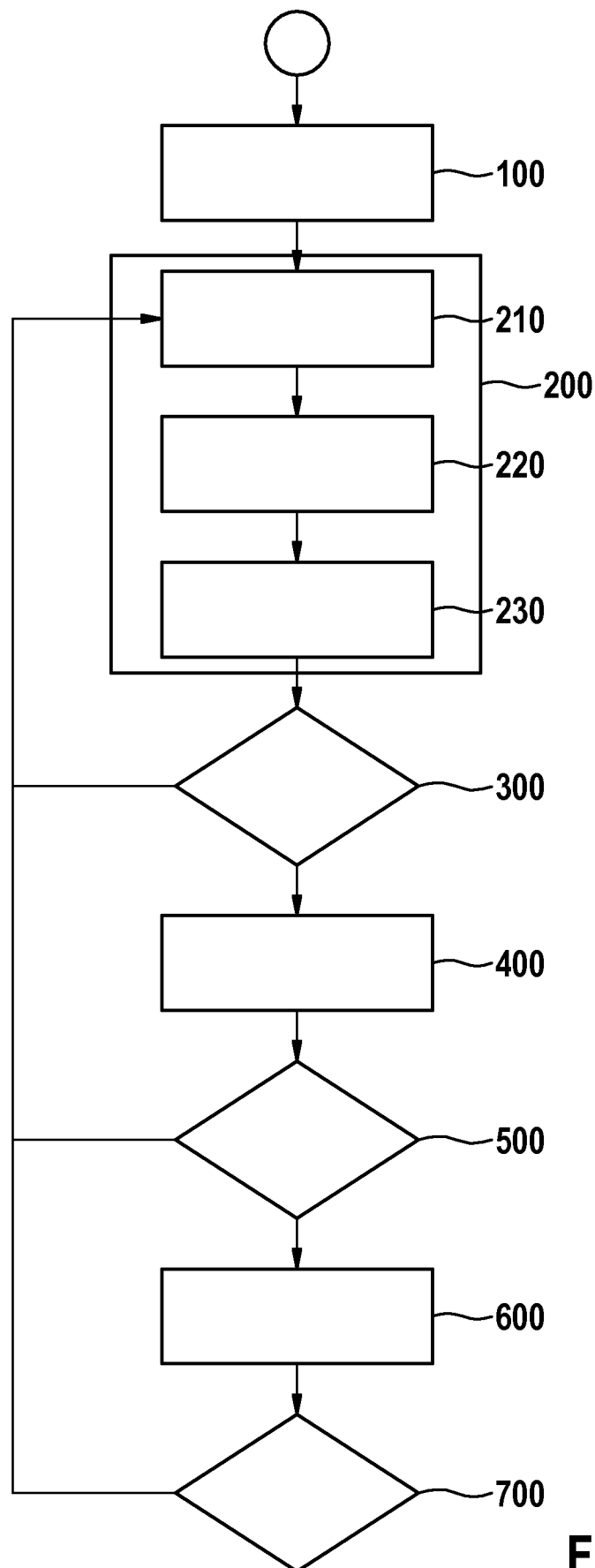


Fig. 2

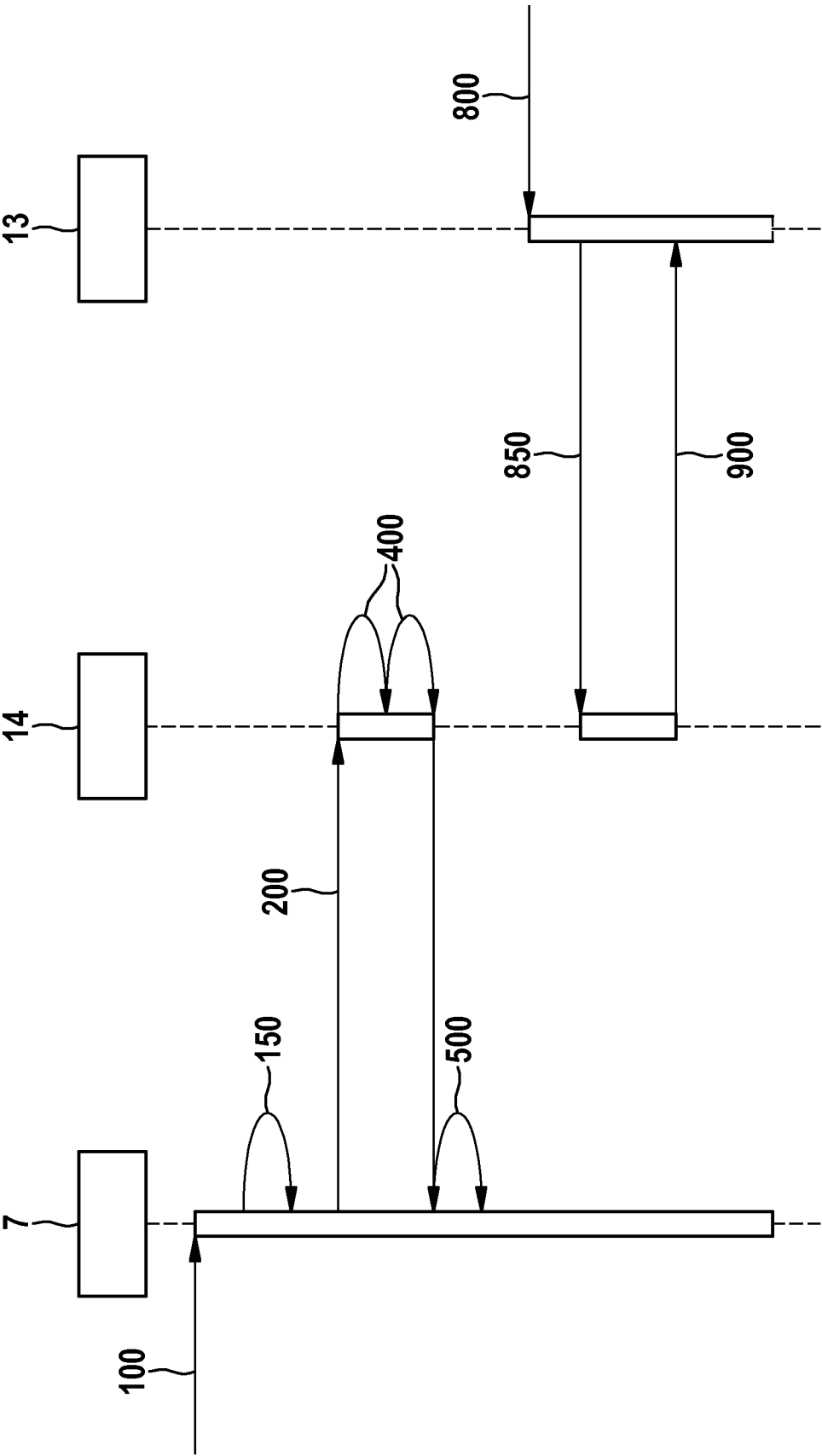


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2013/069627

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/12 G08B13/196
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 G08B

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	US 2006/173997 A1 (TULLBERG JOACIM [SE] ET AL) 3 August 2006 (2006-08-03) abstract paragraphs [0003], [0006], [0007], [1115], [0017], [0021], [0023], [0024], [0042] - [0044], [0046], [0048], [0053], [0054], [0058], [0063], [0064] paragraphs [0070], [0073], [0074] -----	1-12
X	US 2006/195568 A1 (STAURNES JARL O [NO] ET AL) 31 August 2006 (2006-08-31) abstract paragraphs [0002], [0007], [0013], [0017], [0018], [0020] - [0028] -----	1-12



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

13 December 2013

Date of mailing of the international search report

20/12/2013

Name and mailing address of the ISA/

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

Authorized officer

Goller, Wolfgang

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2013/069627

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006173997	A1	03-08-2006	NONE

US 2006195568	A1	31-08-2006	CN 101116337 A 30-01-2008
			EP 1847126 A1 24-10-2007
			NO 323215 B1 29-01-2007
