

(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
28. März 2019 (28.03.2019)



(10) Internationale Veröffentlichungsnummer
WO 2019/057882 A1

(51) Internationale Patentklassifikation:

H04L 12/40 (2006.01) H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2018/075586

(22) Internationales Anmeldedatum:

21. September 2018 (21.09.2018)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:

10 2017 216 808.0

22. September 2017 (22.09.2017) DE

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

(72) Erfinder: BUNIMOV, Viktor; Hornkampsweg 14, 38159 Vechelde (DE). JENTZSCH, Anke; Mühlenweg 10, 38473 Tiddische (DE). KAMP, Birger; Zur Diwelie 23, 38531 Rötgesbüttel (DE). MICHNA, Steven; Lobitzweg 28, 12557 Berlin (DE). RIECHEL, Christoph; Schunterstraße 51, 38106 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,

(54) Title: METHOD FOR MONITORING THE COMMUNICATION ON A COMMUNICATION BUS, AND ELECTRONIC APPARATUS FOR CONNECTION TO A COMMUNICATION BUS

(54) Bezeichnung: VERFAHREN ZUR ÜBERWACHUNG DER KOMMUNIKATION AUF EINEM KOMMUNIKATIONSBUS SOWIE ELEKTRONISCHE VORRICHTUNG ZUM ANSCHLUSS AN EINEN KOMMUNIKATIONSBUS

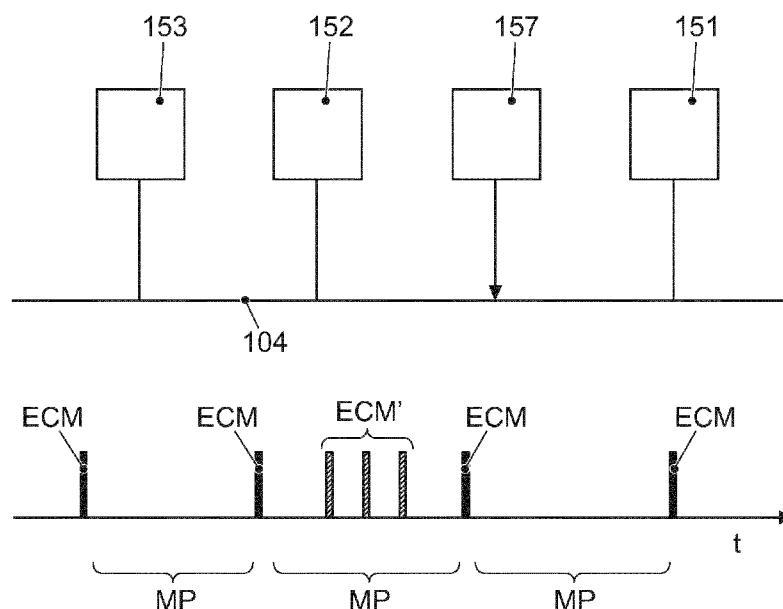


FIG. 7

(57) Abstract: The invention relates to a monitoring method for a communication bus (104) based on a variant of the family of CAN bus standards. The method involves a monitoring module being provided for a station (151, 152, 153, 157) connected to the communication bus. During the method, the messages are denoted by an identifier, wherein each station (151, 152, 153, 157) is provided with a stipulation regarding which messages it can send with which identifier. In this case, an explicitness rule is that it is prohibited for another station (151, 152, 153) to send a useful data message with an identifier that is already reserved for this station (157). This rule is utilised for the monitoring. If a useful data message is sent with an identifier reserved for that particular station (157) by another station (151,



WO 2019/057882 A1

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)

152, 153), unauthorised bus access is detected. In the event of detection of a CAN bus remote frame message reserved for the station, the monitoring module assumes no unauthorised bus access and initiates no countermeasure.

(57) Zusammenfassung: Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus sowie elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus Die Erfindung betrifft ein Überwachungsverfahren für einen Kommunikationsbus (104) nach einer Variante der Familie der CAN-Bus Standards. Das Verfahren beinhaltet, dass ein Überwachungsmodul bei einer an den Kommunikationsbus angeschlossenen Station (151, 152, 153, 157) vorgesehen wird. Bei dem Verfahren werden die Botschaften durch einen Identifizierer gekennzeichnet, wobei für jede Station (151, 152, 153, 157) festgelegt wird, welche Botschaften mit welchem Identifizierer von ihr gesendet werden dürfen. Dabei besteht eine Eindeutigkeitsregel darin, dass es verboten ist, dass eine andere Station (151, 152, 153) eine Nutzdaten-Botschaft mit einem Identifizierer versendet, der schon für diese Station (157) reserviert ist. Diese Regel wird bei der Überwachung ausgenutzt. Wenn eine Nutzdaten-Botschaft mit einem Identifizierer von einer anderen Station (151, 152, 153) gesendet wird, der für die eigene Station (157) reserviert ist, wurde ein unberechtigter Buszugriff erkannt. Im Falle des Erkennens einer CAN-Bus remote Frame Botschaft, der für die Station reserviert ist, wird von dem Überwachungsmodul kein unberechtigter Buszugriff angenommen und keine Gegenmaßnahme eingeleitet.

Beschreibung

Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus sowie elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus

Die Erfindung betrifft das technische Gebiet der Überwachung der Kommunikation auf einem Kommunikationsbus auf unberechtigte Buszugriffe. Dieses Verfahren kann insbesondere bei Kommunikationsbussen eingesetzt werden, die in Fahrzeugen eingesetzt werden. Vernetzte Steuergeräte sind auch in anderen Gebieten der Technik zu finden, z.B. in der Automatisierungstechnik, Prozesstechnik, usw. Die Erfindung betrifft weiterhin eine elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus.

In modernen Fahrzeugen werden eine Vielzahl von Steuergeräten verbaut. Alleine für den Antriebstrang werden eine Anzahl Steuergeräte eingesetzt, so z.B. Motor-Steuergerät, Getriebe-Steuergerät, Wählhebel-Steuergerät, Airbag-Steuergerät und weitere. Daneben gibt es auch noch weitere Steuergeräte, die im Bereich der Fahrzeugkarosserie verbaut werden und für bestimmte Komfortfunktionen sorgen. Als Beispiele werden genannt die Tür- oder Fensterheber-Steuergeräte, Klimaanlage-Steuergeräte, Sitzverstellungs-Steuergeräte, u.a. Dann gibt es weiterhin Steuergeräte, die zu dem Infotainment-Bereich zählen, wie Kamera-Steuergerät zur Umfeldbeobachtung, Navigationsgerät, Kommunikationsmodul und Entertainment-Gerät mit TV, Radio, Video und Musik-Funktion.

Typischerweise werden die Steuergeräte der verschiedenen Kategorien jeweils mit einem separaten, für die Gerätekategorie entsprechend ausgelegten Bus vernetzt. Es können daher mehrere verschiedene Bussysteme im Fahrzeug eingesetzt werden. Die verschiedenen Bussysteme können dabei über Gateways miteinander verbunden sein, um einen Datenaustausch zu ermöglichen. Im Bereich der Antriebstrang-Steuergeräte wird typischerweise der CAN-Bus (Controller Area Network) eingesetzt, ebenfalls im Bereich der Komfort-Steuergeräte. Im Infotainment-Bereich kommen auch andere Bussysteme zum Einsatz, wie Bussysteme die auf Ethernet-Technologie beruhen, z.B. AVB (Audio Video Bridging) der auf der Standard-Familie nach IEEE 802.1 Standard basiert. Auch Bussysteme, bei denen die Datenübertragung über Lichtwellenleiter geschieht, sind einsetzbar. Als Beispiele werden genannt der MOST Bus (Media Oriented System Transport) oder der D2B Bus (Domestic Digital Bus).

Bussysteme im Kraftfahrzeugbereich gelangen zunehmend in den Fokus von Hackerangriffen und den Versuchen, Botschaftsinhalte vorsätzlich zu manipulieren. Solche Hackerangriffe auf das Bussystem geschehen typischerweise über eine Aufschaltung an das

physikalische Übertragungsmedium, also die Busleitung oder über Zugriff auf eine sogenannte OBD-Buchse (On Board Diagnose-Schnittstelle). Die Cyber-Sicherheit gelangt auch deswegen immer mehr in den Fokus, weil immer komplexere Fahrerassistenzsysteme in die Fahrzeuge gelangen bis hin zu dem automatisierten Fahren. Manipulationen müssen hier ausgeschlossen werden.

Es besteht daher ein Bedarf, die Kommunikation auf den Kommunikationsbussen im Fahrzeug wie auch anderswo immer weiter abzusichern.

Der CAN-Bus ist im Kraftfahrzeugbereich besonders verbreitet und wird häufig für die Vernetzung von sicherheitsrelevanter Elektronik im Fahrzeug eingesetzt. Deshalb besteht hier ein besonderer Bedarf für eine Absicherung der Kommunikation.

