(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
29. Dezember 2016 (29.12.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/206820 A1

(51) Internationale Patentklassifikation:
G08C 17/00 (2006.01) *H04L 29/08* (2006.01)
G07C 5/00 (2006.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2016/050651

(22) Internationales Anmeldedatum:
14. Januar 2016 (14.01.2016)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2015 211 668.9 24. Juni 2015 (24.06.2015) DE

(71) Anmelder: **VOLKSWAGEN AKTIENGESELLSCHAFT** [DE/DE]; Berliner Ring 2, 38440 Wolfsburg (DE).

(72) Erfinder: **MROWCZYNSKI, Mirko**; Am Walde 6, 38528 Adenbüttel (DE). **BECKER, Christian**; Madamenweg 30, 38118 Braunschweig (DE). **REMELE, Juri**; Heinrich-Zille-Ring 32, 38471 Rühen (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD AND APPARATUS FOR INCREASING SAFETY FOR REMOTE TRIGGERING, AND MOTOR VEHICLE

(54) **Bezeichnung** : VERFAHREN UND VORRICHTUNG ZUR ERHÖHUNG DER SICHERHEIT BEI EINER FERNAUSLÖSUNG, KRAFTFAHRZEUG

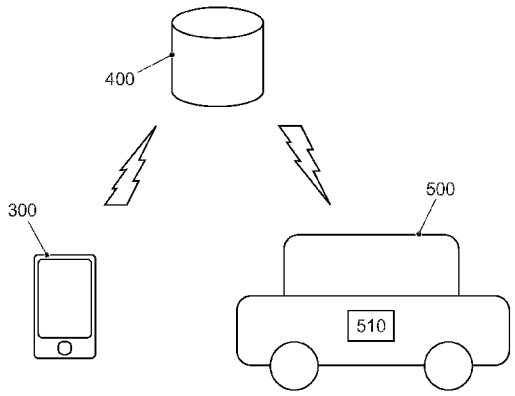


FIG. 6

(57) **Abstract**: The invention relates to a method and an apparatus (510) for a motor vehicle (500) in order to increase safety for remote triggering, and to a motor vehicle (500) having such an apparatus (510). In this case, the data are received from a second device (300), from which there is a communication link to a first device (510). The data are associated with user inputs in an application on the second device (300). The method is characterised in that the first device (510) receives, for each user input, a portion of the data in a data packet of a data packet structure, the first device (510) preventing remote triggering if the data packet structure does not correspond to a predetermined data packet structure. A difference in the reception sequence of the data packets from the predetermined order is an indicator of malfunctioning in the second device. Preventing remote triggering in the event of a difference therefore reduces the risk of remote triggering by a faulty second device and hence faulty remote triggering.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2016/206820 A1

Veröffentlicht:

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

Die Erfindung betrifft ein Verfahren und eine Vorrichtung (510) für ein Kraftfahrzeug (500) zur Erhöhung der Sicherheit bei einer Fernauslösung sowie ein Kraftfahrzeug (500) mit einer solchen Vorrichtung (510). Dabei werden die Daten von einem zweiten Gerät (300), von dem eine Kommunikationsverbindung zu einem ersten Gerät (510) besteht, empfangen. Die Daten sind Nutzereingaben in einer Anwendung auf dem zweiten Gerät (300) zugeordnet. Das Verfahren ist dadurch gekennzeichnet, dass das erste Gerät (510) zu jeder Nutzereingabe einen Teil der Daten in einem Datenpaket einer Datenpaketstruktur empfängt, wobei das erste Gerät (510) die Fernauslösung verhindert, wenn die Datenpaketstruktur nicht in einer vorbestimmten Datenpaketstruktur entspricht. Eine Abweichung in der Empfangsfolge der Datenpakete von der vorbestimmten Reihenfolge ist ein Indikator für eine Fehlfunktionalität des zweiten Gerätes. Das Verhindern der Fernauslösung bei einer Abweichung verringert damit die Gefahr einer Fernauslösung durch ein fehlerhaftes zweites Gerät und damit eine fehlerhafte Fernauslösung.

Beschreibung

Verfahren und Vorrichtung zur Erhöhung der Sicherheit bei einer Fernauslösung, Kraftfahrzeug

Die Erfindung betrifft ein Verfahren und eine Vorrichtung für ein Kraftfahrzeug zur Erhöhung der Sicherheit bei einer Fernauslösung sowie ein Kraftfahrzeug mit einer solchen Vorrichtung.

Die Fernauslösung sicherheitsrelevanter Funktionen, beispielsweise die Fernauslösung eines Parkassistenten oder einer Fahrzeugklimatisierung eines Kraftfahrzeugs unter Verwendung eines Fahrzeugschlüssels oder die Fernauslösung eines Haustechnikgeräts einer Haustechnikanlage unter Verwendung einer Applikationssoftware eines Nutzergeräts gewinnt zunehmend an Bedeutung.

Grundsätzlich erfolgt dabei eine Fernauslösung in Folge von Empfang von Daten, die Nutzereingaben in einer Anwendung auf dem zweiten Gerät zugeordnet sind.

Zur Gewährleistung der Sicherheit bei Fernauslösungen sind verschiedene Mechanismen bekannt. Beispielsweise beschreibt DE 10 2012 024 101 A1 ein Verfahren für ein Fahrzeug, welches eine Benutzeridentifikation umfasst. In DE 10 2013 010 152 A1 ist beschrieben, dass zum Start einer Datenübertragung eine Identifikation über abgespeicherte Applikationssoftware erfolgt, wobei dabei ein Geräterkennungsstandard verwendet werden kann.

Der Erfindung liegt nun die Aufgabe zugrunde, die Sicherheit bei einer Fernauslösung zu erhöhen.

Erfindungsgemäß wird dafür ein Verfahren nach Anspruch 1, ein weiteres Verfahren nach Anspruch 5, eine Vorrichtung nach Anspruch 13, ein Fahrzeug nach Anspruch 14 und eine Speichervorrichtung nach Anspruch 15 vorgeschlagen.

Das Verfahren dient zur Erhöhung der Sicherheit bei einer Fernauslösung einer sicherheitsrelevanten Funktion eines ersten Gerätes in Folge von Empfang von Daten. Dabei werden die Daten von einem zweiten Gerät, von dem eine Kommunikationsverbindung zu dem ersten Gerät besteht, empfangen. Die Daten sind Nutzereingaben in einer Anwendung auf dem zweiten Gerät zugeordnet. Das Verfahren ist dadurch gekennzeichnet, dass das erste Gerät zu jeder Nutzeingabe einen Teil der Daten in einem Datenpaket einer Datenpaketstruktur

empfängt, wobei das erste Gerät die Fernauslösung verhindert, wenn die Datenpaketstruktur nicht einer vorbestimmten Datenpaketstruktur entspricht.

Das weitere Verfahren dient zur Fernauslösung einer sicherheitsrelevanten Funktion eines ersten Gerätes in Folge von Empfang von Daten zu Nutzereingaben in einer Anwendung auf einem zweiten Gerät, von dem eine Kommunikationsverbindung zu dem ersten Gerät besteht. Das weitere Verfahren ist dadurch gekennzeichnet, dass das zweite Gerät zu jeder Nutzereingabe einen Teil der Daten in einem Datenpaket einer vorbestimmten Datenpaketstruktur an das erste Gerät sendet.

Eine Abweichung in der Empfangsfolge der Datenpakete von der vorbestimmten Reihenfolge ist ein Indikator für eine Fehlfunktionalität des zweiten Gerätes. Das Verhindern der Fernauslösung bei einer Abweichung verringert damit die Gefahr einer Fernauslösung durch ein fehlerhaftes zweites Gerät und damit eine fehlerhafte Fernauslösung.

