(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
19. Oktober 2017 (19.10.2017)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2017/178165 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *H04L 29/14* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/055805

(22) Internationales Anmeldedatum:
13. März 2017 (13.03.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2016 205 983.1
11. April 2016 (11.04.2016) DE

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

(72) Erfinder: **RENPENNING, Frank**; Wiedebeinstraße 12, 38118 Braunschweig (DE). **SEIFERT, Matthias**; Celler Str. 44, 38114 Braunschweig (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, 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.

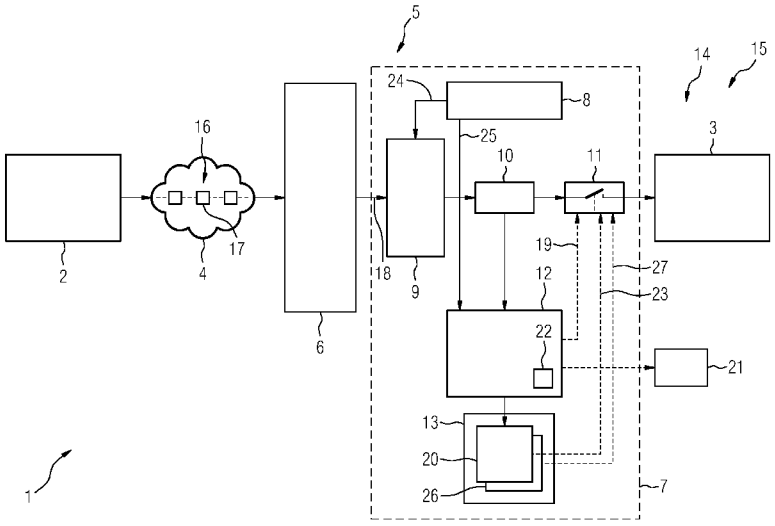
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, 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**: ASSEMBLY FOR CHECKING AT LEAST ONE FIREWALL DEVICE, AND METHOD FOR PROTECTING AT LEAST ONE DATA RECEIVER

(54) **Bezeichnung** : ANORDNUNG ZUM ÜBERPRÜFEN VON WENIGSTENS EINER FIREWALL-EINRICHTUNG UND VERFAHREN ZUM SCHUTZ WENIGSTENS EINES DATENEMPFÄNGERS



(57) **Abstract**: The invention relates to an assembly (7) for checking at least one firewall device (6) and to a method for protecting at least one data receiver (3). In the method according to the invention, permissible and non-permissible data traffic is differentiated in a data traffic (16) in the direction of the data receiver (3) using specific rules; non-permissible data traffic is blocked; and permissible data traffic is allowed through. In order to check the function of the firewall device (6), the data traffic (18) which has been allowed through is interrupted if the data traffic (18) which has been allowed through has non-permissible data traffic.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2017/178165 A1

Die Erfindung betrifft eine Anordnung (7) zum Überprüfen von wenigstens einer Firewall-Einrichtung (6) und Verfahren zum Schutz wenigstens eines Datenempfängers (3). Bei dem erfindungsgemäßen Verfahren wird in einem Datenverkehr (16) in Richtung des Datenempfängers (3) anhand vorbestimmter Regeln zwischen einem erlaubten und einem unerlaubten Datenverkehr unterschieden sowie unerlaubter Datenverkehr blockiert und erlaubter Datenverkehr durchgelassen. Um die Funktion der Firewall-Einrichtung (6) zu überprüfen, ist erfindungsgemäß vorgesehen, dass der durchgelassene Datenverkehr (18) unterbrochen wird, wenn der durchgelassene Datenverkehr (18) unerlaubten Datenverkehr aufweist.

Beschreibung

Anordnung zum Überprüfen von wenigstens einer Firewall-Einrichtung und Verfahren zum Schutz wenigstens eines Datenempfängers

Die Erfindung betrifft eine Anordnung zum Überprüfen von wenigstens einer Firewall-Einrichtung, die anhand vorbestimmter Regeln zum Unterscheiden zwischen einem erlaubten und einem unerlaubten Datenverkehr in Richtung eines Datenempfängers sowie zum Blockieren von unerlaubtem Datenverkehr und zum Durchlassen von erlaubtem Datenverkehr ausgebildet ist.

Ferner betrifft die Erfindung ein Verfahren zum Überprüfen von wenigstens einer Firewall-Einrichtung, bei dem in einem Datenverkehr in Richtung eines Datenempfängers anhand vorbestimmter Regeln zwischen einem erlaubten und einem unerlaubten Datenverkehr unterschieden wird sowie unerlaubter Datenverkehr blockiert und erlaubter Datenverkehr durchgelassen wird.

Sicherheitskritische Anlagen, wie beispielsweise das Signalnetz einer Eisenbahnanlage oder ein Netzwerk innerhalb eines Atomkraftwerks, haben häufig besondere Sicherheitszonen, auf die kein direkter Datenzugriff möglich ist. Trotzdem besteht zunehmender Bedarf an einem Fernzugriff auf die in diesen Sicherheitszonen befindlichen Anlagenelemente, beispielsweise für eine Fernwartung. Daher besteht ein Wunsch an einer Vernetzung sicherheitsrelevanter Anlagen mit herkömmlichen IT-Systemen. Um einen solchen sicheren Zugriff auf sicherheitskritische Anlagen zu ermöglichen, sind Firewall-Einrichtungen bekannt, die einen unerlaubten Datenverkehr in Richtung eines innerhalb einer sicherheitskritischen Anlage befindlichen Datenempfängers blockieren. Da in sicherheitsrelevanten Bereichen andere Überwachungsanforderungen gelten als im normalen IT-Bereich oder im Bereich der Office-IT-Security, sind bekannte Firewall-Einrichtungen für den Datenverkehr mit Daten-

empfängern in einem sicherheitsrelevanten Bereich nicht ausreichend.