Aus der DE 10 2015 205 670 A1 ist ein Angriffserkennungsverfahren für ein Bussystem eines Kraftfahrzeuges und eine entsprechende Vorrichtung bekannt. Es geht dabei darum, Angriffe von außen auf das Bussystem zu erkennen und abzuwehren. Dazu wird in einem Gateway des Bussystems ein Modul installiert, das nach einem allgemeinen Ansatz überprüft, ob die auf dem Bus übertragenen Nachrichten nach den Kommunikationsregeln übertragen wurden. Darunter fallen verschiedene Kommunikationsregeln: Nach einem Aspekt prüft das Modul bestimmte Eigenschaften eines festgelegten Nachrichtenzyklusses. Darunter fallen z.B. jeweils die Zeit zwischen zwei aufeinanderfolgenden Nachrichten und wenn es erkennt, dass der zeitliche Abstand zweier aufeinanderfolgenden Nachrichten nicht mit der vorgegebenen Zyklusdauer übereinstimmt, gibt es eine Warnmeldung aus. Nach einem anderen Aspekt prüft das Modul, ob jeweils aufeinanderfolgend nur identische Nachrichten übertragen werden. Die Überprüfungsaspekte können einen bestimmten Nachrichtentyp betreffen.

Aus der US 2015/172306 A1 ist ebenfalls ein Angriffsüberwachungsverfahren bekannt, bei dem bei zyklisch auftretenden Nachrichten die Zykluszeiten überwacht werden. Ein Angriff wird erkannt, wenn es zu Abweichungen von der gemittelten Zykluszeit kommt. Um auch bei nicht-zyklisch auftretenden Nachrichten eine Überwachung durchführen zu können, werden diese durch Einfügen eines Sicherheitscodes abgesichert. Das Überwachungsmodul wird zentral in einem Gateway des Kfz-Kommunikationsnetzwerkes positioniert.

Die Erfindung setzt sich zum Ziel, ein wirkungsvolles Überwachungsverfahren für einen Kommunikationsbus anzugeben, das zuverlässig unberechtigte Buszugriffe erkennen kann. Dabei soll Verschlüsselung möglichst vermieden werden und es soll sich das Überwachungsverfahren einfach umsetzen lassen ohne größeren Entwicklungsaufwand.

Diese Aufgabe wird durch ein Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus gemäß Anspruch 1 sowie eine elektronische Vorrichtung gemäß Anspruch 15 gelöst.

Die abhängigen Ansprüche beinhalten vorteilhafte Weiterbildungen und Verbesserungen der Erfindung entsprechend der nachfolgenden Beschreibung dieser Maßnahmen.

Die Lösung besteht in einem Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus, durch den eine Anzahl von elektronischen Stationen vernetzt werden. Eine Besonderheit besteht darin, dass das Botschaftsformat so gestaltet ist, dass die Botschaften durch einen Identifizierer gekennzeichnet sind, wobei für jede Station festgelegt wird, welche Botschaften mit welchem Identifizierer von ihr gesendet werden dürfen. Dabei wird eine Eindeutigkeitsregel eingehalten, die verbietet, dass eine andere Station eine Nutzdaten-Botschaft mit einem Identifizierer versendet, der schon für diese Station reserviert ist. Das Verfahren kennzeichnet sich dadurch aus, dass in einer oder mehreren oder allen der elektronischen Stationen ein Überwachungsmodul vorgesehen wird, das überwacht, ob auf dem Kommunikationsbus eine Nutzdaten-Botschaft mit einem Identifizierer von einer anderen Station gesendet wird, der schon für die eigene Station reserviert ist. Das Verfahren ist ebenso einfach wie wirkungsvoll. Bei dem Verfahren wird die besondere Eindeutigkeitsregel ausgenutzt.

Dieses Überwachungsverfahren wird bei dem Kommunikationsbus nach einer Variante der Familie der CAN-Bus Standards, entsprechend Controller Area Network, eingesetzt. Dieses ist insbesondere in dem Kfz-Bereich sehr verbreitet und erfüllt die Voraussetzungen.

Wenn eine CAN-Bus Remote Frame Botschaft erkannt wird mit einem Botschafts Identifizierer, der für die Station reserviert ist, wird kein unberechtigter Buszugriff angenommen und keine Gegenmaßnahme eingeleitet. Ein Remote Frame kann ausnahmsweise denselben Botschafts-Identifizierer benutzen. Diese Botschaft enthält aber keine Nutzdaten und wird deshalb als nicht so gefährlich eingestuft. Sollte durch mehrfaches Aussenden des Remote-Frames von einem Angreifer eine Überflutung des Busses erfolgen, können durch die bekannten Überwachungsmaßnahmen der Zykluszeit solche Angriffe auch unterbunden werden.

Zur Implementierung des Verfahrens ist es von Vorteil, wenn das Überwachungsmodul für die Überwachung auf eine Sendetabelle zugreift, in der alle der für die Station reservierten Identifizierer verzeichnet sind, und den Identifizierer einer empfangenen Botschaft mit den Einträgen in der Sendetabelle vergleicht. Das Anlegen der Tabelle ist bei dem CAN-Bus für die Akzeptanzfilterung auch schon erforderlich und kann entsprechend realisiert werden. Das

Durchführen des Vergleiches lässt sich in einem Mikrocomputer einfach realisieren. Wenn es hier zu einer Überlastung des Prozessors kommen sollte, kann dafür alternativ eine Spezielschaltung, realisiert durch einen FPGA-Chip, eingesetzt werden.

Bei Feststellen einer Übereinstimmung des Botschafts-Identifizierers der empfangenen Botschaft mit einem Eintrag in der Sendetabelle wird von dem Überwachungsmodul ein unberechtigter Buszugriff festgestellt und es können Gegenmaßnahmen eingeleitet werden.

Weil ja die Station, die die Kommunikation auf dem Bus überwacht, selbst auch Botschaften mit den für sie reservierten Identifizierern sendet, ist es nötig, dass während des Zustandes, in dem die Station selbst eine Botschaft über den Kommunikationsbus sendet, die Durchführung der Gegenmaßnahmen unterdrückt wird. Sonst würden die von der Station regulär ausgesendeten Botschaften auch als Angriff erkannt werden und unnötigerweise Gegenmaßnahmen eingeleitet werden. Es gibt mehrere Möglichkeiten, um dies zu erreichen.

In vorteilhafter Weise wird das Überwachungsmodul während des Zustandes, in dem die Station selbst eine Botschaft über den Kommunikationsbus sendet, inaktiv geschaltet und während des Zustandes, wo es Botschaften von dem Kommunikationsbus empfängt, aktiv geschaltet. Während der Sendephase der eigenen Station können keine anderen Botschaften über den Kommunikationsbus übertragen werden, so dass durch Inaktivschaltung des Überwachungsmoduls kein Sicherheitsrisiko entsteht.

Andere Möglichkeiten bestehen darin, dass, wenn die Station selbst sendet, der Bus weiterhin überwacht wird, aber die Gegenmaßnahme nicht eingeleitet wird. Es würde also trotz des Erkennens einer irregulären Botschaft keine Alarmierung, Warnmeldung, usw. erfolgen.

Eine dritte Möglichkeit besteht darin, dass, wenn die Station selbst sendet, die irreguläre Botschaft erkannt wird, eine Alarmierung oder Warnmeldung erfolgt, diese Meldung aber von der Station, die die Meldung empfängt, in einer entsprechend ausgelegten Empfänger-Routine ignoriert wird. Die Alarmierung oder Warnmeldung kann durch Aussenden einer entsprechenden Botschaft über den Kommunikationsbus z.B. an ein Infotainment-Steuergerät im Fahrzeug erfolgen.

In vorteilhafter Weise kann das Verfahren bei einem Kommunikationsbus eingesetzt werden, das für den Austausch von Botschaften zwischen elektronischen Komponenten eines Fahrzeuges ausgelegt ist. Insbesondere dort werden Bussysteme eingesetzt, bei denen solche Identifizierer verbunden mit der beschriebenen Eindeutigkeitsregel eingesetzt werden.

Beispiele von Gegenmaßnahmen, die bei dem Verfahren eingesetzt werden können, sind:

- Ausgeben einer Warnmeldung an den Fahrzeugführer, beispielsweise mit einem optischen, akustischen oder haptischen Signal,
- Einschalten der Alarmanlage,
- Absetzen einer Manipulationsmeldung über Funk an einen Datenbank-Zentralrechner des Autoherstellers oder einer Behörde oder an ein Smartphone des Fahrzeughalters,
- Abspeichern von Ort, Datum, Zeit des Manipulationsereignisses in einem Speicher
- Blockieren des Schlüssels, mit dem das Fahrzeug eingeschaltet wurde.

Die Aufzählung erhebt keinen Anspruch auf Vollständigkeit, auch können mehrere der aufgelisteten Gegenmaßnahmen parallel eingesetzt werden.

Eine weitere Gegenmaßnahme betrifft das sofortige Senden eines Fehlersignals noch während die unberechtigte Botschaft über den Bus gesendet wird.

Diese Gegenmaßnahme nutzt einen Fehlerschutzmechanismus aus, der z.B. beim CAN-Protokoll vorgesehen ist. Das CAN-Protokoll schreibt aus Gründen netzwerkweiter Datenkonsistenz vor, dass bei lokalen Störungen eine fehlererkennende CAN-Busstation alle im CAN-Netzwerk angeschlossenen CAN-Busstationen davon in Kenntnis zu setzen hat. Dazu überträgt die fehlererkennende CAN-Busstation ein Fehlersignal („Error Flag“), welches sich aus sechs dominanten Bits zusammensetzt. Damit wird bewusst die Bitstuffingregel des CAN-Bus-Protokolls verletzt und so ein Bitstuffing-Fehler verursacht.