In bevorzugter Ausgestaltung des Verfahrens ist vorgesehen, dass das erste Gerät die Fernauslösung auch verhindert, wenn die Datenpakete nicht in einer vorbestimmten Zeitdauer empfangen wurden und/oder wenn eine Wartezeitdauer zwischen aufeinanderfolgend empfangenen Datenpaketen eine Höchstwartezeitdauer überschreitet. Entsprechend ist in einer bevorzugten Ausführungsform des weiteren Verfahrens vorgesehen, dass das zweite Gerät die Datenpakete innerhalb einer vorbestimmten Zeitdauer versendet und/oder das zweite Gerät beim Versenden der Datenpakete eine Höchstwartezeitdauer zwischen aufeinanderfolgend versandeten Datenpaketen nicht überschreitet.

Die zeitliche Begrenzung wird bei Fehlfunktionalität des zweiten Gerätes wahrscheinlicher überschritten, so dass die Überwachung von Zeitdauern und Verhinderung von Fernauslösungen nach Ablauf der Zeitdauern die Sicherheit weiter erhöht.

Das zweite Gerät kann zu jedem der Datenpakete eine Prüfsumme bilden und dem jeweiligen Datenpaket hinzufügen. Die Datenpakete können also eine Prüfsumme umfassen und das erste Gerät kann konfiguriert sein, die Fernauslösung auch zu verhindern, wenn bei einem der Datenpakete die Prüfsumme nicht zu restlichen Daten in dem Datenpaket passt.

Prüfsummen sind effiziente Hilfsmittel zur Validierung einzelner Datenpakete. Die Fernauslösung wird weiter in der Sicherheit verbessert, wenn nur eine in richtiger Reihenfolge empfangene Folge von validierten Datenpaketen die Fernauslösung bewirken kann.

Zusätzlich oder alternativ können die Datenpakete vom zweiten Gerät verschlüsselt sein und das erste Gerät kann konfiguriert sein, die Fernauslösung auch zu verhindern, wenn eines der Datenpakete nicht mit entschlüsselt werden kann.

Dabei können die Datenpakete mit unterschiedlichen Schlüsseln verschlüsselt werden, die Positionen in der vorbestimmten Reihenfolge zugeordnet sind.

Es ist möglich, dass das zweite Gerät die unterschiedlichen Schlüssel von dem ersten Gerät erhält.

Die Nutzeingaben können eine Eingabe zum Starten der Anwendung, eine Eingabe einer persönlichen Identifikationsnummer, eine Eingabe eines Captcha-Codes, eine Eingabe zur Auswahl der Fernauslösung und/oder eine Eingabe zur Aktivierung der Fernauslösung umfassen Eines der Datenpakete kann die eingegebene persönliche Identifikationsnummer und ein nachfolgendes Datenpaket kann den eingegebenen Captcha-Code umfassen.

Das erste Gerät kann die Fernauslösung verhindern, wenn die Datenpakete nicht in einer vorbestimmten Reihenfolge empfangen wurden.

Die verschiedenen in dieser Anmeldung genannten Ausführungsformen der Erfindung sind, sofern im Einzelfall nicht anders ausgeführt, mit Vorteil miteinander kombinierbar.

Die Erfindung wird nachfolgend in Ausführungsbeispielen anhand der zugehörigen Zeichnungen erläutert. Es zeigen:

Figur 1 ein Flussdiagramm gemäß einem Ausführungsbeispiel eines Verfahrens,

Figur 2 eine Datenpaketstruktur gemäß einem ersten Ausführungsbeispiel der Erfindung,

Figur 3 eine andere mögliche Zusammensetzung der Datenpakete,

Figur 4 noch eine andere mögliche Zusammensetzung der Datenpakete,

Figur 5 eine Datenpaketstruktur gemäß einem zweiten Ausführungsbeispiel der Erfindung, und

Figur 6 ein System gemäß einem Ausführungsbeispiel der Erfindung.

Die vorliegende Erfindung beruht auf der Idee, dass durch eine Instanz in einem System, beispielsweise einem Fahrzeug, Daten von außerhalb des Systems so plausibilisiert werden können, dass die Daten eine Fernauslösung einer sicherheitsrelevanten Funktion bewirken können, ohne die Sicherheit des Systems zu kompromittieren. Die vorliegende Erfindung ist insbesondere für sicherheitsrelevante Elektrik nach ISO26262 geeignet. Sie macht die Anwendung dieser Norm für Komponenten außerhalb des Fahrzeugs möglich.

Die Erfindung verhindert, dass Einzelfehler außerhalb des Systems zur Auslösung führen, da die Einzelfehler die Datenpaketstruktur verändern. Sich bezüglich der Datenpaketstruktur gegenseitig aufhebende Mehrfachfehler sind hingegen deutlich unwahrscheinlicher.

Die Erfindung basiert darauf, dass eine Inbetriebnahme, beispielsweise ein Pairing zwischen einem ersten Gerät, welches die sicherheitsrelevante Funktion zur Verfügung stellt, etwa eine Fahrzeugvorklimatisierung, und einem zweiten Gerät, von welchem aus ein Nutzer die Funktion auslösen möchte, beispielsweise ein Nutzergerät, grundsätzlich abgeschlossen ist.

Die Erfindung teilt einen Programmablauf zur Fernauslösung in eine vorbestimmte Reihenfolge von Nutzereingabeschritten, zwischen denen jeweils automatisch ausgeführte Schritte liegen. Dies ermöglicht Einzelfehler, beispielsweise durch fehlerhaft detektierte Nutzereingabe oder fehlerhafte Sprünge im Programmablauf, und somit mögliche Risiken bei der Fernauslösung einer sicherheitsrelevanten Funktion zu erkennen. Eine Instanz im Fahrzeug kann also Daten von außerhalb plausibilisieren.

In einem in Figur 1 gezeigten Ausführungsbeispiel der Erfindung werden folgende Schritte ausgeführt, die jeweils eine Nutzerinteraktion erfordern:

In einem Schritt S10 schaltet ein Nutzer ein Nutzergerät (zum Beispiel ein Mobiltelefon) ein entsperrt das Display und startet eine Anwendung (Applikationssoftware, App) auf dem Nutzergerät, die eine Fernauslösungsmöglichkeit von Funktionen eines anderen Geräts (zum Beispiel eines Steuergerätes eines Fahrzeugs) zur Verfügung stellt.

Danach gibt der Nutzer in Schritt S20 ein persönliche Identifikationsnummer (PIN) ein. Anschließend wählt der Nutzer eine Funktion zur Fernauslösung aus. Dies erfolgt in Schritt S30, auf den Schritt S40 folgt, in welchem der Nutzer die Fernauslösung der Funktion aktiviert. Diese Aktivierung muss nachfolgend in Schritt S50 durch Abtippen eines Captcha-Codes (Completely Automated Public Turing test to tell Computers and Humans Apart, beispielsweise Text, der durch Bildfilter verzerrt wurde) bestätigt werden.

Erst nach dieser Folge von Schritten kann tatsächlich eine Fernauslösung erfolgen. Im Ausführungsbeispiel schickt das Nutzergerät automatisch in oder nach zumindest den Schritten S20, S30, S40 und S50 ein Datenpaket an das Steuergerät, so dass eine Empfangsreihenfolge von Datenpaketen entsteht. Die Übertragung kann beispielsweise nach einem Mobilfunkstandard über ein drahtloses lokales Netzwerk (WLAN) oder über Bluetooth erfolgen. In einer beispielhaften Ausführungsform erfolgt die Kommunikation ausschließlich über Mobilfunk (zum Beispiel nach Global System for Mobile Communications- (GSM), Universal Mobile Telecommunications System (UMTS) oder Long Term Evolution (LTE)-Standard). Insbesondere kann während der Fernauslösung jede andere drahtlose Kommunikation unterdrückt werden.