Daher ist es die Aufgabe der vorliegenden Erfindung, eine Anordnung und ein Verfahren der eingangs genannten Art bereitzustellen, durch die ein in einem sicherheitsrelevanten Bereich befindlicher Datenempfänger durch eine Firewall-Einrichtung geschützt und die Anforderungen eines sicherheitsrelevanten Bereichs erfüllt sind.

Die vorliegende Erfindung löst diese Aufgabe dadurch, dass die eingangs genannte Anordnung wenigstens eine Erfassungseinrichtung, die zum Erfassen des von der Firewall-Einrichtung durchgelassenen Datenverkehrs ausgebildet ist, und wenigstens eine Auswerteeinrichtung, die zum Überprüfen des von der Erfassungseinrichtung erfassten Datenverkehrs anhand der vorbestimmten Regeln ausgebildet ist, aufweist.

Für das eingangs genannte Verfahren löst die Erfindung die Aufgabe dadurch, dass der durchgelassene Datenverkehr erfasst wird und auf vorhandenen unerlaubten Datenverkehr überprüft wird.

Die erfindungsgemäße Lösung hat den Vorteil, dass durch eine Überprüfung des durch die Firewall-Einrichtung durchgelassenen Datenverkehrs ein Nachweis der Funktion der Firewall-Einrichtung gegeben ist und so auch ein Einsatz für sicherheitsrelevante Bereiche zulässig ist.

Zwar ist beispielsweise in der DE 10 2013 221 955 A1 ein Security-Gateway mit einer Ausfalloffenbarung beschrieben. Darin findet eine Überprüfung statt, ob die Eingangs- und Ausgangsdaten eines VPN-Gateways fehlerhaft gleich sind, d. h. eine Verschlüsselung nicht stattfindet. Eine Analyse, ob die Firewall selbst durch einen Angriff umkonfiguriert wurde, kann hiermit aber nicht erfolgen.

Die erfindungsgemäße Lösung kann durch vorteilhafte Ausgestaltungen weiterentwickelt werden, die im Folgenden beschrieben sind.

So kann die Anordnung wenigstens eine Abschalteinrichtung aufweisen, die zum Unterbrechen des Datenverkehrs in Richtung des Datenempfängers ausgebildet und wenigstens von der Auswerteeinrichtung aktivierbar ist. Dies hat den Vorteil, dass der Datenverkehr zum Datenempfänger unterbrochen werden kann, wenn die Auswerteeinrichtung eine Fehlfunktion der Firewall-Einrichtung erkennt. Diese Fehlfunktion äußert sich durch unerlaubten Datenverkehr in dem von der Firewall-Einrichtung durchgelassenen Datenverkehr in Richtung des Datenempfängers, der von der Auswerteeinrichtung erfasst und überprüft wird. Durch die Abschalteinrichtung kann der Datenempfänger vor unerlaubtem Datenverkehr effektiv geschützt werden. Bei sicherheitsrelevanten Systemen ist es eine Basisanforderung, dass Ausfälle und Fehlfunktionen nicht gefährlich werden dürfen. Durch die von der Auswerteeinrichtung aktivierbare Abschalteinrichtung ist dies gewährleistet. Ausfälle der Firewall-Einrichtung können somit nicht dazu führen, dass die Filterung des Datenverkehrs aufhört und damit unzulässige Nachrichten zum Datenempfänger gelangen können. Im sicherheitsrelevanten Bereich, beispielsweise einer Bahnanwendung, ist ein expliziter Sicherheitsnachweis zu führen, mit dem für alle Ausfälle unter anderem zu zeigen ist, dass sie zu einem sicheren Zustand führen. Diese Anforderung wird durch die erfindungsgemäße Lösung dieser Ausführungsform gewährleistet. Durch diese Ausführungsform der Erfindung können auch Komponenten der Office-IT-Security, beispielsweise die Firewall-Einrichtung, für eine Netzwerkanbindung zwischen einem sicheren Netz und einem unsicheren Netz eingesetzt werden.

In einer weiteren vorteilhaften Ausgestaltung kann die Anordnung wenigstens eine mit der Auswerteeinrichtung verbundene Überwachungseinrichtung aufweisen, die zur Überwachung einer Betriebsbereitschaft der Auswerteeinrichtung ausgebildet ist. Dies hat den Vorteil, dass ein Ausfall der Auswerteeinrich-

tung nicht unbemerkt bleibt, sondern von der Überwachungseinrichtung erfasst wird und entsprechende Maßnahmen eingeleitet werden können. So kann in einer vorteilhaften Weiterbildung die Überwachungseinrichtung zum Aktivieren der Abschalteinrichtung bei festgestellter nicht bestehender Betriebsbereitschaft ausgestaltet sein. So ist bei einer festgestellten Fehlfunktion das Abschalten des Datenverkehrs zum Datenempfänger gewährleistet, was die Erfüllung der sogenannten „Fail Close"-Anforderung darstellt.

