(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
24. September 2020 (24.09.2020)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2020/187985 A1

(51) Internationale Patentklassifikation:
H04L 12/413 (2006.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2020/057450

(22) Internationales Anmeldedatum:
18. März 2020 (18.03.2020)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2019 001 978.4
21. März 2019 (21.03.2019) DE

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

(72) Erfinder: **KAMP, Birger**; Zur Diwelie 23, 38531 Rötgesbüttel (DE). **BUNIMOV, Viktor**; Hornkampsweg 14, 38159 Vechelde (DE). **KOCVEROVA, Jana**; Piskova Lhota 36, 29431 Krnsko (CZ). **BRABEC, Jan**; Zimova 623/7, 14200 Praha 4 (CZ).

(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, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

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

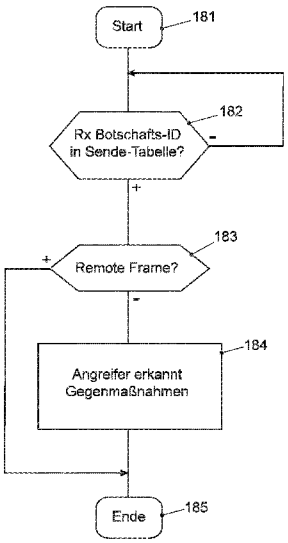

FIG. 7

181 Start
182 Rx message ID in transmit table?
183 Remote Frame?
184 Attacker recognized Countermeasures
185 End

(57) **Abstract:** The invention relates to a monitoring method for a communication bus (104). Said method is used to detect unauthorised bus accesses. According to the method, a station connected to the communication bus (104) is provided with a monitoring module (1517). During the method, the messages are identified by means of an identifier, it being determined for each station (140-163) which messages said station can send with which identifier. According to a uniqueness rule to this effect, it is prohibited for another station (152, 153) to send a payload message with an identifier that is already reserved for this station (151). This rule is used during monitoring so as to monitor whether a payload message with an identifier reserved for a specific station (151) is sent by another station (152, 153) on the communication bus (104). If so, unauthorised bus access is detected. One or more of the following countermeasures are then initiated: the infiltrated message is rendered unusable by clobbering the message with the dominant level, by clobbering the message with a specific bit pattern, by deliberately changing a specific message part, such as the CRC field of the message, or by placing an information entry in an additional field of the transmitted messages; and/or another electronic station (140 - 163) is warned by transmitting implausible data contents in one or more subsequent messages or by transmitting a warning in one or more dedicated warning messages.

(57) **Zusammenfassung:** Die Erfindung betrifft ein Überwachungsverfahren für einen Kommunikationsbus (104). Damit werden unberechtigte Buszugriffe festgestellt. Das Verfahren beinhaltet, dass ein Überwachungsmodul (1517) bei einer an den Kommunikationsbus (104) angeschlossenen Station vorgesehen wird. Bei dem Verfahren werden die Botschaften durch einen Identifizierer gekennzeichnet, wobei für jede Station (140 - 163) 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 (152, 153) eine Nutzdaten-Botschaft mit einem Identifizierer versendet, der schon für diese Station (151) reserviert ist. Diese Regel wird bei der Überwachung ausgenutzt, derart, dass überwacht wird, ob auf dem Kommunikationsbus (104) eine Nutzdaten-Botschaft mit einem

WO 2020/187985 A1

[Fortsetzung auf der nächsten Seite]

(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)*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

Identifizierer von einer anderen Station (152, 153) gesendet wird, der für die eigene Station (151) reserviert ist. Wenn ja, wurde ein unberechtigter Buszugriff erkannt. Es wird dann eine oder mehrere der folgenden Gegenmaßnahmen eingeleitet: Unbrauchbarmachen der eingeschleusten Botschaft durch Überschreiben der Botschaft mit dem dominanten Pegel, durch Überschreiben der Botschaft mit einem bestimmten Bit-Muster, durch das gezielte Verändern eines bestimmten Botschaftsteils, wie das CRC-Feld der Botschaft, oder durch das Setzen eines Informationseintrages in einem zusätzlichen Feld der gesendeten Botschaften; und/oder Warnen einer anderen elektronischen Station (140 - 163) durch Senden von unplausiblen Dateninhalten in einer oder mehreren folgenden Botschaften, oder durch Senden einer Warnung in einer oder mehreren dedizierten Warn-Botschaften.

Beschreibung

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

Die Erfindung betrifft das technische Gebiet der Überwachung der Kommunikation auf einem Kommunikationsbus hinsichtlich unberechtigter 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, Klimaanlagen-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.

Dem Schutz von Bussystemen in Kraftfahrzeugen kommt eine immer stärkere Bedeutung zu. Gerade automatisierte Funktionen und/oder Fahrzeuge benötigen einen wirksamen Schutz vor Angriffen. Ungeschützte oder ungenügend geschützte Systeme können manipuliert werden und stellen eine potenzielle Gefahr für Fahrzeuginsassen und Umwelt dar.

Im Folgenden werden Verfahren und Methoden beschrieben, um verdächtige Botschaften unbrauchbar zu machen, entsprechend zu kennzeichnen, sowie Verfahren, wie betroffene Steuergeräte über einen erkannten Angriff unterrichtet werden können, und die Reaktion betroffener Steuergeräte.

Neben der Erkennung und der Identifizierung eingeschleuster Botschaften sind die beteiligten Steuergeräte von einem Vorfall zu informieren. Dies kann durch das Markieren und/oder Zerstören derartiger Botschaften sowie durch das Versenden einer neuen Botschaft (Warnbotschaft) erfolgen. Diese Empfänger-Steuergeräte müssen entsprechend reagieren und, falls erforderlich, in einen sicheren Zustand übergehen, um weitere Risiken für die Insassen und die Umwelt zuverlässig zu vermeiden. Dabei kann eine sinnvolle Balance zwischen Absicherung und Verfügbarkeit erreicht werden, indem je nach Bedarf verschiedene Datenbereiche gezielt überschrieben werden.

Grundlage für die Identifizierung eingeschleuster Botschaften ist ein dezentrales Erkennungssystem. Im Idealfall kann in jedem Steuergerät ein Überwachungsmodul implementiert werden, das Alarm schlägt, wenn Botschaften mit einem Can-Identifizierer auftreten, die dem eigenen Steuergerät zugeordnet sind. Empfängt das Überwachungsmodul Botschaften mit einem Can-Identifizierer, die nur vom eigenen Steuergerät verwendet werden, so ist das ein Hinweis auf einen Angriff. Dies bedeutet, dass ein anderes Steuergerät Botschaften versendet, die dem Steuergerät mit dem Überwachungsmodul vorbehalten sind. Es kann sich dabei um ein manipuliertes Seriensteuergerät oder um zusätzlich verbaute Hardware handeln. Ein weiterer Aspekt besteht in der Fehlerbehandlung, z.B. der Erkennung fehlerhaft programmierter Steuergeräte.

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. So gibt es für unterschiedliche Nachrichtentypen jeweils angepasste Überprüfungsaspekte.

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.

Aus der EP 3 148 154 B1 ist bei einer CAN-Busstation ein Überwachungsmodul bekannt, mit dem überprüft wird, ob der Identifizierer einer empfangenen CAN-Botschaft mit einem für die Busstation reservierten Identifizierer übereinstimmt. Dadurch wird überprüft, ob die bei dem CAN-Bus gültige Eindeutigkeitsregel für CAN-Botschaften-Identifizierer verletzt wird. Wenn die Verletzung der Eindeutigkeitsregel festgestellt wurde, wird auf einen Angriff von außen auf das Bussystem geschlossen und es wird die empfangene CAN-Botschaft, die die Eindeutigkeitsregel verletzt, noch während des Empfangs für ungültig erklärt. Dies geschieht durch Senden eines Error Flags in dem End of Frame-Feld der empfangenen CAN-Botschaft.

Die Erfindung setzt sich zum Ziel, ein wirkungsvolles Überwachungsverfahren für einen Kommunikationsbus anzugeben, das zuverlässig unberechtigte Buszugriffe erkennen kann und verhindert, dass die manipulierten Botschaften Schaden anrichten können.

Diese Aufgabe wird durch ein Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus gemäß Anspruch 1 sowie eine elektronische Vorrichtung gemäß Anspruch 13 und 14 und ein Fahrzeug 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. Bei dem Verfahren wird in einer oder mehreren oder allen der elektronischen Stationen ein Überwachungsmodul vorgesehen, 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. In dem Fall wird eine oder mehrere Gegenmaßnahmen eingeleitet. Die Gegenmaßnahmen bestehen in dem

Unbrauchbarmachen der eingeschleusten Botschaft durch Überschreiben der Botschaft mit dem dominanten Pegel, durch Überschreiben der Botschaft mit einem bestimmten Bit-Muster, durch das gezielte Verändern eines bestimmten Botschaftsteils, wie das CRC-Feld der Botschaft, oder durch das Setzen eines Informationseintrages in einem zusätzlichen Feld der gesendeten Botschaften; und/oder dem

Warnen eines anderen Steuergerätes durch Senden von unplausiblen Dateninhalten in einer oder mehreren folgenden Botschaften, oder durch Senden einer Warnung in einer oder mehreren dedizierten Warn-Botschaft.

Das Verfahren ist ebenso einfach wie wirkungsvoll. Gegenüber dem bekannten Stand der Technik bestehen weitere Möglichkeiten, wie die verdächtige Botschaft unbrauchbar gemacht werden kann. Selbst wenn die empfangene Botschaft auf diese Art und Weise nicht unbrauchbar gemacht werden kann, erfolgt noch eine Warnung der anderen Steuergeräte.

Dadurch, dass die anderen Steuergeräte noch zusätzlich gewarnt werden, können sie die vorher empfangene manipulierte Botschaft noch unberücksichtigt lassen. Die Warnung muss allerdings unmittelbar erfolgen.

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 in der jeweiligen Station 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 Spezialschaltung, realisiert z.B. durch einen FPGA-Chip oder einen ASIC, eingesetzt werden.

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

In einer Variante wird der Schritt des gezielten Veränderns eines bestimmten Botschaftsteils durchgeführt, indem der Eintrag in einem Fehlerschutz-Datenfeld, insbesondere einem CRC-Feld der Botschaft verändert wird. Das hat den Vorteil, dass dann bei der vorgeschriebenen Fehlerschutzprüfung der empfangenen Botschaft die Botschaft automatisch verworfen wird, weil sie als fehlerhaft erkannt wird. Diese Botschaft kann dann keinen Schaden in dem jeweiligen Steuergerät anrichten.