In einem anderen Ausführungsbeispiel schickt das Nutzergerät alle Datenpakete zusammen als einen Block mit Kommunikationsabsicherung an ein Steuergerät des Fahrzeugs, wobei durch eine Reihenfolge der Datenpakete im Block eine Empfangsreihenfolge der Datenpakete bestimmt ist.

Das Steuergerät prüft in Schritt S25, ob die eingegebene PIN einer hinterlegten PIN entspricht, und in Schritt S55, ob der eingegebene Captcha-Code einem hinterlegten Captcha-Code entspricht. Ist eine dieser Prüfungen erfolglos, verhindert das Steuergerät in Schritt S60 die Fernauslösung. Zusätzlich kann eine Diskrepanz zwischen eingegebener PIN und hinterlegter PIN optional bewirken, dass das Steuergerät das Nutzergerät so ansteuert, dass die Anwendung beendet wird. Wünscht der Nutzer dann weiterhin eine Fernauslösung, so muss er das Verfahren erneut durchführen.

Das Ausführungsbeispiel umfasst einen weiteren Schritt S60, in dem das Steuergerät prüft, ob diese Empfangsreihenfolge einer vorbestimmten Reihenfolge entspricht. Ist dies nicht der Fall, verhindert ein Sicherheitsmechanismus des Steuergeräts die Fernauslösung.

Die Übereinstimmung von Empfangsreihenfolge und vorbestimmter Reihenfolge ist ein guter Hinweis darauf, dass das Nutzergerät fehlerfrei arbeitet. Umgekehrt ist fehlende Übereinstimmung ein Hinweis auf eine Fehlfunktion, die sicherheitskompromittierend sein könnte.

Es ist weiterbildend möglich, dass die PIN auf mehrere Datenpakete verteilt übertragen wird.

Zusätzlich oder alternativ ist es möglich, die Datenpakete mit Zeitstempeln zu versehen. Das Steuergerät führt dann optional einen Schritt S65 aus, in dem geprüft wird, ob keine der Zeitdauern zwischen aufeinanderfolgend empfangenen Datenpaketen eine Wartezeitdauer und/oder eine Gesamtzeitdauer zwischen einem ersten und einem letzten empfangenen Datenpaket eine maximale vorbestimmte Zeitdauer überschreitet. Ergibt diese Prüfung eine Überschreitung, so kann der Sicherheitsmechanismus des Steuergeräts die Fernauslösung verhindern.

Zusätzlich oder alternativ ist es möglich, die Datenpakete mit Prüfsummen zu versehen, um die Integrität der Datenpakete überprüfbar zu machen.

Zusätzlich oder alternativ ist es möglich, die Datenpakete mit einem oder verschiedenen öffentlichen Schlüsseln des Steuergeräts so zu verschlüsseln, dass nur das Steuergerät die Datenpakete entschlüsseln kann. Dabei kann jeder Position in der vorbestimmten Reihenfolge ein eigener Schlüssel zugeordnet sein. Die Abweichung von der vorbestimmten Reihenfolge lässt sich dann direkt aus Unentschlüsselbarkeit mit einem der Empfangsposition zugeordneten Schlüssel ableiten.

Es ist möglich, die Erfindung so weiterzubilden, dass der korrekte Empfang eines jeden Datenpakets dem Nutzergerät vom Steuergerät bestätigt wird und das Nutzergerät das gemäß der vorbestimmten Reihenfolge nächste Datenpaket nur sendet, wenn das jeweilig direkt vorhergehende Datenpaket korrekt empfangen wurde, sonst jedoch das jeweilig direkt vorhergehende Datenpaket erneut sendet. Wird dabei Verschlüsselung eingesetzt, kann dabei entweder derselbe Schlüssel zur Verschlüsselung des vorhergehenden Datenpakets verwendet werden, der bereits bei dem vorherigen Sendeversuch verwendet wurde. Oder es wird ein nächster Schlüssel aus einer Folge von Schlüsseln verwendet.

Der Captcha-Code und/oder die Schlüssel können in vorteilhaften Weiterbildungen vom Fahrzeug, beispielsweise in einem Datensatz, zur Verfügung gestellt werden, beispielsweise in Antwort auf eine in Schritt S10 gesandte entsprechende Anfrage durch das Nutzergerät.

Der Datensatz kann chiffriert übertragen werden. Die Anwendung kann wiederum ausgebildet sein, den Datensatz nach und nach in den jeweiligen Schritten zu dechiffrieren. Der Datensatz kann zeitlich befristet sein. Dann oder auch sonst ist es möglich, dass das Fahrzeug mehrere Datensätze zur Verfügung stellt. Dies verbessert die sicherheitsüberprüfte Fernauslösung bei schlechter Funkverbindung.

Im Fahrzeug können die Datensätze nicht flüchtig in einem Speicher abgelegt sein. Der Captcha-Code kann dabei maschineninterpretierbar, also beispielsweise als der im verzerrten Bild dargestellte Text, abgelegt sein.

Zusätzlich oder alternativ ist es möglich, dass sich Nutzergerät und/oder Fahrzeug gegenüber dem jeweils anderen Gerät authentifizieren, um beispielsweise Fernauslösung in einem falschen Fahrzeug zu verhindern. Beispielsweise verschlüsselt das Nutzergerät die Datenpakete mit einem privaten Schlüssel, so dass die Datenpakete signiert sind.

Dann kann aus Diskrepanz zwischen Empfangsreihenfolge und vorbestimmter Reihenfolge im Steuergerät darauf geschlossen werden, dass das Nutzergerät ein technisches Problem hat. Gegebenenfalls kann dann die Fernauslösung durch dieses Nutzergerät dauerhaft verhindert werden.

In einer vorteilhaften Weiterbildung überprüft das Nutzergerät die PIN auch selbst. Dies kann beispielsweise durch Auswertung einer Hashfunktion erfolgen, ergibt diese zur eingegebenen PIN einen Hashwert, der einem hinterlegten Hashwert entspricht, ist die eingegebene PIN richtig. Die PIN muss dann nicht im Nutzergerät selbst nichtflüchtig hinterlegt sein, so dass auch keine anderen Anwendungen auf die PIN zugreifen können. Temporäre, flüchtige Speicherung der eingebebene PIN ist ausreichend und ermöglicht verbesserten Zugriffsschutz.

Die Anwendung kann beispielsweise konfiguriert sein, eine PIN-Eingabe über einen Touchscreen zu erfordern. Dabei können Mindestbetätigungsdauern und/oder Betätigungspausen, beispielsweise 10, 20, 50 oder 100 ms, zwischen Einzeleingaben erforderlich sein, was gegebenenfalls eine Entprellung des Touchscreens erfordert. Zusätzlich oder alternativ kann es erforderlich sein, die PIN innerhalb einer maximalen Eingabezeitdauer

einzugeben. Eingabe eines PINs, der nicht dem hinterlegten Hashwert entspricht, kann zu einer Sperrzeit führen, die gewartet werden muss, ehe die PIN wiederholt eingegeben werden kann. Eine Folge von beispielsweise 3, 4 oder 5 Eingaben von PINs, die alle nicht dem hinterlegten Hashwert entsprechen, kann zusätzlich oder alternativ zu einer verlängerten Sperrzeit oder einer Dauersperrung führen. Eine Rahmenfläche des Touchscreens kann so definiert sein, dass Berührung der Rahmenfläche zum Abbruch des Fernauslöseverfahrens führt.

