(19) Deutsches Patent- und Markenamt

(10) **DE 10 2018 110 252 A1** 2019.10.31

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2018 110 252.6**
(22) Anmeldetag: **27.04.2018**
(43) Offenlegungstag: **31.10.2019**

(51) Int Cl.: ***H04L 9/18*** (2006.01)
H04L 12/40 (2006.01)
B60R 25/00 (2013.01)

(71) Anmelder:
Infineon Technologies AG, 85579 Neubiberg, DE

(74) Vertreter:
Kraus & Weisert Patentanwälte PartGmbB, 80539 München, DE

(72) Erfinder:
Zeh, Alexander, Dr., 80333 München, DE; Allimuthu Elavarasu, Vivin Richards, 81549 München, DE; Pihet, Eric, 81547 München, DE

(56) Ermittelter Stand der Technik:

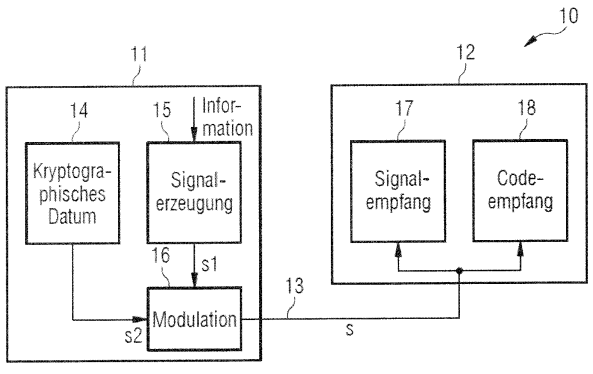
US	**2007 / 0 121 939**	**A1**
US	**2013 / 0 103 959**	**A1**
US	**2013 / 0 163 761**	**A1**
WO	**2015/ 183 784**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Transceiver, System mit Transceivern und Signal**

(57) Zusammenfassung: Es wird ein Transceiver bereitgestellt, aufweisend: einen Transmitter, der dazu ausgebildet ist,
- an einem Ausgang ein erstes Signal gemäß eines physikalischen Kommunikationsprotokolls bereitzustellen, und
- an dem Ausgang ein zweites Signal bereitzustellen, das mindestens ein kryptographisches Datum umfasst, wobei das erste und das zweite Signal als ein Überlagerungssignal an dem Ausgang einander überlagert sind, und wobei das Überlagerungssignal das physikalische Kommunikationsprotokoll erfüllt. Entsprechende Transceiver mit Receiver, Systeme und Signale werden ebenfalls bereitgestellt.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Anmeldung betrifft Transceiver, Systeme mit derartigen Transceivern, entsprechende Signale sowie entsprechende Verfahren.

HINTERGRUND

[0002] Viele Vorrichtungen enthalten eine Vielzahl von Komponenten, die miteinander kommunizieren, um Daten auszutauschen. Ein Beispiel für derartige Vorrichtungen sind Fahrzeuge, in denen eine Vielzahl von Steuereinheiten wie Microcontroller miteinander kommunizieren, um verschiedene Fahrzeugfunktionen zu steuern. Zudem erfassen in Fahrzeugen Sensoren physikalische Größen und kommunizieren mit den oben genannten Steuereinheiten, um die gemessenen Größen mitzuteilen. Beispiele für derartige Steuereinheiten in Fahrzeugen umfassen Motorsteuerungen, Getriebesteuerungen, Steuereinheiten für den Diebstahlschutz und dergleichen. Beispiele für Sensoren umfassen Kameras, Geschwindigkeitssensoren, Radarsensoren, Temperatursensoren und dergleichen.

[0003] Die Kommunikation der verschiedenen Komponenten untereinander kann dabei drahtlos oder drahtgebunden erfolgen, wobei in vielen Anwendungen eine drahtgebundene Kommunikation eingesetzt wird. In Fahrzeugen wird häufig der der CAN(controller area network)-Bus eingesetzt, der nach ISO 11898 standardisiert ist. Auch andere Bussysteme, beispielsweise der FlexRay-Bus (ISO 17458-1 bis ISO 17458-4) oder LIN-Bus (zukünftig ISO 17987-1), können zum Einsatz kommen.

[0004] Bei derartigen Vorrichtungen kann es vorkommen, dass eine Kommunikationseinrichtung unerlaubter Weise an der Kommunikation zwischen den Komponenten teilnehmen will. Beispielsweise kann eine externe Kommunikationseinrichtung mit einem CAN-Bus eines Fahrzeuges verbunden werden, um Manipulationen an dem Fahrzeug vorzunehmen, beispielsweise um einen Kilometerstand eines Tachometers zu verstellen oder um Diebstahlschutzmaßnahmen des Fahrzeuges außer Kraft zu setzen. Daher ist es wünschenswert, derartige Kommunikationseinrichtungen, die einen unerlaubten Eingriff versuchen, erkennen zu können.

KURZFASSUNG

[0005] Es werden Transceiver und ein Signal wie in den unabhängigen Ansprüchen definiert bereitgestellt. Die abhängigen Ansprüche definieren weitere Ausführungsformen sowie ein System mit derartigen Transceivern.

[0006] Gemäß einem Ausführungsbeispiel wird ein Transceiver bereitgestellt, aufweisend:

einen Transmitter, der dazu ausgebildet ist,

- an einem Ausgang ein erstes Signal gemäß eines physikalischen Kommunikationsprotokolls bereitzustellen, und

- an dem Ausgang ein zweites Signal bereitzustellen, das mindestens ein kryptographisches Datum umfasst, wobei das erste und das zweite Signal als ein Überlagerungssignal an dem Ausgang einander überlagert sind, und wobei das Überlagerungssignal das physikalische Kommunikationsprotokoll erfüllt.

[0007] Gemäß einem anderen Ausführungsbeispiel wird ein Transceiver bereitgestellt, aufweisend:

einen Receiver, der dazu ausgebildet ist,

- ein Empfangssignal, welches eine Überlagerung eines ersten Signals gemäß einem physikalischen Kommunikationsprotokoll mit einem zweiten Signal, das ein kryptographisches Datum umfasst, ist, zu empfangen,

- das Empfangssignal gemäß dem physikalischen Kommunikationsprotokoll zu verarbeiten, um in dem ersten Signal übertragene Informationen zu gewinnen, und

- aus dem Empfangssignal das kryptographische Datum zu gewinnen.

[0008] Gemäß einem weiteren Ausführungsbeispiel wird ein Signal bereitgestellt, umfassend eine Überlagerung aus:

- einem erstes Signal gemäß eines physikalischen Kommunikationsprotokolls, und

-einem zweites Signal, das mindestens ein kryptographisches Datum umfasst,

wobei das Signal das physikalische Kommunikationsprotokoll erfüllt.

Figurenliste

Fig. 1 ist ein Blockdiagramm eines Systems gemäß mancher Ausführungsbeispiele.

Fig. 2 ist ein Flussdiagramm eines Verfahrens gemäß mancher Ausführungsbeispiele.

Fig. 3 zeigt ein System gemäß mancher Ausführungsbeispiele.

Fig. 4 zeigt eine Kommunikationsschaltung mit einem Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 5 zeigt eine Treiberschaltung zum Erzeugen verschiedener Signalpegel, welche in manchen Ausführungsbeispielen verwendet werden kann.

Fig. 6-9 zeigen Beispiele für Signale gemäß mancher Ausführungsbeispiele.

Fig. 10 zeigt einen Teil eines Transmitters für einen CAN-Bus.

Fig. 11 zeigt Kurven für die Schaltung der **Fig. 10** bei Variation verschiedener Parameter.

Fig. 12 zeigt Kurven für die Schaltung der **Fig. 10** bei Variation verschiedener Parameter.

Fig. 13 zeigt eine Kommunikationsschaltung für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 14 zeigt Kurven zur Veranschaulichung mancher Ausführungsbeispiele.

Fig. 15 zeigt eine Kommunikationsschaltung gemäß mancher Ausführungsbeispiele.

Fig. 16 zeigt eine Kommunikationsschaltung für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 17 zeigt eine Kommunikationsschaltung für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 18 zeigt eine Kommunikationsschaltung für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 19 zeigt eine Kommunikationsschaltung für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 20 zeigt eine Kommunikationsschaltung für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 21 zeigt Kurven zur Veranschaulichung mancher Ausführungsbeispiele.

Fig. 22 und **Fig. 23** zeigen Diagramme zur Veranschaulichung des Einflusses elektromagnetischer Störungen.

Fig. 24 zeigt ein System gemäß mancher Ausführungsbeispiele.

Fig. 25 zeigt ein Flussdiagramm zur Veranschaulichung eines Verfahrens gemäß mancher Ausführungsbeispiele.

Fig. 27-36 zeigen Kommunikationsschaltungen für Transceiver gemäß mancher Ausführungsbeispiele.

Fig. 37 zeigt ein physikalisches Kommunikationsprotokoll und eine Logikprotokollschicht gemäß manchen Ausführungsbeispiele.