Eine besonders vorteilhafte Variante besteht noch darin, dass von einer Station, die eine von einer mit Überwachungsmodul ausgestatteten anderen Station eine unbrauchbar gemachte Botschaft empfängt oder eine dedizierte Warn-Botschaft, ein Schritt des Überführens der Station in einen sicheren Zustand ausgeführt wird. Dies ist eine wichtige Maßnahme, um zu verhindern, dass ein Unfall passiert, wenn eine Manipulation von Botschaften während des Betriebes erfolgt. Solche Bussysteme werden vielfach in Fahrzeugen eingesetzt, bei denen eine Manipulation im Betrieb zu Unfällen mit fatalen Folgen führen kann. Andererseits werden solche Bussysteme auch in Flugzeugen, Aufzugsteuerungen oder anderen Maschinensteuerungen eingesetzt, bei denen ebenfalls Manipulationen verhindert werden müssen. Diese Maßnahme kann auch durchgeführt werden, wenn die Station an einen anderen Sub-Bus angeschlossen ist als die Station mit Überwachungsmodul. Dazu kann ein

Gateway vorgesehen sein, das in diesem Beispiel die Botschaft von dem Sub-Bus, an den die Station mit Überwachungsmodul angeschlossen ist, an den Sub-Bus weiterleitet, an den die eigentlich betroffene Station angeschlossen ist.

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.

Bei einer anderen Variante, die insbesondere für Fahrzeuge interessant ist, wird als weitere Gegenmaßnahme bei einem für die Ausgabe von Informationen zuständigen Gerät z.B. eines Infotainmentsystems, das eine unbrauchbar gemachte Botschaft empfängt oder eine dedizierte Warnbotschaft, ein Schritt der Warnung des Fahrzeugführers durch Ausgabe eines optischen, akustischen oder haptischen Signals durchgeführt.

Dabei kann die Ausgestaltung auch so sein, dass die mit einem Überwachungsmodul ausgestattete Station eine dedizierte Warnbotschaft an das für die Ausgabe von Informationen zuständige Gerät des Infotainmentsystems sendet, das daraufhin den Schritt der Warnung des Fahrzeugführers durch Ausgabe des optischen, akustischen oder haptischen Signals durchführt.

In diesem Zusammenhang ist es vorteilhaft, wenn als weitere Gegenmaßnahme ein für die Kommunikation mit der Außenwelt zuständiges Gerät in dem Fahrzeug einen Schritt des Absetzens einer Manipulationsmeldung über Funk an einen Zentralrechner des Fahrzeugherstellers oder einer Behörde oder an ein Smartphone des Fahrzeughalters durchgeführt wird. Dadurch wird der Fahrzeughersteller über die Manipulation informiert und kann darauf reagieren. Ggfs. kann er durch Ausgabe einer neuen Softwareversion für ein oder mehrere Steuergeräte die Sicherheitslücke schließen. Auch die Maßnahme, dass die Behörden über die Manipulation informiert werden, kann wichtig sein. So ist es möglich, dass die Manipulation den Strafverfolgungsbehörden mitgeteilt wird. Bevorzugt wird Ort und Zeitpunkt des Auftretens der Manipulation ebenfalls mitgeteilt. Selbst wenn eine unmittelbare Strafverfolgung nicht erfolgreich durchgeführt werden kann, können die Behörden noch Warnungen an die Öffentlichkeit geben. Das für die Kommunikation mit der Außenwelt zuständige Gerät ist in einem Fahrzeug typischerweise ein On-Board Kommunikationsmodul, das für die Kommunikation in einem Mobilfunknetz wie LTE (Long Term Evolution) oder 5G ausgelegt ist und auch für die Fahrzeug-zu-Fahrzeug-Kommunikation V2V nach einem Kommunikationsstandard wie WLAN p, entsprechend IEEE 802.11 p.

Dabei kann die Ausgestaltung auch so sein, dass die mit einem Überwachungsmodul ausgestattete Station eine dedizierte Warnbotschaft an das für die Kommunikation mit der Außenwelt zuständige Gerät sendet, das daraufhin den Schritt des Absetzens einer Manipulationsmeldung über Funk an den Zentralrechner durchführt.

In einer anderen Variante führt das für die Kommunikation mit der Außenwelt zuständige Gerät zusätzlich einen Schritt des Sendens einer dedizierten Warnbotschaft an ein für die Ausgabe von Informationen zuständiges Gerät des Infotainmentsystems durch, welches dann wieder die Ausgabe des Signals zur Warnung des Fahrzeugführers durchführt.

Dieses Überwachungsverfahren kann besonders vorteilhaft bei dem Kommunikationsbus nach einer Variante der Familie der CAN-Bus Standards, entsprechend Controller Area Network, eingesetzt werden. Dieses ist insbesondere in dem Kfz-Bereich sehr verbreitet und erfüllt die Voraussetzungen. Dort werden die Botschaften inhaltsadressiert, d.h. dort beschreibt der CAN-Bus Botschafts-Identifizierer den Inhalt der Botschaft und legt auch gleich die Dringlichkeit der Botschaft fest. Über den CAN-Bus Botschafts-Identifizierer wird in der Arbitrierungsphase bestimmt, welche Station Zugang zum Übertragungsmedium erhält. Zugriffskonflikte werden so über die Wired-AND-Schaltung ohne Verzögerung aufgelöst.

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.

Für eine elektronische Vorrichtung eines anderen Typs zum Anschluss an einen Kommunikationsbus ist es vorteilhaft, wenn die Vorrichtung ein Sicherheitsmodul aufweist, das für die Überführung der elektronischen Vorrichtung in den sicheren Zustand nach dem beschriebenen Überwachungsverfahren ausgelegt ist.

Für ein Fahrzeug ist es vorteilhaft, dass das Fahrzeug mit einer oder beiden Varianten der erwähnten elektronischen Vorrichtungen ausgestattet ist.

Die Botschaften enthalten typischerweise ein Nutzdatenfeld. Darin kann ein Steuerbefehl enthalten sein. 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.

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 das Format des Standard Frame-Übertragungsrahmens beim CAN-Bus;

Fig. 3 das Format des Remote Frame-Übertragungsrahmens beim CAN-Bus;

Fig. 4 das Prinzip von Fahrzeug-zu-Fahrzeug-Kommunikation V2V und Fahrzeug-zu-Allem-Kommunikation V2X mittels Mobilfunkunterstützung;

Fig. 5 ein Blockdiagramm für ein Fahrzeug-Kommunikationsnetzwerk mit Steuergeräten und anderen Stationen verschiedener Kategorie;

Fig. 6 ein Blockschaltbild einer CAN-Bus-Schnittstelle, die mit einem Überwachungsmodul gemäß der Erfindung ausgestattet ist;

Fig. 7 ein Flussdiagramm für ein Programm, das als Überwachungsmodul auf der CAN-Busschnittstelle installiert ist,

Fig. 8 ein Diagramm, das die durch einen Angreifer eingeschleusten Botschaften während der Überwachungsphase illustriert; und

Fig. 9 den Ablauf des erweiterten Überwachungsverfahrens in Form eines Zustandsdiagramms.

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. Der CAN-Bus wird aber nicht nur im Fahrzeugbereich inklusive Flugzeugen eingesetzt, sondern auch in anderen Bereichen. Wie bereits erwähnt betrifft dies den Bereich von Prozess- und Maschinensteuerungen. Hier wird der CAN-Bus auch als Feldbus eingesetzt.

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 das Botschaftsformat eines CAN Standard Frames. Genauer gesagt, veranschaulicht Fig. 2 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 ein 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. 3 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 Identifiern der assoziierten Data Frames entsprechen. Sobald ein CAN-Knoten einen Remote Frame empfängt, dessen Identifizierer mit einem Identifizierer in der eigenen Kommunikationsmatrix identisch ist, antwortet er mit dem entsprechenden Standard Frame.

Fig. 4 zeigt die Systemarchitektur für die Fahrzeugkommunikation mittels Mobilfunk. Die Bezugszahl 10 bezeichnet ein Fahrzeug. Das dargestellte Fahrzeug ist als Personenkraftwagen ausgeführt. Dies soll nicht einschränkend gemeint sein, es kann sich um einen beliebigen Fahrzeugtyp handeln. Beispiele für andere Fahrzeugtypen sind: Busse, Motorräder, Nutzfahrzeuge, insbesondere Lastkraftwagen, landwirtschaftliche Maschinen, Baumaschinen, Schienenfahrzeuge usw. Die Verwendung der Erfindung wäre generell in

Landfahrzeugen, Schienenfahrzeugen, Wasserfahrzeugen und Flugzeugen möglich. Das Fahrzeug 10 ist mit einem On-Board-Kommunikationsmodul 110 mit entsprechender Antenneneinheit ausgestattet, so dass es an den verschiedenen Arten der Fahrzeugkommunikation V2V und V2X teilnehmen kann. Fig. 1 zeigt, dass das Fahrzeug 10 mit der Mobilfunk-Basisstation 210 eines Mobilfunk-Anbieters kommunizieren kann.

Eine solche Basisstation 210 kann eine eNodeB-Basisstation eines LTE-Mobilfunkanbieters (Long Term Evolution) sein. Die Basisstation 210 und die entsprechende Ausrüstung ist Teil eines Mobilfunk-Kommunikationsnetzwerks mit einer Vielzahl von Mobilfunkzellen, wobei jede Zelle von einer Basisstation 210 bedient wird.