Um eine besonders sichere Ausführungsform der Erfindung herzustellen, kann die Überwachungseinrichtung als eine von der Auswerteeinrichtung separate Einheit ausgestaltet sein. Dabei sind beispielsweise mindestens die Überwachungseinrichtung und die Auswerteeinrichtung auf unabhängigen Hardware-Komponenten realisiert. Ferner kann die Überwachungseinrichtung zum Auslösen eines Neustarts der Auswerteeinrichtung bei festgestellter nichtbestehender Betriebsbereitschaft ausgebildet sein. Dies hat den Vorteil, dass die Sicherheit weiter erhöht wird. Die Überwachungseinrichtung kann beispielsweise als ein sogenannter Watch-Dog-Timer ausgebildet sein, der von den internen Prozessen der Auswerteeinrichtung in regelmäßigen Abständen zurückgesetzt wird. Geschieht dieses Zurücksetzen nicht innerhalb einer vorbestimmten Zeit, einer sogenannten Time-Out-Zeit, wird ein Alarm ausgelöst, der beispielsweise zentral signalisiert wird und die Abschalteinrichtung auslösen und damit den Datenverkehr zum Datenempfänger unterbrechen kann. Danach wird die Auswerteeinrichtung auf sichere Weise neu gestartet (Secure-Boot). Ein Programmcode und eine Konfiguration der Auswerteeinrichtung kann in einem nur lesbar eingerichteten Speicher abgelegt sein, so dass beim Neustart der Ausgangszustand wieder hergestellt und damit eine vorherige Manipulation oder Fehlfunktion der Auswerteeinrichtung rückgängig gemacht wird. Während dieses Neustarts und der Fehlererkennung durch die Überwachungseinrichtung ist der Datenverkehr zum Datenempfänger vorteilhafterweise durch die Abschalteinrichtung unterbrochen. Ein Neustart der Auswerteeinrichtung kann darüber hinaus auch in regelmäßigen Abstän-

den und/oder bei erkannten Anomalien durchgeführt werden, um die Sicherheit der Anordnung weiter zu erhöhen.

Die Auswerteeinrichtung kann zusätzlich am Eingang eine Überwachungsfunktion aufweisen, die sicherstellt, dass auch absichtlich in der Länge oder anderweitig veränderte Pakete im Datenverkehr die Auswerteeinrichtung nicht in ihrer Funktion beeinträchtigen. Dabei wird die Datenpaketlänge von der Auswerteeinrichtung erfasst und bei Überschreitung einer parametrierbaren Maximallänge und/oder auch bei einer Überschreitung einer Minimallänge ein Alarm ausgelöst und der Datenverkehr durch die Abschalteinrichtung unterbrochen. Weiterhin kann das Vorhandensein und die Sinnfälligkeit der Protokollelemente des Datenpakets überprüft werden.

In einer weiteren vorteilhaften Ausgestaltung kann die Anordnung wenigstens einen Testdatengenerator aufweisen, der zum Erzeugen eines einen unerlaubten Datenverkehr aufweisenden Test-Datenverkehrs in Richtung des Datenempfängers ausgebildet ist. Dies hat den Vorteil, dass die Funktion der Auswerteeinrichtung auch bei korrekt arbeitender Firewall-Einrichtung geprüft wird. Der Test-Datenverkehr kann der Auswerteeinrichtung vom Testdatengenerator gemeldet und angezeigt und daher von der Auswerteeinrichtung erwartet werden, so dass kein Alarm oder eine andere Schutzreaktion ausgelöst werden muss. Der Test-Datenverkehr kann beispielsweise in regelmäßigen Abständen in den Datenstrom zum Datenempfänger eingefügt werden und überprüft die korrekte Funktion der Auswerteeinrichtung. Die Erkennung des Test-Datenverkehrs kann einen weiteren Watch-Dog-Timer der Überwachungseinrichtung zurücksetzen, der bei Nichterkennen oder Ausbleiben des erwarteten Test-Datenverkehrs einen Alarm auslöst und/oder die Abschalteinrichtung aktiviert und damit den Datenverkehr zum Datenempfänger unterbricht.

Die Erfindung betrifft weiterhin eine Schutzvorrichtung zum Schutz wenigstens eines zu einem Netzwerk mit hoher Sicherheitsanforderung gehörigen Datenempfängers vor unerlaubtem

Datenverkehr, mit wenigstens einer Firewall-Einrichtung, die anhand vorbestimmter Regeln zum Unterscheiden zwischen einem erlaubten und einem unerlaubten Datenverkehr in Richtung des Datenempfängers sowie zum Blockieren von unerlaubten Datenverkehr und zum Durchlassen von erlaubtem Datenverkehr ausgebildet ist. Um eine hohe Sicherheit zu gewährleisten und Anforderungen eines sicherheitsrelevanten Bereichs zu erfüllen, weist die Schutzvorrichtung wenigstens eine Anordnung nach einer der oben genannten Ausführungsformen auf.

Die Erfindung betrifft außerdem eine Netzwerkverbindung zwischen einem Datensender und einem Datenempfänger, wobei der Datenempfänger zu einem Netzwerk mit hoher Sicherheitsanforderung und der einen Datenverkehr sendende Datensender zu einem Netzwerk niedriger Sicherheitsanforderung gehört. Um die Sicherheit zu erhöhen und Anforderungen eines sicherheitsrelevanten Bereichs zu erfüllen, ist es erfindungsgemäß vorgesehen, dass die Netzwerkverbindung wenigstens eine Schutzvorrichtung nach der oben genannten Ausführungsform aufweist.

In einer vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens kann der Datenverkehr zum Datenempfänger unterbrochen werden, wenn der durchgelassene Datenverkehr unerlaubten Datenverkehr aufweist. Dies hat den Vorteil, dass eine sogenannte Fail-Save-Funktion erfüllt ist, die bei erhöhten Sicherheitsanforderungen gewährleistet sein muss, wie oben bereits beschrieben.

Ferner kann der Datenverkehr zum Datenempfänger unterbrochen werden, wenn das Durchlassen und Überprüfen des durchgelassenen Datenverkehrs nicht innerhalb einer vorbestimmten Zeit erfolgt. Durch diese oben bereits beschriebene Watch-Dog-Timer-Funktion wird die ordnungsgemäße Funktion des erfindungsgemäßen Verfahrens regelmäßig überprüft, wie ebenfalls oben bereits beschrieben.