Entsprechend kann wiederholt fehlerhafte Eingabe des Captcha-Codes zu einer Sperrzeit oder Dauersperrung führen. Ob einmalig fehlerhafte Eingabe des Captcha-Codes bereits eine Sperrzeit bewirkt, kann vom Steuergerät, welches die Captcha-Code Eingabe auswertet, festlegbar sein.

Auf dem Nutzergerät kann ein Hintergrundtask ohne Interaktion mit dem Nutzer ablaufen, der Statusinformationen an das Fahrzeug übermittelt, beispielsweise in Antwort auf einen Trigger. Die Aktivierung einer sicherheitsrelevanten Funktion kann ein solcher Trigger sein. Der Trigger kann dabei direkt durch die Anwendung oder indirekt durch das Fahrzeug gesetzt werden, im letzteren Fall mit einer zeitlichen Verzögerung. Der Hintergrundtask bietet eine Monitorfunktionalität auf dem Nutzergerät. Dabei können beispielsweise dem Fahrzeug Statusinformationen aus einem Berichtszeitraum berichtet werden, der beispielsweise so gewählt ist, dass die Eingaben zur Aktivierung einer Funktion stattgefunden haben können.

Die Statusinformationen können beispielsweise einen Einschaltzustand des Displays, eine Darstellung der Anwendung im Vordergrund, eine Eingabemöglichkeit (Konnte überhaupt irgendeine Ausgabe erfolgen?), einen Eingabestatus (Erfolgten irgendwelche Eingaben über Touchscreen?), Routinghäufigkeit und/oder –dauer, Ein- und/oder Ausgabeumleitung und weitere angeschlossene Geräte betreffen.

In einem Ausführungsbeispiel ist das Nutzergerät konfiguriert, zur Ausführung des Hintergrundtasks eine andere zentrale Prozessoreinheit zu verwenden als zur Ausführung der Anwendung, um so höhere Sicherheit zu gewährleisten.

Die Erfindung ermöglicht durch Aufteilung in unabhängige Teile mit eigener Eingabe und eigenem Datenanteil, dass fehlerhafte Sprünge nicht zum Senden vollständiger, gültiger Daten führen.

Es ist zusätzlich möglich, einen Zeitraum (Eingabezeitdauer) für eine letzte Eingabe, die das Senden eines letztes Datenpakets auslöst, kurz zu wählen, etwa 1, 2 oder 5 Sekunden, um die Sicherheit weiter zu erhöhen (Timeout von wenigen Sekunden).

Das erfindungsgemäße Versenden in einer Datenpaketstruktur ermöglicht auch gestaffelte Erstellung und sichere Ablage von Daten. Also kein maximal ungünstiger Zeitpunkt vorhanden.

In einem weiteren Ausführungsbeispiel werden die Datenpakete gemeinsam im Block versendet, wobei der Block einen solch großen Umfang aufweist, dass eine Gefährdung statistisch ausgeschlossen werden kann. Für die Evaluierung des Blocks kann ein vertrauenswürdiger Zeittaktgeber herangezogen werden.

Werden die Datenpakete einzeln versendet, kann sichergestellt werden, dass die vollständige Nachricht nie komplett/gleichzeitig im Speicher des Nutzergerätes ist.

Die Erfindung ermöglicht insbesondere, dass die Datenpakete Nutzereingaben unterschiedlicher Art, also beispielsweise Displayentsperrzeichen oder Tastatureingaben, zugeordnet sind.

Die Kommunikation zwischen dem Nutzergerät und dem Gerät, das die sicherheitsrelevante Funktion zur Verfügung stellt, kann in einem anderen Ausführungsbeispiel über einen vorbestimmten Server (Backend) erfolgen.

Figur 2 zeigt eine Datenpaketstruktur 100 gemäß einem ersten Ausführungsbeispiel der Erfindung. Die Datenpaketstruktur umfasst beispielhaft vier Datenpakete 110, 120, 130, 140, mehr oder weniger Datenpakete sind möglich. Die Datenpakete 110, 120, 130, 140 werden über die Zeit versetzt einzeln versendet. Jedes der Datenpakete 110, 120, 130, 140 enthält Daten 111, 121, 131, 141.

Figur 3 zeigt eine andere mögliche Zusammensetzung der Datenpakete 110, 120, 130, 140. Neben den eigentlichen Daten 111, 121, 131, 141 umfasst jedes Datenpaket einen Zeitstempel 112, 122, 132, 142. Weiterhin umfasst die Datenstruktur ein weiteres Datenpaket 150, welches einem Sender und/oder Empfänger Authentifizierung ermöglicht.

Figur 4 zeigt noch eine andere mögliche Zusammensetzung der Datenpakete110, 120, 130, 140. Neben den eigentlichen Daten 111, 121, 131, 141 umfasst jedes Datenpaket einen

Zeitstempel 112, 122, 132, 142 und eine Prüfsumme 113, 123, 133. Die Datenpakete sind dabei, als Ganzes oder jeder Teil (Prüfsumme, Zeitstempel, Daten) für sich, verschlüsselt. Weiterhin umfasst die Datenstruktur ein weiteres Datenpaket 150, welches eine Sender- und/oder Empfänger-Authentifizierung ermöglicht.

Figur 5 zeigt eine Datenpaketstruktur 200 gemäß einem zweiten Ausführungsbeispiel der Erfindung. Im Unterschied zur Figur 2, in der die Datenpakete 110, 120, 130, 140 nacheinander einzeln versendet werden, bildet die Datenpaketstruktur 200 einen Block, der bevorzugt aber nicht notwendigerweise, unter Verwendung einer Kommunikationsabsicherung übertragen werden kann. Der Block umfasst Datenpakete 110, 120, 130, 140, 150, die den in Zusammenhang mit Figur 3 beschriebenen Datenpaketen entsprechen.

Figur 6 zeigt ein System gemäß einem Ausführungsbeispiel der Erfindung. Im dargestellten Beispiel umfasst ein Fahrzeug 500 ein Steuergerät 510, das eine Fernauslösung einer sicherheitsrelevanten Funktion des Fahrzeug 500 von einem Nutzergerät 300 aus über einen Backend-Server 400 ermöglicht.

Die vorliegende Erfindung verhindert Sicherheitsgefährdungen, die durch beispielsweise einen Fehler „Sprung Instruction Pointer“ ausgelöst werden können. Bei einem Sprung an beliebige Stelle werden, durch die Aufteilung in unabhängige Teile mit eigener Eingabe und eigenem Datenanteil, keine vollständigen und/oder gültigen Daten gesendet. Durch eine sehr kurze Timeout-Zeit (zum Beispiel 1, 2 oder 3 Sekunden) kann außerdem mit hoher Wahrscheinlichkeit verhindert werden, dass Daten eines letzten Pakets, die auch bei einem Sprung an beliebige Stelle konsistent sein können, nach einem solchen Sprung tatsächlich gesendet werden. vor der letzten vom Nutzer erwarteten Eingabe für einen sehr eingeschränkten Zeitraum).

Die vorliegende Erfindung verhindert Sicherheitsgefährdungen, die durch beispielsweise einen Fehler „Daten werden verfälscht oder überschrieben“ ausgelöst werden können. Durch Aufteilung in Teilsequenzen wird eine gestaffelte Erstellung und sichere Ablage von Daten möglich, so dass kein maximal ungünstiger Zeitpunkt vorhanden ist. Zusätzlich oder alternativ kann ein Umfang des zu sendenden Paketes so groß gewählt sein, dass eine Gefährdung statistisch ausgeschlossen werden kann.