Beim CAN-Bus sorgt die Übertragung des „Error Flags“ dafür, dass alle anderen CAN-Busstationen ebenfalls ein „Error Flag“ (sekundäres „Error Flag“) übertragen und somit ebenfalls wie der Sender des primären „Error Flags“ die Datenübertragung abbrechen.

Beim CAN-Bus schließt sich der Aussendung eines „Error Flags“ immer die Übertragung eines „Error Delimiters“ an. Dieser setzt sich aus acht rezessiven Bits zusammen. Der „Error Delimiter“ ersetzt den „ACK-Delimiter“ und den EOF-Code einer regulären Botschaftsübertragung, so dass sich zusammen mit der obligatorischen Sendepause (ITM - Intermission) auf dem CAN-Bus elf rezessive Bit ergeben (Bus-Idle-Kennung).

Dieses Verhalten kann so oder in angepasster Form auch bei einem anderen Bus eingesetzt werden, um das Busüberwachungsverfahren zu erweitern. Das geschieht so, dass, wenn ein Steuergerät einen Angriff erkannt hat, es die eingeschleuste Botschaft durch Senden des Fehler-Signals unbrauchbar macht. Alle Empfänger-Stationen verwerfen dann diese Botschaft. Die Schadbotschaft wird dadurch unmittelbar unschädlich gemacht.

Auf diese Weise kann sofort verhindert werden, daß eingeschleuste Botschaften einen Schaden anrichten können.

Die genannte Nutzdaten-Botschaft soll auch so verstanden werden, dass sie in vorteilhafterweise auch einen Steuerbefehl beinhalten kann. Das ist besonders vorteilhaft, wenn das Überwachungsverfahren bei dem sogenannten LIN-Bus eingesetzt wird, entsprechend Local Interconnect Network Bus. Dort werden die Identifizierer von Botschaften auch zur Kennzeichnung bestimmter Steuerbefehle benutzt.

Darüber hinaus können Nutzdaten in beliebiger Form enthalten sein, z.B. Sensordaten, Einstellparameter, Audiodaten, Videodaten, usw.

Die Nutzdaten-Botschaft könnte einem CAN-Bus Standard Data Frame entsprechen.

Für den Einsatz beim CAN-Bus ist es besonders vorteilhaft, wenn als Fehler-Signal, das über den CAN-Bus als Gegenmaßnahme gesendet wird, das dort für den Fehlerfall vorgesehene „Error-Flag“ gesendet wird.

Für eine elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus ist es vorteilhaft, wenn die Vorrichtung ein Überwachungsmodul aufweist, welches für die Überwachung nach den Schritten nach dem beschriebenen Überwachungsverfahren ausgelegt ist.

Ein Ausführungsbeispiel der Erfindung ist in den Zeichnungen dargestellt und wird nachfolgend anhand der Figuren näher erläutert.

Es zeigen:

- Fig. 1 das Prinzip der Vernetzung von elektronischen Komponenten mittels CAN-Bus;
- Fig. 2 ein Blockdiagramm für ein Fahrzeug-Kommunikationsnetzwerk mit Steuergeräten verschiedener Kategorie;
- Fig. 3 das Format des Standard Frame-Übertragungsrahmens beim CAN-Bus;
- Fig. 4 das Format des Remote Frame-Übertragungsrahmens beim CAN-Bus;
- Fig. 5 ein Blockschaltbild einer CAN-Bus-Schnittstelle, die mit einem Überwachungsmodul gemäß der Erfindung ausgestattet ist;
- Fig. 6 ein Flussdiagramm für ein Programm, das als Überwachungsmodul auf der CAN-Busschnittstelle installiert ist, und
- Fig. 7 ein Diagramm, das die durch einen Angreifer eingeschleusten Botschaften während der Überwachungsphase illustriert.

Die vorliegende Beschreibung veranschaulicht die Prinzipien der erfindungsgemäßen Offenbarung. Es versteht sich somit, dass Fachleute in der Lage sein werden, verschiedene Anordnungen zu konzipieren, die zwar hier nicht explizit beschrieben werden, die aber Prinzipien der erfindungsgemäßen Offenbarung verkörpern und in ihrem Umfang ebenfalls geschützt sein sollen.

Der CAN-Bus wurde schon 1994 standardisiert. Die entsprechende ISO-Norm hat die Nummer ISO 11898. Es gibt eine Norm für den Highspeed-Bereich bis 1 Mbit/s, das ist die Norm ISO 11898-2. Dann gibt es eine Norm für den Lowspeed-Bereich bis 125 kBit/s, das ist die Norm ISO 11898-3. Durch das anwachsende Datenaufkommen ergeben sich immer höhere Buslasten auf den CAN-Bussen. Dies führte zu einer Weiterentwicklung des CAN-Busses. Der erweiterte CAN-Bus ist unter dem Begriff CAN FD-Bus bekannt. FD steht dabei für Flexible Data Rate. Bei dieser CAN-Bus Variante wird die Datenrate umgeschaltet. Für die Arbitrierungsphase bleibt die Rate niedrig, wie beim klassischen CAN-Bus. Für die Übertragung der Nutzdaten wird auf eine höhere Datenrate umgeschaltet. Überträgt man die Nutzdaten einer CAN-FD-Botschaft schneller, so verkürzt sich die Dauer der Busbelegung und die Buslast verringert sich. Wenn die Übertragungsdauer im gleichen Rahmen bleibt wie bei den klassischen CAN-Botschaften, könnten größere Datenmengen mit einer CAN-FD-Botschaft transportiert werden. So wurde es auch bei CAN FD realisiert. Statt des 8 Byte langen Nutzdatenfeldes wird bei CAN FD ein 64 Byte langes Nutzdatenfeld eingesetzt. Die Datenrate steigt für die Übertragung des Nutzdatenfeldes bei einer Umsetzung z.B. von 500 kbit/s auf 2 Mbit/s an.

Es gibt beim klassischen CAN-Bus auch ein spezielles CAN Remote Frame Format. Der CAN Remote Frame wird von einer Station gesendet, um bestimmte Daten von einer anderen Station anzufordern.

Bei der nachfolgenden Beschreibung des Ausführungsbeispiels werden die Busstationen, wie im Kfz-Bereich üblich, als Steuergeräte bezeichnet. Es ist aber auch möglich, dass eine Busstation nicht als Steuergerät ausgelegt ist. Als Beispiele werden genannt bestimmte Sensoren oder Aktoren (z.B. Stellglieder), die an den Bus angeschlossen werden.

Fig. 1 zeigt das Prinzip der Vernetzung von elektronischen Komponenten mittels CAN-Bus. Ein CAN-Netzwerk ist ein Systemverbund aus CAN-Knoten (elektronische Komponenten (Steuergeräte, Sensoren, Aktoren) mit CAN-Schnittstelle), die über ihre jeweiligen CAN-Schnittstellen und einem alle CAN-Schnittstellen verbindendes Übertragungsmedium (CAN-Bus) untereinander Daten austauschen. Es sind drei CAN-Knoten 10 dargestellt. Die Busstruktur des CAN-Bus ist linear. Es gibt daher eine Busleitung 15, an die alle drei CAN-Knoten 10 angeschlossen sind. Als Busleitung 15 wird in den häufigsten Einsatzfällen eine

verdrillte, ungeschirmte Zweidrahtleitung (Unshielded Twisted Pair - UTP) genutzt, über die eine symmetrische Signalübertragung erfolgt. Bei der symmetrischen Signalübertragung werden die Signale als Spannungsdifferenzen über zwei Leitungen übertragen. Das Leitungspaar setzt sich dabei aus einer nicht invertierten CANH und einer invertierten Signalleitung CANL zusammen. Aus der Differenz der auf diesen beiden Leitern anliegenden Signale rekonstruieren die Empfänger das ursprüngliche Datensignal. Dies hat den Vorteil, dass sich Gleichtaktstörungen, die auf beiden Leitern der Busleitung 15 auftreten, durch die Differenzbildung weglöschen und sich so nicht auf die Übertragung auswirken.

Um Signalreflektionen zu vermeiden ist die Busleitung 15 an beiden Leitungsenden mit einem Abschlusswiderstand 13 der Größe des Wellenwiderstandes der Busleitung (120 Ohm) abgeschlossen.

Eine CAN-Schnittstelle setzt sich aus zwei Teilen zusammen: der Kommunikationssoftware und der Kommunikationshardware. Während die Kommunikationssoftware höhere Kommunikationsdienste umfasst, sind die grundlegenden Kommunikationsfunktionen typischerweise in Hardware implementiert: Hier werden zwei Hardware-Komponenten unterschieden: Der CAN-Controller 14 sorgt für die einheitliche Abwicklung des CAN-Kommunikationsprotokolls, und entlastet dadurch den Host 16, auf dem die bereits erwähnte Kommunikationssoftware läuft. Der CAN-Transceiver 12 sorgt für die Ankopplung des CAN-Controllers 14 an den CAN-Bus 15. Er formt die Signale für die Datenübertragung beim Sendevorgang und macht die Signalaufbereitung im Empfangsfall.

