(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
03. Mai 2018 (03.05.2018)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2018/077528 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *H04L 12/40* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/072916

(22) Internationales Anmeldedatum:
12. September 2017 (12.09.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2016 220 895.0
25. Oktober 2016 (25.10.2016) DE

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

(72) Erfinder: **HARTKOPP, Oliver**; Volkswagen Aktiengesellschaft, 38436 Wolfsburg (DE). **OBERSCHACHTSIEK, André**; Lammer Heide 55, 38116 Braunschweig (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

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

(54) Title: DETECTION OF MANIPULATIONS IN A CAN NETWORK BY CHECKING CAN IDENTIFIERS

(54) Bezeichnung: ERKENNUNG VON MANIPULATIONEN IN EINEM CAN-NETZWERK MITTELS ÜBERPRÜFUNG VON CAN-IDENTIFIERN

(57) Abstract: By extending a Basic-CAN controller and/or a Full-CAN controller with a RX filter device, it is possible to compare the CAN identifiers intended for transmission for the CAN controller with those of the received CAN frames. In the case of a match, an interrupt is generated, since in this case an attack takes place. If no hardware expansion is intended, the RX-FIFO or TX-FIFO of a Full-CAN controller can be used for detecting an intrusion.

(57) Zusammenfassung: Durch eine Erweiterung eines Basic-CAN-Controllers bzw. eines Full-CAN-Controllers mit einer RX-Filtereinrichtung ist es möglich, die für den CAN-Controller zum Senden bestimmten CAN-Identifiern mit denjenigen der empfangenen CAN-Frames zu vergleichen. Im Fall einer Übereinstimmung wird ein Interrupt zu erzeugt, da in diesem Fall ein Angriff vorliegt. Falls keine Hardwareerweiterung beabsichtigt ist, so kann das RX-FIFO oder das TX-FIFO eines Full-CAN-Controllers zur Erkennung einer Intrusion herangezogen werden.

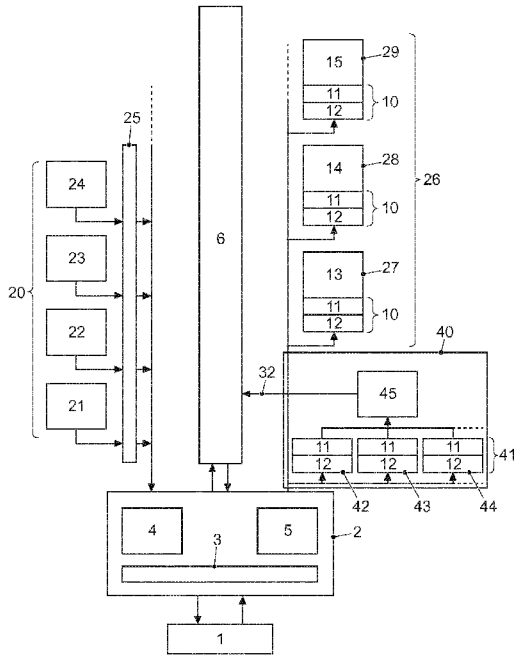

FIG. 5

WO 2018/077528 A1

Beschreibung

ERKENNUNG VON MANIPULATIONEN IN EINEM CAN-NETZWERK MITTELS ÜBERPRÜFUNG VON CAN-IDENTIFIERN

Die Erfindung betrifft einen Basic-CAN-Controller und einen Full-CAN-Controller zum Erkennen einer Manipulation in einem CAN-Netzwerk gemäß dem Oberbegriff der Ansprüche 1 und 2 sowie die Verwendung eines Full-CAN-Controllers gemäß dem Oberbegriff des Anspruchs 4 sowie des Anspruchs 5.

Das vorsätzliche Manipulieren von Inhalten auf CAN-Netzwerken im Fahrzeug, für das üblicherweise die Bezeichnung "Hacken" verwendet wird, ist ein intensiver Diskussionspunkt im Zusammenhang mit Cybersecurity für Fahrzeuge. Bei der Society of Automotive Engineers, kurz SAE, existiert bereits eine Vehicle Cybersecurity Working Group, welche die aktuellen Entwicklungen bei Manipulationen von Fahrzeugelektronik beobachtet und nach Möglichkeiten zu deren Verhinderung sucht.

Grundsätzlich kann eine Manipulation auf einem CAN-Bus auf zwei Arten erkannt werden:

Host-basierte Intrusion Detection, d.h. das Steuergerät selbst erkennt den Angriff, oder

Netzwerk-basierte Intrusion Detection, d.h. eine Kontrollinstanz erkennt den Angriff.

Weil der CAN-Bus eine Multi-Master-Kommunikationsverfahren verwendet, wird die Adressierung über die sog. CAN-Identifier in einer Art spezifiziert, dass Steuergeräte nur auf bestimmten Adressen, also CAN-Identifiern, senden dürfen, was zu einer Sicherstellung des Multimaster-Arbitrierungsverfahrens führt.

Bei einem Angriff werden vom Angreifer im Allgemeinen CAN-Botschaften gesendet, deren CAN-Identifier bereits für Steuergeräte sendeseitig zugewiesen wurden, um die Empfänger der zusätzlichen gesendeten Inhalte mit Identischem CAN-Identifier zu manipulieren.

Das ursprünglich sendende Steuergerät kann daher einen Angriff dadurch erkennen, dass es CAN-Identifier empfängt, welche eigentlich nur vom Steuergerät selbst hätten gesendet werden dürften. Dieses Host-basierte Verfahren ist bekannt und wird in der Literatur auch beschrieben.

Dabei werden CAN-Netzwerke durch die Vernetzung von Steuergeräten, sogenannten CAN-Controllern, mit einem CAN-Bus gebildet, wobei grundsätzlich zwei CAN-Controller-Architekturen unterschieden werden können:

Basic-CAN: Der Basic-CAN-Controller weist eine einfache Filterung mit typischerweise einem Filter für den Empfang von CAN-Nachrichten, sog. CAN-Frames, sowie wenig Speicherplatz für CAN-Nachrichten auf. Dies resultiert in einer hohen CPU-Belastung, da die Filterung primär durch Software erfolgt. Ferner ist die Hardware-Komplexität relativ zu den Kosten gering.

Full-CAN: Der Full-CAN-Controller umfasst mehrere Nachrichtenfilter mit zugehörigem Speicherplatz für CAN-Nachrichten, was zu einer geringeren CPU-Belastung führt, da die Filterung primär durch die Hardware erfolgt. Ferner ist das Verhältnis Hardware-Komplexität zu Kosten größer.

Die Überwachung des Empfang von CAN-Identifiern, die nur der CAN-Knoten selbst senden darf, kann nach dem Stand der Technik nur dadurch erreicht werden, dass für die entsprechenden CAN-Identifier Empfangsfilter im CAN-Controller konfiguriert werden. Die Menge der Empfangsfilter in einem CAN-Controller sind stark limitiert beispielsweise auf 4, 8, 16 oder 32 Filter. Diese Filter deduzieren die Anzahl der Interrupts des Steuergeräteprozessors und werden üblicherweise benötigt, um Anwendungsdaten von anderen CAN-Teilnehmern zu empfangen.

Diese wenigen (Empfangs-)Filter für die Überwachung von eigenen (Sende-)Identifiern einzusetzen ist aufgrund der mengenmäßigen Limitierungen nicht oder nur unvollständig realisierbar. Zudem muss das Steuergerät empfangene Anwendungsnachrichten von empfangenen Sendenachrichten im Fall eines Angriffs unterschiedlich verarbeiten.

Reicht die Menge der Empfangsfilter für die Überwachung der eigenen Sende-Identifier nicht aus, kann auch ein Filter definiert werden, der auf viele CAN-Identifier gleichzeitig reagiert. Dies

hat zur Folge, dass dabei die Anzahl der Interrupts vergleichsweise stark ansteigen wird, was zu einer zusätzlichen Belastung des Prozessors des Steuergerätes führt.

Grundsätzlich wird aufgrund dieser Restriktionen der CAN-Controller das an sich sinnvolle Erkennungsverfahren derzeit nur selten in Fahrzeugsteuergeräten realisiert.

So betrifft die Druckschrift DE 10 2013 200 525 A1 ein Verfahren und eine Vorrichtung zum Betrieb eines Kommunikationsnetzwerks, insbesondere eines Kraftfahrzeugs, wobei wenigstens zwei Steuergeräte über das Kommunikationsnetz datentechnisch miteinander verbunden sind. Insbesondere ist vorgesehen, dass der Datenverkehr in dem Kommunikationsnetzwerk erfasst wird, der erfasste Datenverkehr mit vorher erfassten Daten des Datenverkehrs verglichen und als Ergebnis des Vergleichs eine mögliche Datenmanipulation erkannt wird. Im Falle einer erkannten Datenmanipulation wird wenigstens ein Abschaltsignal an wenigstens ein Steuergerät übermittelt und das wenigstens eine ein Abschaltsignal empfangende Steuergerät in einen sicheren Betriebszustand übergeführt.

Weiterhin betrifft die Druckschrift DE 10 2013 200 535 A1 ein Verfahren und eine Vorrichtung zum Betrieb eines Kommunikationsnetzwerks eines Kraftfahrzeugs, wobei wenigstens zwei Steuergeräte mit dem Kommunikationsnetz gekoppelt sind. Insbesondere ist vorgesehen, dass von einem ersten Steuergerät an ein zweites Steuergerät gesendete Daten oder Nachrichten über wenigstens zwei Kommunikationspfade des Kommunikationsnetzwerks übertragen werden und dass die über die wenigstens zwei Kommunikationspfade bei dem zweiten Steuergerät eingehenden Daten bzw. Nachrichten anhand einer Plausibilitätsprüfung auf eine mögliche Datenmanipulation hin geprüft werden.