Da durch Datenverfälschung allein ein Paket nicht gesendet wird, muss eine Verfälschung nach Erzeugung, aber vor Versenden einer Nachricht auf Nutzerwunsch erfolgen. Das direkte Senden einzelner Teilsequenzen nach ihrer Erzeugung, wie es in beispielhaften

Ausführungsformen der Erfindung erfolgt, verringert die Möglichkeit zur Verfälschung, unter anderem auch, da nie die vollständige Nachricht im Speicher vorhanden ist.

Die vorliegende Erfindung verhindert Sicherheitsgefährdungen, die durch beispielsweise einen Fehler „CPU Fehler“ ausgelöst werden können. Beispielsweise kann jeder der unterschiedlichen Sequenzteile mit unterschiedlichen Befehlen realisiert sein. Dabei kann ein insgesamt kleiner Befehlssatz verwendet werden, der lediglich auf Befehlen basiert, die von anderen Anwendungen auch häufig verwendet werden. Wird einer dieser Befehle fehlerhaft ausgeführt, da die CPU fehlerhaft ist, so tritt auch bei den anderen Anwendungen ein Fehlverhalten des Gerätes auf, so dass ein Nutzer die fehlerhafte Ausführung bemerken und den Defekt des Gerätes erkennen kann.

Die vorliegende Erfindung verhindert durch Tastensperre, PIN, Captcha-Code-Eingabe, Abbruch bei Berühren der Rahmenfläche des Touchscreens und/oder Timeout bei Fehleingaben Sicherheitsgefährdungen, die durch beispielsweise einen Fehler „Phantomeingaben“ ausgelöst werden können.

Die vorliegende Erfindung verhindert weiterhin durch Kommunikationsabsicherung, durch Chiffrieren und/oder Signieren des Inhalts, und/oder Empfang nur von festgelegtem Server (Backend) einen Fehler „Beliebiges Gerät im Internet sendet beliebigen Inhalt an OCU des Fahrzeugs“.

Sicherheitsgefährdungen, die durch beispielsweise einen Fehler „Falsche Handy zu Fahrzeug Zuordnung im Backend“ ausgelöst werden können, werden ebenfalls zuverlässig verhindert oder minimiert. Durch eine Kommunikationsabsicherung für den Inhalt, bei der das mobile Endgerät nur den Schlüssel eines einzigen zugeordneten Fahrzeugs kennt, wird verhindert dass ein Nutzer von Anfang an Aktionen auf einem fremden Fahrzeug ausführen oder dass eine unerkannte Verfälschung nachträglich erfolgen kann.

Wird die Rahmenfläche, deren Berühren zum Abbruch führt, so gewählt, dass lediglich ein Eingabefeld zur Eingabe der PIN verbleibt, und wird eine Sperrzeit nach 2, 3 oder mehr Fehleingaben aktiviert, so kann die Wahrscheinlichkeit einer PIN-Fehler bedingten Gefährdung auf 1:10.000 oder noch darunter gesenkt werden.

Wird die Rahmenfläche, deren Berühren zum Abbruch führt, so gewählt, dass lediglich ein Eingabefeld zur Eingabe des Captcha-Codes verbleibt, und wird eine Sperrzeit nach 2, 3 oder

mehr Fehleingaben aktiviert, so kann auch die Wahrscheinlichkeit einer Captcha-Code-Fehler bedingten Gefährdung auf 1:10.000 oder noch darunter gesenkt werden.

Kontinuierliche Phantomeingaben können aktiv erkannt werden, wenn eine aktive Wartezeit zwischen Eingaben, beispielsweise 3 Sekunden, in der der Touchscreen nicht berührt werden darf, erforderlich ist.

Bezugszeichenliste

100, 200	Datenpaketstruktur
110, 120, 130, 140	Datenpakete
111, 121, 131, 141	Daten
112, 122, 132, 142	Zeitstempel
113, 123, 133, 134	Prüfsumme
150	weiteres Datenpaket
300	Nutzergerät (Mobiltelefon)
400	Server (Backend)
500	Fahrzeug
510	Steuergerät

Patentansprüche

1. Verfahren zur Erhöhung der Sicherheit bei einer Fernauslösung einer sicherheitsrelevanten Funktion eines ersten Gerätes (510) in Folge von Empfang von Daten (111, 112, 113, 114), von einem zweiten Gerät (300), von dem eine Kommunikationsverbindung zu dem ersten Gerät (510) besteht, wobei die Daten (111, 112, 113, 114) Nutzereingaben in einer Anwendung auf dem zweiten Gerät (300) zugeordnet sind, dadurch gekennzeichnet, dass das erste Gerät (510) zu jeder Nutzereingabe einen Teil der Daten (111, 112, 113, 114) in einem Datenpaket einer Datenpaketstruktur (100, 200) empfängt, wobei das erste Gerät (510) die Fernauslösung verhindert, wenn die Datenpaketstruktur (100, 200) nicht einer vorbestimmten Datenpaketstruktur entspricht.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das erste Gerät (510) die Fernauslösung auch verhindert, wenn Datenpakete (110, 120, 130, 140, 150) der Datenpaketstruktur (100, 200) nicht in einer vorbestimmten Zeitdauer empfangen wurden und/oder wenn eine Wartezeitdauer zwischen aufeinanderfolgend empfangenen Datenpaketen (110, 120, 130, 140, 150) eine Höchstwartezeitdauer überschreitet.

3. Verfahren nach einem der Ansprüche 1 und 2, dadurch gekennzeichnet, dass die Datenpakete (110, 120, 130, 140) eine Prüfsumme (113, 123, 133, 143) umfassen und das erste Gerät die Fernauslösung auch verhindert, wenn bei einem der Datenpakete die Prüfsumme nicht zu restlichen Daten in dem Datenpaket passt.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Datenpakete (110, 120, 130, 140, 150) verschlüsselt sind und das erste Gerät (510) die Fernauslösung auch verhindert, wenn eines der Datenpakete (110, 120, 130, 140, 150) nicht mit entschlüsselt werden kann.

5. Verfahren zur Fernauslösung einer sicherheitsrelevanten Funktion eines ersten Gerätes (510) in Folge von Empfang von Daten (111, 121, 131, 141, 151) zu Nutzereingaben in einer Anwendung auf einem zweiten Gerät (300), von dem eine Kommunikationsverbindung zu dem ersten Gerät (510) besteht, dadurch gekennzeichnet, dass das zweite Gerät (300) zu jeder Nutzereingabe einen Teil der Daten in einem Datenpaket (110, 120, 130, 140, 150) einer vorbestimmten Datenpaketstruktur (100, 200) an das erste Gerät (510) sendet.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass das zweite Gerät die Datenpakete einzeln innerhalb einer vorbestimmten Zeitdauer versendet.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass das zweite Gerät beim Versenden der Datenpakete eine Höchstwartezeitdauer zwischen aufeinanderfolgend versandeten Datenpaketen nicht überschreitet.

8. Verfahren nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass das zweite Gerät zu jedem der Datenpakete eine Prüfsumme bildet und dem jeweiligen Datenpaket hinzufügt.

9. Verfahren nach einem der Ansprüche 5 bis 8, dadurch gekennzeichnet, dass das zweite Gerät die Datenpakete verschlüsselt.

10. Verfahren nach Anspruch 4 oder 9, dadurch gekennzeichnet, dass die Datenpakete mit unterschiedlichen Schlüsseln verschlüsselt sind, die Positionen in der vorbestimmten Reihenfolge zugeordnet sind.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass das zweite Gerät die unterschiedlichen Schlüssel von dem ersten Gerät erhält.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Nutzereingaben eine Eingabe zum Starten der Anwendung, eine Eingabe einer persönlichen Identifikationsnummer, eine Eingabe eines Captcha-Codes, eine Eingabe zur Auswahl der Fernauslösung und/oder eine Eingabe zur Aktivierung der Fernauslösung umfasst, wobei eines der Datenpakete die eingegebene persönliche Identifikationsnummer und ein nachfolgendes Datenpaket den eingegebenen Captcha-Code umfasst.