Um die Sicherheit des erfindungsgemäßen Verfahrens weiter zu erhöhen, kann ein durchgelassener Test-Datenverkehr, der un-

erlaubten Datenverkehr aufweist, erzeugt werden und geprüft werden, ob der unerlaubte Datenverkehr erkannt wird. Ferner kann der Datenverkehr zum Datenempfänger unterbrochen werden, wenn der unerlaubte Datenverkehr des Test-Datenverkehrs innerhalb einer vorbestimmten Zeit nicht erkannt wird oder der Test-Datenverkehr innerhalb einer vorbestimmten Zeit nicht erzeugt wird. Durch diese Watch-Dog-Timer-Funktion werden Manipulationen erkannt und führen zum automatischen Unterbrechen des Datenverkehrs.

Schließlich kann der Datenverkehr mit einer Ende-zu-Ende-Verschlüsselung übertragen werden, um die inhaltliche Integrität der übertragnen Daten und ggf. deren Vertraulichkeit sicher zu stellen. Die Entschlüsselung findet dabei im Datenempfänger statt, der zusätzlich den Inhalt auf Plausibilität prüfen kann. Bei Ende-zu-Ende-verschlüsselten Daten kommt der Vorteil der erfindungsgemäßen Lösung besonders zum Tragen, da solche Nachrichten beispielsweise mit bekannten Security-Gateways nicht genutzt werden können.

Im Folgenden wird die Erfindung mit Bezug auf die beigefügte Zeichnung und die darin dargestellte beispielhafte Ausführungsform beschrieben.

Die Figur zeigt eine schematische Darstellung einer beispielhaften Ausführungsform einer erfindungsgemäßen Netzwerkverbindung.

Eine erfindungsgemäße Netzwerkverbindung 1 verläuft von einem Datensender 2 zu einem Datenempfänger 3. Die Netzwerkverbindung 1 umfasst ein IP-Netzwerk 4 und eine erfindungsgemäße Schutzvorrichtung 5, die vor dem Datenempfänger 3 angeordnet ist und diesen vor unerlaubtem Datenverkehr schützt.

Die Schutzvorrichtung 5 umfasst eine Firewall-Einrichtung 6 und eine erfindungsgemäße Anordnung 7, die zum Überprüfen der Firewall-Einrichtung 6 ausgebildet ist.

Die erfindungsgemäße Anordnung 7 weist einen Test-Datengenerator 8, ein Verteilmittel 9, eine Erfassungseinrichtung 10, eine Abschalteinrichtung 11, eine Auswerteeinrichtung 12 und eine Überwachungseinrichtung 13 auf.

Bei der in der Figur dargestellten beispielhaften Ausführungsform ist der Datenempfänger 3 innerhalb einer Sicherheitszone 14, einer sicherheitskritischen Anlage 15 angeordnet. Die sicherheitskritische Anlage 15 ist beispielsweise eine eisenbahntechnische Anlage oder ein Kraftwerk und die Sicherheitszone 14 ist ein Bereich, in dem eine erhöhte Sicherheit im Datenverkehr gilt. Für einen möglichen Fernzugriff von außen auf diesen Bereich gelten beispielsweise die Anforderungen der Norm IEC 62443-3-3.

Der Datensender 2 befindet sich außerhalb der Sicherheitszone 14 der sicherheitskritischen Anlage 15 in einem Bereich mit einer niedrigeren Sicherheitsanforderung als sie in der Sicherheitszone 14 gilt. Die erfindungsgemäße Netzwerkverbindung 1 zwischen dem Datensender 2 und dem Datenempfänger 3 wird beispielsweise für eine Fernwartung der sicherheitskritischen Anlage 15 verwendet. Das IP-Netzwerk 4, über das die Netzverbindung 1 hergestellt wird, ist beispielsweise das Internet oder ein anderes Datennetzwerk.

Um den Datenempfänger 3 vor einem unerlaubten Datenverkehr zu schützen, ist in dem Datenverkehr in Richtung des Datenempfängers 3 vor dem Datenempfänger 3 die Firewall-Einrichtung 6 angeordnet.

Die Firewall-Einrichtung 6 unterscheidet anhand vorbestimmter Regeln zwischen einem erlaubten und einem unerlaubten Datenverkehr, wobei der unerlaubte Datenverkehr zum Schutz des Datenempfängers von der Firewall-Einrichtung 6 blockiert und somit herausgefiltert wird. Der übrige, erlaubte Datenverkehr wird durchgelassen und kann zum Datenempfänger 3 gelangen. Der Datenverkehr 16 enthält hier bei der beispielhaften Ausführungsform Ende-zu-Ende-verschlüsselte Daten 17 für den Da-

tenempfänger 3. Der erlaubte Datenverkehr umfasst Daten 17, die von einer oder mehreren erlaubten IP-Adressen an genau eine oder mehrere erlaubte IP-Adressen beim Datenempfänger 3 gesendet werden dürfen. Die für die Übertragung erforderlichen Protokollelemente befinden sich unverschlüsselt am Anfang und am Ende der Daten 17, um eine standardkonforme Übertragung über das IP-Netzwerk 4 sicherzustellen, und zusätzlich verschlüsselt im Innern der Daten 17. Die vorbestimmten Regeln, anhand derer die Firewall-Einrichtung 6 zwischen erlaubten und unerlaubten Datenverkehr unterscheidet, sind somit hier zulässige IP-Adressen für den Datensender 2 und den Datenempfänger 3. Die Firewall-Einrichtung 6 lässt bei korrekter Konfiguration also nur erlaubten Datenverkehr in Richtung des Datenempfängers 3 in die Sicherheitszone 14 zu. Allerdings kann die Firewall-Einrichtung 6 beispielsweise durch einen feindseligen Angriff unzulässig verändert worden sein, so dass diese auch unerlaubten Datenverkehr durchlässt. Ein solcher Fehlerfall der Firewall-Einrichtung 6 ist möglich und soll daher erfindungsgemäß verhindert werden.