Die Druckschrift US 20140337976 A1 betrifft ein Verfahren zum Betreiben eines in einem Fahrzeug installierten mobilen Routers. Dabei umfasst das Fahrzeug ein Netzwerk in Form eines Busses, der mit einer Vielzahl von elektronischen Steuergeräten verbunden ist. Ferner umfasst der mobile Router eine Schnittstelle für ein Weitverkehrsfunknetz (WWAN), eine Schnittstelle für ein lokales Funkverkehrsnetzwerk (WLAN), eine Schnittstelle zu einem Netzwerkbusses eines Fahrzeugs, einen Prozessor und einen Speicher mit einer Vielzahl von Programmen. Die Vielzahl von Programmen umfasst ein vom Prozessor ausführbares Intrusionserkennungsprogramm. Das Verfahren zum Betreiben des mobilen Routers umfasst das Überwachen des Daten auf dem Netzwerkbus, das Erkennen einer oder mehrerer Anomalien in den überwachten Daten von dem Intrusionserkennungsprogramm und das Erzeugen einer Warnung nach dem Erkennen einer oder mehrerer Anomalien.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zu schaffen, womit eine Manipulation auf einem CAN-Netzwerk bzw. CAN-Bus einfach und sicher erkannt werden kann.

Diese Aufgabe wird gelöst durch einen Basic-CAN-Controller mit den Merkmalen des Anspruchs 1, einen Full-CAN-Controller mit den Merkmalen des Anspruchs 2, durch die Verwendung eines Full-CAN-Controllers mit den Merkmalen des Anspruchs 4 sowie durch die Verwendung eines Full-CAN-Controllers mit den Merkmalen des Anspruchs 5. Bevorzugte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

Der erfindungsgemäße Basic-CAN-Controller zum Erkennen einer Manipulation in einem CAN-Netzwerk umfasst

- einen CAN-Transceiver zum Verbinden des Basic-CAN-Controllers mit einem CAN-Bus,
- eine CAN-Protocol-Engine zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
  ein TX-FIFO zum Speichern von zu übertragenden CAN-Frames,
  ein RX-FIFO zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei vor dem RX-FIFO ein Filterelement angeordnet ist, welches die für den Basic-CAN-Controller bestimmten CAN-Frames filtert und zulässige CAN-Frames an das RX-FIFO weiterleitet, und
- ein Host-Control-Interface zur Kommunikation von Steuerinformationen zwischen der CAN-Protocol-Engine und einem Hostrechner, wobei
- der Basic-CAN-Controller eine RX-Filtereinrichtung aufweist, welche anhand der dem Basic-CAN-Controller zum Senden von CAN-Frames zugeordneten, für den Basic-CAN-Controller spezifischen CAN-Identifiern überprüft, ob ein empfangenes CAN-Frame einen CAN-Identifier aufweist, welcher mit einem der für den Basic-CAN-Controller spezifischen CAN-Identifiern identisch ist, und im Fall einer Übereinstimmung einen Intrusionserkennungs-Interrupt IDS-IRQ an das Host-Control-Interface auslöst.

Der erfindungsgemäße Full-CAN-Controller zum Erkennen einer Manipulation in einem CAN-Netzwerk umfasst

- eine CAN-Transceiver zum Verbinden des Full-CAN-Controllers mit einem CAN-Bus,
- eine CAN-Protocol-Engine zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
- ein TX-FIFO zum Speichern von zu sendenden CAN-Frames,
- einen Prioritätsselektor zum Übertragen eines zu sendenden CAN-Frames an die CAN-Protocol-Engine als Funktion der Priorität,
- ein RX-FIFO zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei das RX-FIFO eine Vielzahl von CAN-Filter-Speicherelementen und jedes CAN-Filter-Speicherelement ein Filterelement zum Filtern zulässiger, für den Full-CAN-Controller bestimmter CAN-Frames aus den empfangenen CAN-Frames und zum Speichern eines zulässigen CAN-Frames in einem CAN-Frame-Speicherelement aufweist, und
- ein Host-Control-Interface zur Kommunikation von Steuerinformationen zwischen der CAN-Protocol-Engine und einem Hostrechner, wobei
- der Full-CAN-Controller eine RX-Filtereinrichtung aufweist, welche anhand der dem Full-CAN-Controller zum Senden von CAN-Frames zugeordneten, für den Full-CAN-Controller spezifischen CAN-Identifiern überprüft, ob ein empfangenes CAN-Frame einen CAN-Identifier aufweist, welcher mit einem der für den Full-CAN-Controller spezifischen CAN-Identifiern identisch ist, und im Fall einer Übereinstimmung einen Intrusionserkennungs-Interrupt IDS-IRQ an das Host-Control-Interface auslöst.

Vorzugsweise weist die RX-Filtereinrichtung eine Filterbank umfassend ein oder mehrere Filterelemente auf, wobei die Filterelemente eine Überprüfung eines empfangenen CAN-Frames dahingehend vornehmen, ob dessen CAN-Identifier einem der für den CAN-Controller spezifischen, zum Senden bestimmten CAN-Identifiern entspricht, und weist ein Speicherelement zur Speicherung eines empfangenen CAN-Frames auf, dessen CAN-Identifier mit einem für den CAN-Controller spezifischen CAN-Identifier übereinstimmt.

Bei der erfindungsgemäßen Verwendung eines Full-CAN-Controllers zur Erkennung von Manipulationen in einem CAN-Netzwerk, wobei der Full-CAN-Controller aufweist

- einen CAN-Transceiver zum Verbinden des Full-CAN-Controllers mit einem CAN-Bus,
- eine CAN-Protocol-Engine zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,

- ein TX-FIFO zum Speichern von zu sendenden CAN-Frames,
- einen Prioritätsselektor zum Übertragen eines zu sendenden CAN-Frames an die CAN-Protocol-Engine als Funktion der Priorität,
- ein RX-FIFO zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei das RX-FIFO eine Vielzahl von CAN-Filter-Speicherelementen und jedes CAN-Filter-Speicherelement ein Filterelement zum Filtern zulässiger, für den Full-CAN-Controller bestimmter CAN-Frames aus den empfangenen CAN-Frames und zum Speichern eines zulässigen CAN-Frames in einem CAN-Frame-Speicherelement aufweist, und
- ein Host-Control-Interface zur Kommunikation von Steuerinformationen zwischen der CAN-Protocol-Engine und einem Hostrechner,

sind die Filterelemente einer Teilmenge der CAN-Filter-Speicherelementen des RX-FIFOS mit den für den Full-CAN-Controller zum Senden eines CAN-Frames spezifischen CAN-Identifiern belegt, so dass eine Überprüfung der CAN-Identifier der empfangenen CAN-Frames mit den für den Full-CAN-Controller spezifischen CAN-Identifiern in den jeweiligen Filterelementen erfolgt. Im Fall einer Übereinstimmung eines empfangenen CAN-Identifiers mit einem der spezifischen CAN-Identifier des Full-CAN-Controllers wird ein Abspeichern des empfangenen CAN-Identifiers in dem entsprechenden CAN-Frame-Speicherelement und ein Erzeugen eines Intrusionserkennungs-Interrupts IDS-IRQ an das Host-Control-Interface bewirkt.

Bei einer weiteren erfindungsgemäßen Verwendung eines Full-CAN-Controllers zur Erkennung von Manipulationen in einem CAN-Netzwerk, wobei der Full-CAN-Controller aufweist

- einen CAN-Transceiver zum Verbinden des Full-CAN-Controllers mit einem CAN-Bus,
- eine CAN-Protocol-Engine zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
- ein TX-FIFO mit einer Vielzahl von CAN-Frame-Speicherelementen zum Speichern von zu sendenden CAN-Frames,
- einen Prioritätsselektor zum Übertragen eines zu sendenden CAN-Frames an die CAN-Protocol-Engine als Funktion der Priorität,
- ein RX-FIFO zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei das RX-FIFO eine Vielzahl von CAN-Filter-Speicherelementen und jedes CAN-Filter-Speicherelement ein Filterelement zum Filtern zulässiger, für den Full-CAN-Controller bestimmter CAN-Frames aus den empfangenen CAN-Frames und zum Speichern eines zulässigen CAN-Frames in einem CAN-Frame-Speicherelement aufweist, und

- ein Host-Control-Interface zur Kommunikation von Steuerinformationen zwischen der CAN-Protocol-Engine und einem Hostrechner,

werden empfangene CAN-Frames den CAN-Frame-Speicherelementen des TX-FIFOs zur Empfangszeit zugeführt und auf eine Übereinstimmung des CAN-Identifier des empfangenen CAN-Frames mit den in den CAN-Frame-Speicherelementen vorliegenden, zum Senden bestimmten CAN-Identifiern verglichen und im Fall einer Übereinstimmung wird ein Erzeugen eines Intrusionserkennungs-Interrupts IDS-IRQ an das Host-Control-Interface bewirkt.