Fig. 2 zeigt den typischen Aufbau eines Kommunikationsnetzwerkes eines modernen Kraftfahrzeuges. Mit der Bezugszahl 151 ist ein Motorsteuergerät bezeichnet. Die Bezugszahl 152 entspricht einem Wählhebel-Steuergerät und die Bezugszahl 153 bezeichnet ein Getriebe-Steuergerät. Weitere Steuergeräte, wie ein zusätzliches Fahrdynamik-Steuergerät (für Fahrzeuge mit elektrisch verstellbaren Dämpfern), Airbag-Steuergerät usw., können im Kraftfahrzeug vorhanden sein. Die Vernetzung solcher Steuergeräte, die alle der Kategorie des Antriebsstrangs zugerechnet werden, geschieht typischerweise mit dem CAN-Bussystem (Controller Area Network) 104, welches als ISO Norm standardisiert ist, meist als ISO 11898-1. Für verschiedene Sensoren im Kraftfahrzeug, die nicht mehr nur an einzelne Steuergeräte angeschlossen werden sollen, ist es ebenfalls vorgesehen, dass sie an das Bussystem 104 angeschlossen werden und deren Sensordaten über den Bus zu den einzelnen Steuergeräten übertragen werden. Beispiele von Sensoren im Kraftfahrzeug sind Raddrehzahlsensoren, Lenkwinkelsensoren, Beschleunigungssensoren, Drehratensensoren, Reifendrucksensoren, Abstandssensoren, Klopfensensoren, Luftgütesensoren usw. Mit der Wählhebel-Bedienvorrichtung, die mit dem

Wählhebel-Steuergerät verbunden ist, kann der Fahrer Fahrmodi anwählen. Darunter fallen Gangwahl und Motoreinstellungen wie Sport-Modus, Normal-Modus, Allradantrieb, usw.

Das moderne Kraftfahrzeug kann aber noch weitere Komponenten aufweisen, wie Videokameras, z.B. als Rückfahrkamera oder als Fahrerüberwachungskamera. Im Kraftfahrzeug befinden sich dann auch noch weitere elektronische Vorrichtungen. Diese sind mehr im Bereich der Fahrgastzelle angeordnet und werden oft auch von dem Fahrer bedient. Beispiele sind eine Benutzerschnittstellenvorrichtung, mit der der Fahrer Einstellungen vornehmen kann, aber auch klassische Komponenten bedienen kann. Darunter fallen die Blinker-Steuerung, Scheibenwischersteuerung, Lichtsteuerung, Audioeinstellungen für das Radio, andere Einstellungen für das Autotelefon, Navigationssystem usw. Diese Benutzerschnittstellenanordnung ist mit der Bezugszahl 130 versehen. Die Benutzerschnittstellenanordnung 130 ist oft auch mit einem Dreh/Druckschalter ausgestattet, über den der Fahrer die verschiedenen Menüs anwählen kann, die auf einem Display im Cockpit angezeigt werden. Andererseits fällt auch ein berührungsempfindliches Display in diese Kategorie. Selbst die Spracheingabe für die Bedienungsunterstützung fällt in diesen Bereich.

Das Navigationssystem hat die Bezugszahl 120, welches ebenfalls im Bereich des Cockpits verbaut wird. Die Route, welche auf einer Karte angezeigt wird, kann natürlich ebenfalls auf dem Display im Cockpit dargestellt werden. Weitere Komponenten, wie eine Freisprecheinrichtung, können vorhanden sein, sind aber nicht näher dargestellt. Die Bezugszahl 110 bezeichnet noch eine On-Board Unit. Diese On-Bord Unit 110 entspricht einem Kommunikationsmodul, über das das Fahrzeug mobile Daten empfangen und senden kann. Typischerweise handelt es sich hier um ein Mobilfunk-Kommunikationsmodul, z. B. nach dem LTE-Standard. All diese Geräte sind dem Infotainment-Bereich zuzuordnen. Sie werden deshalb über ein auf die speziellen Bedürfnisse dieser Gerätekategorie ausgelegtes Bussystem 102 vernetzt. Im gezeigten Beispiel wird davon ausgegangen, dass auch das Bussystem 102 in einer Variante des CAN-Bus realisiert wurde. In Frage käme der schon erwähnte CAN FD-Bus, da dort Daten mit höherer Datenrate transportiert werden können, was für die vernetzten Steuergeräte im Infotainment-Bereich von Vorteil ist.

Oft wird für den Infotainment-Bereich ein anderes Bussystem eingesetzt. Es wird diesbezüglich auf die Bussysteme AVB (Audio Video Bridging), den MOST Bus (Media Oriented System Transport) oder den D2B Bus (Domestic Digital Bus) als Beispiel hingewiesen. Zu dem Zweck, dass fahrzeugrelevante Sensordaten über die Kommunikationsschnittstelle 110 zu einem anderen Fahrzeug oder zu einem externen Zentralrechner einer Datenbank übertragen werden sollen, ist das Gateway 140 vorgesehen. Dieses ist mit beiden verschiedenen Bussystemen 102 und 104 verbunden. Das Gateway

140 ist dazu ausgelegt, die Daten, die es über den CAN-Bus 104 empfängt, so umzusetzen, dass sie in das Übertragungsformat des Infotainment-Busses 102 umgesetzt werden, so dass sie in den dort spezifizierten Paketen verteilt werden können. Für die Weiterleitung dieser Daten nach extern, also zu einem anderen Kraftfahrzeug oder zu dem Zentralrechner, ist die On-Board-Unit 110 mit der Kommunikationsschnittstelle dazu ausgerüstet, diese Datenpakete zu empfangen und wiederum in das Übertragungsformat des entsprechend eingesetzten Mobilfunkstandards umzusetzen. Eine Umsetzung ist ebenfalls erforderlich, wenn der Bus 102 als CAN FD-Bus realisiert wird.

Wie in Fig. 2 dargestellt, wird in jedem der an den jeweiligen CAN-Bus 102, 104 angeschlossenen Steuergeräte ein Überwachungsmodul 18 vorgesehen.

Fig. 3 zeigt das Botschaftsformat eines CAN Standard Frames. Genauer gesagt, veranschaulicht Fig. 3 ein CAN-Übertragungsrahmenformat gemäß dem CAN-Kommunikationsstandard.

Es sind viele verschiedene einzelne Bits im Übertragungsrahmen nach ISO 11898-1 vorhanden, die Steuerungszwecke erfüllen. Die verschiedenen Felder und Steuerungsbits des Übertragungsrahmens sind mit ihrer Bezeichnung in englischer Sprache in der folgenden Tabelle aufgelistet. Ebenfalls wird die Länge der einzelnen Felder angegeben. Bei der nachfolgenden Erwähnung dieser Bits wird die ausführliche Bezeichnung nicht mehr wiederholt.

Control Bit	Ausführliche Bezeichnung	Länge
SOF	Start of Frame	1 Bit
Identifier	Identifier	9 Bits
RTR	Remote Transmission Request	1 Bit
IDE	Identifier Extension	1 Bit
r	Reserved Bit	1 Bit
DLC	Data Length Code	4 Bit
Data Field	Data Field	0-8 Bytes
CRC	CRC Sequence	
DEL	CRC Delimiter	1 Bit
ACK	Acknowledge	1 Bit
DEL	ACK Delimiter	1 Bit
EOF	End of Frame Code	4 Bit

Ein CAN-Frame enthält ein Start-of-Frame (SOF) -Feld, ein Arbitrationsfeld, ein Steuerfeld, ein Datenfeld, ein Cyclic Redundancy Check (CRC) Feld, ein ACK-Feld, ein End-of-Frame (EOF) und eine Intermission Sequence (ITM) Feld.

Gemäß einer beispielhaften Ausführungsform der Erfindung ist das SOF-Feld ein Feld, das den Beginn eines CAN-Rahmens anzeigt, d.h. den Beginn einer Nachricht. Das Arbitrierungsfeld identifiziert eine Nachricht und weist der Nachricht eine Priorität zu. Gemäß der Länge eines in dem Arbitrierungsfeld zugeordneten Identifikationsfeldes wird der CAN-Rahmen in ein Standardformat und ein erweitertes Format aufgeteilt (gezeigt ist das Standardformat). Im Standardformat hat das Arbitrierungsfeld eine Länge von 11 Bits. Für das erweiterte Format beträgt die Länge des Identifikationsfeldes im Arbitrierungsfeld 29 Bits.

Der Identifizierer legt die Priorität des Datenrahmens fest und sorgt zusammen mit der Akzeptanzfilterung für die in der Kommunikationsmatrix definierten Sender-Empfänger-Relationen im CAN-Netzwerk. In der Kommunikationsmatrix ist für jedes Steuergerät festgelegt, welche Botschaften es verarbeitet. Wenn also eine Botschaft eingeht, dessen Botschafts-Identifizierer nicht dort aufgelistet ist, wird diese Botschaft durch die Akzeptanzfilterung aussortiert und nicht an die Applikation weitergeleitet.

Mittels des RTR-Bit teilt die Sendestation den Empfängern den Frametyp (Data Frame oder Remote Frame) mit. Ein dominantes RTR-Bit zeigt einen Data Frame an, entsprechend ein rezessives Bit den Remote Frame. Zusätzlich kann das Arbitrierungsfeld ein Identifikationserweiterungsfeld (IDE) mit einer Länge von 1 Bit enthalten, um zu identifizieren, ob ein Rahmen das Standardformat oder das erweiterte Format hat. Wenn der Wert des IDE-Feldes 0 ist, zeigt dies das Standardformat an. Wenn der Wert 1 ist, bedeutet dies das erweiterte Format.