			US 2006195568 A1 31-08-2006
			WO 2006083171 A1 10-08-2006

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. H04L29/12 G08B13/196
 ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 H04L G08B

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	US 2006/173997 A1 (TULLBERG JOACIM [SE] ET AL) 3. August 2006 (2006-08-03) Zusammenfassung Absätze [0003], [0006], [0007], [1115], [0017], [0021], [0023], [0024], [0042] - [0044], [0046], [0048], [0053], [0054], [0058], [0063], [0064] Absätze [0070], [0073], [0074] -----	1-12
X	US 2006/195568 A1 (STAURNES JARL O [NO] ET AL) 31. August 2006 (2006-08-31) Zusammenfassung Absätze [0002], [0007], [0013], [0017], [0018], [0020] - [0028] -----	1-12



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

13. Dezember 2013

Absendedatum des internationalen Recherchenberichts

20/12/2013

Name und Postanschrift der Internationalen Recherchenbehörde

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

Bevollmächtigter Bediensteter

Goller, Wolfgang

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2013/069627

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2006173997	A1	03-08-2006	KEINE

US 2006195568	A1	31-08-2006	CN 101116337 A 30-01-2008
			EP 1847126 A1 24-10-2007
			NO 323215 B1 29-01-2007
			US 2006195568 A1 31-08-2006
			WO 2006083171 A1 10-08-2006