Zusammenfassend wird durch die Erweiterung eines Basic-CAN-Controllers bzw. eines Full-CAN-Controllers mit einer RX-Filtereinrichtung die Möglichkeit geschaffen, die für den CAN-Controller zum Senden bestimmten CAN-Identifiern mit denjenigen der empfangenen CAN-Frames zu vergleichen und ein Interrupt zu erzeugen, falls eine Übereinstimmung aufgefunden wird, da in diesem Fall ein Angriff vorliegt. Die zusätzliche RX-Filtereinrichtung bedingt jedoch eine Erweiterung der Hardware des CAN-Controllers, wobei sowohl das vorhandene TX-FIFO als auch das RX-FIFO für die Intrusionserkennung keine Funktion übernehmen.

Falls keine Hardwareerweiterung beabsichtigt ist, so kann das RX-FIFO oder das TX-FIFO eines Full-CAN-Controllers zur Erkennung einer Intrusion herangezogen werden.

Der Intrusionserkennungs-Interrupt IDS-IRQ, welcher die Erkennung einer Intrusion an das Host-Control-Interface meldet, kann als separate Leitung ausgeführt sein. Vorzugsweise wird der Intrusionserkennungs-Interrupt IDS-IRQ als zusätzliche Interrupt-Quelle im Interrupt-Control-Register des CAN-Controllers ausgeführt, in dem auch andere Interrupt-Quellen, wie beispielsweise TX-, RX-, Error-, Overflow-Interrupts, konfiguriert werden können.

Eine bevorzugte Ausgestaltung der Erfindung wird nachfolgend anhand der Zeichnungen erläutert. Dabei zeigt

Fig. 1 einen Basic-CAN-Controller nach dem Stand der Technik,

Fig. 2 einen Full-CAN-Controller nach dem Stand der Technik,

Fig. 3 einen Full-CAN-Controller mit einer ersten Variante einer Intrusionserkennung,

Fig. 4 einen Full-CAN-Controller mit einer zweiten Variante einer Intrusionserkennung,

Fig. 5 einen Full-CAN-Controller mit einem Filtereinrichtung zur Intrusionserkennung, und

Fig. 6 einen Basic-CAN-Controller mit einem Filtereinrichtung zur Intrusionserkennung.

In Fig. 1 ist in schematischer Darstellung ein bekannter Basic-CAN-Controller mit seinen wesentlichen Elementen dargestellt, wie er beispielsweise in dem Basic-CAN-Controller SJA1000 der Firma NXP realisiert ist. Da sich im Bereich der CAN-Busse die englische Bezeichnung der einzelnen Elemente durchgesetzt hat, wird diese in der folgenden Beschreibung beibehalten. Die Verbindung zum zweidrahtigen CAN-Bus (nicht dargestellt) erfolgt über einen CAN-Transceiver 1, der vom Bus die codierten Signale abgreift bzw. diese auf den Bus legt. Der CAN-Transceiver 1 wiederum ist mit einer CAN-Protocol-Engine 2 verbunden, die den empfangenen Bitstrom dekodiert bzw. den zu sendenden Bitstrom entsprechend dem CAN-Protokoll kodiert. Zu diesem Zweck umfasst die CAN-Protocol-Engine 2 einen Bitstrom-Encoder 4 und einen Bitstrom-Decoder 5, wobei eine Steuerlogik 3 den Betrieb überwacht und steuert.

Eine CAN-Nachricht, welche hier auch als CAN-Frame bezeichnet wird, umfasst einen vorausgestellten CAN-Identifier, der im Standard-Frame-Format eine Länge von 11 Bit und im Extended-Frame-Format eine Länge von 28 Bit aufweist, dem außer bei einem RTR Frame (Remote Transmission Request) Nutzdaten nachfolgen, beispielsweise 8 Byte. Dabei kennzeichnet ein CAN-Identifier, der auch als Objekt Identifiziert wird, den Inhalt des CAN-Frames und nicht die Adresse des Gerätes. Zum Beispiel kann in einem Messsystem den Parametern Temperatur, Spannung und Druck jeweils ein eigener Identifier zugewiesen sein. Es können mehrere Parameter unter einem CAN-Identifier vereint sein, solange die Summe der Daten die maximal mögliche Länge des Nutzdatenfeldes, also hier im Beispiel 8 Byte bzw. im Fall von CAN FD maximal 64 Byte, nicht überschreitet. Die Empfänger entscheiden anhand des CAN-Identifiers, ob die Nachricht für sie relevant ist oder nicht. Zudem dient der CAN-Identifier auch der Priorisierung der CAN-Nachrichten bzw. CAN-Frames. Als ID-Value wird der "Wert" des CAN-Identifiers bezeichnet

Der in Fig. 1 dargestellte Basic-CAN-Controller umfasst einen Filter 10, wodurch die Möglichkeit besteht empfangene CAN-Frames zu filtern, d.h. zu akzeptieren oder auszusortieren. Um eine Filterung durchführen zu können, weist der Filter 10 eine ID-Maske 11 auf, die den CAN-Identifier 12 und den empfangenen CAN-Identifier über eine UND-Funktion logisch verknüpft.

Ein empfangenes CAN-Frame wird daher vom Filter 10 akzeptiert, wenn gilt:
(empfangene CAN-ID UND ID-Maske 11) ist gleich (ID-Value 12 UND ID-Maske 11)

Hat der Filter 10 einen CAN-Frame akzeptiert, so wird dieser in einen Empfangs-Speicherbereich verschoben, welches als RX-FIFO 18 bezeichnet wird, wobei RX für "Receive" steht. Das RX-FIFO 18 im Beispiel der Fig. 1 umfasst vier Speicherbereiche 13, 14, 15 und 16, in denen jeweils ein CAN-Frame abgespeichert werden kann, welches den jeweiligen CAN-Identifier, Flags und Daten umfasst. Ferner ist das abgespeichert CAN-Frame gegebenenfalls mit einem Datum, also einem Timestamp, versehen. In der einfachsten Ausbaustufe besteht das RX-FIFO 18 aus nur einem Speicherbereich 13, was zwangsläufig dazu führt, dass mit dem Erhalt und Abspeichern eines gefilterten und damit zulässigen CAN-Frames über das Host-Control-Interface 6 ein Interrupt an den Host-Rechner (nicht dargestellt) gesendet werden muss, damit das im Speicherbereich 13 gespeicherte CAN-Frame vor dem Eintreffen eines nächsten zulässigen CAN-Frames vom Host-Rechner übernommen wird. Ist daher der Host-Rechner überlastet und kann trotz Erhalt eines Interrupts vom Host-Control-Interface 6 die aktuelle CAN-Nachricht aus dem Speicherbereich 13 nicht abrufen, so wird gegebenenfalls die aktuelle gespeicherte CAN-Nachricht durch die nächste zulässige CAN-Nachricht überschrieben. Durch die Verwendung eines entsprechend großen RX-FIFOs 18 mit mehreren Speicherbereichen 13, 14, 15, 16 wird diese Möglichkeit des Überschreibens herabgesetzt.

Auf der linken Seite der Fig. 1 ist der Sende-Speicherbereich dargestellt, der als das TX-FIFO 9 bezeichnet wird, welches den FIFO-Speicher für die auszugebenden CAN-Frames zeigt. Dabei umfasst das TX-FIFO 9, wobei TX für "Transmit" steht, zwei Speicherbereiche 7, 8 zur vorübergehenden Speicherung der zu übertragenden CAN-Frames mit CAN-Identifier, Flags und Daten.

Die Fig. 2 zeigt einen Full-CAN-Controller nach dem Stand der Technik, wie er beispielsweise im oben genannten Full-CAN-Controller 82C900 von der Firma Infineon realisiert ist, wobei gleiche Bezugszeichen in üblicher Weise identische Komponenten bezeichnen.

Die Verbindung zum zweidrahtigen CAN Bus (nicht dargestellt) erfolgt wie beim Basic-CAN-Controller über den CAN-Transceiver 1, der vom Bus die codierten Signale abgreift bzw. die codierten Signale auf den Bus legt. Der CAN Transceiver 1 erhält den Bitstrom bzw. schickt den empfangenen Bitstrom in die CAN-Protocol-Engine 2, die den empfangenen Bitstrom dekodiert bzw. den zu sendenden Bitstrom entsprechend dem CAN-Protokoll kodiert. Zu diesem Zweck

weist die CAN-Protocol-Engine 2 einen Bitstrom-Encoder 4 und einen Bitstrom-Decoder 5 auf, wobei eine Steuerlogik 3 den Betrieb der CAN-Protocol-Engine 2 überwacht und steuert. Ferner ist die CAN-Protocol-Engine 2 mit einem Host-Control-Interface 6 verbunden, welches die Verbindung zu einem Hostrechner (nicht dargestellt) herstellt, um beispielsweise mittels einer Interrupt-Generierung dem Host-Rechner den Erhalt eines CAN-Frames anzuzeigen.

Ein empfangenes CAN-Frame wird in dem Full-CAN-Controller einem RX-Nachrichtenpuffer 26 zugeführt, der eine vorgegebene Anzahl von Filter-Speicherelementen 27, 28, 29 und 30 aufweist. In der Fig. 2 sind vier Filter-Speicherelemente 27, 28, 29, 30 angegeben, jedoch ist die Anzahl der Filter-Speicherelemente 27, 28, 29, 30 nur beispielhaft zu verstehen und an die an den CAN-Controller gestellten Anforderungen anpassbar.