In dem DLC-Feld wird den Empfängern die Anzahl der in der Botschaft enthaltenen Nutzdaten-Bytes angezeigt. Transportiert werden die Nutzdaten-Bytes im Data Field. Maximal können mit einem Data Frame acht Nutzdaten-Bytes übertragen werden. Gegen Übertragungsfehler werden die Nutzdaten-Bytes mithilfe einer im CRC-Feld übertragenen Prüfsumme unter Anwendung des Cyclic Redundancy Checks abgesichert.

Ausgehend vom Ergebnis des CRC Checks quittieren die Empfänger im ACK-Slot positiv oder negativ den Empfang. Dabei wird ein ACK-Bit am Ende der Nachricht durch die CAN-Controller übertragen, die die Nachricht genau empfangen haben. Der Knoten, der die Nachricht gesendet hat, prüft, ob das ACK-Bit auf dem CAN-Bus vorhanden ist oder nicht.

Wenn ACK nicht gefunden wird, ist dies ein Indiz, dass ein Knoten die Nachricht nicht korrekt empfangen konnte und die Sendestation kann eine erneute Übertragung versuchen.

Beendet wird die Übertragung eines Daten-Rahmens mit sieben rezessiven Bits, das entspricht dem End Of Frame Code EOF.

Fig. 4 zeigt noch das Botschaftsformat eines CAN Remote Frames. Mit dem Remote Frame kann ein Steuergerät gewünschte Nutzdaten anfordern, wenn diese nicht sowieso zyklisch gesendet werden. Bei Anwendungen im Automobil kommt dieser Rahmentyp kaum zur Anwendung, da dort die Datenübertragung nicht auf Nachfrage, sondern im Wesentlichen zyklisch erfolgt.

Bis auf das fehlende Datenfeld entspricht der Aufbau des Remote Frames dem des Data Frames. Die Unterscheidung zwischen Data und Remote Frame erfolgt mittels des RTR-Bit. Im Falle eines Data Frames wird das RTR-Bit dominant gesendet. Ein Remote Frame ist durch ein rezessives RTR-Bit gekennzeichnet.

Prinzipiell können für alle existierenden Data Frames im CAN-Netzwerk entsprechende Remote Frames definiert werden. Dazu hat man nur darauf zu achten, dass die Identifier der Remote Frames den Identifier der assoziierten Data Frames entsprechen. Sobald ein CAN-Knoten einen Remote Frame empfängt, dessen Identifier mit einem Identifier in der eigenen Kommunikationsmatrix identisch ist, antwortet er mit dem entsprechenden Standard Frame.

Die Fig. 5 zeigt jetzt die Implementierung des Überwachungsmoduls 18 in Form eines Softwaremoduls. Mit der Bezugszahl 1510 ist die CAN-Schnittstelle des Motor-Steuergerätes 151 bezeichnet. Diese besteht aus den Hardware-Komponenten CAN-Controller 1513 und CAN-Transceiver (nicht dargestellt) und aus den beiden Softwarekomponenten Applikations-Software 1511 und dem Überwachungsmodul 1518. Zwischen beiden Software-Komponenten gibt es eine Schnittstelle 1514. Die CAN-Botschaften, die über den CAN-Bus ein- und ausgehen, stehen auf der entsprechenden Leitung 1516 an.

Die Arbeitsweise des Überwachungsmoduls 1518 wird jetzt mit Hilfe des Flussdiagramms in Fig. 6 und der Fig. 7 erläutert.

Das Überwachungsmodul 1518 wird immer dann aktiv, wenn die CAN-Schnittstelle im Empfangsbetrieb arbeitet. Oft sendet ein Steuergerät seine Daten zyklisch auf den Bus. Dazu wird für jeden Zyklus im Steuergerät ein entsprechender Timer eingerichtet. Verschiedene Nutzdaten können mit verschiedenen Zyklen gesendet werden. Die

Applikationssoftware 1511 übernimmt die Einrichtung der verschiedenen Timer. Es kann sich um Software-unterstützte Timer oder Hardware-unterstützte Timer handeln (nicht dargestellt). Im Bereich der Steuergeräte des Antriebsstrangs werden üblicherweise Mikrocontroller eingesetzt, die mit einer programmierbaren Timer/Counter-Einheit ausgestattet sind, so dass die Timer hier oft Hardware-unterstützt sind. Bei Ablauf eines Timers wird ein Interrupt ausgelöst, wodurch das Steuergerät vom Empfangsbetrieb in den Sendebetrieb wechselt. Jedes Mal nach Durchführung des Sendebetriebs wechselt das Steuergerät wieder zurück in den Empfangsbetrieb. Dies kann durch Setzen eines Flags im Steuergerät signalisiert werden. Das Setzen dieses Flags wird dann den Start des Überwachungsmoduls auslösen. Daneben gibt es aber auch eine Reihe von anderen Sendarten bei Steuergeräten. Als Beispiele werden die Sendarten (ifActiv, ifAcitivWithRepetition, OnChange, OnChangeWithRepetition) genannt, die nur im Normal-/Ruhezustand zyklisch senden. Tritt ein bestimmtes, definiertes Ereignis ein, z.B. die Änderung eines Sensorwertes, dann werden die Daten außerhalb des Normalzyklus häufig mit einer schnelleren Zykluszeit versendet.

Der Start des Überwachungsprogramms ist in Fig. 6 mit der Bezugszahl 181 bezeichnet. Im Schritt 182 überprüft das Programm jede empfangene Botschaft ähnlich wie bei der Akzeptanzfilterung darauf, ob diese Botschaft mit einem Botschaftsidentifizierer gekennzeichnet ist, der selbst in der stationseigenen Sendetabelle 1515 verzeichnet wurde. In der stationseigenen Sendetabelle 1515 sind alle Botschaftsidentifizierer aufgelistet, die bei der Aussendung von Nutzdaten benutzt werden. Diese Sendetabelle 1515 kann als Teil der stationseigenen Kommunikationsmatrix angesehen werden.

Wenn ein Botschaftsidentifizierer empfangen wurde, der nicht in der Sendetabelle 1515 aufgelistet ist, verzweigt das Programm zum Anfang. Wenn ein Botschaftsidentifizierer empfangen wurde, der in der Sendetabelle 1515 aufgelistet ist, kann es sich um eine Botschaft handeln, die von einem Angreifer auf dem Bus eingeschleust wurde. Es könnte sich allerdings auch um einen Remote Frame handeln, der von einem anderen Steuergerät gesendet wurde. Deshalb wird noch im Schritt 183 überprüft, ob es sich um einen Remote Frame handelt. Dies kann, wie zuvor erläutert, an dem RTR-Bit erkannt werden. Handelt es sich um einen Remote Frame, wird das Überwachungsmodul im Schritt 185 beendet. Wenn es sich nicht um einen Remote Frame handelt, dann kann die Botschaft gefährlich sein, weil sie dann mit Nutzdaten kommt. Dann steht auch für das Überwachungsmodul fest, dass es sich um eine irreguläre Botschaft handelt. Wegen des eingangs erwähnten Eindeutigkeitsprinzips, welches für den CAN-Bus gilt, darf ja kein anderes Steuergerät denselben Botschaftsidentifizierer bei Aussendung seiner Botschaften verwenden. Deshalb werden dann im nächsten Schritt 184 die Gegenmaßnahmen eingeleitet. Als Gegenmaßnahme kommen verschiedene Maßnahmen in Betracht. Dazu gehören

beispielsweise das Ansteuern der Alarmanlage, das Einschalten von Warnlichtern, das Absetzen einer Manipulationsmeldung über Funk an einen Zentralrechner des Autoherstellers oder einer Behörde oder an ein Smartphone des Fahrzeughalters, das Abspeichern von Ort, Datum, Zeit des Manipulationsereignisses in einem Speicher, das Sperren der Zündung für eine bestimmte Zeit usw.

Fig. 7 zeigt jetzt noch das Prinzip des Überwachungsverfahrens. Gleiche Bezugswahlen bezeichnen dieselben Komponenten, wie zuvor erläutert. Der Angreifer ist in Fig. 7 mit der Bezugswahl 157 gekennzeichnet. In dem Beispiel hat er sich mit einem entsprechenden Werkzeug an den CAN-Bus 104 aufgeschaltet. Dies gelingt in einer Werkstatt sicherlich problemlos, trotzdem, dass der CAN-Bus oft an unzugänglicher Stelle im Fahrzeug verlegt wird. Es gibt aber in der Regel bestimmte Stellen am Fahrzeug, wo der CAN-Bus zugänglich ist. Im unteren Teil der Fig. 7 ist ein Zyklus dargestellt, mit dem das Motorsteuergerät 151 eine Botschaft ECM auf den Bus sendet. Zur jeweiligen Sendephase ist das Überwachungsmodul 1518 nicht aktiv. In den markierten Phasen MP findet die Überwachung des Busverkehrs statt. Bei der zweiten Phase MP treten weitere ECM-Botschaften auf. Da diese denselben Botschafts-Identifizierer benutzen, der für das Steuergerät 151 reserviert ist, werden sie vom Überwachungsmodul als irregulär erkannt, wie oben beschrieben. Das Motor-Steuergerät 151 leitet daraufhin, wie beschrieben, Gegenmaßnahmen ein.

Die Offenbarung ist nicht auf die hier beschriebenen Ausführungsbeispiele beschränkt. Es gibt Raum für verschiedene Anpassungen und Modifikationen, die der Fachmann aufgrund seines Fachwissens als auch zu der Offenbarung zugehörend in Betracht ziehen würde.