DETAILLIERTE BESCHREIBUNG

[0009] Im Folgenden werden verschiedene Ausführungsbeispiele detailliert beschrieben. Es ist zu bemerken, dass diese Ausführungsbeispiele lediglich zur Veranschaulichung dienen und nicht als einschränkend auszulegen sind. So ist eine Beschreibung eines Ausführungsbeispiels mit einer Vielzahl von Merkmalen (z.B. Komponenten, Eigenschaften, Vorgängen etc.) nicht dahingehend auszulegen, dass alle diese Merkmale zur Implementierung des jeweiligen Ausführungsbeispiels notwendig sind. Vielmehr können manche Merkmale durch alternative Merkmale ersetzt werden oder weggelassen werden. Zusätzlich zu den explizit dargestellten Merkmalen können auch zusätzliche Merkmale, beispielsweise in herkömmlichen Kommunikationsschaltungen verwendete Merkmale, bereitgestellt werden.

[0010] Merkmale verschiedener Ausführungsbeispiele können miteinander kombiniert werden, sofern nichts anderes angegeben ist. Variationen und Abwandlungen, welche für eines der Ausführungsbeispiele beschrie-

ben werden, sind auch auf andere Ausführungsbeispiele anwendbar und werden daher nicht wiederholt beschrieben.

[0011] Im Folgenden werden verschiedene Ausführungsbeispiele für Kommunikationsschaltungen und Anordnungen derartiger Kommunikationsschaltungen detailliert erläutert. Auch wenn die Kommunikationsschaltungen teilweise unter Bezugnahme auf bestimmte Kommunikationsmedien, insbesondere bestimmte Bussysteme wie einen CAN-Bus, beschrieben werden, sind die dargestellten Techniken auch auf andere Kommunikationsmedien, beispielsweise drahtgebundene Kommunikationsmedien, drahtlose Kommunikationsmedien oder optische Kommunikationsmedien wie Glasfasern, anwendbar. Die Verwendung spezifischer Beispiele dient hier also lediglich der Veranschaulichung.

[0012] In der Beschreibung wird teilweise auf eine physikalisches Kommunikationsprotokoll der Kommunikation und eine Logikprotokollschicht der Kommunikation Bezug genommen. Das physikalische Kommunikationsprotokoll definiert Funktionen entsprechend der physikalischen Schicht des OSI-Schichtenmodells und definiert, wie zu sendende Daten, z.B. ein Bitstrom, in physikalische Signale auf einem Übertragungsmedium umgesetzt werden. Die Logikprotokollschicht ist dem physikalischen Kommunikationsprotokoll übergeordnet und betrifft dem gegenüber beispielsweise höhere Schichten des OSI-Modells oder auch Schichten oberhalb des OSI-Modells (Anwendungen) und kann insbesondere betreffen, welche Daten übertragen werden, einschließlich einer Codierung oder Verschlüsselung der Daten. Dies ist in **Fig. 37** mit einem physikalischen Kommunikationsprotokoll **370** und einer übergeordneten Logikprotokollschicht **371** veranschaulicht.

[0013] **Fig. 1** ist eine schematische Darstellung eines Systems **10** gemäß mancher Ausführungsbeispiele mit einer ersten Kommunikationsschaltung **11**, welche in dem dargestellten Beispiel als Transmitter, d.h. als Sender dient, und einer zweiten Kommunikationsschaltung **12**, welche in dem dargestellten Beispiel als Receiver, d.h. Empfänger dient. Das System **10** kann Teil einer Vorrichtung wie einem Fahrzeug sein, und die Kommunikationsschaltungen **11**, **12** können in Komponenten dieser Vorrichtung angeordnet sein, um eine Kommunikation der Komponenten miteinander zu ermöglichen.

[0014] Die Kommunikationsschaltung **11** sendet über ein Kommunikationsmedium **13** Signale an die Kommunikationsschaltung **12**. Das Kommunikationsmedium **13** kann ein drahtloses Kommunikationsmedium, ein drahtgebundenes Kommunikationsmedium oder auch ein optisches Kommunikationsmedium sein. Im Falle eines drahtgebundenen Kommunikationsmediums kann es sich insbesondere um ein Bussystem wie einen CAN-Bus, einen FlexRay-Bus oder einen LIN-Bus handeln, ist jedoch nicht hierauf beschränkt.

[0015] Während in **Fig. 1** die Kommunikationsschaltung **11** als Transmitter und die Kommunikationsschaltung **12** als Receiver dargestellt ist, kann die Kommunikationsschaltung **11** auch zusätzlich Schaltungsteile zum Empfangen von Signalen und/oder die Kommunikationsschaltung **12** zusätzlich Schaltungsteile zum Senden von Signalen enthalten, um eine bidirektionale Kommunikation zu ermöglichen, sodass die Kommunikationsschaltungen **11**, **12** beide als Transceiver (Sendeempfänger) ausgebildet sind.

[0016] Die Kommunikation über das Kommunikationsmedium **13** erfolgt dabei gemäß einem physikalischen Kommunikationsprotokoll. Derartige physikalische Kommunikationsprotokolle sind für verschiedene Arten der Kommunikation definiert und definieren wie oben erläutert insbesondere, wie eine zu sendende Information (Nutzdaten, Steuerdaten und dergleichen) in physikalische Signale (auf einem Kommunikationsmedium oder drahtlos) umgesetzt werden soll. Beispielsweise sind für den CAN-Bus und ähnliche Bussysteme Spannungspegel definiert, welche zwei verschiedene Zustände entsprechend einer logischen 1 und einer logischen 0 definieren, und Signale werden als Abfolge derartiger Spannungspegel gesendet. Es sind jedoch auch andere Arten von Signalen möglich, z.B. frequenzmodulierte Signale, wechselstromförmige Signale, Quadraturamplituden(QAM)-modulierte Signale und dergleichen.

[0017] Hierzu empfängt eine Signalerzeugungsschaltung **15** eine zu sendende Information, z.B. zu sendende Nutzdaten oder Steuerdaten, und erzeugt ein erstes Signal **s1** entsprechend dem physikalischen Kommunikationsprotokoll. Die zu sendende Information kann als Logiksignal von einer über dem physikalischen Kommunikationsprotokoll angeordneten Logikprotokollschicht gemäß einem Logikprotokoll erhalten werden. Dieses erste Signal **s1** kann wie erläutert z.B. zwei oder mehrere verschiedene Spannungs- oder Strompegel aufweisen, um die Information in das Signal umzusetzen. Diese Signalerzeugung kann in jeder herkömmlichen Weise für das jeweilige physikalische Kommunikationsprotokoll erfolgen.

[0018] Zudem wird mittels einer Modulationsschaltung **16** das erste Signal **s1** mit einem zweiten Signal **s2**, welches ein kryptographisches Datum **14** umfasst, überlagert. Ein kryptographisches Datum ist dabei insbe-

sondere ein Code oder anderes Datum, der eine Authentifizierung eines über das Kommunikationsmedium **13** gesendeten Signals als von einem autorisierten Kommunikationsteilnehmer (d.h. Kommunikationsteilnehmer, denen es gestattet ist, miteinander zu kommunizieren) kommend ermöglicht. Beispielsweise kann das kryptographische Datum eine vorgegebene Bitfolge sein, die nur autorisierten Kommunikationsteilnehmern bekannt ist oder durch diese bestimmbar ist. Ein nicht autorisierter Kommunikationsteilnehmer, z.B. eine Kommunikationsvorrichtung, die unerlaubter Weise mit dem Kommunikationsmedium **13** gekoppelt wird, wie Eingangs erläutert, kennt das kryptographische Datum hingegen nicht, z.B. weil ihm kein entsprechender Schlüssel bereitgestellt wird. Das kryptographische Datum kann mithilfe herkömmlicher kryptographischer Verfahren erzeugt werden, z.B. auf Basis eines kryptographischen Schlüssels, den der Transmitter **11** von einer übergeordneten Instanz erhalten kann, wie später erläutert werden wird. Der Begriff „kryptographisch“ ist hier also nicht im engeren Sinne als Verschlüsselung zu verstehen, sondern im weiteren Sinne als ein Element bezeichnend, das dazu beiträgt, das System **10** widerstandsfähig gegen Manipulation zu machen. Das kryptographische Datum kann dabei insbesondere einen Sicherheitscode des Transmitters **11** darstellen, welcher den Transmitter **11** als Quelle eines gesendeten Signals identifiziert und somit eine Authentifizierung ermöglicht.

[0019] Bei der Modulationsschaltung **16** wird das zweite Signal **s2** mit dem kryptographischen Datum auf der physikalischen Ebene auf das von der Signalerzeugungsschaltung **15** erzeugte erste Signal **s1** moduliert, z.B. durch Modifizieren von Signalpegeln des ersten Signals **s1**, um so ein Überlagerungssignal s zu bilden. Dies unterscheidet sich von Ansätzen, bei welchen zu sendende Informationen verschlüsselt werden, was einer Verschlüsselung auf einer Logikprotokollschicht entspricht. Wie später erläutert werden wird kann jedoch eine derartige Verschlüsselung oder andere Codierung auf Logikprotokollschicht zusätzlich vorgenommen werden.