Jedes Filter-Speicherelement 27, 28, 29, 30 des RX-Nachrichtenpuffers 26 umfasst einen Filter 10, bestehend aus der Verknüpfung zwischen dem ID-Value 11 des CAN-Identifiers und der ID-Maske 12, sowie einen nachfolgenden Speicherbereich 13, 14, 15, 16, in welchem der gefilterte CAN-Frame mit ID-Value, Flags, Daten und Zeitstempel abgespeichert wird und zur Abholung durch den Hostrechner (nicht dargestellt) bereitsteht. Zwar wird durch die Verwendung mehrerer Filter 10 im jeweiligen Filter-Speicherelement 27, 28, 29, 30 die Verwendung mehrerer voneinander unabhängiger ID-Masken möglich, jedoch ist die Bereitstellung der empfangenen CAN-Frames an den Hostrechner zeitkritisch und ein Interrupt muss innerhalb der Zeit abgearbeitet werden, innerhalb derer ein Filter-Speicherelement 27, 28, 29, 30 mit einem nächsten zulässigen CAN-Frame überschrieben werden könnte. Ist beispielsweise das erste Filter-Speicherelement 27 mit einem zulässigen CAN-Frame belegt, was bedeutet, dass ein ankommendes CAN-Frame einen zur ID-Maske 11 passenden ID-Value aufweist, so wird dem Hostrechner per Interrupt mitgeteilt, dass ein CAN-Frame zur Abholung ansteht. Wird nun der Interrupt innerhalb eines vorgegebenen Zeitraums, der beispielsweise vom einem Messzyklus vorgegeben ist, nicht schnell genug abgearbeitet, so kann innerhalb des vorgegebenen Zeitraums ein nächstes CAN-Frame mit einem zur ID-Maske 11 passenden ID-Value 12 zur Speicherung an dem speziellen Filter-Speicherelement 27 anstehen, wodurch das abgespeicherte vorherige CAN-Frame überschrieben wird und somit verloren geht.

Die Sendeseite des Full-CAN-Controllers der Fig. 2 umfasst eine TX-Sendepuffer 20, der mehrere CAN-Frame-Speicherbereiche 21, 22, 23 und 24 aufweist, in welche vom Hostrechner CAN-Frames zur Versendung abgelegt werden können. Nachfolgend dem TX-Sendepuffer 20 ist ein Prioritätsselektor 25 angeordnet, der CAN-Frames mit höherer Priorität bevorzugt sendet. Dabei wird die Priorität über den ID-Value festgelegt. Das vom Prioritätsselektor 25 zur

Sendung bestimmte CAN-Frame wird dann von der CAN-Protocol-Engine 2 über den CAN-Transceiver 1 auf den CAN-Bus (nicht dargestellt) gelegt.

Fig. 3 zeigt einen Full-CAN-Controller entsprechend demjenigen der Fig. 2, bei dem eine erste Variante einer Intrusionserkennung realisiert ist. Identische Bezugszeichen der Full-CAN-Controller der Figuren 2 und 3 bezeichnen identische Elemente, so dass zur Beschreibung deren Funktionalität auf Fig. 2 verwiesen wird. Kurz zusammengefasst umfasst der CAN-Controller der Fig. 3 einen CAN-Transceiver 1 zur Verbindung mit dem CAN-BUs (nicht dargestellt), eine CAN-Protocol-Engine 2 zur Kodierung und Dekodierung der vom CAN-Transceiver empfangenen Daten, ein Host-Control-Interface 6 zur Verbindung des Full-CAN-Controllers mit einem Hostrechner, einem RX-Nachrichtenpuffer 26 zur temporären Speicherung von für diesen CAN-Controller bestimmten CAN-Frames und einem TX-Nachrichtenpuffer zum temporären Speichern von zu übertragenden CAN-Frames.

Wie bereits erwähnt, ist jedem CAN-Controller einen Anzahl von CAN-Identifier zum Senden von CAN-Frames zugeordnet, die zulässig und zu benutzen sind. Empfängt ein CAN-Controller daher ein CAN-Frame mit einem zugehörigen CAN-Identifier, so kann der CAN-Controller bzw. der entsprechende Hostrechner anhand des CAN-Identifiers feststellen, ob dieses CAN-Frame ein Angriff darstellt oder nicht. Ist das CAN-Frame als Angriff erkannt, da ein CAN-Identifier benutzt wurde, der eigentlich dem empfangenden CAN-Controller zur Aussendung zugeordnet ist, so kann eine entsprechende Reaktion des CAN-Controllers erfolgen, beispielsweise indem dieses unzulässige CAN-Frame mittels eines entsprechenden Error-Frames für andere lesende CAN-Controller des Netzwerkes unschädlich gemacht wird.

Um eine Intrusion, also einen Angriff, erkennen zu können, werden daher eine Anzahl von CAN-Filter-Speicherelementen 27, 28, 29 und 30 derart konfiguriert, dass in den jeweiligen ID-Maskenbereichen 11 die dem CAN-Controller zugewiesenen eigenen, zum Senden dienenden CAN-Identifier abgelegt werden. Akzeptiert nun ein CAN-Filter-Speicherelement 27, 28, 29, 30 ein CAN-Frame mit einem für den CAN-Controller spezifischen CAN-Identifier aufgrund einer positiven Filterung des entsprechenden Filterelements 10, so wird ein Intrusion-Interrupt-Request, ein sogenannter IDS-IRQ 32, ausgelöst und mittels des Host-Control-Interface 6 an den nicht dargestellten Hostrechner übermittelt, der dann beispielsweise das Senden eines entsprechenden Error-Frames bewirkt.

Allerdings wird durch die Benutzung einiger der CAN-Filter-Speicherelemente als Detektoren für CAN-Frames mit den eigenen spezifischen CAN-Identifiern die Anzahl der für den Empfang der für den CAN-Controller bestimmten CAN-Frames mit zulässigen CAN-Identifiern verringert.

Fig. 4 zeigt einen Full-CAN-Controller entsprechend demjenigen der Fig. 2, bei dem eine zweite Variante der Intrusionserkennung realisiert ist. Die Erkennung eines Angriffs erfolgt wie im Beispiel des Full-CAN-Controllers der Fig. 3 über die Untersuchung des CAN-Identifiers eines empfangenen CAN-Frames. Im Full-CAN-Controller der Fig. 4 erfolgt die Überprüfung der empfangenen CAN-Frames mittels der CAN-Frame-Speicherelemente 21, 22, 23, 24 des TX-Nachrichtenpuffers 20. Dazu werden die empfangenen CAN-Frames hinter dem Bitstream-Decoder 5 der CAN-Protocol-Engine 2 parallel zum RX-Nachrichtenpuffer 26 abgegriffen und den CAN-Frame-Speicherelementen 21, 22, 23, 24 des TX-Nachrichtenpuffers 20 zugeführt. In den CAN-Frame-Speicherelementen 21, 22, 23, 24 wird der CAN-Identifier eines empfangenen CAN-Frames zur Empfangszeit geprüft und ein IDS-IRQ 32 erzeugt und dem Hostrechner (nicht dargestellt) zugeführt, wenn der empfangene CAN-Identifier einem solchen entspricht, der für den Full-CAN-Controller reserviert und damit spezifisch ist. Als Resultat kann der Full-Can-Controller ein entsprechendes Error-Frame erzeugen und auf den CAN-Bus legen, wodurch der Angriff unschädlich gemacht wird.

Fig. 5 zeigt einen Full-CAN-Controller entsprechend demjenigen der Fig. 2, bei dem eine Intrusionserkennung mittels einer separaten RX-Filtereinrichtung 40 realisiert ist, welche die empfangenen CAN-Frames unmittelbar hinter der CAN-Protocol-Engine 2 abgreift, d.h. unmittelbar nach dem Empfang. Dabei umfasst die RX-Filtereinrichtung eine Filterbank 41 umfassend eine Mehrzahl von Filterelementen 42, 43, 44, wobei die hier dargestellt Anzahl von drei Filterelementen 42,43, 44 nur symbolisch zu verstehen ist und die Anzahl der Filterelemente 42, 43, 44 üblicherweise größer als drei ist. Ein Filterelement 42, 43, 44 wird dabei aus einer ID-Maske 11 und einem ID-Identifierwert 12 gebildet. Dabei werden in den ID-Identifierwerten 12 der Filterelemente 42, 43, 44 die CAN-Identifier der zu überwachenden CAN-Frames eingebracht. Da üblicherweise auf genau einen CAN-Identifier in einem Filterelement 42, 43, 44 gefiltert werden soll, wird in die ID-Maske 11 ein Wert eingetragen, bei dem alle Bits des Filters gesetzt sind. Alternativ kann das Filterelement 42, 43, 44 auch in der Form ausgestaltet sein, dass nur ein ID-Identifierwert 12 eingetragen werden muss, um eine Filterung durchzuführen.

In den Filterelementen 42, 43, 44 der Filterbank 41 erfolgt nun eine Vergleich zwischen den abgelegten CAN-Identifiern des Full-CAN-Controllers und den empfangenen CAN-Identifiern. Wird eine Übereinstimmung festgestellt, so erfolgt ein Ablegen des entsprechenden CAN-Frames im Speicherelement 45 der RX-Filtereinrichtung 40 und es ein Erzeugen eines Interrupts IDS-IRQ 32 , welches über das Host-Control-Interface 6 an den Hostrechner (nicht dargestellt) weitergeleitet wird. Zusätzlich kann der CAN-Controller bei entsprechender Konfiguration das Erzeugen und Versenden eines Error-Frames einleiten. Mit anderen Worten, wenn ein empfangenes CAN-Frame in das Speicherelement 45 der RX-Filtereinrichtung abgelegt wird, so ist dieses CAN-Frame als Angriff erkannt worden, da ein CAN-Identifier benutzt wurde, der dem Full-CAN-Controller sendeseitig vorbehalten ist. Mit Hilfe des Inhalts aus Speicherelement 45 kann das zum Angriff genutzte CAN-Frame für forensische Zwecke ausgelesen werden.