Erfindungsgemäß ist zwischen der Firewall-Einrichtung 6 und dem Datenempfänger 3 die erfindungsgemäße Anordnung 7 vorgesehen, die die korrekte Funktion der Firewall-Einrichtung 6 überprüft.

Der von der Firewall-Einrichtung 6 durchgelassene Datenverkehr 18 wird innerhalb der Anordnung 7 zunächst von der Erfassungseinrichtung 10 erfasst. Die Erfassungseinrichtung 10 ist beispielsweise als eine Mithöreinrichtung, ein sogenannter Tap, ausgebildet, die den durchgelassenen Datenverkehr 18 rückwirkungsfrei mithört. Der mitgehörte durchgelassene Datenverkehr 18 wird von der mit der Erfassungseinrichtung 10 verbundenen Auswerteeinrichtung 12 überprüft. Bei der Überprüfung durch die Auswerteeinrichtung 12 wird kontrolliert, dass der durchgelassene Datenverkehr 18 keinen unerlaubten Datenverkehr enthält. Falls unerlaubter Datenverkehr, also unerlaubte IP-Absenderadressen oder unerlaubte IP-Zieladressen, Portnummern, etc. erkannt werden, kann nur eine

Fehlfunktion der Firewall-Einrichtung 6 die Ursache sein. In einem solchen Fehlerfall aktiviert die Auswerteeinrichtung 12 die Abschalteinrichtung 11 über ein entsprechendes Abschaltsignal 19.

Die Abschalteinrichtung 11 ist zum Unterbrechen des Datenverkehrs in Richtung des Datenempfängers 3 ausgebildet und arbeitet sinngemäß wie ein Schalter, der den Datenverkehr zum Datenempfänger 3 unterbricht, wenn er aktiviert wird. Durch das Abschaltsignal 19 von der Auswerteeinrichtung 12 ist gewährleistet, dass ein im durchgelassenen Datenverkehr 18 erkannter unerlaubter Datenverkehr nicht den Datenempfänger 3 und die Sicherheitszone 14 erreicht. Die Auswerteeinrichtung 12 ist in der beispielhaften Ausführungsform der Figur so ausgestaltet, dass sie nur lokal konfiguriert wird und keine zusätzliche bidirektionale Netzwerkanbindung besitzt. Dadurch werden die Angriffsmöglichkeiten gegen die Auswerteeinrichtung 12 minimiert und die Sicherheit durch die erfindungsgemäße Anordnung 7 erhöht.

Ferner ist die Überwachungseinrichtung 13 mit der Auswerteeinrichtung 12 verbunden, die auf einer von der Auswerteeinrichtung 12 unabhängigen Hardware ausgebildet ist. Die Überwachungseinrichtung 13 weist einen ersten Watch-Dog-Timer 20 auf, der durch die Auswerteeinrichtung 12, beispielsweise von deren internen Prozessen, in regelmäßigen Zeitabständen zurückgesetzt wird. Ist die Auswerteeinrichtung 12 beispielsweise durch einen feindseligen Angriff funktionsunfähig, wird der Watch-Dog-Timer 20 nicht zurückgesetzt und erreicht eine vorbestimmte sogenannte Time-Out-Zeit. Bei Erreichen dieser Time-Out-Zeit wird von der Auswerteeinrichtung 12 ein Alarm 21 ausgelöst und zusätzlich das Abschaltsignal 19 an die Abschalteinrichtung 11 ausgegeben. Dadurch führt der Fehlerfall der Auswerteeinrichtung 12 zur Unterbrechung des Datenverkehrs in Richtung des Datenempfängers 3 und somit vorteilhafterweise zu einem sicheren Zustand. Der Alarm 21 kann beispielsweise in einer Zentrale (nicht dargestellt) der sicherheitskritischen Anlage 15 ausgelöst werden.

Nach dem Auslösen des Alarms 21 erfolgt bei der Auswerteeinrichtung 12 in der in der Figur beispielhaft dargestellten Ausführungsform automatisch ein Neustart, um die Sicherheit des Systems wieder herzustellen. Die Auswerteeinrichtung 12 weist einen nur lesbar ausgebildeten Speicher 22 auf, der einen Programmcode und eine Konfiguration der Auswerteeinrichtung 12 enthält. Beim Neustart der Auswerteeinrichtung 12 wird dieser Programmcode und die Konfiguration aus dem Speicher 22 ausgelesen, so dass der Ausgangszustand der Auswerteeinrichtung 12 wieder hergestellt und damit eine vorherige Manipulation oder Fehlfunktion der Auswerteeinrichtung 12 rückgängig gemacht wird. Während der erkannten Fehlfunktion und des Neustarts der Auswerteeinrichtung 12 bleibt der Datenverkehr durch die Abschalteinrichtung 11 unterbrochen und wird erst nach Rücknahme des Abschaltsignals 23 durch den Watch-Dog-Timer 20 wieder freigegeben. Zusätzlich wird bei der beispielhaften Ausführungsform in der Figur der Neustart der Auswerteeinrichtung 12 in regelmäßigen Abständen und bei erkannten Anomalien automatisch durchgeführt.

Ferner kann über eine Überwachungsfunktion am Eingang der Auswerteeinrichtung 12 sichergestellt werden, dass auch absichtlich in der Länge oder anderweitig veränderte Daten 17 im durchgelassenen Datenverkehr 18 die Auswerteeinrichtung 12 nicht in ihrer Funktion beeinträchtigen. Dabei wird die Datenpaketlänge von der Auswerteeinrichtung 12 erfasst und bei Überschreitung einer parametrierbaren Maximallänge und/oder auch bei einer Überschreitung einer Minimallänge ein Alarm ausgelöst und der Datenverkehr durch die Abschalteinrichtung 11 unterbrochen. Weiterhin kann das Vorhandensein und die Sinnfälligkeit der Protokollelemente des Datenpakets überprüft werden.