[0020] Bei manchen Ausführungsbeispielen definiert das Kommunikationsprotokoll Toleranzen für zu verwendende Pegel. Beispielsweise kann das Kommunikationsprotokoll spezifizieren, dass ein Pegel, der einer logischen 1 entspricht, innerhalb eines ersten Spannungsbereiches liegen muss und/oder dass ein Pegel, der einer logischen 0 entspricht, innerhalb eines zweiten Spannungsbereiches liegen muss, um jeweils gültig als 1 oder 0 erkannt zu werden. Bei Ausführungsbeispielen moduliert die Modulationsschaltung das erste Signal durch Überlagerung mit dem zweiten dann so, dass die Pegel des Signals innerhalb der spezifizierten Bereiche bleiben. Auch bei anderen Arten von Kommunikationsprotokollen können Amplituden des zweiten Signals **s2** derart klein sein, dass das Überlagerungssignal s das physikalische Kommunikationsprotokoll erfüllt, d.h. dass das Überlagerungssignal s gemäß dem physikalischen Kommunikationsprotokoll verarbeitbar ist, um die Informationen des ersten Signals **s1** wiederzugewinnen. Dies kann bei manchen Ausführungsbeispielen eine Rückwärtskompatibilität sicherstellen, d.h. auch Empfänger, die nicht wie später für die Empfangsschaltung **12** diskutiert ausgerüstet sind, können das Signal korrekt empfangen. Beispiele für derartige Überlagerungen von Signalen werden später noch näher erläutert.

[0021] Zu beachten ist auch, dass die Signalerzeugungsschaltung **15** und die Modulationsschaltung **16** zwar zur Veranschaulichung als hintereinander geschaltete Blöcke dargestellt sind, wie später erläutert die Modulation und die Signalerzeugung jedoch auch gleichzeitig stattfinden kann. Die dargestellte Anordnung dient somit nur der Veranschaulichung der verschiedenen Funktionen.

[0022] Das so modulierte Überlagerungssignal s wird dann über das Kommunikationsmedium **13** an die Kommunikationsschaltung **12** gesendet. Die Kommunikationsschaltung **12** umfasst eine Signalempfangsschaltung **17**, welche die Information, welche von der Signalerzeugungsschaltung **15** in das erste Signal **s1** umgesetzt wurde, wiedergewinnt. Zudem weist die Kommunikationsschaltung **12** eine Codeempfangsschaltung **18** auf, welche das in dem durch die Modulationsschaltung **16** aufmodulierten zweiten Signal **s2** enthaltene kryptographische Datum wiedergewinnt. Wenn das kryptographische Datum, welches auf diese Weise wiedergewonnen wurde, nicht mit einem erwarteten kryptographischen Datum (z.B. einem in der Kommunikationsschaltung **12** hinterlegten kryptographischen Datum oder einem aus einem bereitgestellten Schlüssel gewonnenen kryptographischen Datum) übereinstimmt, können Maßnahmen ergriffen werden. Beispielsweise kann das empfangene Signal und die daraus gewonnene Information verworfen werden, ein entsprechendes Signal kann erzeugt werden, um andere Komponenten von dem nicht authentifizierten Signal zu informieren, und/oder ein Benutzer kann informiert werden. Auf diese Weise können bei manchen Ausführungsbeispielen nicht autorisierte Zugriffsversuche erkannt werden, und Gegenmaßnahmen können ergriffen werden.

[0023] Die Signalempfangsschaltung **17** kann dabei in herkömmlicher Weise für das jeweilige physikalische Kommunikationsprotokoll ausgestaltet sein. Beispiele für die Codeempfangsschaltung **18** und insbesondere Kalibrierungsmöglichkeiten für die Codeempfangsschaltung **18** werden später näher erläutert. Zu bemerken ist, dass die Kommunikationsschaltung **12** auch Empfangssignale verarbeiten kann, die nur das erste Signal

enthalten bzw. bei denen das zweite Signal z.B. aufgrund von Störungen nicht verarbeitbar ist. In diesem Fall wird z.B. nur die Signalempfangsschaltung **17** verarbeitet.

[0024] **Fig. 2** zeigt ein Flussdiagramm zur Veranschaulichung von Verfahren gemäß manchen Ausführungsbeispielen. Um Wiederholungen zu vermeiden, wird das Verfahren der **Fig. 2** unter Bezugnahme auf die **Fig. 1** erläutert. Das Verfahren der **Fig. 2** ist jedoch auch unabhängig von der Vorrichtung der **Fig. 1** verwendbar.

[0025] Bei **20** wird eine zu sendende Information in ein erstes Signal umgesetzt. Wie bereits für die Signalerzeugungsschaltung **15** erläutert, kann dies auf Basis eines physikalischen Kommunikationsprotokolls erfolgen, sodass ein Signal erzeugt wird, welches Pegel aufweist, die eine logische 1 und eine logische 0 repräsentieren können, oder auf andere Weise die zu sendende Information überträgt.

[0026] Bei **21** wird das Sendesignal gemäß einem zweiten Signal, welches ein kryptographisches Datum umfasst, moduliert, wie für die Modulationsschaltung **16** in **Fig. 1** beschrieben. Das kryptographische Datum kann auf Basis eines Schlüssels erzeugt werden. So wird ein Überlagerungssignal erzeugt, welches das physikalische Kommunikationsprotokoll erfüllt, wie oben beschrieben. Wie für die Signalerzeugungsschaltung **15** und die Modulationsschaltung **16** der **Fig. 1** beschrieben müssen auch das Umsetzen bei **20** und das Modulieren bei **21** nicht nacheinander stattfinden, sondern können z.B. auch gleichzeitig durchgeführt werden.

[0027] Empfängerseitig wird dann bei **22** die Information aus dem Überlagerungssignal wiedergewonnen, wie für die Signalempfangsschaltung **17** beschrieben, und bei **23** wird das kryptographische Datum aus dem Überlagerungssignal wiedergewonnen, wie für die Codeempfangsschaltung **18** der **Fig. 1** beschrieben. Auch das Gewinnen der Information bei **22** und das Gewinnen des kryptographischen Datums bei **23** müssen nicht wie in **Fig. 2** dargestellt nacheinander erfolgen, sondern können auch gleichzeitig oder in anderer Reihenfolge geschehen. Entspricht das bei **23** gewonnene kryptographische Datum nicht einem erwarteten kryptographischen Datum, können entsprechende Maßnahmen ergriffen werden, wie bereits unter Bezugnahme auf die **Fig. 1** erläutert.

[0028] Die **Fig. 3** zeigt eine Kommunikationsschaltungsanordnung gemäß manchen Ausführungsbeispielen, bei welcher als Kommunikationsmedium ein CAN-Bus **36** verwendet wird. Bei dem Ausführungsbeispiel der **Fig. 3** dient eine Kommunikationsschaltung **30**, **35** als Sender, und eine Kommunikationsschaltung **31**, **37** als Empfänger. Das Bezugszeichen **30** bezeichnet dabei einen Sendeknoten, der einen Transceiver **35** mit zu sendenden Daten und einem Sicherheitscode versorgt. Der Transceiver **35** kann zudem zum Empfangen von Daten dienen, was in **Fig. 3** nicht explizit dargestellt ist. Der Sendeknoten **30** kann mittels eines Microcontrollers implementiert sein.

[0029] Zu sendende Daten werden in einen Sendepuffer **33** des Sendeknotens **30** in herkömmlicher Weise geschrieben. Diese zu sendenden Daten werden durch eine Sendeschaltung **34** in eine zu sendende Bitfolge umgesetzt, d.h. eine Folge logischer Einsen und Nullen, da dann als Signal **Tx** an den Transceiver **35** gesendet wird.

[0030] Ein Sicherheitscodegenerator **32** empfängt einen Schlüssel und erzeugt basierend auf diesem Schlüssel einen Sicherheitscode als kryptographisches Datum. Der Schlüssel kann dabei von einer Schlüsselverwaltungseinrichtung, die speziell geschützt ist, empfangen werden, insbesondere von einem Hardwaresicherheitsmodul (HSM; hardware security module), wie es später noch näher erläutert werden wird.

[0031] Der Sicherheitscodegenerator **32** empfängt des Weiteren Informationen über die zu sendenden Daten und über eine Position von sogenannten dominanten Sendebits, und erzeugt den Sicherheitscode in dem dargestellten Beispiel des CAN-Protokolls so, dass der Sicherheitscode nur auf dominante Bits eines Datenteils der Übertragung moduliert wird. Auch bei anderen physikalischen Kommunikationsprotokollen können bestimmte Pegel ausgewählt werden, auf die das zweite Signal mit dem kryptographischen Datum moduliert wird.

[0032] Dominante Bits sind dabei Bits, bei welchen ein Bus wie der CAN-Bus **36** aktiv auf einen Pegel getrieben wird, während er bei sogenannten rezessiven Bits durch Widerstände passiv auf einen anderen Pegel gezogen wird. Bei der CAN-Übertragung sind Bits, welche eine logische 0 repräsentieren, dominante Bits, und Bits, die eine logische 1 repräsentieren, rezessive Bits. Bei andere Kommunikationsstandards kann dies anders sein, und es können beispielsweise alle Bits aktiv getrieben werden. „Nur auf einen Datenteil“ bezieht sich darauf, dass die Übertragung bei CAN und anderen Kommunikationsprotokollen in sogenannten Datenrahmen (frames) erfolgt, die einen sogenannten Header gefolgt von dem Datenteil für Nutzdaten aufweisen. Bei manchen Ausführungsbeispielen wird der Sicherheitscode nur auf diesen Datenteil moduliert. Dies kann

beim CAN-Protokoll vorteilhaft sein, da während des Headers mehrere Transmitter gleichzeitig auf dem CAN-Bus senden können. Bei anderen Ausführungsbeispielen, insbesondere anderen physikalischen Kommunikationsprotokollen, können auch Headerbits zur Modulation mit dem Sicherheitscode verwendet werden.