Fig. 6 zeigt einen Basic-CAN-Controller entsprechend demjenigen der Fig. 1, bei dem eine Intrusionserkennung mittels einer separaten RX-Filtereinrichtung 40 realisiert ist. Dabei entspricht die RX-Filtereinrichtung 40 derjenigen der Fig. 5, so dass für eine ausführliche Erläuterung der Funktionsweise auf die entsprechende Beschreibung der Fig. 5 verwiesen wird. Die für den Basic-CAN-Controller zum Senden vorgesehenen CAN-Identifier werden in den Filterelementen 42, 43, 44 der Filterbank 41 gespeichert und mit den CAN-Identifiern der empfangenen CAN-Frames verglichen. Im Fall einer Übereinstimmung liegt daher ein Angriff oder eine Intrusion vor und es erfolgt nach der Ablage des ermittelten CAN-Frames im Speicherelement 45 die Erzeugung eines Interrupts IDS-IRQ 32.

Bezugszeichenliste

1	CAN Transceiver
2	CAN Protocol Engine
3	Steuerlogik
4	Bitstream Encoder
5	Bitstream Decoder
6	Host Control Interface
7	CAN-Frame-Speicherbereich
8	CAN-Frame-Speicherbereich
9	TX- Nachrichtenpuffer /TX-FIFO
10	Filtereinrichtung
11	ID-Maskenbereich
12	ID-Identifier-Bereich
13	CAN-Frame-Speicherelement
14	CAN-Frame-Speicherelement
15	CAN-Frame-Speicherelement
16	CAN-Frame-Speicherelement
18	RX- Nachrichtenpuffer / RX-FIFO
20	TX-Nachrichtenpuffer /TX-FIFO
21	CAN-Frame-Speicherelement
22	CAN-Frame-Speicherelement
23	CAN-Frame-Speicherelement

24 CAN-Frame-Speicherelement

25 Prioritätsselektor

26 RX- Nachrichtenpuffer / RX-FIFO

27 CAN-Filter-Speicherelement

28 CAN-Filter-Speicherelement

29 CAN-Filter-Speicherelement

30 CAN-Filter-Speicherelement

32 IDS-IRQ

40 RX-Filtereinrichtung

41 Filterbank

42 Filterelement

43 Filterelement

44 Filterelement

45 Speicherelement

Patentansprüche

1. Basic-CAN-Controller mit
einem CAN-Transceiver (1) zum Verbinden des Basic-CAN-Controllers mit einem CAN-Bus,
einer CAN-Protocol-Engine (2) zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
einem TX-FIFO (9) zum Speichern von zu übertragenden CAN-Frames,
einem RX-FIFO (18) zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei vor dem RX-FIFO (18) ein Filterelement (10) angeordnet ist, welches die für den Basic-CAN-Controller bestimmten CAN-Frames filtert und zulässige CAN-Frames an das RX-FIFO (18) weiterleitet, und
einem Host-Control-Interface (6) zur Kommunikation von Steuerinformationen zwischen der CAN-Protocol-Engine (2) und einem Hostrechner,
dadurch gekennzeichnet, dass
der Basic-CAN-Controller eine RX-Filtereinrichtung (40) aufweist, welche anhand der dem Basic-CAN-Controller zum Senden von CAN-Frames zugeordneten, für den Basic-CAN-Controller spezifischen CAN-Identifiern dahingehend überprüft, ob ein empfangenes CAN-Frame einen CAN-Identifier aufweist, welcher mit einem der für den Basic-CAN-Controller spezifischen CAN-Identifiern identisch ist, und im Fall einer Übereinstimmung einen Intrusionserkennungs-Interrupt IDS-IRQ (32) an das Host-Control-Interface auslöst.

2. Full-CAN-Controller mit
einem CAN-Transceiver (1) zum Verbinden des Full-CAN-Controllers mit einem CAN-Bus,
einer CAN-Protocol-Engine (2) zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
einem TX-FIFO (20) zum Speichern von zu sendenden CAN-Frames,
einem Prioritätsselektor (25) zum Übertragen eines zu sendenden CAN-Frames an die CAN-Protocol-Engine (2) als Funktion der Priorität,

einem RX-FIFO (26) zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei das RX-FIFO (26) eine Vielzahl von CAN-Filter-Speicherelementen (27, 28, 29, 30) und jedes CAN-Filter-Speicherelement (27, 28, 29, 30) ein Filterelement (10) zum Filtern zulässiger, für den Full-CAN-Controller bestimmter CAN-Frames aus den empfangenen CAN-Frames und zum Speichern eines zulässigen CAN-Frames in einem CAN-Frame-Speicherelement (13, 14, 15, 16) aufweist, und
einem Host-Control-Interface (6) zur Kommunikation von Steuerinformationen zwischen der CAN-Protocol-Engine (2) und einem Hostrechner,
dadurch gekennzeichnet, dass
der Full-CAN-Controller eine RX-Filtereinrichtung (40) aufweist, welche anhand der dem Full-CAN-Controller zum Senden von CAN-Frames zugeordneten, für den Full-CAN-Controller spezifischen CAN-Identifiern überprüft, ob ein empfangenes CAN-Frame einen CAN-Identifier aufweist, welcher mit einem der für den Full-CAN-Controller spezifischen CAN-Identifiern identisch ist, und im Fall einer Übereinstimmung einen Intrusionserkennungs-Interrupt IDS-IRQ (32) an das Host-Control-Interface (6) auslöst.

3. Basic-CAN-Controller nach Anspruch 1 oder Full-Can-Controller nach Anspruch 2, **dadurch gekennzeichnet**, dass die RX-Filtereinrichtung (40) eine Filterbank (41) umfassend ein oder mehrere Filterelemente (42, 43, 44) aufweist, wobei die Filterelemente (42, 43, 44) eine Überprüfung eines empfangenen CAN-Frames vornehmen, ob dessen CAN-Identifier einem der für den -CAN-Controller spezifischen, zum Senden bestimmten CAN-Identifier entspricht, und ein Speicherelement (45) zur Speicherung eines empfangenen CAN-Frames aufweist, dessen CAN-Identifier mit einem für den CAN-Controller spezifischen CAN-Identifier übereinstimmt.

4. Verwendung eines Full-CAN-Controllers zur Erkennung von Manipulationen in einem CAN-Netzwerk, wobei der Full-CAN-Controller aufweist
einen CAN-Transceiver (1) zum Verbinden des Basic-CAN-Controllers mit einem CAN-Bus,
eine CAN-Protocol-Engine (2) zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
ein TX-FIFO (20) zum Speichern von zu sendenden CAN-Frames,
einen Prioritätsselektor (25) zum Übertragen eines zu sendenden CAN-Frames an die CAN-Protocol-Engine (2) als Funktion der Priorität,

ein RX-FIFO (26) zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei das RX-FIFO (26) eine Vielzahl von CAN-Filter-Speicherelementen (27, 28, 29, 30) und jedes CAN-Filter-Speicherelement (27, 28, 29, 30) ein Filterelement (10) zum Filtern zulässiger, für den Full-CAN-Controller bestimmter CAN-Frames aus den empfangenen CAN-Frames und zum Speichern eines zulässigen CAN-Frames in einem CAN-Frame-Speicherelement (13, 14, 15, 16) aufweist, und
ein Host-Control-Interface (6) zur Kommunikation von Steuerinformationen zwischen CAN-Protocol-Engine (2) und Hostrechner,
dadurch gekennzeichnet, dass
die Filterelemente (10) einer Teilmenge der CAN-Filter-Speicherelementen (27, 28, 29, 30) des RX-FIFOS (26) mit den für den Full-CAN-Controller zum Senden eines CAN-Frames spezifischen CAN-Identifiern belegt sind, so dass eine Überprüfung der CAN-Identifier der empfangenen CAN-Frames mit den für den Full-CAN-Controller spezifischen CAN-Identifiern in den jeweiligen Filterelementen (10) erfolgt und im Fall einer Übereinstimmung eines empfangenen CAN-Identifiers mit einem der spezifischen CAN-Identifier des Full-CAN-Controllers ein Abspeichern des empfangenen CAN-Identifiers in dem entsprechenden CAN-Frame-Speicherelement (13, 14, 14, 16) und ein Erzeugen einen Intrusionserkennungs-Interrupt IDS-IRQ (32) an das Host-Control-Interface (6) bewirkt.