Das beschriebene Überwachungsverfahren ließe sich auch bei anderen Bussystemen als dem CAN-Bus einsetzen. Besonders erwähnt wird noch der LIN Bus (Local Interconnect Bus) als Beispiel. Bei dem LIN-Bus handelt es sich aber um einen Master/Slave-Bus bei dem im Botschaftsformat ebenfalls ein Identifizierer vorgesehen ist, der aber auch einen bestimmten Steuerbefehl kennzeichnen kann.

Alle hierin erwähnten Beispiele wie auch bedingte Formulierungen sind ohne Einschränkung auf solche speziell angeführten Beispiele zu verstehen. So wird es zum Beispiel von Fachleuten anerkannt, dass das hier dargestellte Blockdiagramm eine konzeptionelle Ansicht einer beispielhaften Schaltungsanordnung darstellt. In ähnlicher Weise ist zu erkennen, dass ein dargestelltes Flussdiagramm, Zustandsübergangsdiagramm, Pseudocode und dergleichen verschiedene Varianten zur Darstellung von Prozessen darstellen, die im Wesentlichen in computerlesbaren Medien gespeichert und somit von einem Computer oder Prozessor ausgeführt werden können.

Es sollte verstanden werden, dass das vorgeschlagene Verfahren und die zugehörigen Vorrichtungen in verschiedenen Formen von Hardware, Software, Firmware, Spezialprozessoren oder einer Kombination davon implementiert werden können. Spezialprozessoren können anwendungsspezifische integrierte Schaltungen (ASICs), Reduced Instruction Set Computer (RISC) und / oder Field Programmable Gate Arrays (FPGAs) umfassen. Vorzugsweise wird das vorgeschlagene Verfahren und die Vorrichtung als eine Kombination von Hardware und Software implementiert. Die Software wird vorzugsweise als ein Anwendungsprogramm auf einer Programmspeichervorrichtung installiert. Typischerweise handelt es sich um eine Maschine auf Basis einer Computerplattform, die Hardware aufweist, wie beispielsweise eine oder mehrere Zentraleinheiten (CPU), einen Direktzugriffsspeicher (RAM) und eine oder mehrere Eingabe/Ausgabe (I/O) Schnittstelle(n). Auf der Computerplattform wird typischerweise außerdem ein Betriebssystem installiert. Die verschiedenen Prozesse und Funktionen, die hier beschrieben wurden, können Teil des Anwendungsprogramms sein oder ein Teil, der über das Betriebssystem ausgeführt wird.

Bezugszeichenliste

10	CAN-Knoten
12	CAN-Transceiver
13	Abschlusswiderstand
14	CAN-Controller
15	Busleitung
16	Host
18	Überwachungsmodul
100	Kfz-Elektronik
102	Infotainment-CAN-Bus
104	CAN-Bus
110	On-Board Unit
120	Navigationssystem
130	Bedienungseinheit
140	Gateway
151	Motor-Steuergerät
152	ESP-Steuergerät
153	Getriebe-Steuergerät
157	Angreifer
181	Programmstart
182	Vergleich Botschafts-ID mit Sendetabelle
183	Prüfung auf Remote Frame
184	Gegenmaßnahmen
185	Programmende
1510	Architektur CAN-Busschnittstelle
1511	Applikations-Software
1512	1. Schnittstelle
1513	CAN-Controller
1514	2. Schnittstelle
1515	Sendetabelle
1516	3. Schnittstelle
1518	Überwachungsmodul
ECM	eine Botschaft des Motorsteuergeräts
MP	Überwachungsphase

Patentansprüche

1. Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus (104), wobei durch den Kommunikationsbus (104) eine Anzahl von elektronischen Stationen (51, 52, 53) vernetzt sind,
wobei der Kommunikationsbus (104) nach einer Variante der Familie der CAN-Bus Standards, entsprechend Controller Area Network, ausgelegt wird,
wobei die über den Kommunikationsbus (104) übertragenen Botschaften mit einem Identifizierer gekennzeichnet sind, wobei für jede Station (51, 52, 53) festgelegt wird, welche Botschaften mit welchem Identifizierer von ihr gesendet werden dürfen,
wobei eine Eindeutigkeitsregel eingehalten wird, die verbietet, dass eine andere Station (52, 53) eine Nutzdaten-Botschaft mit einem Identifizierer versendet, der schon für diese Station (51) reserviert ist,
wobei in einer oder mehreren oder allen der elektronischen Stationen (51, 52, 53) ein Überwachungsmodul (18, 1518) vorgesehen wird, das überwacht, ob auf dem Kommunikationsbus (104) eine Nutzdaten-Botschaft von einer anderen Station (52, 53) gesendet wird mit einem Identifizierer, der für die eigene Station (51) reserviert ist
wobei im Falle des Erkennens einer CAN-Bus Remote Frame Botschaft mit einem Botschafts-Identifizierer, der für die Station (51) reserviert ist, von dem Überwachungsmodul (18, 1518) kein unberechtigter Buszugriff angenommen wird und keine Gegenmaßnahme eingeleitet werden.
2. Verfahren nach Anspruch 1, wobei das Überwachungsmodul (18, 1518) für die Überwachung auf eine Sendetabelle (1515) zugreift, in der alle der für die Station (51) reservierten Identifizierer verzeichnet sind und den Identifizierer einer empfangenen Botschaft mit den Einträgen in der Sendetabelle (1515) vergleicht.
3. Verfahren nach Anspruch 1 oder 2, wobei bei Übereinstimmung des Identifizierers der empfangenen Nutzdaten-Botschaft (ECM) mit einem Eintrag in der Sendetabelle (1515) von dem Überwachungsmodul (18, 1518) ein unberechtigter Buszugriff festgestellt wird und Gegenmaßnahmen eingeleitet werden.
4. Verfahren nach Anspruch 3, wobei während des Zustandes, in dem die Station (51) selbst eine Botschaft über den Kommunikationsbus (104) sendet, die Durchführung der Gegenmaßnahme unterdrückt wird.
5. Verfahren nach Anspruch 4, wobei die Durchführung der Gegenmaßnahme dadurch unterdrückt wird, dass das Überwachungsmodul (18, 1518) während des Zustandes, in dem die Station (51) selbst eine Botschaft über den Kommunikationsbus (104) sendet,

inaktiv geschaltet wird und während des Zustandes, wo es Botschaften von dem Kommunikationsbus (104) empfängt, aktiv geschaltet wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Kommunikationsbus (104) für den Austausch von Botschaften zwischen elektronischen Komponenten eines Fahrzeuges ausgelegt wird.
7. Verfahren nach einem der Ansprüche 3 bis 6, wobei als Gegenmaßnahmen eine oder mehrere der folgenden Maßnahmen durchgeführt werden:
 - Ausgeben einer Warnung des Fahrzeugführers mit einem optischen, akustischen oder haptischen Signal
 - Einschalten der Alarmanlage
 - Absetzen einer Manipulationsmeldung über Funk an einen Zentralrechner des Autoherstellers oder einer Behörde oder an ein Smartphone des Fahrzeughalters,
 - Abspeichern von Ort, Datum, Zeit des Manipulationsereignisses in einem Speicher
 - Blockieren des Schlüssels, mit dem das Fahrzeug eingeschaltet wurde.
8. Verfahren nach einem der Ansprüche 3 bis 7, wobei als Gegenmaßnahme von der Station, die einen unberechtigten Buszugriff feststellt, ein Fehler-Signal über den Bus gesendet wird, wodurch die aktuell übertragene Botschaft als ungültig erklärt wird.
9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nutzdaten-Botschaft einen Steuerbefehl beinhaltet.
10. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Identifizierer einem CAN-Bus Botschafts-Identifizierer entspricht.
11. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nutzdaten-Botschaft einem CAN-Bus Standard Data Frame entspricht.
12. Verfahren nach Anspruch 8, wobei das Fehler-Signal, das über den CAN-Bus als Gegenmaßnahme gesendet wird, einem „Error-Flag“ gemäß CAN-Bus-Protokoll entspricht.
13. Elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus (104), dadurch gekennzeichnet, dass die Vorrichtung ein Überwachungsmodul (18, 1518) aufweist, das für die Überwachung nach den Schritten nach einem der vorhergehenden Ansprüche ausgelegt ist.