[0033] Der Transceiver **35** moduliert dann die Amplituden der dominanten Bits entsprechend dem Sicherheitscode, was in diesem Ausführungsbeispiel der Überlagerung des zweiten Signals entspricht. Durch Kenntnis der Daten und der Bitpositionen kann der Sicherheitscodegenerator den Sicherheitscode entsprechend so erzeugen, dass Bitwechsel des Sicherheitscodes (von 0 auf 1 oder von 1 auf 0) nur bei dominanten Bits auftreten. Ein Beispiel hierfür wird später erläutert. Hier ist das zweite Signal also ein pulsförmiges Signal mit zwei Zuständen entsprechend 0 und 1. Bei anderen Ausführungsbeispielen können auch andere Arten von zweiten Signalen, z.B. welchselstromförmige Signale wie QAMmodulierte Signale, verwendet werden, solange ein kryptographisches Datum übertragbar ist.

[0034] Empfängerseitig decodiert ein CAN-Transceiver **37** den Sicherheitscode aus dem gesendeten Signal und stellt eine Empfangsschaltung **38** eines Empfangsknotens **31** zudem ein Empfangssignal basierend auf den empfangenen Pegeln gemäß dem CAN- Kommunikationsprotokoll bereit. Die Empfangsschaltung **38** erfolgt aus dem Signal Rx Empfangsdaten, die in einem Empfangspuffer **39** gespeichert werden.

[0035] Der wiedergewonnene Sicherheitscode, die Position von empfangenen Bits und die empfangenen Daten werden einer Verifizierungsschaltung **310** bereitgestellt. Die Verifizierungsschaltung **310** empfängt den Schlüssel, auf Basis dessen der Sicherheitscodegenerator **32** den Sicherheitscode erzeugt hat. Basierend auf dem Schlüssel, den Empfangsdaten und der Empfangsbitposition kann die Verifizierungsschaltung **310** einen erwarteten Sicherheitscode nach den gleichen Regeln bestimmen, nach denen der Sicherheitscodegenerator **32** den Sicherheitscode aus dem Schlüssel, den Sendedaten und der Sendebitposition bestimmt hat. Beispiele hierfür werden noch erläutert. Dieser erwartete Sicherheitscode wird dann mit dem empfangenen Sicherheitscode verglichen. Bei Übereinstimmung ist die Authentifizierung erfolgreich und die empfangenen Daten können verwendet werden. Bei Nichtübereinstimmung ist die Authentifizierung fehlgeschlagen, und es können wie bereits unter Bezugnahme auf die **Fig. 1** erläutert Maßnahmen ergriffen werden.

[0036] Ein Beispiel für den Aufbau von CAN-Transceivern gemäß Ausführungsbeispielen, beispielsweise den CAN-Transceivern **35**, **37** der **Fig. 3**, werden nunmehr unter Bezugnahme auf die **Fig. 4** und **Fig. 5** erläutert.

[0037] **Fig. 4** zeigt einen CAN-Transceiver **41** gemäß einem Ausführungsbeispiel, welcher mit einem Microcontroller **40** kommuniziert. Der Microcontroller **40** kann dabei insbesondere die für den Sendeknoten **30** der **Fig. 3** und/oder den Empfangsknoten **31** der **Fig. 3** erläuterten Funktionen übernehmen, insbesondere ein zweites Signal und ein kryptographisches Datum, wie einen Sicherheitscode, und ein zu sendendes erstes Signal bereitstellen.

[0038] In **Fig. 4** sind als erstes Signal zu sendende Sendedaten mit Tx, aus einem Empfangssignal wiedergewonnene Empfangsdaten mit Rx, der als zweites Signal zu sendende Sicherheitscode mit sc_send und der empfangene Sicherheitscode mit sc_empf gekennzeichnet.

[0039] Die zu sendenden ersten Sendedaten **Tx**, welche das erste Signal bestimmen, und der als zweites Signal zu sendende Sicherheitscode werden an einen Transmitter **42** des Transceivers **41** übermittelt. Dieser erzeugt auf CAN-Leitungen CANH, CANL, ein entsprechendes Überlagerungssignal gemäß dem CAN-Kommunikationsprotokoll, welches durch den Sicherheitscode moduliert wird. Die Leitungen CANH, CANL, sind dabei wie durch die oben erwähnten CAN-Standards spezifiziert mit einem Widerstand **45** von etwa **60** Ohm verbunden. Bei rezessiven Bits gleicht sich das Potenzial der Leitungen CANH, CANL über den Widerstand **45** einander an, sodass im Wesentlichen keine Potenzialdifferenz zwischen den Leitungen vorliegt. Bei dominanten Bits werden die Leitungen CANH, CANL von dem Transmitter **42** aktiv auf eine Spannungsdifferenz getrieben.

[0040] Beispiele für die Implementation des Transmitters **42** hierzu werden später noch näher erläutert. Zum Empfangen sind die Leitungen CANH, CANL mit einem Receiver **43** verbunden, der das erste Signal **s1** wiedergewinnt. Zudem sind die Leitungen mit einer Überwachungsschaltung **44** verbunden, welche aus der Differenzspannung zwischen den Spannungen an den Leitungen CANH, CANL den Sicherheitscode wiedergewinnt. Hierzu kann die Differenzspannung insbesondere mit einem Schwellenwert verglichen werden, wie dies später noch näher erläutert werden wird.

[0041] Die **Fig. 5** zeigt einen Teil eines Transmitters, insbesondere einen Treiber als Beispiel für eine mögliche Implementierung des Transmitters **42** der **Fig. 5**. Allgemein wird in der dominanten Phase die Leitung CANH über einen Widerstand mit einer positiven Spannung (beispielsweise VDD, VCC oder einer anderen Versorgungsspannung Vs) verbunden, und die Leitung CANL wird über einen Widerstand mit einer hierzu kleineren Spannung (beispielsweise VSS, Masse oder dergleichen) verbunden. Dieses Verbinden kann schrittweise über mehrere Widerstände geschehen. Die **Fig. 5** zeigt eine entsprechende Schaltung für die Leitung CANH. Eine entsprechende Schaltung kann auch für die Leitung CANL vorgesehen sein.

[0042] Der Treiber der **Fig. 5** umfasst eine Parallelschaltung **50** einer Vielzahl von Widerständen **55**, **53**, **51**, welche jeweils mit einem zugeordneten Schalter **56**, **54**, **52** in Reihe geschaltet ist. Die Schalter können mittels Transistoren implementiert sein. Ein erster Anschluss der Widerstände **55**, **53 51** ist mit einer Versorgungsspannung Vs verbunden, und ein jeweiliger zweiter Anschluss ist mit einem ersten Anschluss des jeweils zugeordneten Schalters verbunden. Zweite Anschlüsse der Schalter **56**, **54**, **52** sind über eine Diode **57** mit den Leitung CANH verbunden. Die Anzahl von drei Widerständen und drei zugeordneten Schaltern ist dabei als Beispiel zu verstehen, und es kann jede Anzahl von Widerständen mit jeweils zugeordneten Schaltern bereitgestellt sein.

[0043] Bei einem rezessiven Bit sind alle Schalter **56**, **54**, **52** geöffnet, und über den Widerstand **45** der **Fig. 4** wird eine Spannungsdifferenz zwischen CANH und CANl ausgeglichen. Bei einem dominanten Bit werden die Schalter **56**, **54**, **52** sukzessive geschlossen, sodass der Spannungspegel auf der Leitung CANH letztendlich durch die Versorgungsspannung **Vs** den Wert der Widerstände **55**, **53**, **51**, dem Wert des Widerstandes **45** sowie dem Wert entsprechender Widerstände einer entsprechenden Schaltung, die mit der Leitung CANL verbunden ist, bestimmt wird.

[0044] Bei der Sendeschaltung **42** der **Fig. 4** bestimmt der Sicherheitscode, wie viele Schalter bei einem dominanten Bit, z.B. bei einem Wechsel von **Tx** in **Fig. 4** von 1 auf 0, geschlossen werden. Beispielsweise wird ein Teil der Schalter **56**, **54**, **52**, z.B. alle Schalter außer dem Schalter **52**, im dominanten Fall immer geschlossen. Ein anderer Teil der Schalter, beispielsweise der Schalter **52**, wird im dominanten Fall in Abhängigkeit von dem Sicherheitscode gesteuert. Auf diese Weise wird z.B. durch Schließen der Schalter **56**, **54** der Pegel für ein dominantes Bit der CAN-Übertragung erzeugt, und durch wahlweise Schließen des Schalters **52** wird der Sicherheitscode aufmoduliert. Der Widerstand **51** ist in diesem Beispiel dann so dimensioniert, dass durch Öffnen und Schließen des Schalters **52** der Spannungspegel auf der Leitung CANH einen durch das Kommunikationsprotokoll, in diesem Fall des CAN-Protokolls, spezifizierten Spannungsbereichs für den dominanten Pegel nicht verlässt. Dieser kann bei manchen Ausführungsbeispielen eine Rückwärtskompatibilität sicherstellen. Bei anderen Ausführungsbeispielen kann auch mehr als ein Schalter zur Modulation des Sicherheitscodes auf das Signal verwendet werden.