5. Verwendung eines Full-CAN-Controllers zur Erkennung von Manipulationen in einem CAN-Netzwerk, wobei der Full-CAN-Controller aufweist
einen CAN-Transceiver (1) zum Verbinden des Basic-CAN-Controllers mit einem CAN-Bus,
eine CAN-Protocol-Engine (2) zum Kodieren eines CAN-Frames in einen zu sendenden Bitstrom zur Übertragung auf dem CAN-Bus und zum Dekodieren eines empfangenen Bitstroms des CAN-Bus in ein CAN-Frame,
ein TX-FIFO (20) mit einer Vielzahl von CAN-Frame-Speicherelementen (21, 22, 23, 24) zum Speichern von zu sendenden CAN-Frames,
einen Prioritätsselektor (25) zum Übertragen eines zu sendenden CAN-Frames an die CAN-Protocol-Engine (2) als Funktion der Priorität,
ein RX-FIFO (26) zum temporären Speichern der empfangenen CAN-Frames vor der Übertragung an den Hostrechner, wobei das RX-FIFO (26) eine Vielzahl von CAN-Filter-Speicherelementen (27, 28, 29, 30) und jedes CAN-Filter-Speicherelement (27, 28, 29, 30) ein Filterelement (10) zum Filtern zulässiger, für den Full-CAN-Controller bestimmter

CAN-Frames aus den empfangenen CAN-Frames und zum Speichern eines zulässigen CAN-Frames in einem CAN-Frame-Speicherelement (13, 14, 15, 16) aufweist, und
ein Host-Control-Interface (6) zur Kommunikation von Steuerinformationen zwischen CAN-Protocol-Engine (2) und Hostrechner,
dadurch gekennzeichnet, dass
empfangene CAN-Frames den CAN-Frame-Speicherelementen (21, 22, 23, 24) des TX-FIFOs (20) zur Empfangszeit zugeführt und auf eine Übereinstimmung des CAN-Identifier des empfangenen CAN-Frames mit den in den CAN-Frame-Speicherelementen (21, 22, 23, 24) vorliegenden, zum Senden bestimmten CAN-Identifiern verglichen werden und im Fall einer Übereinstimmung ein Erzeugen einen Intrusionserkennungs-Interrupt IDS-IRQ (32) an das Host-Control-Interface (6) bewirkt wird.

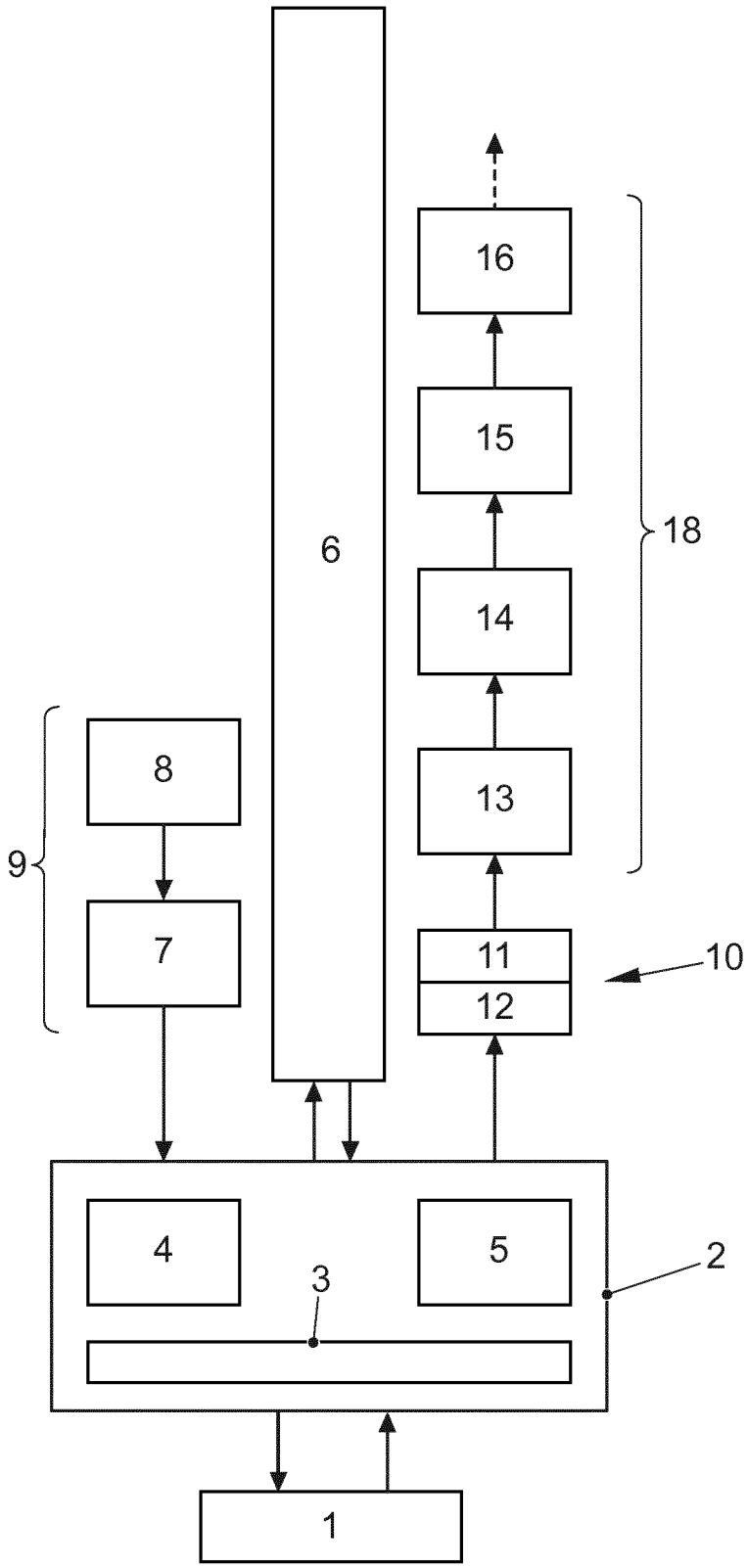

FIG. 1
(Stand der Technik)

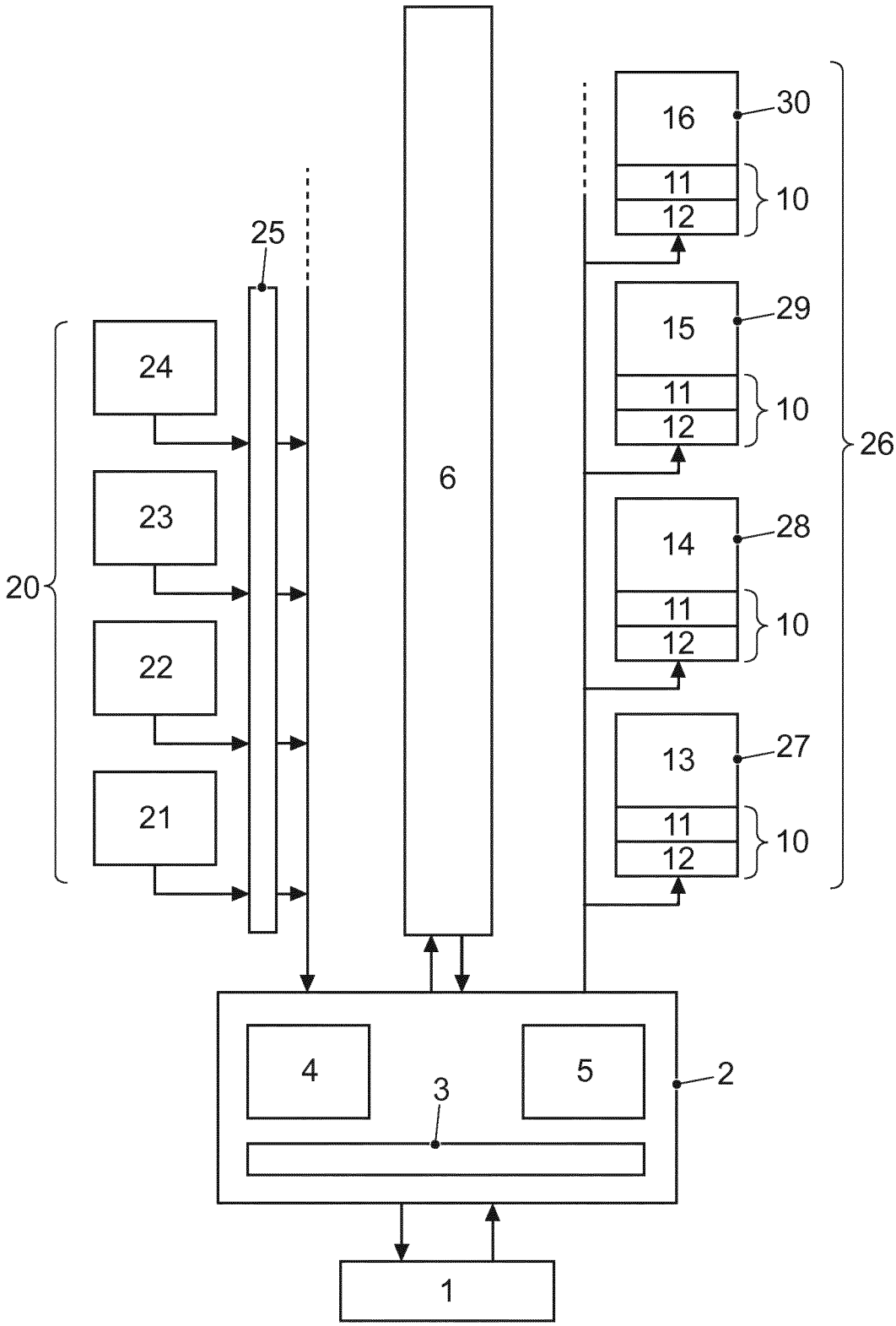

FIG. 2
(Stand der Technik)