1/4

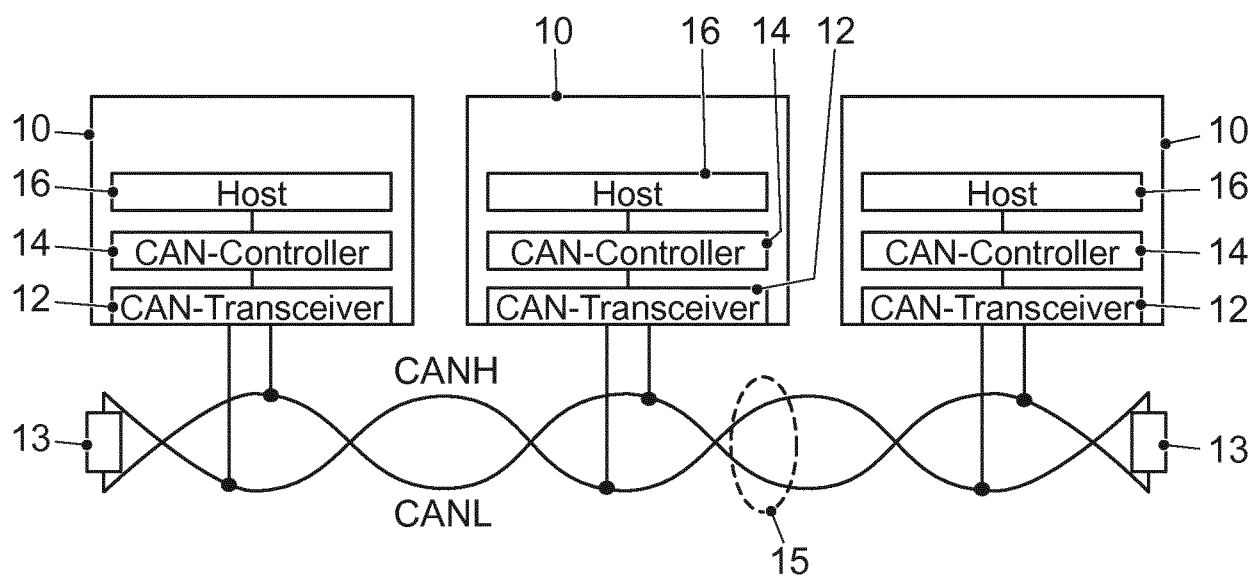


FIG. 1

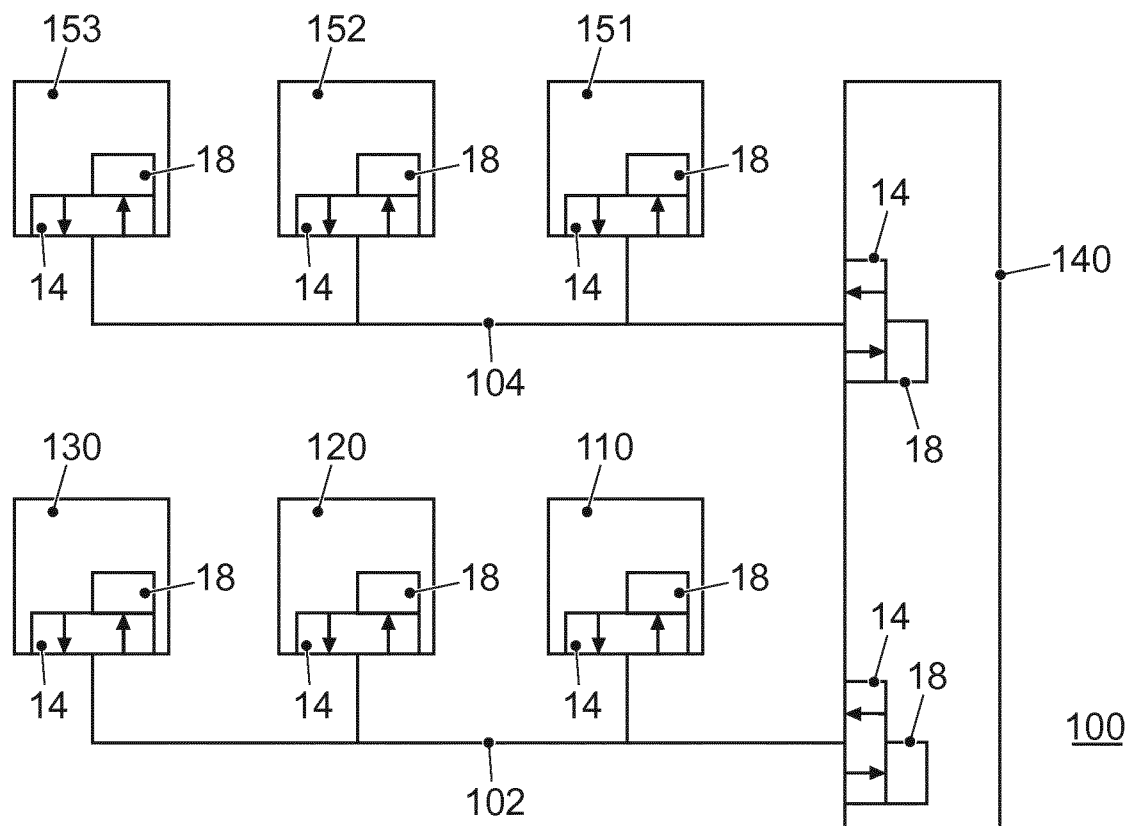


FIG. 2

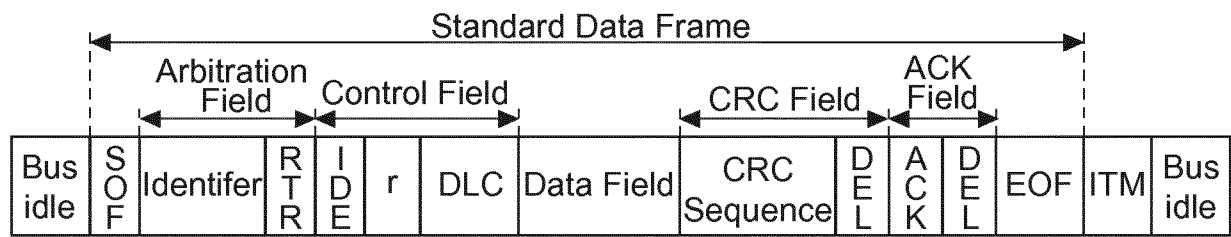


FIG. 3

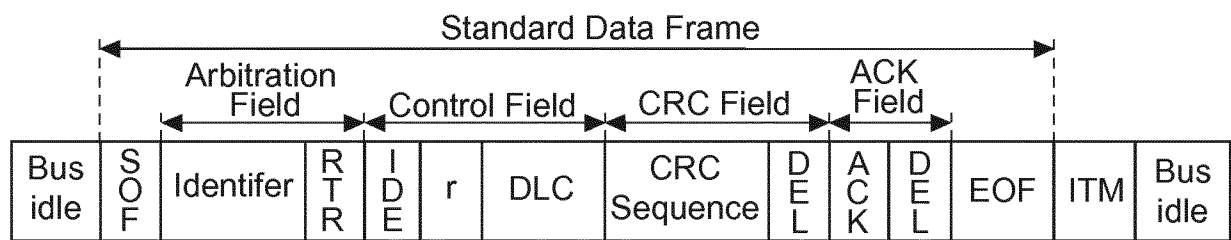


FIG. 4

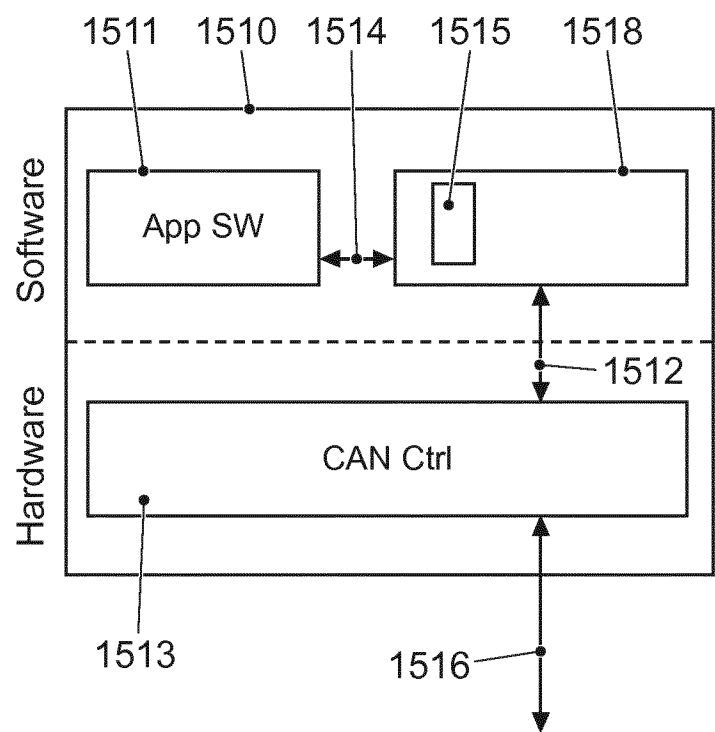


FIG. 5

3/4

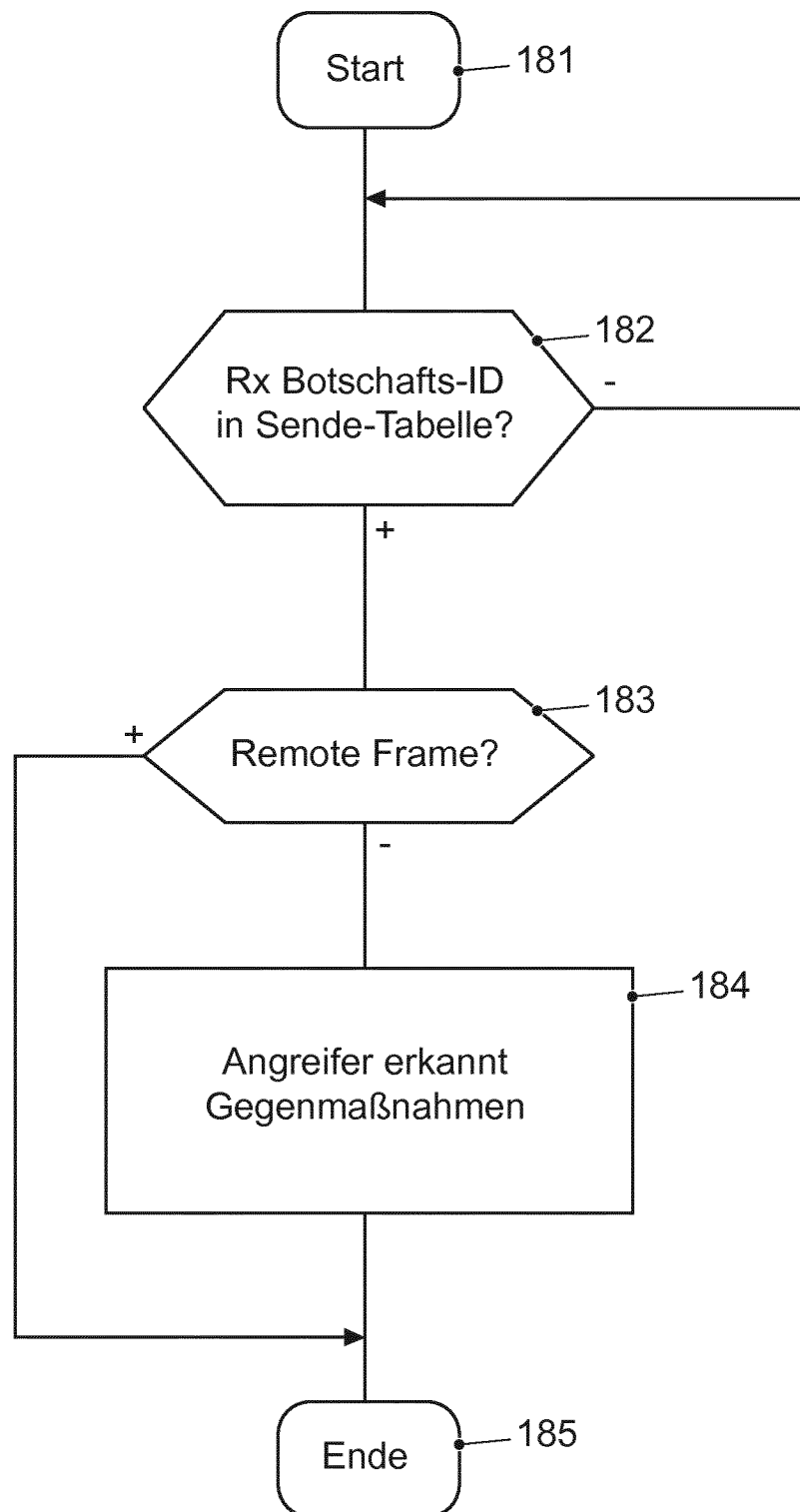


FIG. 6

4/4

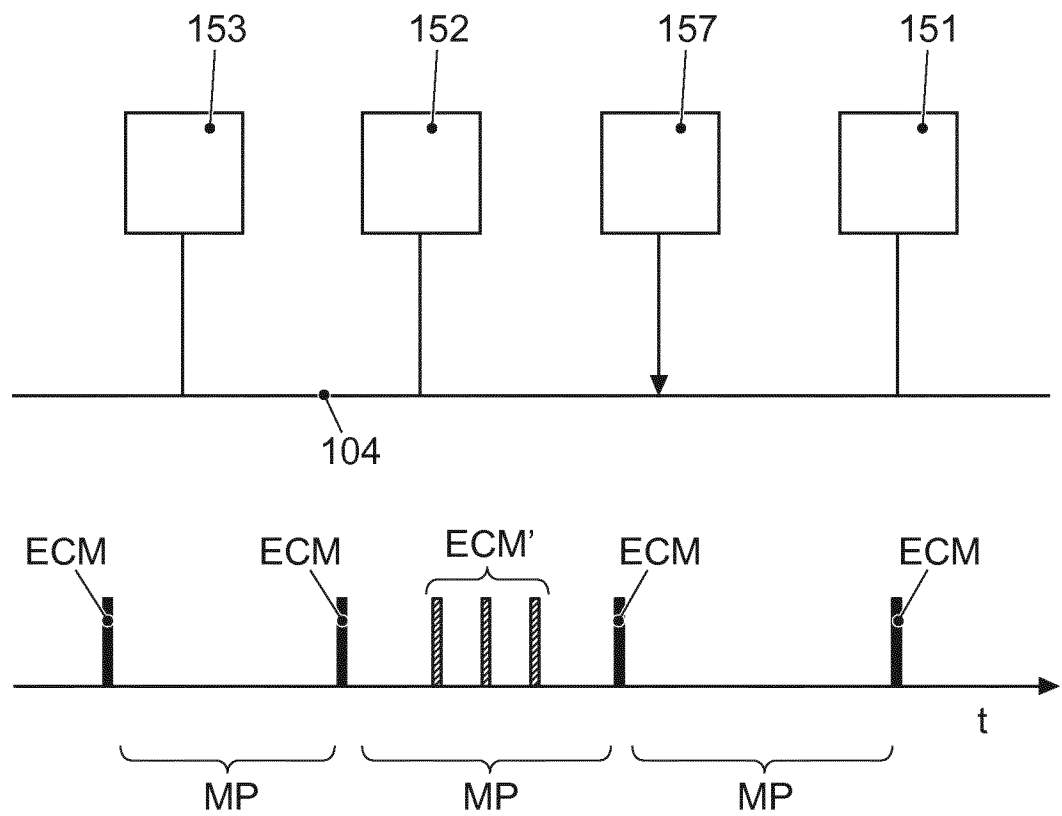


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2018/075586

A. CLASSIFICATION OF SUBJECT MATTER <i>H04L 12/40</i> (2006.01)i; <i>H04L 29/06</i> (2006.01)i; <i>H04L 12/26</i> (2006.01)n 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 A	EP 3148154 A1 (NXP BV [NL]) 29 March 2017 (2017-03-29) figures 1,3a,3b,4a,4b,5,7 paragraph [0001] paragraph [0038] paragraph [0039] paragraph [0040] paragraph [0041] paragraph [0043]	1-6,8-13 7		
A	DE 112014003345 T5 (YAZAKI CORP [JP]) 21 April 2016 (2016-04-21) paragraph [0009] - paragraph [0010] paragraph [0023] - paragraph [0027] figures 1,3a-3b, 4a-4c	1-13		
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> * 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 </td> <td style="width: 50%; vertical-align: top;"> "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 </td> </tr> </table>			* 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
* 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 20 November 2018		Date of mailing of the international search report 30 November 2018		
Name and mailing address of the ISA/EP European Patent Office p.b. 5818, Patentlaan 2, 2280 HV Rijswijk Netherlands Telephone No. (+31-70)340-2040 Facsimile No. (+31-70)340-3016		Authorized officer Nold, Michael Telephone No.		

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2018/075586

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TSUTOMU MATSUMOTO ET AL. "A Method of Preventing Unauthorized Data Transmission in Controller Area Network" <i>2012 IEEE 75TH VEHICULAR TECHNOLOGY CONFERENCE (VTC SPRING 2012) : YOKOHAMA, JAPAN, 6 - 9 MAY 2012, IEEE, PISCATAWAY, NJ,</i> 06 May 2012 (2012-05-06), pages 1-5 DOI: 10.1109/VETECS.2012.6240294 ISBN: 978-1-4673-0989-9. XP032202711 the whole document	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2018/075586