Um die ordnungsgemäße Funktion der erfindungsgemäßen Anordnung 7 regelmäßig zu prüfen, ist der Testdatengenerator 8 erfindungsgemäß vorgesehen. Der Testdatengenerator 8 erzeugt in regelmäßigen Zeitabständen ein oder mehrere definierte Test-

daten in einem Test-Datenverkehr 24. Der Test-Datenverkehr 24 wird mittels des Verteilmittels 9, das beispielsweise ein Switch ist, in den durchgelassenen Datenverkehr 18 in Richtung des Datenempfängers 3 eingespeist. Der Test-Datenverkehr 24 enthält unerlaubten Datenverkehr, der die Erfassungseinrichtung 10 erreicht. Dadurch kann die ordnungsgemäße Funktion der Erfassungseinrichtung 10 und der Auswerteeinrichtung 12 geprüft werden.

Der Testdatengenerator 8 ist direkt mit der Auswerteeinrichtung 12 verbunden und gibt ein Testdatensignal 25 aus, wenn der Test-Datenverkehr 24 in den durchgelassenen Datenverkehr 18 eingespeist wurde. Dadurch erwartet die Auswerteeinrichtung 12 den testweise eingespeisten unerlaubten Datenverkehr im durchgelassenen Datenverkehr 18 und löst daher keinen Alarm 21 aus und aktiviert die Abschalteinrichtung 11 nicht.

Der Test-Datenverkehr 24 wird beispielsweise in regelmäßigen Abständen von dem Testdatengenerator 8 erzeugt, um die korrekte Funktion der Auswerteeinrichtung 12 zu prüfen. Das Erkennen des Test-Datenverkehrs 24 durch die Auswerteeinrichtung 12 setzt einen weiteren Watch-Dog-Timer 26 der Überwachungseinrichtung 13 zurück. Wird der Test-Datenverkehr 24 von der Auswerteeinrichtung 12 nicht innerhalb einer festgelegten Time-Out-Zeit des Watch-Dog-Timers 26 erkannt, wird der Alarm 21 ausgelöst und zusätzlich oder alternativ ein Abschaltsignal 27 an die Abschalteinrichtung 11 übermittelt, durch das der Datenverkehr zum Datenempfänger 3 unterbrochen wird.

Die erfindungsgemäße Auswerteeinrichtung 12 kann sich weitgehend einem Angriff von außen entziehen, weil sie lediglich über die Erfassungseinrichtung 10 am Datenverkehr angeschlossen ist und dies auch nur durch einen unidirektionalen, lesenden Abgriff. Selbst wenn die Auswerteeinrichtung 12 durch einen geeigneten Datenverkehr deaktiviert wird, würde die Überwachungseinrichtung 13 über die Watch-Dog-Timer 20 und 26 die Abschalteinrichtung 11 auslösen. Wenn durch einen Angriff

die Auswerteeinrichtung 12 deaktiviert werden würde, wird dies bereits beim nächsten Test-Datenverkehr 24 auffällig, was ebenfalls die Aktivierung der Abschalteinrichtung 11 bewirkt. Durch die erfindungsgemäße Anordnung 7 wird eine schadhafte Konfigurationsänderung der Firewall-Einrichtung 6 erkannt, weil ein durchgelassener unerlaubter Datenverkehr erkannt und durch die Abschalteinrichtung 11 blockiert wird. Vorteilhafterweise können über die erfindungsgemäße Netzwerkverbindung 1 auch Ende-zu-Ende-verschlüsselte Daten 17 übertragen werden.

Patentansprüche

1. Anordnung (7) zum Überprüfen von wenigstens einer Firewall-Einrichtung (6), die anhand vorbestimmter Regeln zum Unterscheiden zwischen einem erlaubten und einem unerlaubten Datenverkehr in Richtung eines Datenempfängers (3) sowie zum Blockieren von unerlaubtem Datenverkehr und zum Durchlassen von erlaubtem Datenverkehr ausgebildet ist,
d a d u r c h g e k e n n z e i c h n e t , dass
die Anordnung (7) wenigstens eine Erfassungseinrichtung (10), die zum Erfassen des von der Firewall-Einrichtung (6) durchgelassenen Datenverkehrs (18) ausgebildet ist, und wenigstens eine Auswerteeinrichtung (12), die zum Überprüfen des von der Erfassungseinrichtung (10) erfassten Datenverkehrs anhand der vorbestimmten Regeln ausgebildet ist, aufweist.

2. Anordnung (7) nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t , dass
die Anordnung (7) wenigstens eine Abschalteinrichtung (11) aufweist, die zum Unterbrechen des Datenverkehrs in Richtung des Datenempfängers (3) ausgebildet und wenigstens von der Auswerteeinrichtung (12) aktivierbar ist.

3. Anordnung (7) nach Anspruch 1 oder 2,
d a d u r c h g e k e n n z e i c h n e t , dass
die Anordnung (7) wenigstens eine mit der Auswerteeinrichtung (12) verbundene Überwachungseinrichtung (13) aufweist, die zur Überwachung einer Betriebsbereitschaft der Auswerteeinrichtung (12) ausgebildet ist.

4. Anordnung (7) nach Anspruch 2 und 3,
d a d u r c h g e k e n n z e i c h n e t , dass
die Überwachungseinrichtung (13) zum Aktivieren der Abschalteinrichtung (11) bei festgestellter nicht bestehender Betriebsbereitschaft ausgestaltet ist.

5. Anordnung (7) nach Anspruch 3 oder 4,

d a d u r c h g e k e n n z e i c h n e t , dass die Überwachungseinrichtung (13) als eine von der Auswerteeinrichtung (12) separate Einheit ausgestaltet ist.