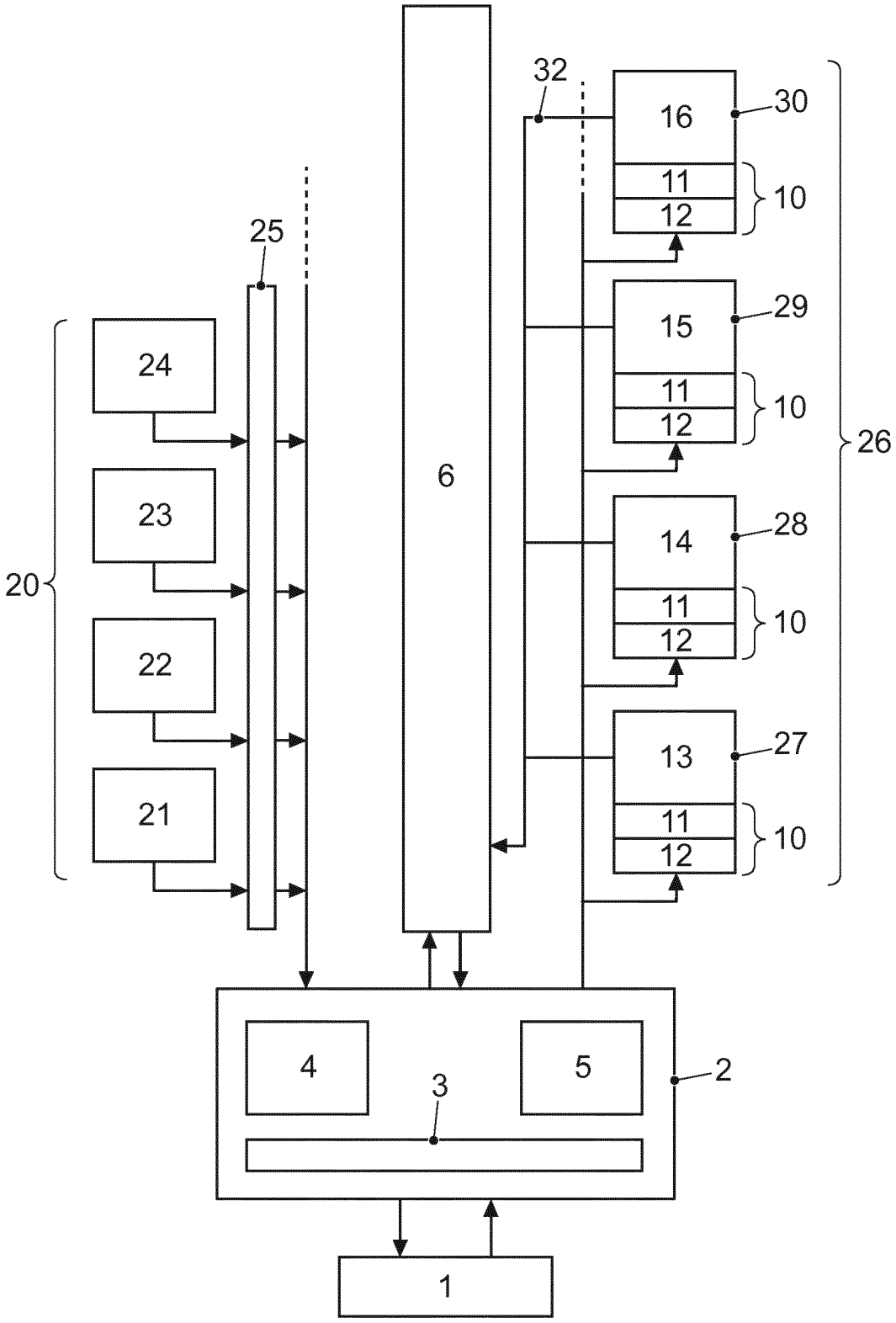
32
16
30
11
12
10
25
15
29
24
11
12
10
26
6
23
14
28
20
11
12
10
22
13
27
11
12
10
21
4
5
2
3
1