[0045] Zur weiteren Veranschaulichung zeigt die **Fig. 6** Beispiele für Signale des Ausführungsbeispiels der **Fig. 4**. Es ist zu bemerken, dass diese und auch andere in dieser Anmeldung dargestellten Signalformen nur der Veranschaulichung dienen und sich die exakten Signalformen in Abhängigkeit von der Implementierung, zu übertragenden Informationen und einem gewählten Sicherheitscode oder anderen kryptographischen Daten, verwendeten Kommunikationsprotokollen sowie in Abhängigkeit von äußeren Umständen wie Temperatur ändern können.

[0046] Mit **60** sind die Sendedaten **Tx** in **Fig. 4** bezeichnet, d.h. die von dem Microcontroller **40** in dem Transceiver **41** empfangenen zu sendenden Daten, die das erste Signal bestimmen. Die Daten stellen eine Abfolge aus logischen Einsen und Nullen dar.

[0047] Mit **61** wird der zu sendende Sicherheitscode bezeichnet, der das zweite Signal bestimmt. Mit **62** ist ein letztendlich auf den CAN-bus gesendetes Überlagerungssignal dargestellt, wobei die Differenz zwischen den Spannungen auf den Leitungen CANH, CANL, auch als Vdiff bezeichnet, dargestellt ist. Bei einer logischen 1 der Sendedaten **60** liegt ein rezessiver Zustand des Busses vor, d.h. die Leitungen CANH, CANL werden nicht aktiv getrieben, und über den Widerstand **45** gleicht sich das Potenzial der Leitungen CANH, CANL einander an. Das Überlagerungssignal **62**, welches die Differenzspannung Vdiff widerspiegelt, ist also bei oder nahe 0. Bei einer logischen 0 (niedriger Pegel) des Signals **60** werden die Leitungen CANH, CANL jeweils über Widerstände mit Spannungen verbunden, wie unter Bezugnahme auf **Fig. 5** erläutert, sodass sich eine Differenzspannung ergibt. Während dieser dominanten Phasen wird der Sicherheitscode **61** als zweites Signal aufmoduliert. Wie an dem Überlagerungssignal **62** zu sehen ist, ist während der dominanten Phasen die Spannung **Vdiff** etwas höher, auf einem Pegel **65**, wenn das Signal **61** auf logisch 1 (hoher Pegel) ist, und etwas niedriger, auf einem Pegel **66**, wenn der Sicherheitscode **61** auf logisch 0 (niedriger Pegel) ist. Dies kann

wie unter Bezugnahme auf die **Fig. 5** erläutert durch wahlweises Schließen des Schalters wie des Schalters **52** erreicht werden.

[0048] Mit **63** sind die aus dem Signal **62** wiedergewonnenen Empfangsdaten **Rx** bezeichnet. Dieses entspricht dem Signal **60** mit einer Verzögerung, die von einer Wahl der Abtastzeitpunkte abhängt. Mit **64** ist der wiedergewonnene Sicherheitscode bezeichnet. Dieser entspricht ebenso mit einer Verzögerung dem gesendeten Sicherheitscode **61**. Damit dies möglich ist, werden Signalwechsel wie oben bereits kurz erläutert des Sicherheitscodes **61** so gewählt, dass sie während dominanter Phasen liegen, beispielsweise wie in **Fig. 6** gezeigt, mit dem Beginn dominanter Phasen zusammenfallen, wofür wie bereits unter Bezugnahme auf die **Fig. 3** erläutert ein Sicherheitscodegenerator Information über die zu sendenden Daten erhält. Ein Flankenwechsel des Signals **61** während einer rezessiven Phase würde hingegen nicht sofort im Signal **62** wiedergespiegelt werden, sondern ggf. erst bei dem nächsten dominanten Bit, was zu einer Änderung des Signals **64** verglichen mit dem Signal **61** führen würde.

[0049] Zu beachten ist, dass je nach zu sendenden Daten relativ viele rezessive Bits sukzessive gesendet werden können. Je nach verwendetem physikalischen Kommunikationsprotokoll ist aber eine gewisse Anzahl an dominanten Phasen sichergestellt, sodass der Sicherheitscode oder allgemein ein zweites Signal, welches ein kryptographisches Datum umfasst, aufmoduliert werden kann.

[0050] Wie oben erläutert entsteht durch die Wahl der Abtastzeitpunkte (und ggf. auch durch andere Effekte wie Signallaufzeiten) eine Verzögerung zwischen den Sendedaten **Tx**, welche zu senden sind, und den wiedergewonnenen Empfangsdaten **Rx**. Dies wird nun unter Bezugnahme auf die **Fig. 7** und **Fig. 8** noch näher erläutert. Die **Fig. 7** und **Fig. 8** betreffen dabei insbesondere das Wiedergewinnen des Sicherheitscodes und die Wahl von Abtastzeitpunkten hierzu, d.h. die Wahl von Zeitpunkten, zu denen die Spannungsdifferenz Vdiff zum Gewinnen des Sicherheitscodes ausgewertet wird.

[0051] Die **Fig. 7** zeigt als Verlauf **70** die Sendedaten **Tx**, als Überlagerungssignal **71** die Spannung Vdiff, als Verlauf **72** die Empfangsdaten **Rx** und als Verlauf **73** den wiedergewonnenen Sicherheitscode. In diesem Beispiel wird die Spannung **Vdiff** bezüglich des Sicherheitscodes bei der fallenden Flanke des Signals **Rx** ausgewertet. In anderen Worten wird, sobald eine fallende Flanke des Signals **Rx** und somit ein Übergang zu einer dominanten Phase erkannt wird, die Spannungsdifferenz Vdiff ausgewertet, um einen Wert für den Sicherheitscode wiederzugewinnen. Dies kann durch Vergleich der Spannungsdifferenz **Vdiff** mit einem Schwellenwert geschehen, der zwischen den beiden möglichen Signalpegeln im dominanten Fall liegt (vgl. die beiden in **Fig. 6** gezeigten Pegel **65**, **66**, als Schwellenwert wird dann eine Spannung zwischen diesen Pegeln gewählt), wie später noch erläutert werden wird. In diesem Fall ist der wiedergewonnene Sicherheitscode **73** zu den Empfangsdaten **72** hinsichtlich Flankenwechseln synchron. Hierfür ist nötig, dass zu diesem Zeitpunkt das Überlagerungssignal **71** für das Abtasten zum Wiedergewinnen des Sicherheitscodes „gültig“ ist, d.h. seinen stationären Wert erreicht hat. Dies ist beispielsweise der Fall, wenn die Schleifenverzögerung (im Englischen als loop delay bezeichnet) kleiner ist als die Zeitdauer eines Bits bei der höchsten Bitrate (beispielsweise entspricht dies bei 5 Megabit pro Sekunde **200** Nanosekunden), da sich sonst der Bitzustand schon wieder geändert haben könnte.

[0052] Eine Alternative ist in **Fig. 8** gezeigt. Die **Fig. 8** zeigt Sendedaten **Tx**, ein Überlagerungssignal **81** als Spannungsdifferenz **Vdiff** auf dem Bus, Empfangsdaten **Rx** und einen wiedergewonnenen Sicherheitscode **83**. Hier erfolgt das Abtasten der Differenzspannung **Vdiff** eine vorgegebene Zeit dt nach der fallenden Flanke von Sendedaten **80**, wobei die Zeit dt kleiner als die Zeitdauer eines Bits bei der höchsten auftretenden Bitrate gewählt ist. So wird sichergestellt, dass sich im Abtastzeitpunkt das Bit nicht wieder geändert hat. In diesem Fall ist der wiedergewonnene Sicherheitscode **83** hinsichtlich Flankenwechsel nicht synchron zu den Empfangsdaten **82**.

[0053] Diese Abtastzeitpunkte sind lediglich als Beispiel zu verstehen, und es können allgemein Abtastzeitpunkte gewählt werden, bei welchen das Signal die abzutastenden Signalpegel soweit angenommen hat, dass die verschiedenen Pegel des aufmodulierten Sicherheitscodes unterscheidbar sind.

[0054] Bei manchen Implementierungen, beispielsweise bei manchen Kommunikationsprotokollen, kann es wünschenswert sein, dass Signale hinsichtlich des Verlaufs ansteigender und fallender Flanken sich immer gleich verhalten. Durch das Überlagern des zweiten Signals, z.B. Aufmodulieren des Sicherheitscodes, kann es bei manchen Implementierungen vorkommen, dass dies nicht gewährleistet ist. Zur Veranschaulichung sind in **Fig. 9** Sendedaten **Tx**, welche eine zu sendende Bitfolge repräsentieren, dargestellt. Eine Kurve **91** zeigt einen Fall für das übertragende Überlagerungssignal, wenn ein logisch hoher Pegel des Sicherheitscodes

aufmoduliert wird. Eine gestrichelte Kurve **92** zeigt den Fall des Überlagerungssignals, in dem ein logisch niedriger Pegel des Sicherheitscodes aufmoduliert wird, wobei in dem Beispiel der Kurven **91**, **92** Schalter sukzessive geschlossen werden, wie unter Bezugnahme auf die **Fig. 5** erläutert. Wie zu sehen ist, sind die ansteigenden Flanken in beiden Fällen bis zum Erreichen des jeweiligen Signalpegels identisch. Die fallenden Flanken können jedoch zeitlich versetzt sein. Wenn eine bestimmte Abtastschwelle zum Abtasten des Signals **91** bzw. **92** verwendet wird, kann dies wie durch Kurven **93**, **94** angedeutet zu verschiedenen Empfangsdaten **Rx** führen, deren Flanken leicht zueinander versetzt sind. Dies kann bei manchen Anwendungen mit hohen Bitraten nachteilhaft sein.