6. Anordnung (7) nach Anspruch 3, 4 oder 5, d a d u r c h g e k e n n z e i c h n e t , dass die Überwachungseinrichtung (13) zum Auslösen eines Neustarts der Auswerteeinrichtung (12) bei festgestellter nicht bestehender Betriebsbereitschaft ausgebildet ist.

7. Anordnung (7) nach einem der oben genannten Ansprüche, d a d u r c h g e k e n n z e i c h n e t , dass die Anordnung (7) wenigstens einen Testdatengenerator (8) aufweist, der zum Erzeugen eines einen unerlaubten Datenverkehr aufweisenden Test-Datenverkehrs (24) in Richtung des Datenempfängers (3) ausgebildet ist.

8. Schutzvorrichtung (5) zum Schutz wenigstens eines zu einem Netzwerk mit hoher Sicherheitsanforderung gehörigen Datenempfängers (3) vor unerlaubtem Datenverkehr, mit wenigstens einer Firewall-Einrichtung (6), die anhand vorbestimmter Regeln zum Unterscheiden zwischen einem erlaubten und einem unerlaubten Datenverkehr in Richtung des Datenempfängers (3) sowie zum Blockieren von unerlaubtem Datenverkehr und zum Durchlassen von erlaubtem Datenverkehr ausgebildet ist, d a d u r c h g e k e n n z e i c h n e t , dass die Schutzvorrichtung (5) wenigstens eine Anordnung (7) nach einem der oben genannten Ansprüche aufweist.

9. Netzwerkverbindung (1) zwischen einem Datensender (2) und einem Datenempfänger (3), wobei der Datenempfänger (3) zu einem Netzwerk mit hoher Sicherheitsanforderung und der einen Datenverkehr sendende Datensender (2) zu einem Netzwerk mit niedrigerer Sicherheitsanforderung gehört, d a d u r c h g e k e n n z e i c h n e t , dass die Netzwerkverbindung (1) wenigstens eine Schutzvorrichtung (5) nach Anspruch 8 aufweist.

10. Verfahren zum Überprüfen von wenigstens einer Firewall-Einrichtung (6),
bei dem in einem Datenverkehr in Richtung eines Datenempfängers (3) anhand vorbestimmter Regeln zwischen einem erlaubten und einem unerlaubten Datenverkehr unterschieden wird sowie unerlaubter Datenverkehr blockiert und erlaubter Datenverkehr durchgelassen wird,
d a d u r c h g e k e n n z e i c h n e t , dass
der durchgelassene Datenverkehr erfasst wird und auf vorhandenen unerlaubten Datenverkehr überprüft wird.

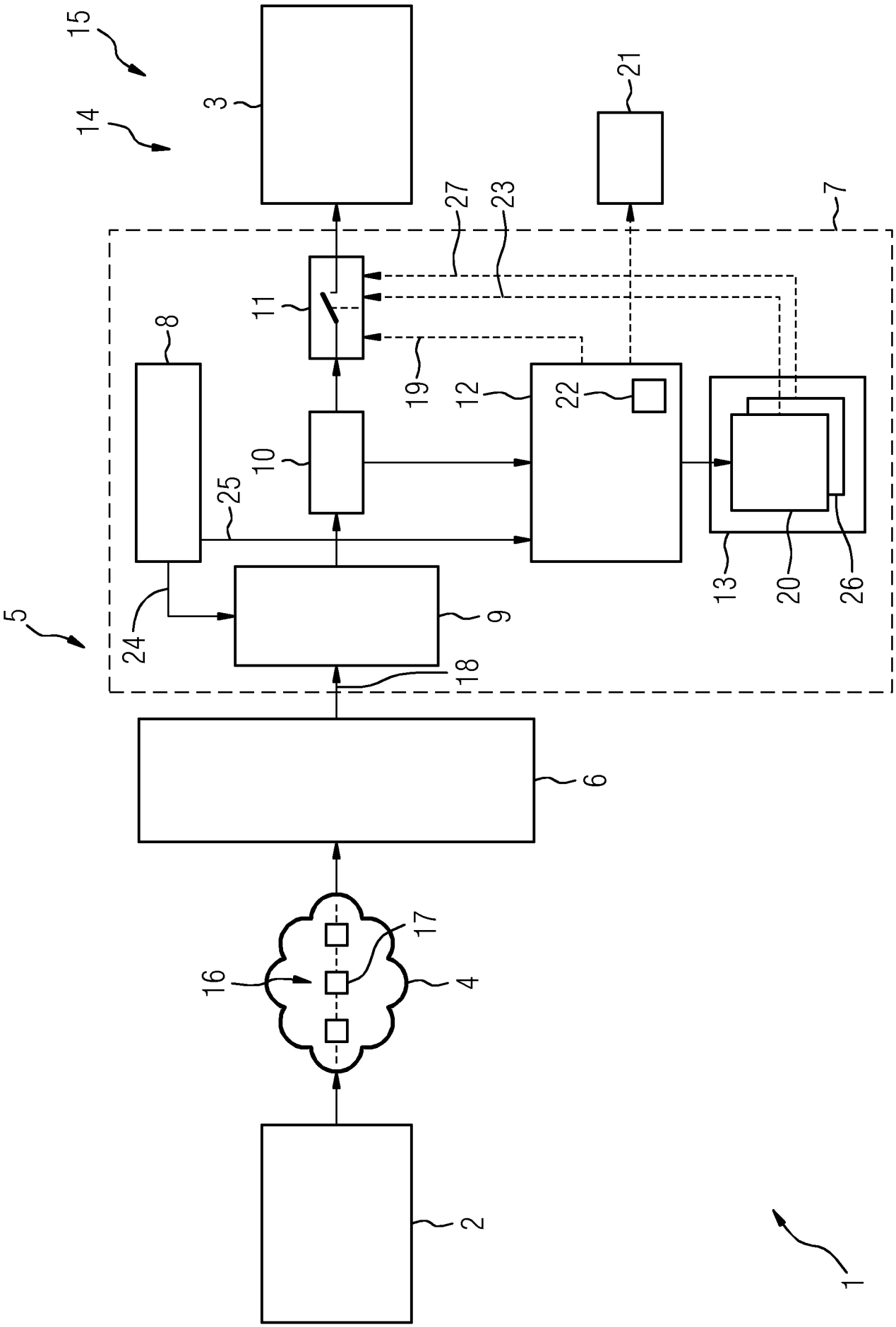
11. Verfahren nach Anspruch 10,
d a d u r c h g e k e n n z e i c h n e t , dass
der Datenverkehr zum Datenempfänger (3) unterbrochen wird, wenn der durchgelassene Datenverkehr unerlaubten Datenverkehr aufweist.