FIG. 3

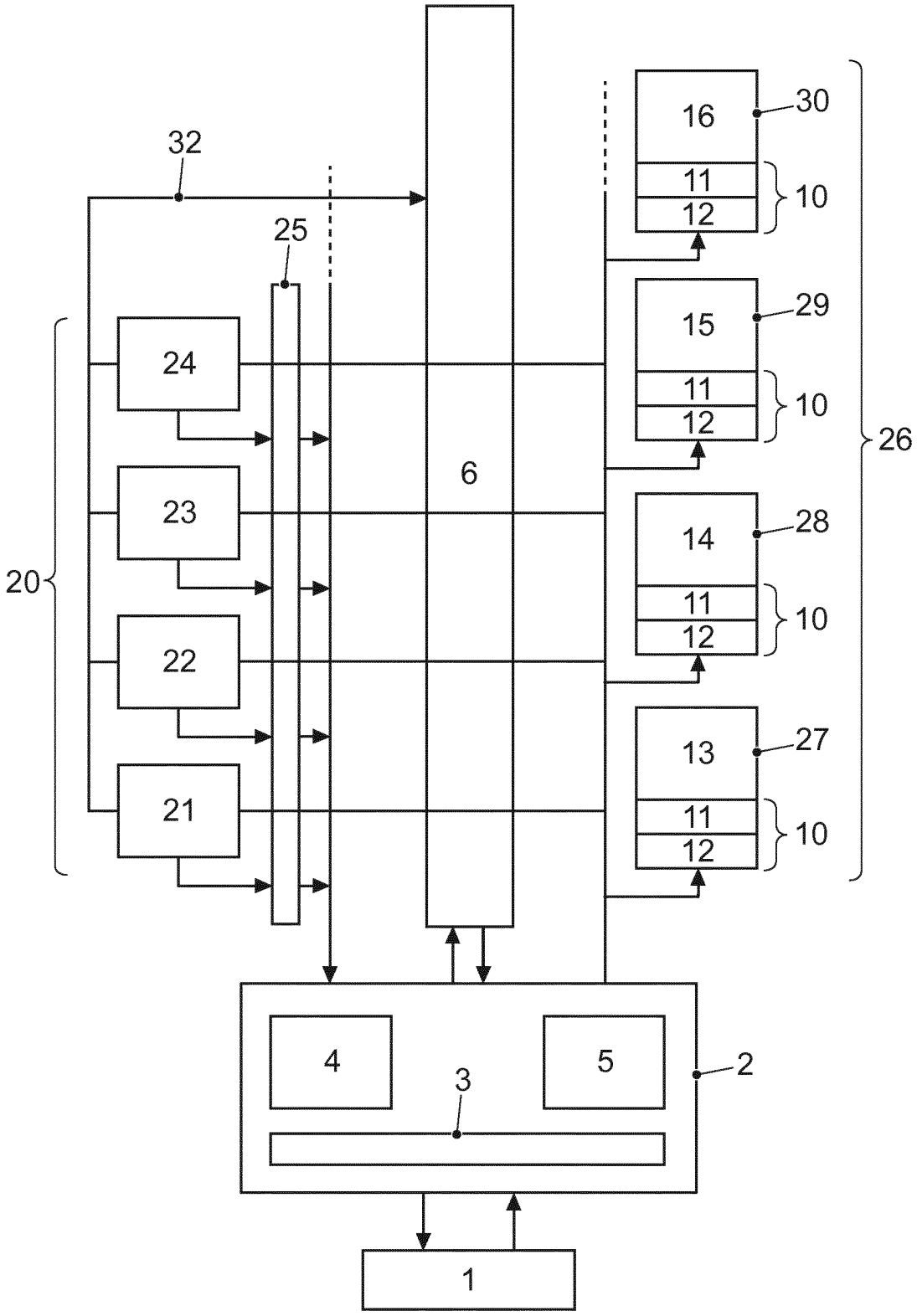

FIG. 4

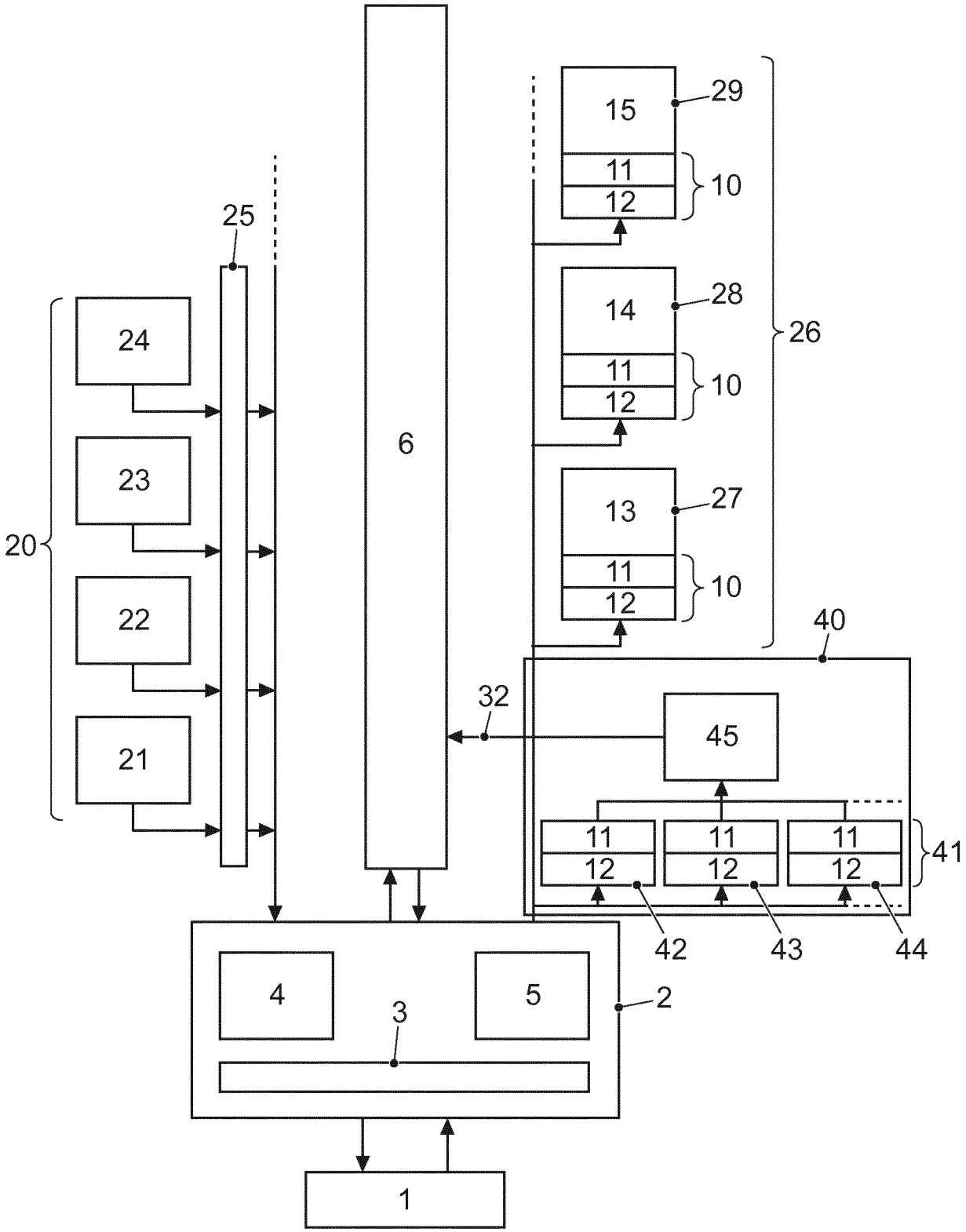
15
29
11
12
10
25
14
28
24
26
6
23
13
27
20
22
40
32
45
21
11
11
11
41
12
12
12
42
43
44
4
5
2
3
1

FIG. 5

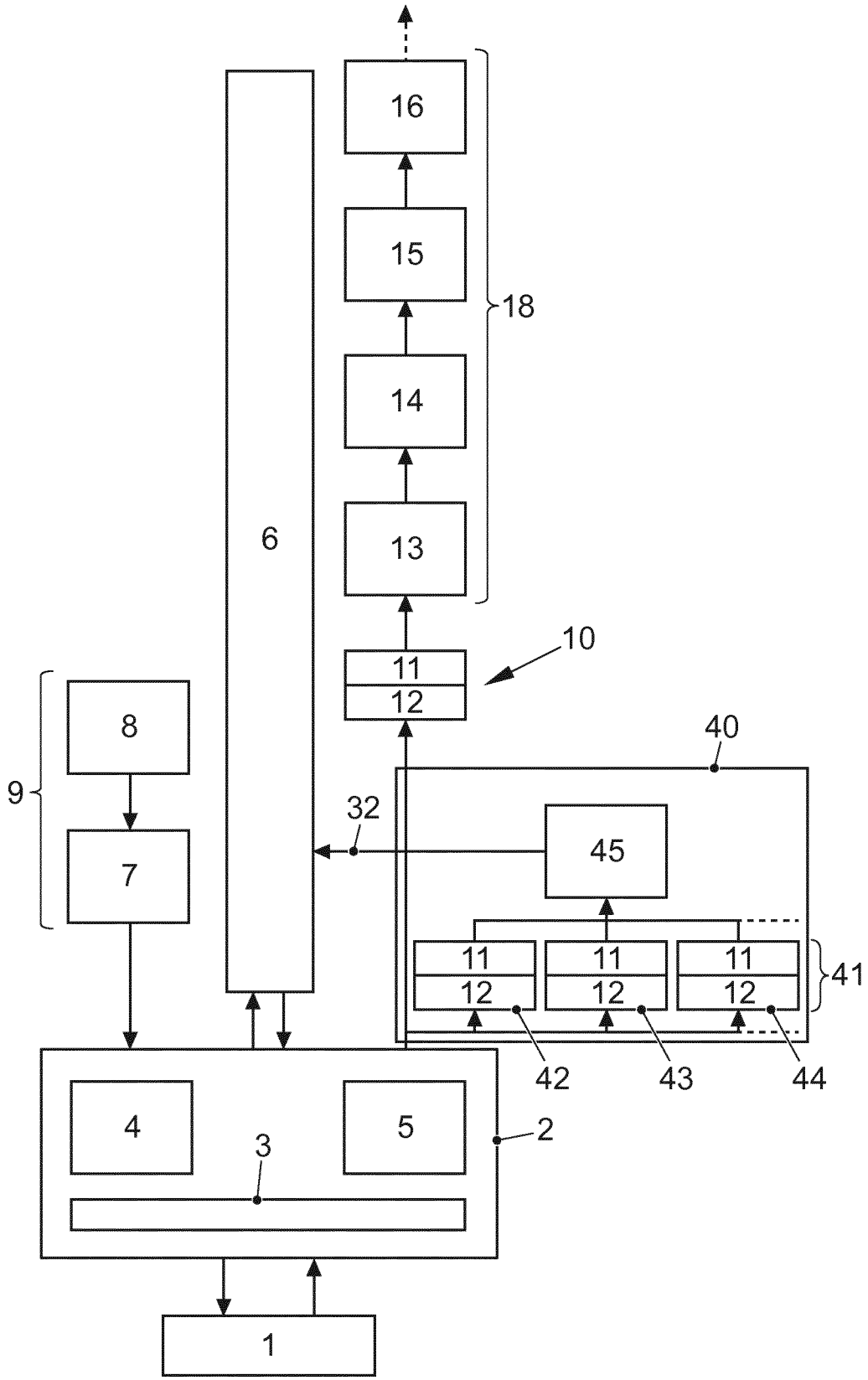
16
15
18
14
13
6
10
11
12
8
9
40
32
45
7
11
12
11
12
11
12
41
42
43
44
4
5
2
3
1

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/072916

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. H04L12/40

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 G06F G05B

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	JP 2015 192216 A (TOYOTA MOTOR CORP) 2 November 2015 (2015-11-02) abstract paragraph [0001] - paragraph [0023] paragraph [0026] - paragraph [0032]; figure 1 paragraph [0033] - paragraph [0041]; figure 2 paragraph [0042] - paragraph [0047]; figure 4 ----- -/--	1-5

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 2017	12/12/2017

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

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Siemens: "Data Sheet Microcomputer Components SAE 81C90/91 Standalone Full-CAN Controller", , 23 September 2004 (2004-09-23), XP055426938, Retrieved from the Internet: URL:http://pdf.datasheetcatalog.com/datasheet/infineon/1-d81c91_1.pdf [retrieved on 2017-11-20] page 6 - page 9 -----	1-5
A	US 2015/113638 A1 (VALASEK CHRISTOPHER [US] ET AL) 23 April 2015 (2015-04-23) abstract paragraph [0005] - paragraph [0008] paragraph [0021] - paragraph [0039] -----	1-5
A	Philips: "DATA SHEET Stand-alone CAN controller SJA1000", , 4 January 2004 (2004-01-04), XP055426193, Retrieved from the Internet: URL:https://www.nxp.com/docs/en/data-sheet/SJA1000.pdf [retrieved on 2017-11-17] page 4 page 7 - page 8 -----	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/072916

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2015192216 A	02-11-2015	NONE	
US 2015113638 A1	23-04-2015	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/072916

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

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G06F G05B

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	JP 2015 192216 A (TOYOTA MOTOR CORP) 2. November 2015 (2015-11-02) Zusammenfassung Absatz [0001] - Absatz [0023] Absatz [0026] - Absatz [0032]; Abbildung 1 Absatz [0033] - Absatz [0041]; Abbildung 2 Absatz [0042] - Absatz [0047]; Abbildung 4	1-5

-/--

[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
30. November 2017	12/12/2017

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

5

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	Siemens: "Data Sheet Microcomputer Components SAE 81C90/91 Standalone Full-CAN Controller", , 23. September 2004 (2004-09-23), XP055426938, Gefunden im Internet: URL:http://pdf.datasheetcatalog.com/datasheet/infineon/1-d81c91_1.pdf [gefunden am 2017-11-20] Seite 6 - Seite 9 -----	1-5
A	US 2015/113638 A1 (VALASEK CHRISTOPHER [US] ET AL) 23. April 2015 (2015-04-23) Zusammenfassung Absatz [0005] - Absatz [0008] Absatz [0021] - Absatz [0039] -----	1-5
A	Philips: "DATA SHEET Stand-alone CAN controller SJA1000", , 4. Januar 2004 (2004-01-04), XP055426193, Gefunden im Internet: URL:https://www.nxp.com/docs/en/data-sheet/SJA1000.pdf [gefunden am 2017-11-17] Seite 4 Seite 7 - Seite 8 -----	1-5

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/072916

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
JP 2015192216 A	02-11-2015	KEINE	
US 2015113638 A1	23-04-2015	KEINE	