Die Basisstation 210 ist nahe einer Hauptstraße positioniert, auf der die Fahrzeuge 10 fahren. In der Terminologie von LTE entspricht ein mobiles Endgerät einer Benutzerausrüstung UE, die es einem Benutzer ermöglicht, auf Netzwerkdienste zuzugreifen, wobei er sich über die Funkschnittstelle mit dem UTRAN oder dem Evolved-UTRAN verbindet. Typischerweise entspricht eine solche Benutzerausrüstung einem Smartphone. Solche mobilen Endgeräte werden von den Passagieren in den Fahrzeugen 10 verwendet. Zusätzlich sind die Fahrzeuge 10 jeweils mit einem On-Board-Kommunikationsmodul 110 ausgestattet. Dieses On-Board-Kommunikationsmodul 110 entspricht einem LTE-Kommunikationsmodul, mit dem das Fahrzeug 10 mobile Daten empfangen kann (Downlink) und solche Daten in Aufwärtsrichtung senden kann (Uplink). Dieses On-Board-Kommunikationsmodul 110 kann ferner mit einem WLAN p-Modul ausgestattet sein, um an einem Ad-hoc-V2X-Kommunikationsmodus teilnehmen zu können. V2V und V2X Kommunikation wird aber auch durch die neue 5. Generation von Mobilfunksystemen unterstützt. Dort wird die entsprechende Funkschnittstelle als PC5 Schnittstelle bezeichnet. In Bezug auf das LTE-Mobilfunk-Kommunikationssystem besteht das Evolved UMTS Terrestrial Radio Access-Netzwerk E-UTRAN von LTE aus mehreren eNodeBs, die die E-UTRA-Benutzerebene (PDCP / RLC / MAC / PHY) und die Steuerebene (RRC) bereitstellen. Die eNodeBs sind mittels der sogenannten X2-Schnittstelle miteinander verbunden. Die eNodeBs sind auch über die sogenannte S1-Schnittstelle mit dem EPC (Evolved Packet Core) 200 verbunden.

Aus dieser allgemeinen Architektur zeigt Fig. 4, dass die Basisstation 210 über die S1-Schnittstelle mit dem EPC 200 verbunden ist und der EPC 200 mit dem Internet 300 verbunden ist. Ein Backend-Server 320, an den die Fahrzeuge 10 Nachrichten senden können und von diesem empfangen können, ist ebenfalls mit dem Internet 300 verbunden. Im Bereich des kooperativen und autonomen Fahrens befindet sich der Backend-Server 320

typischerweise in einer Verkehrszentrale. Diese kann einer Behörde, auch Strafverfolgungsbehörde und Polizei, zugeordnet sein oder einem Fahrzeughersteller oder einem technischen Überwachungsverein etc. Schließlich ist auch eine Straßeninfrastrukturstation 310 gezeigt. Diese kann beispielsweise durch eine straßenseitige Einheit, die im Fachjargon oft als Road Side Unit RSU 310 bezeichnet wird, veranschaulicht werden. Zur Vereinfachung der Implementierung wird davon ausgegangen, dass allen Komponenten eine Internetadresse zugewiesen wurde, typischerweise in Form einer IPv6-Adresse, so dass die Pakete, die Nachrichten zwischen den Komponenten transportieren, entsprechend geroutet werden können. Die erwähnten verschiedenen Schnittstellen sind standardisiert. Es wird diesbezüglich auf die entsprechenden LTE Spezifikationen verwiesen, die veröffentlicht sind.

Fig. 5 zeigt den typischen Aufbau eines Kommunikationsnetzwerkes eines modernen Kraftfahrzeuges. Mit der Bezugszahl 151 ist ein Motorsteuergerät bezeichnet. Die Bezugszahl 152 entspricht einem ESP-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 161 bis 163 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, Klopfsensoren, Luftgütesensoren 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. (nicht dargestellt). Mit der Bezugszahl 130 ist eine Recheneinrichtung bezeichnet. Daran angeschlossen ist ein

berührungsempfindliches Anzeigegerät (LCD-Touchscreen) 135. Ein Navigationssystem hat die Bezugszahl 120, welches ebenfalls im Bereich des Cockpits verbaut wird. Die Route, welche auf einer Karte angezeigt wird, wird auf dem Anzeigegerät 135 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. Daran angeschlossen ist ein Antennenmodul AM. Typischerweise handelt es sich hier um ein Mobilfunk-Kommunikationsmodul, z. B. nach dem LTE-Standard oder 5G-Standard. Mit der Bezugszahl 105 ist noch eine Kamera 105 bezeichnet, die als Front-Kamera zur Umfeldbeobachtung ausgelegt ist. Zusätzliche Kameras können vorhanden sein für die Beobachtung in andere Richtungen, Seiten und Heck. Auch eine Kamera für den Einsatz als Innenraumüberwachungskamera kann zusätzlich vorhanden sein. Die erwähnten 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 das Bussystem 102 als ein für den Infotainment-Bereich speziell ausgelegtes anderes Bussystem ausgelegt ist. 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. In Frage käme alternativ auch 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.

Zu dem Zweck, dass fahrzeugrelevante Sensordaten über die Kommunikationsschnittstelle 110 zu einem anderen Fahrzeug oder zu einem externen Zentralrechner 320 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.

Die Fig. 6 zeigt jetzt die Implementierung von Überwachungsmodul und Sicherheitsmodul in Form von Softwaremodulen. 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 Softwarekomponenten Applikations-Software 1511, einem Überwachungsmodul 1517 und einem Sicherheitsmodul 1518. Zwischen beiden diesen 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 Fig. 6 zeigt eine mögliche Variante einer Architektur. Die Implementierung kann auch mit anderen Varianten erfolgen.

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

Das Überwachungsmodul 1517 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 Sendebetriebes 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 1517 auslösen. Daneben gibt es aber auch eine Reihe von anderen Sendearten bei Steuergeräten. Als Beispiele werden die Sendearten (ifActiv, ifAcitvWithRepetition, 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. 7 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 kein anderes Steuergerät denselben Botschaftsidentifizierer bei Aussendung seiner Botschaften verwenden. Deshalb werden dann im nächsten Schritt 184 die Gegenmaßnahmen eingeleitet. Es können sofortige Gegenmaßnahmen eingeleitete werden, die darauf abzielen, die eingeschleuste Botschaft noch während ihrer Übertragung unbrauchbar zu machen.

Überschreiben mit dominantem Buspegel
Dies kann durch Überschreiben des an den Bus angelegten Buspegels mit dem dominanten Buspegel geschehen. Die Veränderung kann sich auf das Datenfeld der Botschaft oder ein anderes Feld beziehen. Sehr effektiv ist auch das Verändern bzw. Überschreiben des Botschaftsfeldes für die Fehlerschutzdaten. Bei dem CAN-Bus Botschaftsformat wird dafür das CRC-Feld vorgesehen. Im Empfänger werden die eingegangenen Botschaften mit dem CRC-Prüfcode auf Fehler überprüft. Wenn dabei ein Fehler erkannt wird, wird die Botschaft verworfen. Wenn kein Fehler erkennt wird, quittiert der Empfänger den Eingang der Botschaft positiv. Dazu legt er einen dominanten Buspegel an den Bus an während das ACK-Feld übertragen wird. Im Fehlerfall legt er entsprechend den rezessiven Buspegel an. Liegt keine einzige positive Bestätigung vor, wird also der rezessive ACK-Slot von keinem Empfänger überschrieben, detektiert der Sender einen ACK-Fehler und bricht die laufende Nachrichtenübertragung mit dem Aufschalten eines Error Flags sofort ab. Eingeschleuste Daten werden auf diese Weise bewusst verändert und damit unbrauchbar gemacht. Mit dem gezielten Verändern bestimmter Botschaftsteile bzw. deren CRC-Absicherung ist zudem im gewissen Rahmen eine Steuerung der Reaktion betroffener Steuergeräte möglich. Das Überschreiben kann mit einem konstanten dominanten Pegel erfolgen. Durch gezieltes

Überschreiben einzelner Bits mit dem dominanten Pegel kann auch ein bestimmtes Bit-Muster generiert werden.

a. Ein derartiges Bitmuster kann vorzugsweise aus einer bestimmten Folge von Bits mit dominantem Buspegel bzw. nicht-dominantem Buspegel bestehen.
b. Bei entsprechender Gestaltung des Bitmusters ist dieses auch zur Informationsübertragung geeignet. Diese Information kann in das entsprechende Bitmuster kodiert werden.
c. Die Art des Bitmusters (d.h. die Länge der dominanten/nicht-dominanten Sequenzen) kann so gewählt werden, dass die Empfänger-Steuergeräte mit ausreichend hoher Wahrscheinlichkeit sowohl einen Angriff erkennen können als auch die im Bitmuster enthaltenen Informationen dekodieren können.
d. Das Bitmuster kann sich über den kompletten Datenbereich erstrecken, bzw. einen oder mehrere Teilbereiche umfassen.
e. Wird nur ein bestimmter Bereich im Datenfeld benutzt, um mit einem Bitmuster eine kompromittierte Botschaft zu kennzeichnen, kann ein weiterer Bereich im Datenfeld verwendet werden, mit dem das betroffene Steuergerät Informationen zum Empfängersteuergerät, das den Angriff erkannt hat, überträgt.
   - Dieses Bitmuster kann eine Empfängerbestätigung der in a genannten Mitteilung darstellen.
   - Dieses Bitmuster kann zusätzliche Informationen zur Reaktion des Empfängersteuergerätes enthalten.
f. Vorzugsweise überschreibt das Empfängersteuergerät, das den Angriff erkannt hat, wie beschrieben das Datenfeld noch während die kompromittierte Botschaft versendet wird.

Wenn das CRC-Feld mit einem ungültigen CRC-Code überschrieben wird, kann dies auch so erfolgen, dass eine Information in den „ungültigen CRC-Code“ kodiert wird. Diese Information kann z.B. angeben, welches Signal manipuliert wurde oder wie viele Botschaften dieser Art schon manipuliert wurden. In dem Fall stellt die Information einen Manipulationszähler dar.

Als Gegenmaßnahme kommen noch verschiedene andere Maßnahmen in Betracht, die einzeln oder in Kombination eingesetzt werden können:

Warnung mittels Botschaftssignal

Eine weitere Möglichkeit, Steuergeräte nach einem Angriff zu warnen, besteht in der Einfügung eines zusätzlichen Signals im Datenteil von regulären Botschaften. In der

einfachsten Ausführungsform kann ein bestehendes/zusätzliches Bit des Datenfeldes dafür reserviert werden, mit dem in regulären Botschaften ein Angriff signalisiert wird. Nach einem Angriff versendet das Steuergerät, dessen Überwachungsmodul den Angriff erkannt hat, eine oder mehrere Botschaften, deren Signalbit auf einen bestimmten, definierten Wert gesetzt wird. Bei einer anderen Ausführungsform besteht das Signal aus einem bestimmten Bitmuster, das zu diesem Zweck festgelegt wird.