[0055] In einem derartigen Fall kann das Schalten auf einen höheren Pegel für eine logische 1 des Sicherheitscodes zeitlich versetzt erfolgen, wie dies in einem unteren Teil der **Fig. 9** dargestellt ist. Dabei sind wieder Sendedaten **Tx** gezeigt, und ein Verlauf **96** zeigt eine verzögerte Version der Sendedaten **95**. In diesem Falle erfolgt die Erzeugung des Überlagerungssignals **97** ohne den aufmodulierten Sicherheitscode auf Basis des verzögerten Signals **96**. Das Ende der Aufmodulierung des Sicherheitscodes erfolgt hingegen mit der steigenden Flanke des Signals **95**, sodass der Sicherheitscode beabstandet zu den Flanken des Signals aufmoduliert wird, wie durch das Signal **97** gezeigt. In anderen Worten erfolgt hier eine Überlagerung des zweiten Signals gemäß dem Sicherheitscode, nachdem für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgte und für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgen wird. Eine Schwellenspannung **98**, auf deren Basis der Signalwechsel des Empfangssignals erfolgt, wird somit unabhängig von dem aufmodulierten Sicherheitscode immer zur gleichen Zeit gekreuzt. Die steigende Flanke der Sendedaten **95** kann zudem dann zum Abtasten des Sicherheitscodes verwendet werden (siehe die Erläuterungen zu den **Fig. 7** und **Fig. 8** hinsichtlich des Abtasten des Sicherheitscodes).

[0056] Durch die Modulation des Sicherheitscodes wie in dem Überlagerungssignal **97** wird die Schleifenverzögerung geringfügig erhöht, da die verzögerten Sendedaten **96** als Grundlage für die Erzeugung des Signals verwendet werden, es bleibt jedoch das Verhalten hinsichtlich steigender und fallender Flanken bei manchen Ausführungsbeispielen unabhängig von dem aufmodulierten Sicherheitscode.

[0057] Wie bereits vorstehend erläutert kann der Sicherheitscode wiedergewonnen werden, indem das empfangene Signal im Falle eines CAN-Busses die Differenzspannung, mit einem Schwellenwert (z.B. Schwellenspannung) verglichen wird. Dieser Schwellenwert liegt zweckmäßigerweise zwischen den beiden möglichen Pegeln des Sicherheitscodes, beispielsweise zwischen den Pegeln **65** und **66** der **Fig. 6**. Diese beiden Pegel liegen bei manchen Ausführungsbeispielen relativ nah beieinander, beispielsweise um sicherzustellen, dass beide Pegel innerhalb eines Toleranzbereichs für einen entsprechenden Signalpegel des Signals gemäß dem Kommunikationsprotokoll liegen, wie erläutert. Bei manchen Implementierungen können die Pegel zusätzlich in Abhängigkeit von Umständen wie Temperatur, Versorgungsspannung, Herstellungstoleranzen von Komponenten und dergleichen schwanken, was bei manchen Ausführungsbeispielen eine geeignete Wahl der Schwellenspannung erschweren kann. Dies wird nunmehr unter Bezugnahme auf die **Fig. 10** und **Fig. 11** am Beispiel eines CAN-Busses erläutert, und dann werden nachfolgend verschiedene Kalibrierungsmöglichkeiten erläutert, welche es ermöglichen, auch in Implementierungen, bei denen derartige Variationen auftreten, eine geeignete Schwellenspannung zu bestimmen.

[0058] **Fig. 10** zeigt schematisch einen Treiber eines Transmitters für einen CAN-Bus im dominanten Zustand. Die **Fig. 10** zeigt die beiden bereits diskutierten Leitungen CANH, CANL eines CAN-Busses, welche über einen Lastwiderstand **100** entsprechend dem Lastwiderstand **45** der **Fig. 4** verbunden sind. Der Lastwiderstand **100** weist bei CAN-Bussen einen Wert von **60** Ohm auf, wobei hier Toleranzen in einem Bereich von etwa **50** Ohm bis **75** Ohm zugelassen sind. Die Leitung CANH ist über einen Widerstand **101** mit einem Widerstandwert RH und eine Diode **102** mit einer positiven Versorgungsspannung VCC verbunden, und die Leitung CANL ist über eine Diode **103** und einen Widerstand **104** mit einem Widerstandwert RL mit Masse verbunden. Der Widerstand **101** entspricht dabei beispielsweise denjenigen Widerständen **55**, **53**, **51** der **Fig. 5**, deren Schalter im dominanten Zustand geschlossen sind, ist also ein Ersatzschaltbild für die parallelen Schalter und Widerstände der **Fig. 5** im dominanten Zustand, und die Diode **102** entspricht der Diode **57** der **Fig. 5**. Die Diode **103** und der Widerstand **104** entsprechen entsprechenden Komponenten zwischen CANL und Masse. Die differenzielle Spannung Vdiff zwischen CANH und CANL berechnet sich zu:

$$\mathrm{Vdiff} = (\mathrm{VCC} - 2\mathrm{Ud}) * \mathrm{Rload} / (\mathrm{RH} + \mathrm{RL} + \mathrm{Rload}),$$

wobei Rload der Widerstandswert des Widerstandswert **100** und Ud die Diodenspannung der Dioden **102**, **103** in Durchlassrichtung ist.

[0059] RH und RL variieren dabei zwischen den beiden Pegeln, die in dem dargestellten Sicherheitscode verwendet werden. Um ein Zahlenbeispiel zu geben, kann RH=RL=20 Ohm für den einen Pegel des Sicherheitscodes und RH=RL=15 Ohm für den anderen Pegel sein. Mit Beispielwerten VCC=5 Volt, Rload=60 Ohm und Ud=0,7 Volt ergibt sich dann mit der obigen Formal Vdiff,low=2,16 Volt und Vdiff,high=2,4 Volt für die beiden möglichen Pegel, mit denen der Sicherheitscode moduliert wird. Die Spannungsdifferenz zwischen diesen beiden Pegeln liegt bei diesem Beispiel also etwas über 200 mV.

[0060] Wie aus der obigen Gleichung ersichtlich ist hängt die Spannung Vdiff von der Versorgungsspannung VCC sowie dem Lastwiderstand **100** ab. Zudem hängen die Größen in der Gleichung, beispielsweise die Diodenspannung Ud, auch von der Temperatur ab. Die Abhängigkeit von der Versorgungsspannung und von Rload ist in der **Fig. 11** schematisch dargestellt. Die **Fig. 12** veranschaulicht zudem eine Abhängigkeit von der Temperatur.

[0061] In der **Fig. 11** zeigen Kurven **110**-**115** die Spannung Vdiff gemäß obiger Gleichung über dem Lastwiderstand Rload. Rload variiert dabei zwischen **50** und **75** Ohm, was beispielsweise einem erlaubten Variationsbereich für CAN-Busse entsprechen kann. In **Fig. 12** ist die Spannung Vdiff über der Temperatur aufgetragen.

[0062] Die Kurven **110**-**115** zeigen die Spannung Vdiff für verschiedene Versorgungsspannungen und für einen hohen Pegel (entsprechend dem obigen Vdiff,high) und einen niedrigen Pegel (entsprechend dem obigen Vdiff,low) für die Beispielwerte für RH, RL von **15** bzw. **20** Ohm wie oben erläutert. Insbesondere zeigt die Kurve **110** Vdiff,high für VCC=5,25 Volt, die Kurve **1111** Vdiff,high für VCC=5, die Kurve **112** Vdiff,low für VCC= 5,25 Volt, die Kurve **113** Vdiff,high für VCC=4,75 Volt, die Kurve **114** Vdiff,low für VCC=5 Volt und die Kurve **115** Vdiff,low für VCC=4,75 Volt. In **Fig. 12** zeigt die Kurve **120** Vdiff,high für VCC=5 Volt und Rload=75 Ohm, die Kurve **121** Vdiff,high für VCC=5 Volt und Rload=60 Ohm, die Kurve **122** Vdiff,low für VCC=5 Volt und Rload= 75 Ohm, die Kurve **123** Vdiff,high für VCC=5 Volt und Rload=50 Ohm, die Kurve **124** Vdiff,low für VCC=5 Volt und Rload=60 Ohm und die Kurve **125** Vdiff,low für VCC=5 Volt und Rload=50 Ohm.

[0063] Der externe Lastwiderstand **100** ist dabei a priori nicht bekannt und kann eben variieren wie erläutert. Auch die Versorgunsspannung kann variieren, beispielsweise zwischen 4,75 Volt und 5,25 Volt wie in **Fig. 11** angegeben. Wie aus den **Fig. 11** und **Fig. 12** ersichtlich kann bei derartigen Implementierungen, bei denen solche Variationen auftreten können, kein einziger Schwellenwert (d.h. in diesem Fall eine Schwellenspannung) festgelegt werden, mit dem zwischen Vdiff,high und Vdiff,low für alle auftretenden Lastwiderstände, Spannungen und Temperaturen unterschieden werden kann. Z.B. würden bei einem Schwellenwert von 2,30 Volt wie in **Fig. 4** ersichtlich bei einem Widerstand Rload über **60** Ohm und einer Versorgungsspannung von 5,75 Volt sowohl Vdiff,high (Kurve **110**) als auch Vdiff,low (Kurve **112**) über diesem Schwellenwert liegen, sodass eine Unterscheidung nicht möglich wäre. Gleiches gilt auch für andere mögliche Schwellenwerte.