12. Verfahren nach Anspruch 10 oder 11,
d a d u r c h g e k e n n z e i c h n e t , dass
der Datenverkehr zum Datenempfänger (3) unterbrochen wird, wenn das Durchlassen und Überprüfen des durchgelassenen Datenverkehrs nicht innerhalb einer vorbestimmten Zeit erfolgt.

13. Verfahren nach einem der Ansprüche 10 bis 12,
d a d u r c h g e k e n n z e i c h n e t , dass
ein durchgelassener Test-Datenverkehr (24), der unerlaubten Datenverkehr aufweist, erzeugt wird und geprüft wird, ob der unerlaubte Datenverkehr erkannt wird.

14. Verfahren nach Anspruch 13,
d a d u r c h g e k e n n z e i c h n e t , dass
der Datenverkehr zum Datenempfänger (3) unterbrochen wird, wenn der unerlaubte Datenverkehr des Test-Datenverkehrs (24) innerhalb einer vorbestimmten Zeit nicht erkannt wird oder der Test-Datenverkehr innerhalb einer vorbestimmten Zeit nicht erzeugt wird.

15. Verfahren nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, dass der Datenverkehr mit einer Ende-zu-Ende-Verschlüsselung übertragen wird.


15
14
3
21
27
23
7
11
8
19
12
22
10
25
13
20
26
5
24
9
18
6
16
17
4
2
1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/055805

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. H04L29/14

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	DE 10 2013 214522 A1 (SIEMENS AG [DE]) 29 January 2015 (2015-01-29) paragraph [0001] paragraph [0025] paragraph [0031] paragraph [0057] - paragraph [0058] paragraph [0066]; figure 1 paragraph [0073] -----	1-15
X	DE 10 2013 216847 A1 (SIEMENS AG [DE]) 26 February 2015 (2015-02-26) paragraph [0025] paragraph [0042] paragraph [0059] -----	1-15

-/--

[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
21 April 2017	02/05/2017

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	Tenbieg, Christoph

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	EP 2 154 827 A1 (ALCATEL LUCENT [FR]) 17 February 2010 (2010-02-17) paragraph [0003] - paragraph [0004] paragraph [0016] paragraph [0021] - paragraph [0026] -----	1-15
A	US 2005/076235 A1 (ORMAZABAL GASTON S [US] ET AL) 7 April 2005 (2005-04-07) paragraph [0117] - paragraph [0128] -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/055805

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102013214522 A1	29-01-2015	DE 102013214522 A1	29-01-2015
		EP 2987301 A1	24-02-2016
		WO 2015010824 A1	29-01-2015
DE 102013216847 A1	26-02-2015	CN 105493469 A	13-04-2016
		DE 102013216847 A1	26-02-2015
		EP 3001884 A1	06-04-2016
		US 2016205069 A1	14-07-2016
		WO 2015024722 A1	26-02-2015
EP 2154827 A1	17-02-2010	NONE	
US 2005076235 A1	07-04-2005	US 2005076235 A1	07-04-2005
		US 2009083845 A1	26-03-2009

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/055805

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06
ADD. H04L29/14

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	DE 10 2013 214522 A1 (SIEMENS AG [DE]) 29. Januar 2015 (2015-01-29) Absatz [0001] Absatz [0025] Absatz [0031] Absatz [0057] - Absatz [0058] Absatz [0066]; Abbildung 1 Absatz [0073] -----	1-15
X	DE 10 2013 216847 A1 (SIEMENS AG [DE]) 26. Februar 2015 (2015-02-26) Absatz [0025] Absatz [0042] Absatz [0059] -----	1-15

-/--

[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
21. April 2017	02/05/2017

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	Tenbieg, Christoph

1

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/055805

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 2 154 827 A1 (ALCATEL LUCENT [FR]) 17. Februar 2010 (2010-02-17) Absatz [0003] - Absatz [0004] Absatz [0016] Absatz [0021] - Absatz [0026]	1-15
A	US 2005/076235 A1 (ORMAZABAL GASTON S [US] ET AL) 7. April 2005 (2005-04-07) Absatz [0117] - Absatz [0128]	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/055805

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102013214522 A1	29-01-2015	DE 102013214522 A1	29-01-2015
		EP 2987301 A1	24-02-2016
		WO 2015010824 A1	29-01-2015
DE 102013216847 A1	26-02-2015	CN 105493469 A	13-04-2016
		DE 102013216847 A1	26-02-2015
		EP 3001884 A1	06-04-2016
		US 2016205069 A1	14-07-2016
		WO 2015024722 A1	26-02-2015
EP 2154827 A1	17-02-2010	KEINE	
US 2005076235 A1	07-04-2005	US 2005076235 A1	07-04-2005
		US 2009083845 A1	26-03-2009