Warnung mittels unplausibler Dateninhalte

Betroffene Steuergeräte können auch durch unplausible Dateninhalte vor einem Angriff gewarnt werden. Das Steuergerät, das den Angriff erkannt hat, sendet nach dem Angriff eine oder mehrere Botschaften mit unplausiblen Daten. Das Datenfeld oder bestimmte Signale im Datenfeld werden nach einem erkannten Angriff auf nicht-plausible Werte gesetzt. Als Beispiel wird erwähnt, dass eine unplausible physikalische Größe, wie Geschwindigkeit, Beschleunigung, Drehzahl, Drosselklappenstellung, Öldruck, Benzinverbrauch etc. übertragen wird. In den Steuergeräten, die die Botschaft empfangen, wird eine Plausibilitätsüberprüfung durchgeführt. Wird dabei festgestellt, dass die empfangenen Daten unplausible Werte betreffen, wird die empfangene Botschaft verworfen. Unplausibel kann dabei so definiert werden, dass es sich um Signale außerhalb eines bestimmten zulässigen Wertebereiches handelt.

Warnung durch Versand einer Warnbotschaft

Von einem Angriff betroffene Steuergeräte können auch durch zusätzliche Warnbotschaften über einen Angriff informiert werden. Diese Warnbotschaften werden nur im Fall eines erkannten Angriffes verwendet. Dafür können eigene Can-Bus Botschafts-Identifizierer vergeben werden, die für jede Station eindeutig sind oder individuell für jede in der Station verwendeten Botschaft eindeutig zugeordnet werden. Auf diese Weise können betroffene Steuergeräte erkennen, welche Botschaft angegriffen wurde und eine dementsprechende Reaktion einleiten.

Reaktion betroffener Steuergeräte

Neben der Erkennung von eingeschleusten Botschaften kommt der Reaktion von betroffenen Steuergeräten eine besondere Bedeutung zu. Ein im Steuergerät implementiertes Sicherungsmodul überführt im Falle eines Angriffes das betroffene Steuergerät in einen sog. sicheren Zustand. Dies ist für jedes Steuergerät vorgesehen und wird bei der Softwareentwicklung programmiert. Es gibt vordefinierte Regeln, wie der Übergang in den sicheren Zustand erfolgen sollte. Diesbezüglich wird auf die ISO-Norm ISO 26262 mit dem Titel „Funktionale Sicherheit“ hingewiesen.

Zusätzlich können im Falle einer empfangenen Angriffsbenachrichtigung bereits implementierte Standardmaßnahmen, wie z.B. die zugehörige Reaktion bei Ausfall des CAN-Busses oder bestimmte Degradationskonzepte, angewendet werden.

Fig. 8 zeigt jetzt noch das Prinzip des Überwachungsverfahrens. Gleiche Bezugszahlen bezeichnen dieselben Komponenten, wie zuvor erläutert. Der Angreifer ist in Fig. 8 mit der Bezugszahl 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. 8 ist ein Zyklus dargestellt, mit dem das Motorsteuergerät 151 eine Botschaft ECM auf den Bus sendet. Zur jeweiligen Sendephase ist das Überwachungsmodul 1517 nicht aktiv. In den markierten Phasen MP findet die Überwachung des Busverkehrs statt. Bei der zweiten Phase MP treten weitere ECM‘ Botschaften auf, die der Angreifer 157 sendet. Da diese denselben Botschafts-Identifizierer benutzen, der für das Steuergerät 151 reserviert ist, werden sie vom Überwachungsmodul 1517 als irregulär erkannt, wie oben beschrieben. Das Motor-Steuergerät 151 leitet daraufhin, wie beschrieben, Gegenmaßnahmen ein.

Die Fig. 9 zeigt noch ein Zustandsdiagramm, mit dem der Überwachungsvorgang und die Einleitung von Gegenmaßnahmen beschrieben wird. Gleiche Bezugszahlen bezeichnen die gleichen Komponenten wie in den anderen Figuren. Der in Fig. 9 dargestellte Zustandsautomat beschreibt die Funktionsweise des neuen Systems von der Busüberwachung bis zum Erreichen des sicheren Zustandes bei einem betroffenen Steuergerät 152 sowie die Benachrichtigung der für die Kommunikation mit dem Fahrer, dem Zentralrechner 320, anderer Verkehrsteilnehmer 10 und Infrastruktur 310 zuständigen Steuergeräte 110. Dabei werden verschiedene Varianten der Benachrichtigung dargestellt. Diese können sowohl einzeln als auch in beliebiger Kombination durchgeführt werden.

Zunächst wird davon ausgegangen, dass das Motorsteuergerät 151 mit dem Überwachungsmodul 1517 eine Busüberwachung durchführt. Entsprechend befindet sich das Steuergerät in dem Zustand Z1. Wird von dem Überwachungsmodul 1517 durch eine der oben beschriebenen Überprüfungsmaßnahmen ein Angriff erkannt, so wechselt das Motorsteuergerät 151 in den Zustand Z2. Der Zustandsübergangswechsel ist mit der Bezugszahl ① bezeichnet. Im Zustand Z2 werden Gegenmaßnahmen durchgeführt. Zunächst erfolgt eine Benachrichtigung des betroffenen Steuergerätes. Das betroffene

Steuergerät entspricht im gezeigten Beispiel dem ESP-Steuergerät 152. Die von einem Angreifer auf den Bus gebrachte Botschaft ist also eine Botschaft, die für das Motorsteuergerät 151 reserviert ist. Das Motorsteuergerät 151 wird als erste Gegenmaßnahme versuchen, die Botschaft zu invalidieren. Dies geschieht bei dem Zustandsübergang ② dadurch, dass die noch eingehende Botschaft durch Anlegen des dominanten Buspegels an den Bus 102 zerstört wird. Es kann sowohl das Datenfeld wie auch das CRC-Feld so überschrieben werden. Es kann auch ein bestimmtes Bitmuster auf diese Art und Weise übertragen werden, das eindeutig als Warnung vor einem erkannten Angriff interpretiert wird. Beim Zustandsübergang ③ wird eine neue Botschaft mit dem gleichen Botschafts-Identifizierer generiert, in der im Datenfeld unplausible Daten eingetragen sind. Beim Zustandsübergang ④ wird eine neue Botschaft generiert, die speziell als Warnbotschaft spezifiziert wurde. Für diese Warnbotschaft wurde ein eigener Botschafts-Identifizierer reserviert. Das ESP-Steuergerät 152 wechselt aufgrund einer der bei den Zustandsübergängen ②, ③, ④ gelieferten Botschaften in den Zustand Z3, in dem die Benachrichtigungen eines betroffenen Steuergerätes nach Erkennung eines Angriffs verarbeitet werden. Beim Zustandsübergang ⑤ wird eine neue Botschaft erzeugt, die einen Botschafts-Identifizierer beinhaltet, der an die Recheneinrichtung 130 gerichtet ist. Die Recheneinrichtung 130 stellt fest, dass es sich um eine Warnmeldung über einen Angriff handelt und geht in den Zustand Z5 über, in dem sie einen Warnhinweis generiert, der auf der Anzeigeeinheit 135 für den Fahrer angezeigt wird. Dies kann durch optische Anzeige (z.B. Warnsymbol oder Text), akustische oder durch haptische Warnungen geschehen. Beim Zustandsübergang ⑥ wird eine neue Botschaft erzeugt, die einen Botschafts-Identifizierer beinhaltet, der an das Kommunikationsmodul 110 gerichtet ist. Das Gateway 140 muss diese Nachricht umsetzen in das Format des Bussystems 104. Das Kommunikationsmodul 110 erkennt darin dann einen Warnhinweis über einen erfolgten Angriff und geht in den Zustand Z6 über. In dem Zustand Z6 erfolgt die Generierung einer Botschaft, die an den Zentralrechner 320 adressiert wird. Darin wird dem Zentralrechner 320 mitgeteilt, dass ein Angriff erfolgte. Es wird der Botschaftstyp sowie Ort und Zeitpunkt des Angriffs zum Zentralrechner 320 übertragen.

Im Zustand Z3 kann auch das ESP-Steuergerät 152 weitere Maßnahmen einleiten. Dann wird es beim Zustandsübergang ⑦ eine Botschaft an die Recheneinrichtung 130 absenden mit dem gleichen Inhalt, wie es beim Zustandsübergang ⑤ erfolgte. Schließlich erfolgt noch beim Zustandsübergang ⑧ eine Benachrichtigung des Kommunikationsmoduls 110 wie beim Zustandsübergang ⑥. Beim Zustandsübergang ⑨ findet ein Wechsel des Zustands bei dem ESP-Steuergerät 152 statt. Das Steuergerät wechselt dabei in den sicheren Zustand Z4. Auch im Zustand Z5 der Recheneinrichtung 130 kann diese Form der Benachrichtigung des

Kommunikationsmoduls 110 bei Zustandsübergang ⑩ in einer anderen Variante noch erfolgen.