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
EP	3148154	A1	29 March 2017	EP	3148154	A1	29 March 2017
				US	2017093659	A1	30 March 2017
DE	112014003345	T5	21 April 2016	DE	112014003345	T5	21 April 2016
				JP	6099269	B2	22 March 2017
				JP	2015020613	A	02 February 2015
				US	2016368457	A1	22 December 2016
				WO	2015008833	A1	22 January 2015

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. H04L12/40 H04L29/06
 ADD. H04L12/26

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	EP 3 148 154 A1 (NXP BV [NL]) 29. März 2017 (2017-03-29)	1-6,8-13
A	Abbildungen 1,3a,3b,4a,4b,5,7 Absatz [0001] Absatz [0038] Absatz [0039] Absatz [0040] Absatz [0041] Absatz [0043]	7
A	DE 11 2014 003345 T5 (YAZAKI CORP [JP]) 21. April 2016 (2016-04-21) Absatz [0009] - Absatz [0010] Absatz [0023] - Absatz [0027] Abbildungen 1,3a-3b, 4a-4c ----- -/-	1-13



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

20. November 2018

Absendedatum des internationalen Recherchenberichts

30/11/2018

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

Nold, Michael

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	TSUTOMU MATSUMOTO ET AL: "A Method of Preventing Unauthorized Data Transmission in Controller Area Network", 2012 IEEE 75TH VEHICULAR TECHNOLOGY CONFERENCE (VTC SPRING 2012) : YOKOHAMA, JAPAN, 6 - 9 MAY 2012, IEEE, PISCATAWAY, NJ, 6. Mai 2012 (2012-05-06), Seiten 1-5, XP032202711, DOI: 10.1109/VETECS.2012.6240294 ISBN: 978-1-4673-0989-9 das ganze Dokument -----	1-13

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2018/075586

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 3148154 A1	29-03-2017	EP 3148154 A1	29-03-2017
		US 2017093659 A1	30-03-2017

DE 112014003345 T5	21-04-2016	DE 112014003345 T5	21-04-2016
		JP 6099269 B2	22-03-2017
		JP 2015020613 A	02-02-2015
		US 2016368457 A1	22-12-2016
		WO 2015008833 A1	22-01-2015