13. Vorrichtung (510) für ein Fahrzeug (500) zur Erhöhung der Sicherheit bei einer Fernauslösung einer sicherheitsrelevanten Funktion des Fahrzeugs (500) in Folge von Empfang von Daten (111, 121, 131, 141) zu Nutzereingaben in einer Anwendung auf einem externen Gerät (300), von dem eine Kommunikationsverbindung zu der Vorrichtung (510) besteht, dadurch gekennzeichnet, dass die Vorrichtung (510) konfiguriert ist, zu jeder Nutzereingabe einen Teil der Daten in einem Datenpaket (110, 120, 130, 140, 150) zu empfangen und die Fernauslösung zu verhindern, wenn die Datenpakete (110, 120, 130, 140, 150) nicht in einer vorbestimmten Reihenfolge empfangen wurden.

14. Fahrzeug (500) mit einer Vorrichtung (510) nach Anspruch 13.

15. Speichervorrichtung umfassend prozessorausführbare Anweisungen, dadurch gekennzeichnet, dass ein Prozessor unter Verwendung der Anweisungen zur Ausführung des Verfahrens nach einem der Ansprüche 1 bis 12 konfiguriert werden kann.

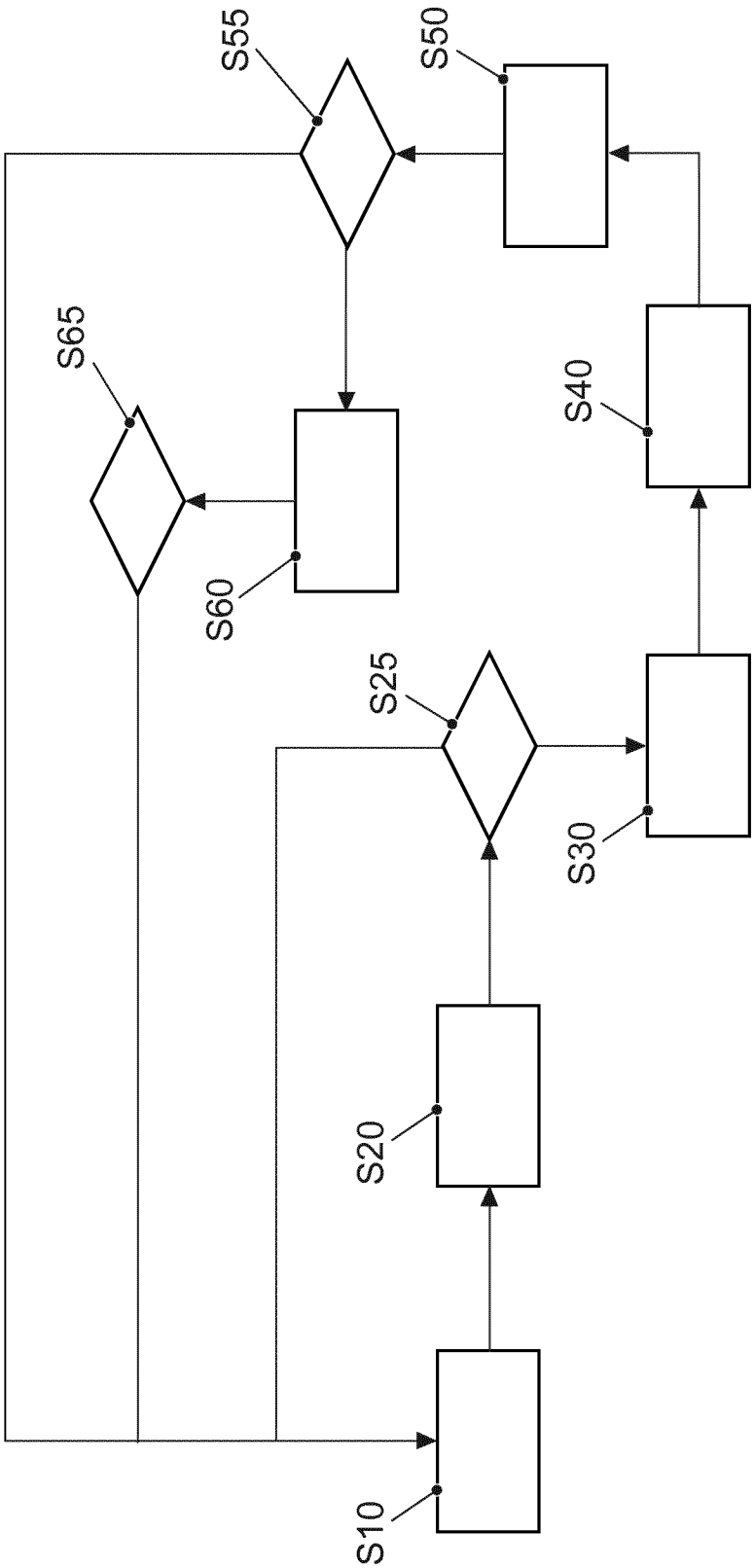


FIG. 1

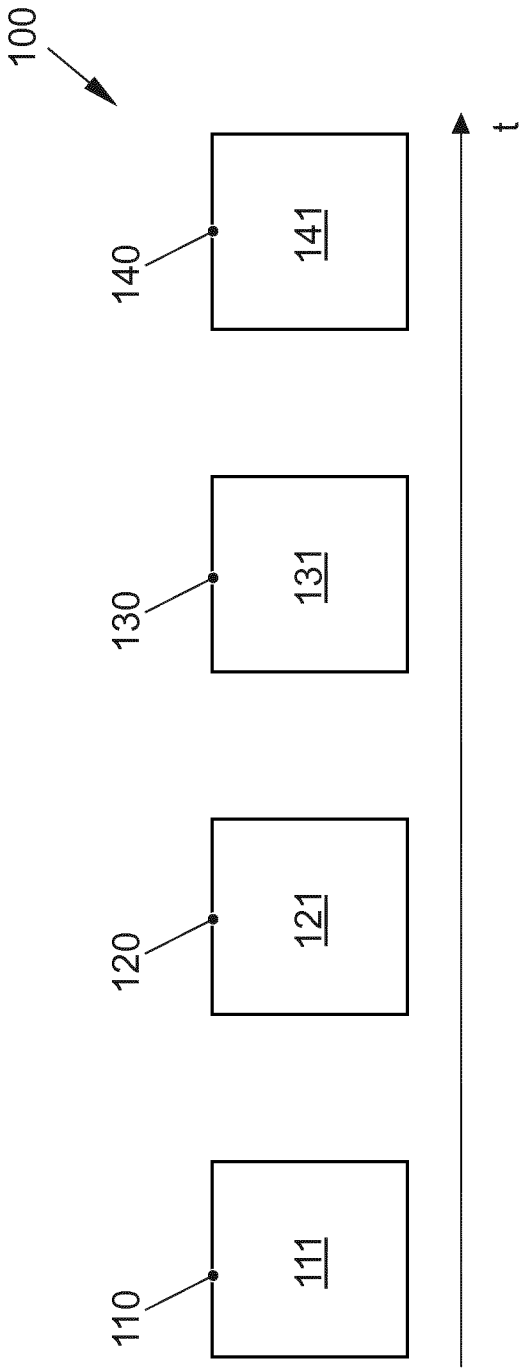


FIG. 2

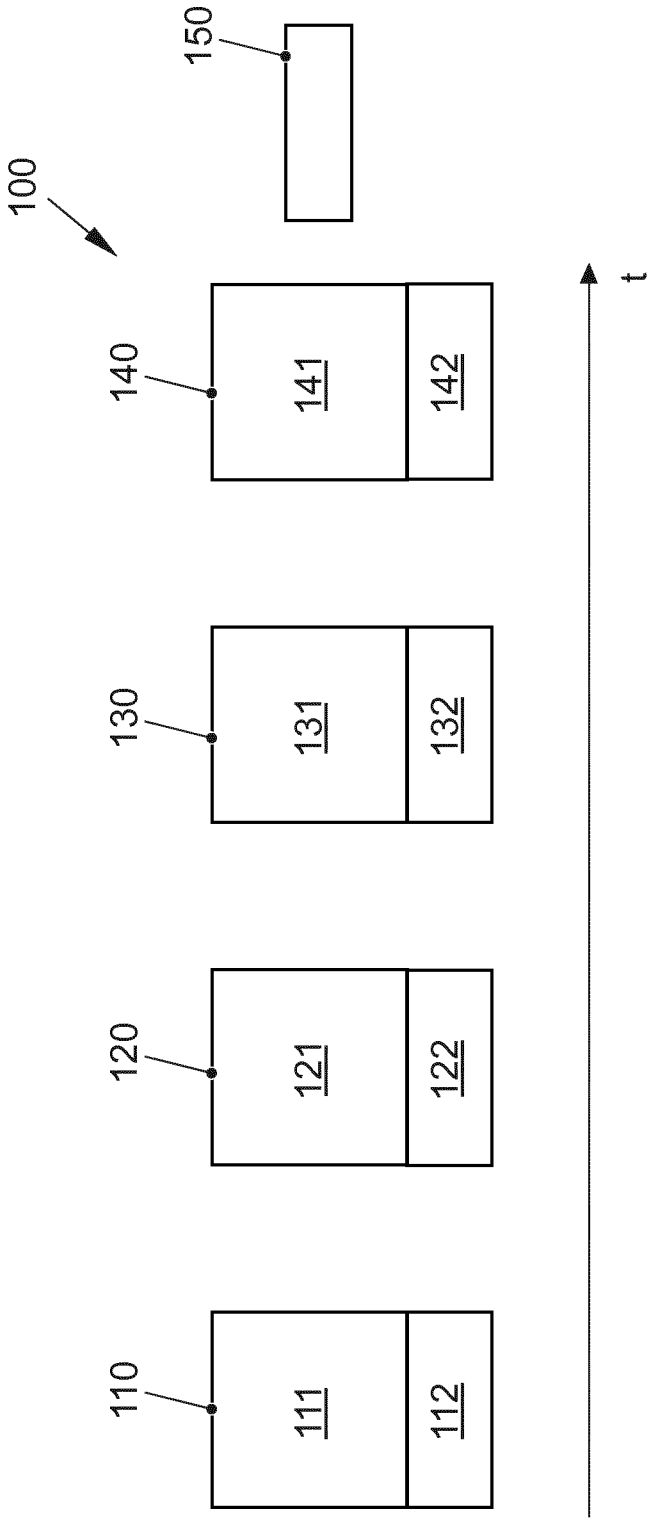