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 werden 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
20	Fahrzeug
100	Kfz-Elektronik
102	Infotainment-Bus
104	CAN-Bus
110	On-Board Kommunikationsmodul
120	Navigationssystem
130	Recheneinrichtung
135	Anzeigeeinheit
140	Gateway
151	Motor-Steuergerät
152	ESP-Steuergerät
153	Getriebe-Steuergerät
157	Angreifer
161	1. Sensor
162	2. Sensor
163	3. Sensor
181	Programmstart
182	Vergleich Botschafts-ID mit Sendetabelle
183	Prüfung auf Remote Frame
184	Gegenmaßnahmen
185	Programmende
200	Evolved Packet Core
210	Basisstation
300	Internet
310	Road Side Unit
320	Zentralrechner
1510	Architektur CAN-Busschnittstelle
1511	Applikations-Software

1512	1. Schnittstelle
1513	CAN-Controller
1514	2. Schnittstelle
1515	Sendetabelle
1516	3. Schnittstelle
1517	Überwachungsmodul
1518	Sicherheitsmodul
AM	Antennenmodul
ECM	eine Botschaft des Motorsteuergeräts
ECM‘	eine eingeschleuste Botschaft eines Angreifers
MP	Überwachungsphase
Z1 -	
Z6	verschiedene Zustände
①-⑩	verschiedene Zustandsübergänge

Patentansprüche

1. Verfahren zur Überwachung der Kommunikation auf einem Kommunikationsbus (104), wobei durch den Kommunikationsbus (104) eine Anzahl von elektronischen Stationen (140 - 163) vernetzt sind, wobei die über den Kommunikationsbus (104) übertragenen Botschaften mit einem Identifizierer gekennzeichnet sind, wobei für jede Station (140 - 163) festgelegt wird, welche Botschaften mit welchem Identifizierer von ihr gesendet werden dürfen, wobei eine Eindeutigkeitsregel eingehalten wird, die verbietet, dass eine andere Station (140 - 163) eine Nutzdaten-Botschaft mit einem Identifizierer versendet, der schon für diese Station (140 - 163) reserviert ist, wobei in einer oder mehreren oder allen der elektronischen Stationen (140 - 163) ein Überwachungsmodul (1517) vorgesehen wird, das überwacht, ob auf dem Kommunikationsbus (104) eine Nutzdaten-Botschaft von einer anderen Station (140 - 163) gesendet wird mit einem Identifizierer, der für die eigene Station (140 - 163) reserviert ist, wobei, wenn von dem Überwachungsmodul (1517) festgestellt wird, dass die Eindeutigkeitsregel verletzt ist, eine oder mehrere der folgenden Gegenmaßnahmen eingeleitet werden:

- Unbrauchbarmachen der eingeschleusten Botschaft durch Überschreiben der Botschaft mit dem dominanten Pegel, durch Überschreiben der Botschaft mit einem bestimmten Bit-Muster, durch das gezielte Verändern eines bestimmten Botschaftsteils, wie das CRC-Feld der Botschaft, oder durch das Setzen eines Informationseintrages in einem zusätzlichen Feld der gesendeten Botschaften; und/oder
- Warnen einer anderen elektronischen Station (140 - 163) durch Senden von unplausiblen Dateninhalten in einer oder mehreren folgenden Botschaften oder durch Senden einer Warnung in einer oder mehreren dedizierten Warn-Botschaft.

2. Verfahren nach Anspruch 1, wobei das Überwachungsmodul (1517) für die Überwachung auf eine Sendetabelle (1515) zugreift, in der alle der für die Station (140 - 163) 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 (1517) ein unberechtigter Buszugriff festgestellt wird und die eine oder mehrere der Gegenmaßnahmen eingeleitet werden.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Schritt des gezielten Veränderns eines bestimmten Botschaftsteils, das Verändern des Eintrages in einem Fehlerschutz-Datenfeld, insbesondere einem CRC-Feld der Botschaft betrifft.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei von einer Station (140 - 163), die eine von einer mit Überwachungsmodul (1517) ausgestatteten anderen Station (140 - 163) eine unbrauchbar gemachte Botschaft empfängt oder eine dedizierte Warn-Botschaft, ein Schritt des Überführens der Station (140 - 163) in einen sicheren Zustand (Z4) ausgeführt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei als weitere Gegenmaßnahme ein für die Ausgabe von Informationen zuständiges Gerät (130), insbesondere ein Gerät eines Infotainmentsystems, das eine unbrauchbar gemachte Botschaft empfängt oder eine dedizierte Warnbotschaft, einen Schritt der Warnung des Fahrzeugführers mit einem optischen, akustischen oder haptischen Signal durchführt.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die mit einem Überwachungsmodul (1517) ausgestattete Station (1518) eine dedizierte Warnbotschaft an das für die Ausgabe von Informationen zuständige Gerät (130), insbesondere das Gerät des Infotainmentsystems sendet, das daraufhin den Schritt der Warnung des Fahrzeugführers durch Ausgabe des optischen, akustischen oder haptischen Signals durchführt.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei als weitere Gegenmaßnahme ein für die Kommunikation mit der Außenwelt zuständiges Gerät (110) einen Schritt des Absetzens einer Manipulationsmeldung über Funk an einen Zentralrechner (320) des Autoherstellers oder einer Behörde oder an ein Smartphone des Fahrzeughalters durchführt.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die mit einem Überwachungsmodul (1517) ausgestattete Station (140 - 163) eine dedizierte Warnbotschaft an das für die Kommunikation mit der Außenwelt zuständige Gerät (110) sendet, das daraufhin den Schritt des Absetzens einer Manipulationsmeldung über Funk an den Zentralrechner (320) durchführt.

10. Verfahren nach Anspruch 9, wobei das für die Kommunikation mit der Außenwelt zuständige Gerät (110) zusätzlich einen Schritt des Sendens einer dedizierten

Warnbotschaft an ein für die Ausgabe von Informationen zuständiges Gerät (130) des Infotainmentsystems durchführt.

11. Verfahren nach einem der vorgehenden Ansprüche, wobei der Kommunikationsbus (104) nach einer Variante der Familie der CAN-Bus Standards, entsprechend Controller Area Network, ausgelegt wird.

12. Verfahren nach Anspruch 11, wobei der Identifizierer einem CAN-Bus Botschafts-Identifizierer entspricht.

13. Elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus (104), dadurch gekennzeichnet, dass die Vorrichtung ein Überwachungsmodul (1517) aufweist, das für die Überwachung nach den Schritten nach einem der vorhergehenden Ansprüche ausgelegt ist.

14. Elektronische Vorrichtung zum Anschluss an einen Kommunikationsbus (104), dadurch gekennzeichnet, dass die Vorrichtung ein Sicherheitsmodul (1518) aufweist, das für die Überführung des Steuergerätes (152) in den sicheren Zustand nach den Schritten nach Anspruch 5 ausgelegt ist.

15. Fahrzeug, dadurch gekennzeichnet, dass das Fahrzeug (10) mit einer oder beiden elektronischen Vorrichtungen nach Anspruch 13 oder 14 ausgestattet ist.