[0064] Daher wird bei manchen Ausführungsbeispielen, bei welchen derartige Variationen auftreten können, eine Kalibrierung durchgeführt, für welche im Folgenden verschiedene Möglichkeiten erörtert werden. Bei Ausführungsbeispielen, bei denen derartige Variationen nicht oder in geringem Ausmaß auftreten, kann hingegen ein einziger Schwellenwert gewählt werden, und die Kalibrierung kann weggelassen werden.

[0065] Die **Fig. 13** zeigt eine für eine derartige Kalibrierung verwendete Schaltung gemäß mancher Ausführungsbeispiele. Bei dem Ausführungsbeispiel der **Fig. 13** wird eine Nachbildung des in **Fig. 10** dargestellten Treibers bereitgestellt, um eine Referenzspannung Vref zu gewinnen. Eine Nachbildung eines Schaltungsteils ist dabei eine Schaltung, die allgemein dem Schaltungsteil entsprechende Komponenten enthält, welche bezüglich des Schaltungsteils skaliert sein können (beispielsweise eine um einen Skalierungsfaktor verkleinerte Fläche aufweisen können, eine um einen Skalierungsfaktor vergrößerten Widerstand aufweisen können und dergleichen). Die Nachbildung im Ausführungsbeispiel der **Fig. 13** umfasst einen Widerstand **131** entsprechend dem Widerstand **101**, eine Diode **132** entsprechend der Diode **102**, eine Diode **133** entsprechend der Diode **103** und einen Widerstand **134** entsprechend dem Widerstand **104**. Wie in **Fig. 13** angedeutet sind die Widerstände **133**, **134** bezüglich der Widerstände **101**,**104** um einen Faktor n skaliert, insbesondere um einen Faktor **n** höher, was einen Stromfluss durch die Nachbildung begrenzt. Die Dioden **132**, **133** weisen verglichen mit den Dioden **102**, **103** eine um den Skalierungsfaktor n verkleinerte Fläche auf, was einen Flächenbedarf für die Nachbildung verringert und die Stromaufnahme verringert. Bei typischen Werten kann n > 30 gelten, um eine Stromaufnahme der Nachbildung unter 1 mA zu halten. Deutlich höhere Werte von n würden zwar die Stromaufnahme weiter verringern, könnten aber je nach Implementierung das Matching der Nachbildung zu dem in **Fig. 10** dargestellten Treiber verschlechtern. Für die Widerstände **131**, **134** kann dabei ein Zwischenwert zwischen den Werten n*RH und n*RL für den hohen und niedrigen Pegel des Sicherheitscodes verwendet werden. Über dem Widerstand **130** fällt dann eine Spannung ab, die als Referenzspannung bei manchen

Ausführungsbeispielen verwendet wird. Schwankungen der Versorgungsspannung VCC sowie der Temperatur wirken sich mit einer derartigen Schaltung in gleicher Weise auf die Spannung Vdiff und auf die durch die Nachbildung gewonnene Referenzspannung Vref aus, sodass hierdurch der Einfluss von schwankenden Referenzspannungen und Temperaturen ausgeglichen werden kann.

[0066] Allerdings werden hierdurch noch nicht Schwankungen des Widerstandwerts Rload des Widerstands **100** ausgeglichen. Da der Widerstand **100** bei vielen Implementierungen ein externer Widerstand ist, ist dieser häufig nicht a priori bekannt.

[0067] Bei Ausführungsbeispielen, bei welchen derartige Variationen eines Lastwiderstandes auftreten, welche die Pegel des aufmodulierten zweiten Signals, z.B. auf Basis des diskutierten Sicherheitscodes (in diesem Fall die Spannung Vdiff) beeinflussen, kann zusätzlich der Widerstand **130**, welche den Widerstand **100** nachbildet, einstellbar sein und auf einen Wert RL_RF=n*Rload kalibriert werden, wobei n wiederum die Skalierung ist. Möglichkeiten, wie eine derartige Kalibrierung vorgenommen werden kann, werden später noch näher erläutert. Das Ergebnis einer derartigen Kalibrierung ist in **Fig. 14** dargestellt. In **Fig. 14** zeigt eine Kurve **140** die Spannung Vdiff,high für eine Versorgungsspannung von 5 Volt und einen Lastwiderstand Rload von **55** Ohm über der Temperatur, und eine Kurve **142** zeigt die Spannung Vdiff,low für die Versorgungsspannung und den Lastwiderstand von **55** Ohm. Eine Kurve **141** zeigt eine Referenzspannung Vref über der Temperatur, welche mit einem Widerstand **130** gewonnen wurde, dessen Widerstandwert RL RF auf **55** Ohm*n eingestellt wurde. Die Widerstände **131**, **134** betrugen dabei jeweils n*17 Ohm, d.h. ein Wert zwischen den oben erwähnten Beispielwerten von **20** Ohm und **15** Ohm für niedrigen und hohen Pegeln des Sicherheitscodes.

[0068] Ähnliche Resultate werden bei anderen Werten von Rload erhalten. Somit kann durch eine Kalibrierung des Widerstandwertes RL RF bei manchen Ausführungsbeispielen eine Referenzspannung erzeugt werden, die als Schwellenspannung benutzt werden kann, um die zwei Pegel zu unterscheiden.

[0069] **Fig. 15** zeigt eine Kalibrierungsschaltung gemäß manchen Ausführungsbeispielen, mit welchen eine derartige Kalibrierung eines nachgebildeten Widerstandes zum Bestimmen einer geeigneten Schwellenspannung (Referenzspannung) als Schwellenwert erfolgen kann. Die **Fig. 15** umfasst den Teil des Treibers des Transmitters mit den Bezugszeichen **100**-**104**, welcher bereits unter Bezugnahme auf die **Fig. 10** beschrieben wurde. Wie bereits erläutert können die Widerstände **101**, **104** jeweils zwei verschiedene Werte (z.B. **15** Ohm und **20** Ohm) annehmen, und diese sind in **Fig. 15** mit **R1** und **R2** bezeichnet. **R1** entspricht dabei dem Widerstandswert für den niedrigen Pegel (**20** Ohm in dem obigen Beispiel) und **R2** für den hohen Pegel (**15** Ohm in dem obigen Beispiel), d.h. **R2 < R1**.

[0070] Die Schaltung der **Fig. 15** umfasst zwei Nachbildungen dieses Treibers. Eine erste Nachbildung umfasst einen Widerstand **153**, entsprechend dem Widerstand **101**, eine Diode **154** entsprechend der Diode **102**, einen verstellbaren Widerstand **155** entsprechend dem Widerstand **100**, eine Diode **156** entsprechend der Diode **103** und einen Widerstand **157** entsprechende der Diode **104**. Die Dioden **154**, **156** sind bezüglich der Dioden **102**, **103** um einen Faktor n skaliert (beispielsweise um n kleiner Fläche) und die Widerstandwerte der Widerstände **153**, **157** betragen n*R2, d.h. sind bezüglich des Widerstandswertes der Widerstände **101**, **104** für den hohen Pegel des Sicherheitscodes skaliert.

[0071] Eine zweite Nachbildung umfasst einen Widerstand **158** entsprechend dem Widerstand **101**, eine Diode **159** entsprechend der Diode **102**, einen verstellbaren Widerstand **1510** entsprechend dem Lastwiderstand **100**, eine Diode **1511** entsprechend der Diode **103** und einen Widerstand **1512** entsprechend dem Widerstand **104**. Die Dioden **159**, **1511** sind wiederum bezüglich der Dioden **102**, **103** um den Faktor n skaliert weisen beispielsweise also eine n-mal kleiner Fläche auf. Die Widerstände **158**, **1512** sind bezüglich des Widerstandswertes **R1** um n skaliert, d.h. bezüglich des Widerstandwertes für den niedrigen Pegel.

[0072] Eine Kalibrierschaltung **152** misst die differenzielle Spannung Vdiff an dem Widerstand **100**. Zur Kalibrierung kann beispielsweise am Anfang eines CAN-Telegramms oder während einer Kalibrierphase die Sendeschaltung zunächst den Widerstand **R1** für die Widerstände **101**, **104** einstellen und dann den Widerstand **R2** oder umgekehrt.

[0073] Zudem misst die Kalibrierschaltung **152** den Spannungsabfall über den Widerstand **155**, in **Fig. 15** als Vref2 bezeichnet, und den Spannungsabfall über den Widerstand **1510**, in **Fig. 15** als Vref1 bezeichnet, wobei die Widerstände **155**, **1510** auf den gleichen Widerstandswert eingestellt sind.

[0074] Während der Kalibrierphase stellt die Kalibrierschaltung **152** den während der Phase, in der die Widerstände **101**, **104** auf **R1** eingestellt sind, den Widerstand **1510** und den Widerstand **155** so ein, dass Vref1= Vdiff gilt. Da die Widerstände **158** und **1512** gleich n x **R1** sind, gilt nach dieser Einstellung, dass der Wert der Widerstände **1510**, **155** gleich n x Rload ist. Auf diese Weise werden also die Widerstände **155** und **1510** dem Widerstandwert Rload des Widerstands so angepasst, dass die Referenzspannungen **Vref1**, **Vref2** den beiden möglichen Werten des Signals **Vdiff** für hohen und niedrigen Pegeln des Sicherheitscodes entsprechen. Aus den Werten **Vref1**, **Vref2** kann dann ein Schwellenwert Vref zum Wiedergewinnen des Sicherheitscodes bestimmt werden, indem Vref auf einen Wert zwischen **Vref1** und **Vref2** gesetzt wird.