FIG. 3

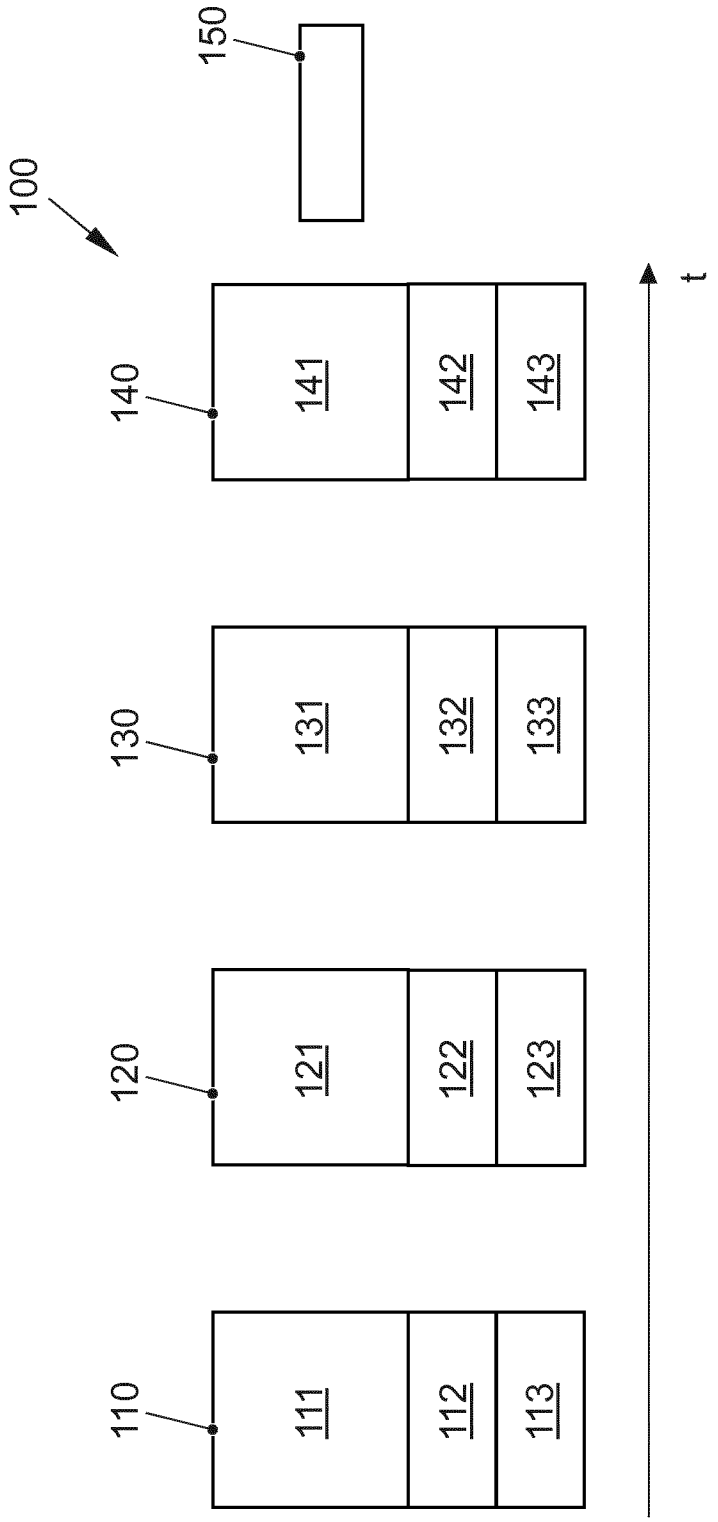

150
100
140
141
142
143
130
131
132
133
120
121
122
123
110
111
112
113
t

FIG. 4

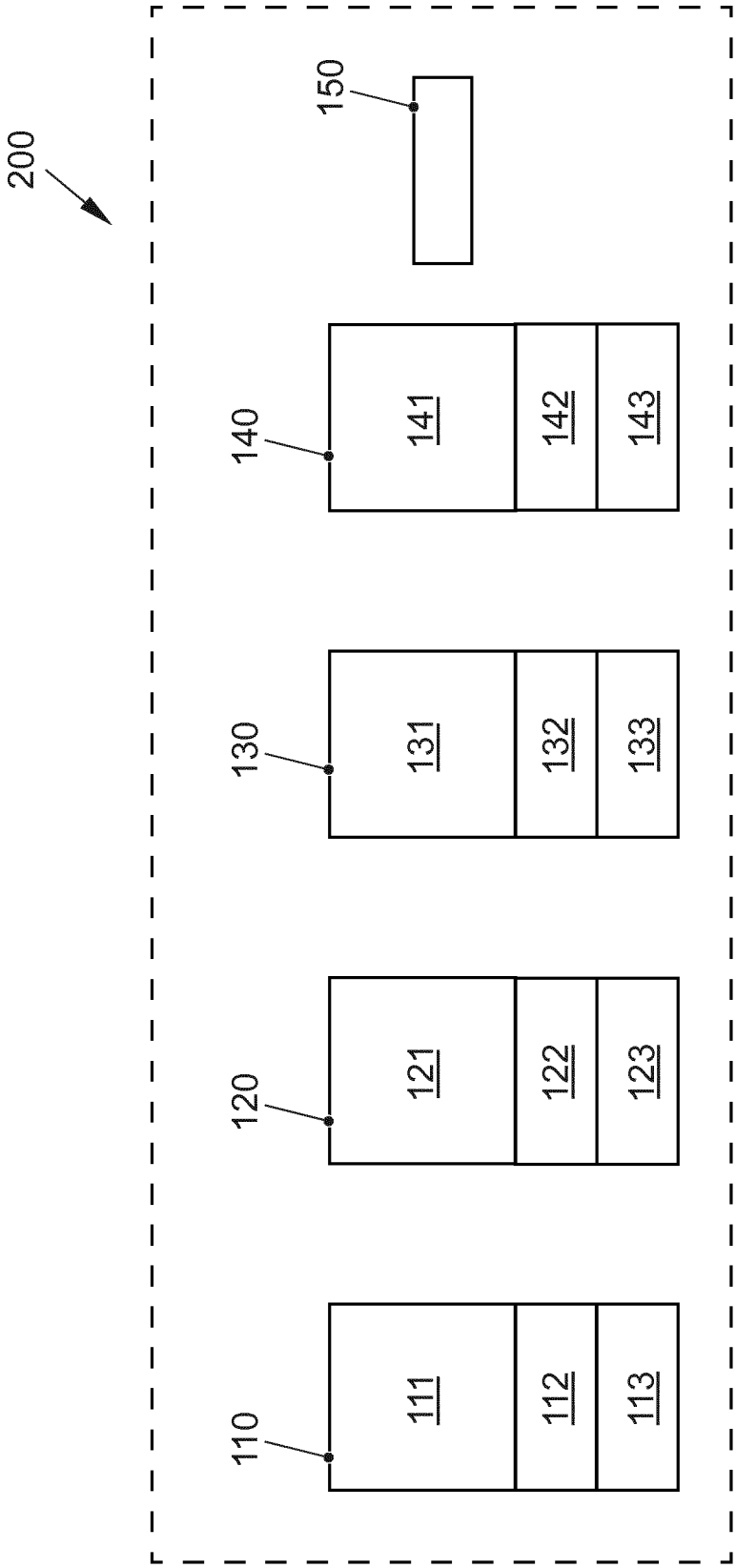

200
150
140
141
142
143
130
131
132
133
120
121
122
123
110
111
112
113

FIG. 5

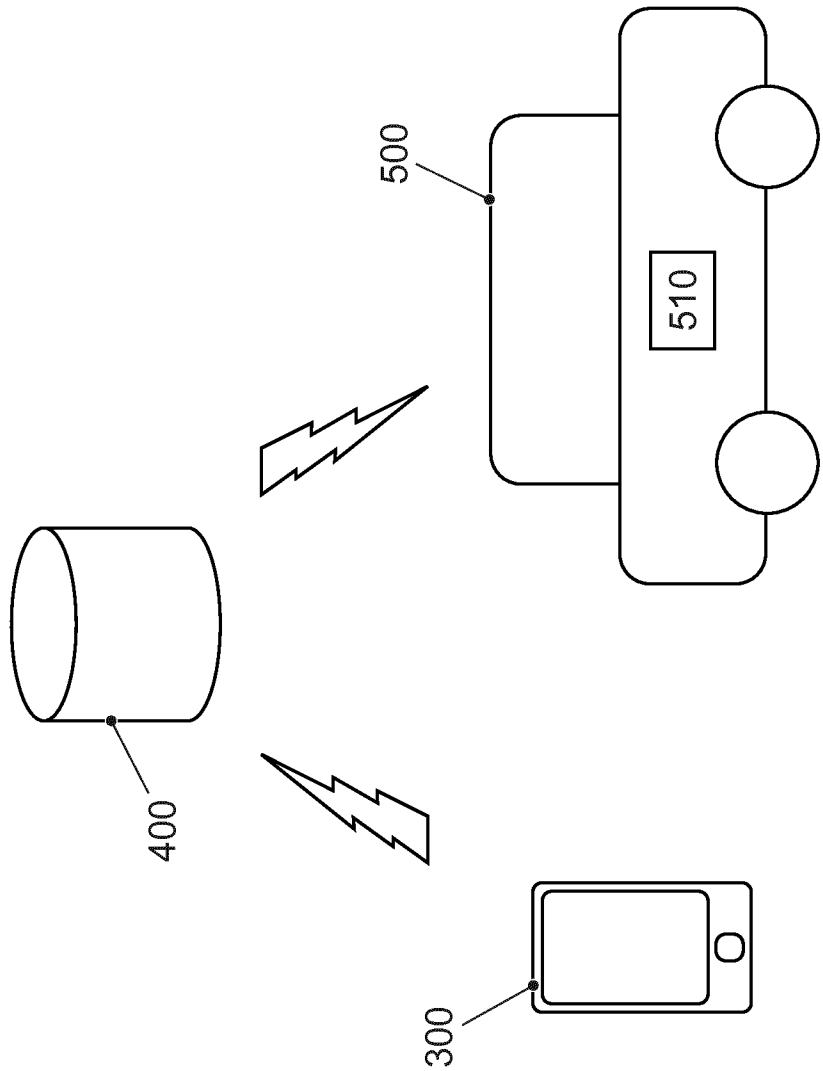


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/050651

A. CLASSIFICATION OF SUBJECT MATTER
INV. G08C17/00 G07C5/00 H04L29/08 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G08C G07C 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, COMPENDEX, INSPEC, PAJ, IBM-TDB, 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 2010 029931 A1 (BAYERISCHE MOTOREN WERKE AG [DE]) 15 December 2011 (2011-12-15) abstract paragraph [0006] - paragraph [0024] paragraph [0040] - paragraph [0058] figure 1 -----	1-15
A	DE 10 2008 030562 A1 (BAYERISCHE MOTOREN WERKE AG [DE]) 31 December 2009 (2009-12-31) abstract paragraph [0006] - paragraph [0008] -----	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 2016	04/04/2016

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/050651

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102010029931 A1	15-12-2011	NONE	
DE 102008030562 A1	31-12-2009	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2016/050651

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G08C17/00 G07C5/00 H04L29/08 H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G08C G07C 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, COMPENDEX, INSPEC, PAJ, IBM-TDB, 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 2010 029931 A1 (BAYERISCHE MOTOREN WERKE AG [DE]) 15. Dezember 2011 (2011-12-15) Zusammenfassung Absatz [0006] - Absatz [0024] Absatz [0040] - Absatz [0058] Abbildung 1 -----	1-15
A	DE 10 2008 030562 A1 (BAYERISCHE MOTOREN WERKE AG [DE]) 31. Dezember 2009 (2009-12-31) Zusammenfassung Absatz [0006] - Absatz [0008] -----	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. März 2016	04/04/2016

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

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2016/050651

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102010029931 A1	15-12-2011	KEINE	
DE 102008030562 A1	31-12-2009	KEINE	