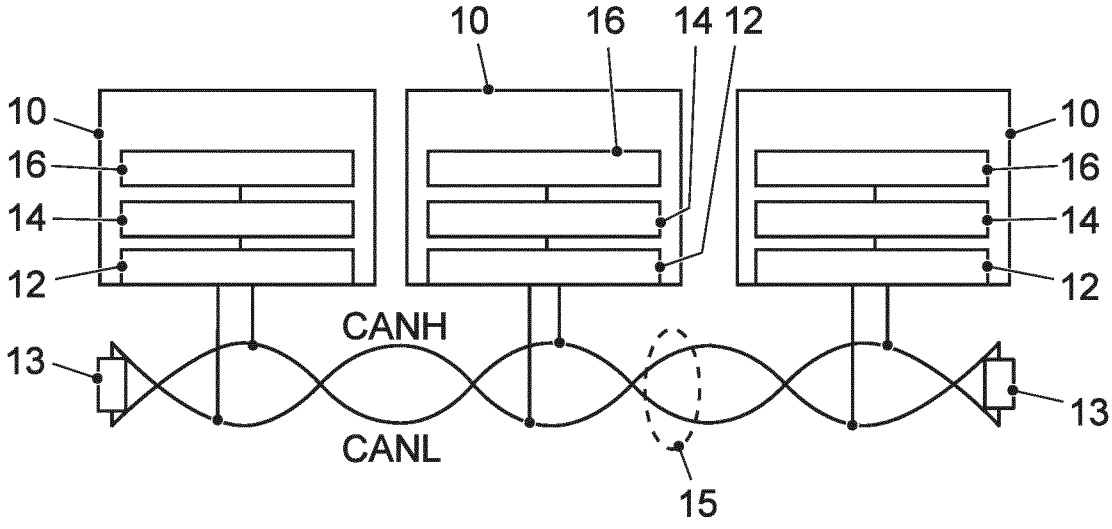

FIG. 1

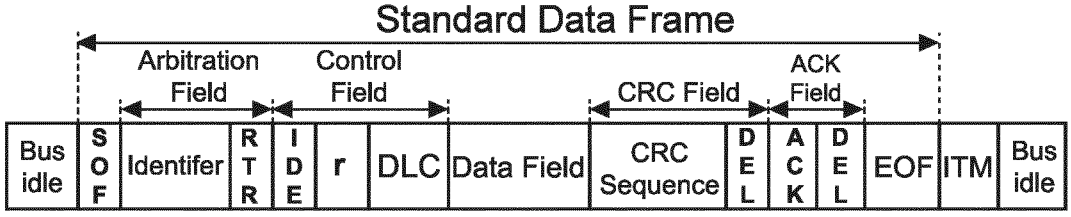

FIG. 2

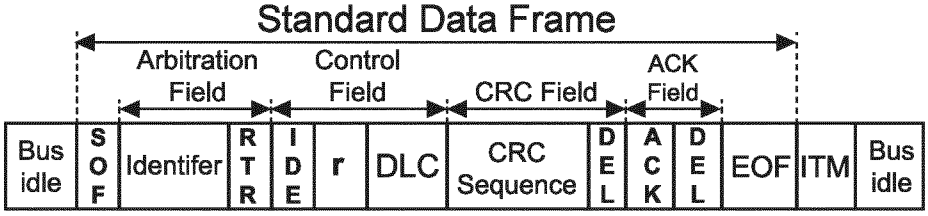

FIG. 3

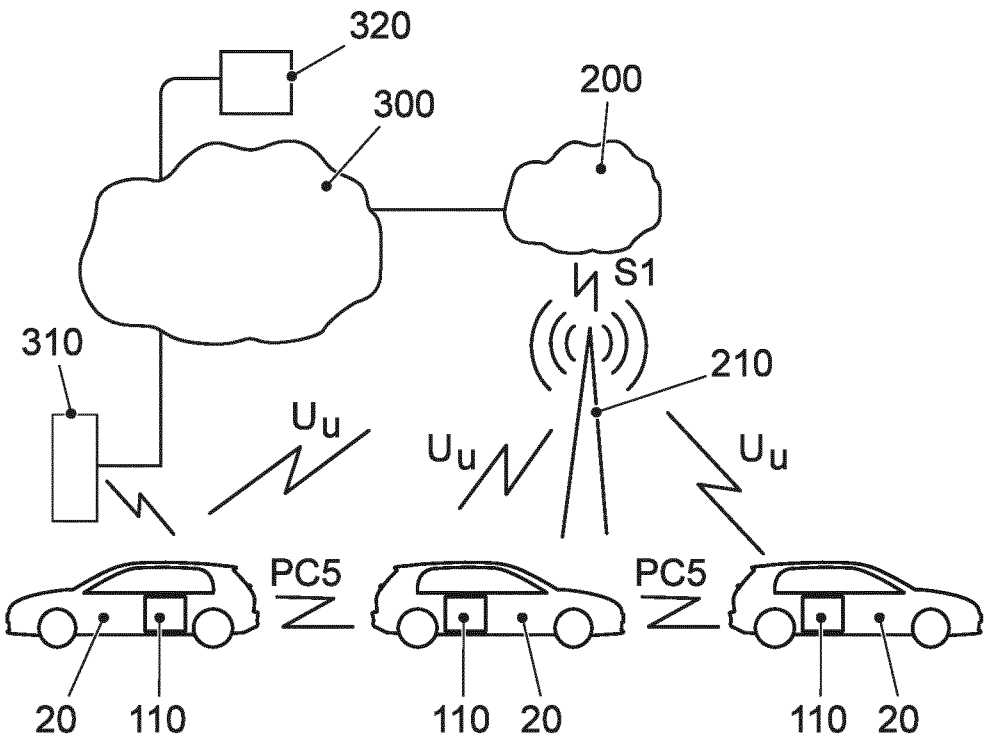

FIG. 4

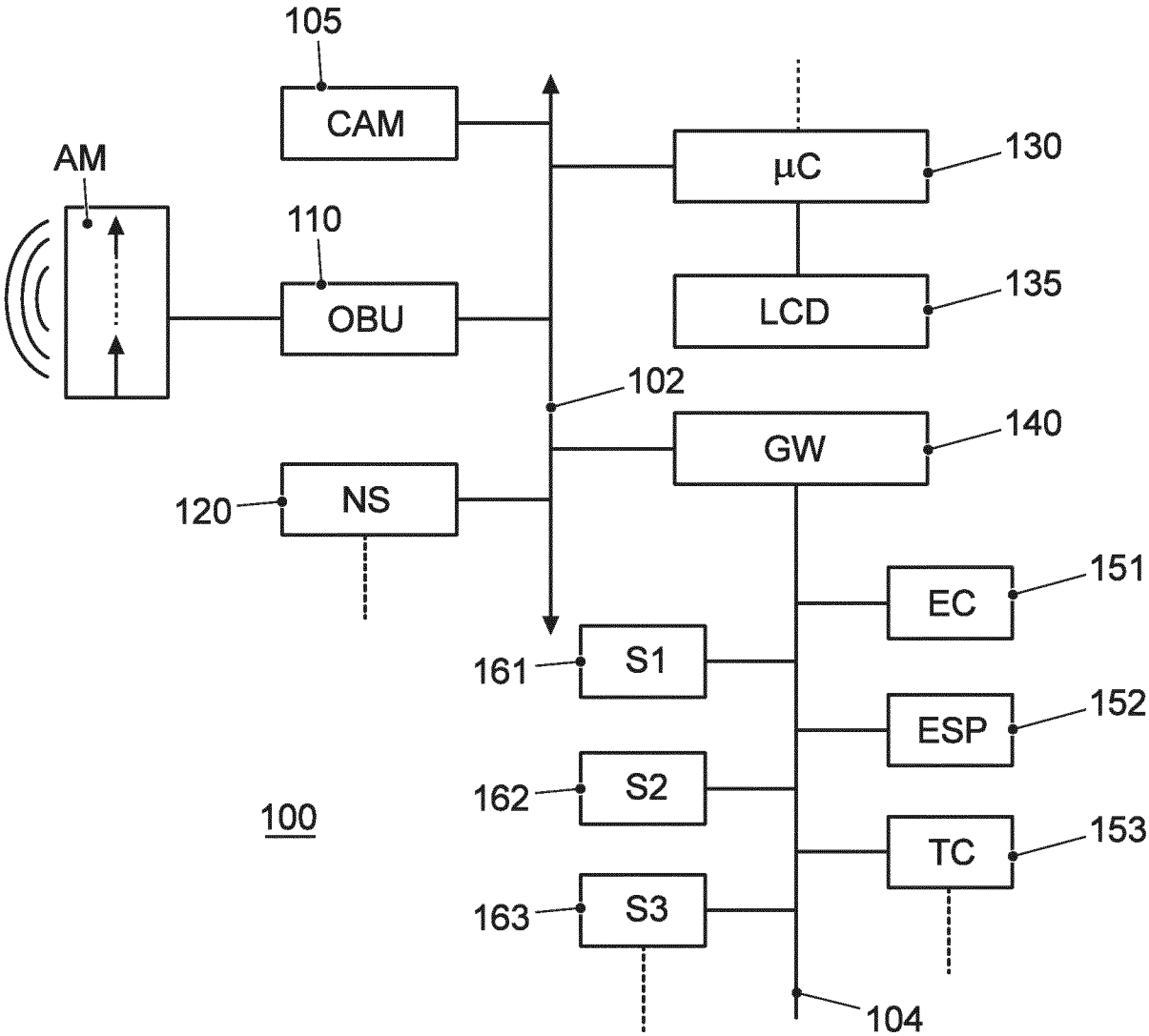
105
CAM
AM
110
OBU
102
120
NS
µC
130
LCD
135
GW
140
EC
151
161
S1
ESP
152
162
S2
TC
153
163
S3
104
100

FIG. 5

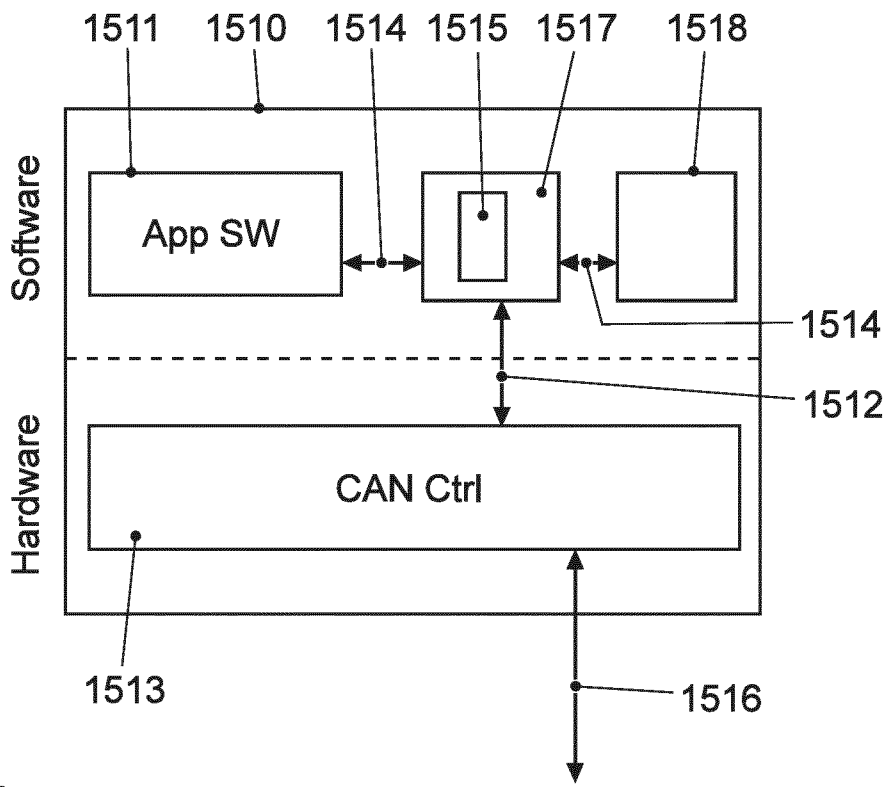
1511
1510
1514
1515
1517
1518
Software
App SW
1514
1512
Hardware
CAN Ctrl
1513
1516

FIG. 6

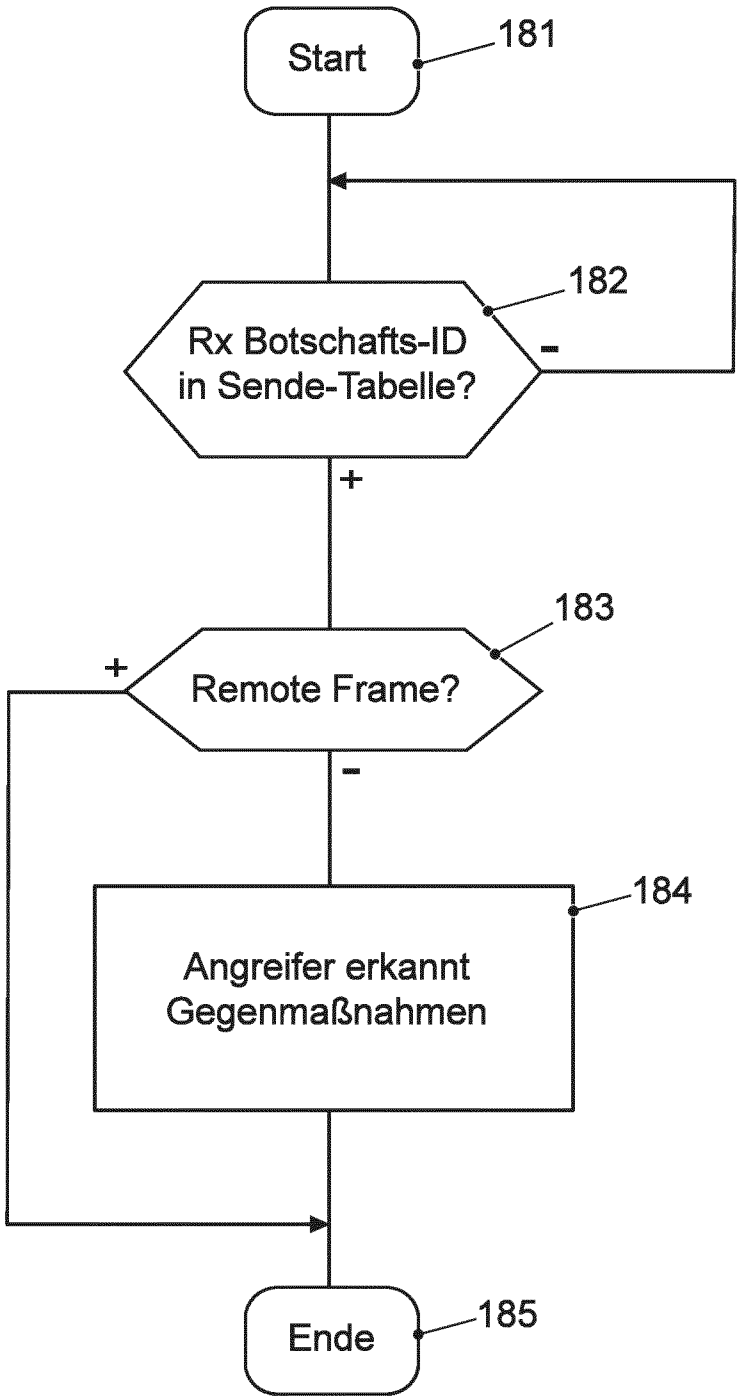
Start
181
Rx Botschafts-ID
in Sende-Tabelle?
182
-
+
Remote Frame?
183
+
-
Angreifer erkannt
Gegenmaßnahmen
184
Ende
185

FIG. 7

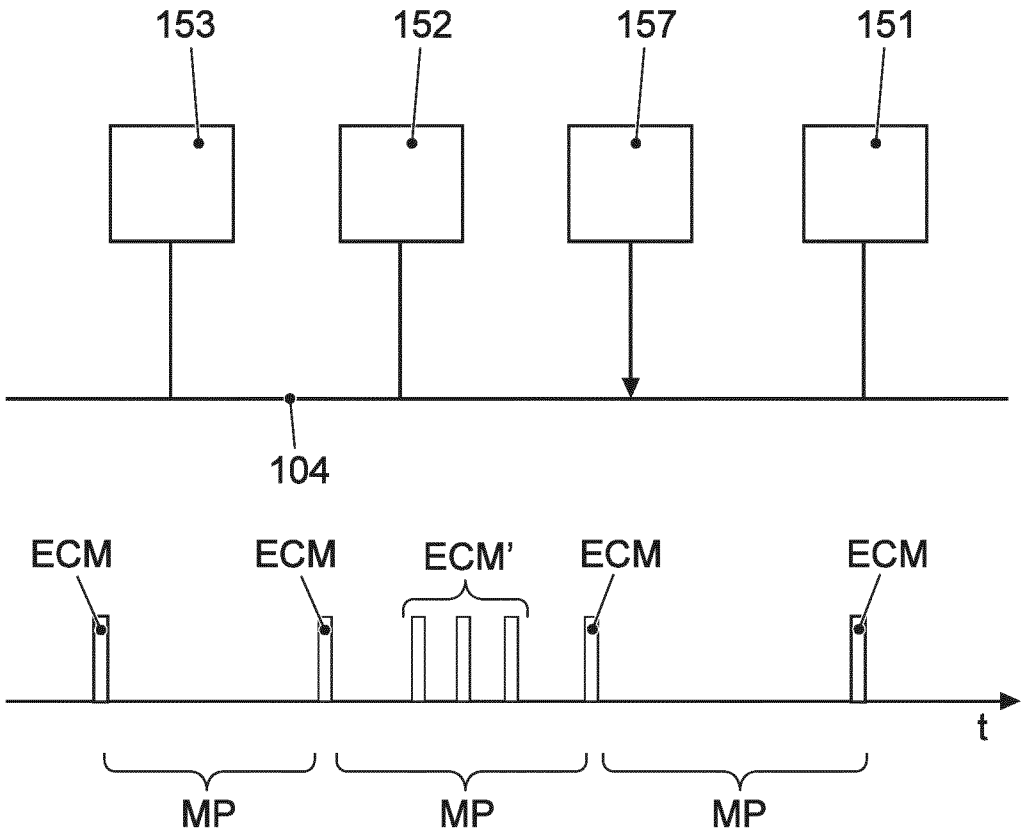

FIG. 8

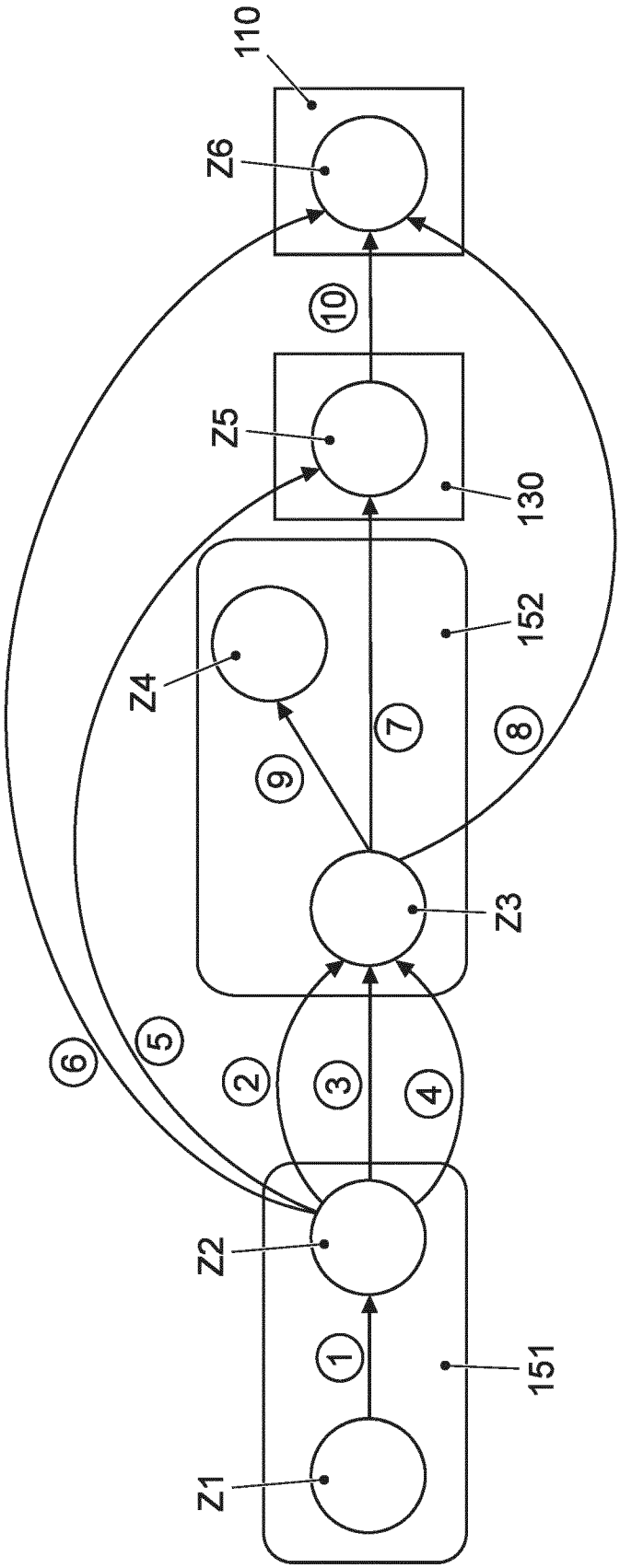

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/057450

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/413(2006.01)i; ***H04L 29/06***(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 102009026995 A1 (BOSCH GMBH ROBERT [DE]) 31 March 2011 (2011-03-31) paragraphs [0002], [0006], [0007] paragraph [0009] - paragraph [0020]; figure 1	1-4,11-13,15
X	DE 102015219996 A1 (BOSCH GMBH ROBERT [DE]) 20 April 2017 (2017-04-20) paragraph [0002] paragraph [0005] - paragraph [0021]	1-4,11-13,15
X	EP 3148154 B1 (NXP BV [NL]) 07 March 2018 (2018-03-07) cited in the application paragraph [0003]; figure 1	1-4,11-13,15
X	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,* 06 May 2012 (2012-05-06), pages 1-5 DOI: 10.1109/VETECS.2012.6240294 ISBN: 978-1-4673-0989-9. XP032202711 chapter "V. PROPOSED METHOD"; page 3 - page 4	1-4,11,13,15

☑ 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
20 May 2020	**20 July 2020**
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 **Raible, Markus** Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 102017209556 A1 (BOSCH GMBH ROBERT [DE]) 13 December 2018 (2018-12-13) paragraphs [0004], [0009], [0018] paragraph [0024] - paragraph [0028]	1-4,11-13,15
X	DE 102017209557 A1 (BOSCH GMBH ROBERT [DE]) 13 December 2018 (2018-12-13) paragraph [0004] - paragraph [0005]	1-4,11-13,15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/057450

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. claims: 2-4, 11-13, 15(in full); 1(in part)
This group contains variants of claim 1 (1a) for rendering the infiltrated communication unusable by overwriting the communication with the dominant bus level, or by the targeted modification of a specific part of the communication such as the CRC field of the communication, or (1b) by sending a warning in one or more dedicated warning communications, as well as various technical features of dependent claims 2, 3, 4, 11, 12, 13 and 15.

2. claim: 1(in part)
The special technical feature of this invention consists in "rendering the infiltrated communication unusable by overwriting the communication with a specific bit pattern". The special technical feature of this invention has the technical effect according to which the contents of the infiltrated communication are overwritten with bit patterns, wherein said bit patterns can be used to encode additional information. It solves the objective technical problem of how harmful information can be rendered void on the one hand while locally determined additional information relating to the attack can be distributed at the same time.

3. claim: 1(in part)
The special technical feature of this invention consists in "rendering the infiltrated communication unusable by placing an information entry in an additional field of the transmitted communications". The special technical feature of this invention has the technical effect according to which information relating to a recognised attack can be transmitted in the communication in addition to the information contained in said communication. It solves the objective technical problem of how the original content of the message can be retained, and how to evaluate it for more specific analysis of the attack.

4. claim: 1(in part)
The special technical feature of this invention consists in "warning another electronic station by transmitting implausible data content in one or more subsequent communications". The special technical feature of this invention results in the technical effect according to which preexisting safety mechanisms can also be used to identify cyber attacks. It solves the objective technical problem of how electronic stations which can verify the correct functioning of the system using validity checks of physical measurement values can be made capable of also reacting to cyber attacks.

5. claims: 5, 14
The special technical feature of this invention consists in the following: "a station carrying out a step of transferring the station into a secure state (Z4)". The special technical feature of this invention results in the technical effect according to which the system components are transferred into a secure state. It solves the objective technical problem of how a system affected by an attack can be transferred into a state of functional security.

6. claims: 6, 7
The special technical feature of this invention consists in the following: "as a further counter measure, a step of warning the vehicle driver with an optical acoustic or haptic signal is carried out". The special technical feature of this invention results in the technical effect according to which a local operator of a device in which the method is being carried out is warned prior to a potential malfunction of the device. It solves the objective technical problem of how a local operator of a device in which the method is being carried out can be warned prior to a potential malfunction of the device that was caused by a cyber attack.

7. claims: 8-10
The special technical feature of this invention consists in the following: as "a further counter measure, a step is carried out of issuing a notification of manipulation via radio to a central computer of the motor vehicle manufacturer or an authority or to a smartphone of the vehicle owner". The special technical feature of this invention results in the technical effect according to which a remote entity is informed of an attempted manipulation. It solves the objective technical problem of how a cyber attack can be discovered even if it has no recognisable effects locally or if the attacked system is damaged, for example as a consequence of the attack.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/057450

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☑ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: **2-4, 11-13, 15 (in full); 1 (in part)**

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2020/057450

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
DE 102009026995 A1	31 March 2011	CN 102804698 A	28 November 2012
		DE 102009026995 A1	31 March 2011
		EP 2443798 A1	25 April 2012
		RU 2012101207 A	27 July 2013
		US 2012210178 A1	16 August 2012
		WO 2010145985 A1	23 December 2010
DE 102015219996 A1	20 April 2017	CN 108141399 A	08 June 2018
		DE 102015219996 A1	20 April 2017
		EP 3363164 A1	22 August 2018
		KR 20180069843 A	25 June 2018
		US 2018302431 A1	18 October 2018
		WO 2017064001 A1	20 April 2017
EP 3148154 B1	07 March 2018	EP 3148154 A1	29 March 2017
		US 2017093659 A1	30 March 2017
DE 102017209556 A1	13 December 2018	CN 109005147 A	14 December 2018
		DE 102017209556 A1	13 December 2018
		US 2018359271 A1	13 December 2018
DE 102017209557 A1	13 December 2018	CN 109005148 A	14 December 2018
		DE 102017209557 A1	13 December 2018
		US 2018359262 A1	13 December 2018

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2020/057450

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L12/413 H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2009 026995 A1 (BOSCH GMBH ROBERT [DE]) 31. März 2011 (2011-03-31) Absätze [0002], [0006], [0007] Absatz [0009] - Absatz [0020]; Abbildung 1	1-4, 11-13,15
X	DE 10 2015 219996 A1 (BOSCH GMBH ROBERT [DE]) 20. April 2017 (2017-04-20) Absatz [0002] Absatz [0005] - Absatz [0021]	1-4, 11-13,15
X	EP 3 148 154 B1 (NXP BV [NL]) 7. März 2018 (2018-03-07) in der Anmeldung erwähnt Absatz [0003]; Abbildung 1	1-4, 11-13,15

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

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

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Mai 2020	20/07/2020

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	Raible, Markus

1

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2020/057450

Feld Nr. II Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein internationaler Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche diese Behörde nicht verpflichtet ist, nämlich

2. ☐ Ansprüche Nr.
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, dass eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich

3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefasst sind.

Feld Nr. III Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Diese Internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere Erfindungen enthält:

siehe Zusatzblatt

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.

2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung solcher Gebühren aufgefordert.

3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.

4. ☒ Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Dieser internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfasst:
2-4, 11-13, 15(vollständig); 1(teilweise)

Bemerkungen hinsichtlich eines Widerspruchs

☐ Der Anmelder hat die zusätzlichen Recherchengebühren unter Widerspruch entrichtet und die gegebenenfalls erforderliche Widerspruchsgebühr gezahlt.

☐ Die zusätzlichen Recherchengebühren wurden vom Anmelder unter Widerspruch gezahlt, jedoch wurde die entsprechende Widerspruchsgebühr nicht innerhalb der in der Aufforderung angegebenen Frist entrichtet.

☐ Die Zahlung der zusätzlichen Recherchengebühren erfolgte ohne Widerspruch.

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	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 Chapter "V. PROPOSED METHOD"; Seite 3 - Seite 4	1-4,11, 13,15
X	DE 10 2017 209556 A1 (BOSCH GMBH ROBERT [DE]) 13. Dezember 2018 (2018-12-13) Absätze [0004], [0009], [0018] Absatz [0024] - Absatz [0028]	1-4, 11-13,15
X	DE 10 2017 209557 A1 (BOSCH GMBH ROBERT [DE]) 13. Dezember 2018 (2018-12-13) Absatz [0004] - Absatz [0005]	1-4, 11-13,15

1

WEITERE ANGABEN **PCT/ISA/** 210

Die internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere (Gruppen von) Erfindungen enthält, nämlich:

1. Ansprüche: 2-4, 11-13, 15(vollständig); 1(teilweise)

Diese Gruppe beinhaltet Varianten des Anspruchs 1 (1a) zum Unbrauchbarmachen der eingeschleusten Botschaft durch Überschreiben der Botschaft mit dem dominanten Pegel oder durch das gezielte Verändern eines bestimmten Botschaftsteils, wie das CRC-Feld der Botschaft oder (1b) durch Senden einer Warnung in einer oder mehreren dedizierten Warn-Botschaft sowie diverse technische Merkmale der abhängigen Ansprüche 2, 3, 4, 11, 12, 13 und 15.

---

2. Anspruch: 1(teilweise)

Das spezielle technische Merkmal dieser Erfindung besteht im "Unbrauchbarmachen der eingeschleusten Botschaft durch Überschreiben der Botschaft mit einem bestimmten Bit-Muster".
Das spezielle technische Merkmal dieser Erfindung bewirkt den technischen Effekt, dass die Inhalte der eingeschleusten Nachricht durch Bit-Muster überschrieben werden, wobei die Bitmuster zur Kodierung zusätzlicher Informationen dienen können. Es löst die objektive technische Aufgabe, wie einerseits Schadinformationen unwirksam gemacht werden können und gleichzeitig lokal ermittelte zusätzliche Informationen über den Angriff verteilt werden können.

---

3. Anspruch: 1(teilweise)

Das spezielle technische Merkmal dieser Erfindung besteht im "Unbrauchbarmachen der eingeschleusten Botschaft durch das Setzen eines Informationseintrages in einem zusätzlichen Feld der gesendeten Botschaften".
Das spezielle technische Merkmal dieser Erfindung bewirkt den technischen Effekt, dass eine Information über einen erkannten Angriff zusätzlich zu den in der Botschaft enthaltenen Informationen in der Botschaft übertragen werden kann. Es löst die objektive technische Aufgabe, wie der ursprüngliche Inhalt der Nachricht erhalten werden kann, etwa um ihn zur genaueren Analyse des Angriffs auszuwerten.

---

4. Anspruch: 1(teilweise)

Das spezielle technische Merkmal dieser Erfindung besteht im "Warnen einer anderen elektronischen Station durch Senden von unplausiblen Dateninhalten in einer oder mehreren folgenden Botschaften".
Das spezielle technische Merkmal dieser Erfindung bewirkt den technischen Effekt, dass bereits vorhandene

Sicherheitsmechanismen auch zur Erkennung von Cyberangriffen genutzt werden können. Es löst die objektive technische Aufgabe, wie elektronische Stationen, die die korrekte Funktion des Systems durch Plausibilitätsprüfungen physikalischer Messwerte überprüfen können, in die Lage versetzt werden können, auch auf Cyberangriffe zu reagieren.

---

5. Ansprüche: 5, 14

Das spezielle technische Merkmal dieser Erfindung besteht darin dass "von einer Station ein Schritt des Überführens der Station in einen sicheren Zustand (Z4) ausgeführt wird." Das spezielle technische Merkmal dieser Erfindung bewirkt den technischen Effekt, dass dass Systembestandteile in einen sicheren Zustand überführt werden. Es löst die objektive technische Aufgabe, wie ein von einem Angriff betroffenes System in einen Zustand funktionaler Sicherheit überführt werden kann.

---

6. Ansprüche: 6, 7

Das spezielle technische Merkmal dieser Erfindung besteht darin dass "als weitere Gegenmaßnahme ein Schritt der Warnung des Fahrzeugführers mit einem optischen, akustischen oder haptischen Signal durchgeführt wird."
Das spezielle technische Merkmal dieser Erfindung bewirkt den technischen Effekt, dass ein lokaler Bediener einer Vorrichtung, in der das Verfahren ausgeführt wird, vor einer möglichen Fehlfunktion der Vorrichtung gewarnt wird. Es löst die objektive technische Aufgabe, wie ein lokaler Bediener einer Vorrichtung, in der das Verfahren ausgeführt wird, vor einer möglichen Fehlfunktion der Vorrichtung, die durch eine Cyberattacke verursacht wird, gewarnt werden kann.

---

7. Ansprüche: 8-10

Das spezielle technische Merkmal dieser Erfindung besteht darin dass als "weitere Gegenmaßnahme ein Schritt des Absetzens einer Manipulationsmeldung über Funk an einen Zentralrechner des Autoherstellers oder einer Behörde oder an ein Smartphone des Fahrzeughalters durchgeführt wird". Das spezielle technische Merkmal dieser Erfindung bewirkt den technischen Effekt, dass eine entfernte Instanz über einen Manipulationsversuch informiert wird. Es löst die objektive technische Aufgabe, wie ein Cyberangriff selbst dann entdeckt werden kann. wenn er lokal keine erkennbaren Auswirkungen hat oder das angegriffene System beispielsweise als Folge des Angriffs zerstört wurde.

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2020/057450

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102009026995 A1	31-03-2011	CN 102804698 A	28-11-2012
		DE 102009026995 A1	31-03-2011
		EP 2443798 A1	25-04-2012
		RU 2012101207 A	27-07-2013
		US 2012210178 A1	16-08-2012
		WO 2010145985 A1	23-12-2010
DE 102015219996 A1	20-04-2017	CN 108141399 A	08-06-2018
		DE 102015219996 A1	20-04-2017
		EP 3363164 A1	22-08-2018
		KR 20180069843 A	25-06-2018
		US 2018302431 A1	18-10-2018
		WO 2017064001 A1	20-04-2017
EP 3148154 B1	07-03-2018	EP 3148154 A1	29-03-2017
		US 2017093659 A1	30-03-2017
DE 102017209556 A1	13-12-2018	CN 109005147 A	14-12-2018
		DE 102017209556 A1	13-12-2018
		US 2018359271 A1	13-12-2018
DE 102017209557 A1	13-12-2018	CN 109005148 A	14-12-2018
		DE 102017209557 A1	13-12-2018
		US 2018359262 A1	13-12-2018