[0075] In dem Ausführungsbeispiel der **Fig. 16** ist zusätzlich zu den beiden Nachbildungen der **Fig. 15** eine dritte Nachbildung umfassend einen Widerstand **160** entsprechend dem Widerstand **101**, eine Diode **161** entsprechend der Diode **102**, einen einstellbaren Widerstand **162** entsprechend dem Lastwiderstand **100**, eine Diode **163** entsprechend der Diode **103** und ein Widerstand **164** entsprechend dem Widerstand **104** bereitgestellt. Der Widerstand **160** und der Widerstand **164** sind bezüglich eines Widerstandes mit einem Widerstandwert, der zwischen **R1** und **R2** liegt, um einen Faktor n skaliert. Wenn wie in dem Zahlenbeispiel R1=20 Ohm und R2=15 Ohm ist, kann ein Widerstandswert der Widerstände **160** und **164** beispielsweise n*17 Ohm oder n-mal ein anderer Wert zwischen **R1** und **R2** sein. Die Dioden **161** und **163** sind verglichen mit den Dioden **102** und **103** ebenfalls um den Faktor n skaliert, weisen beispielsweise eine n-mal kleinere Fläche auf.

[0076] In diesem Fall werden die Widerstände **155**, **1510** und **162** gleichzeitig wie oben erläutert eingestellt, z.B. sodass Vref1 = Vdiff in einer Phase, in der die Widerstände **101**, **104** auf **R1** sind, gilt. Durch die Wahl der Widerstände **160**, **164** fällt dann an dem Widerstand **162** eine Referenzspannung Vref ab, welche zwischen Vdiff,high und Vdiff,low liegt und somit als Schwellenwert für die Gewinnung des Sicherheitscodes aus dem empfangenen Signal verwendet werden kann.

[0077] Eine weitere Möglichkeit zu Bestimmung einer Spannung Vref, welche als Schwellenwert dienen kann, ist in **Fig. 17** dargestellt. Verglichen mit der **Fig. 15** sind bei dem Ausführungsbeispiel der **Fig. 17** zusätzlich Widerstände **170**, **171**, **172**, **173** bereitgestellt, welche wie in **Fig. 17** dargestellt mit den Widerständen **1510**, **155** verschaltet sind. Bei manchen Ausführungsbeispielen weisen alle Widerstände **170**-**173** einen gleichen Widerstandswert **R** auf. Zwischen einem ersten Knoten, welcher zwischen den Widerständen **170**, **171** liegt und einem zweiten Knoten, welcher zwischen den Widerständen **172**, **173** liegt, kann dann eine Spannung Vref die als Schwellenwert dienen kann, abgegriffen werden. Weisen alle Widerstände **170-173** einen gleichen Widerstandswert auf, gilt Vref=(Vref1+Vref2)/2. Durch Änderung der Widerstandswerte **170-173** kann dies verändert werden, beispielsweise Vref näher an **Vref1** oder näher an **Vref2** geschoben werden. Bei Ausführungsbeispielen weisen die Widerstände **170-173** höhere Widerstandwerte auf als die Widerstände **153**, **157**, **158** und **1512**. Bei manchen Ausführungsbeispielen kann dies einen Fehler bei der Bestimmung der Referenzspannung Vref verringern.

[0078] Bei manchen Ausführungsbeispielen können Störungen auf Kommunikationsleitungen wie beispielsweise Busleitungen, im Falle eines CAN-Busses den Leitungen CANH, CANL auftreten. Beispiele für derartige Störungen umfassen hochfrequente Störungen (RF-Störungen), welche beispielsweise durch elektromagnetische Übersprechen (EMI, electromagnetic interference) entstehen können.

[0079] Wenn derartige Störungen während der beschriebenen Kalibrierungsvorgänge auftreten, können sie das Ergebnis der Kalibrierung verfälschen. Um dies zu vermeiden, können bei manchen Ausführungsbeispielen Maßnahmen ergriffen werden. Beispielsweise kann bei dem Ausführungsbeispiel der **Fig. 16** eine zusätzliche Spannungsüberwachung **1513** optional bereitgestellt werden, welche die Spannung auf den Busleitungen CANH, CANL überwacht und überprüft, ob diese in einem erlaubten Bereich sind. Bei einem CAN-Bus kann der erlaubte Bereich beispielsweise zwischen 1 und 4 Volt sein. Bei anderen Kommunikationsmedien können andere erlaubte Bereiche vorliegen.

[0080] Eine Kalibrierung, d.h. eine Einstellung der Widerstände **1510**, **155**, um entsprechend der gemessenen Spannung **Vdiff**, ist nur dann gültig, wenn die Spannungen auf den Bussen auf den Leitungen CANH, CANL in dem erlaubten Bereich liegen. Liegen sie außerhalb des erlaubten Bereichs, ist die Kalibrierung ungültig und muss wiederholt werden.

[0081] Bei einem anderen Ausführungsbeispiel, welches in der **Fig. 18** dargestellt ist, können die Widerstände **1510** und **155** unabhängig voneinander von zwei Kalibrierschaltungen eingestellt werden. Dementsprechend ist verglichen mit der **Fig. 15** in der **Fig. 18** die Kalibrierschaltung **152** durch eine erste Kalibrierschaltung **180** zum Einstellen des Widerstandes **155** und eine zweite Kalibrierschaltung **181** zum Einstellen des Widerstan-

des **1510** ersetzt. Die Kalibrierungen können dabei zeitlich versetzt erfolgen. Eine Vergleichsschaltung **182** vergleicht die Kalibrierresultate. Bei einer korrekten Kalibrierung sollten die für die Widerstände **155** und **1510** eingestellten Widerstandswerte zumindest näherungsweise gleich sein. Unterscheiden sie sich um mehr als einen vorgegebenen Schwellenwert, wird bei manchen Ausführungsbeispielen die Einstellung der Widerstände **155**, **1510** verworfen, und die Kalibrierung wird wiederholt. Diese Maßnahmen zum Sicherstellen einer erfolgreichen Kalibrierung, welche auch als Validierung der Kalibrierung bezeichnet werden können, die unter Bezugnahme auf die **Fig. 16** und **Fig. 18** erläutert wurden, sind auch auf andere Ausführungsbeispiele anwendbar, beispielsweise das Ausführungsbeispiel der **Fig. 17**.

[0082] Bei manchen Ausführungsbeispielen wird die oben erläuterte Kalibrierung nur in manchen Phasen einer Kommunikation ausgeführt. Beispielsweise gibt es bei einem CAN-Bus Phasen der Kommunikation wie eine Arbitrierungsphase zum Beginn der Kommunikation, welchem viele Sender in einem dominanten Zustand sein können. Eine Kalibrierung zu einem derartigen Zeitpunkt könnte das Ergebnis der Kalibrierung in manchen Fällen verfälschen. Daher wird bei manchen Ausführungsbeispielen eine Kalibrierung nur außerhalb einer solchen Arbitrierungsphase durchgeführt.

[0083] Bei manchen Ausführungsbeispielen kann die Kalibrierung durch ein separates Signal von einem Microcontroller oder einer anderen Steuerung aktiviert werden. Ein Beispiel hierfür ist in **Fig. 19** dargestellt. Das Ausführungsbeispiel der **Fig. 19** ist eine Abwandlung des Ausführungsbeispiels der **Fig. 4**, und gleiche Komponenten tragen die gleichen Bezugszeichen und werden nicht nochmals erläutert.

[0084] Zusätzlich zu den in **Fig. 4** dargestellten Komponenten kann die Microcontroller **40** durch einen Pfeil **190** dargestellt mit einem Signal calibration_en die Kalibrierung aktivieren und deaktivieren. So kann der Microcontroller **40** z.B. die Kalibrierung während der oben erwähnte Arbitrierungsphase deaktivieren.

[0085] Oben wurden verschiedene Möglichkeiten erläutert, wie bei variablem externen Widerstand wie dem Lastwiderstand **100** eine Kalibrierung erfolgen kann, um eine Referenzspannung Vref als Schwellenwert zu gewinnen.

[0086] Bei anderen Ausführungsbeispielen kann ein Unterschied zwischen Spannungspegeln für den Sicherheitscode so gewählt werden, dass in einem gesamten erlaubten Bereich von Lastwiderständen eine gleiche Referenzspannung verwendet werden kann, die dann nicht kalibriert werden muss. Dies kann als Kalibrierung des Treibers auf der Senderseite angesehen werden. Ein entsprechendes Ausführungsbeispiel ist in **Fig. 20** dargestellt.

[0087] Die **Fig. 20** zeigt wiederum den beschriebenen Teil der Sendeschaltung mit den Bezugszeichen **100-104**. Zudem wird eine Nachbildung bereitgestellt, bei der ein Widerstand **201** dem Widerstand **101**, eine Diode **202** der Diode **102**, ein Widerstand **200** dem Widerstand **100**, eine Diode **203** der Diode **103** und ein Widerstand **204** dem Widerstand **104** entspricht. Die Dioden **202** und **203** sind bezüglich der Dioden **102** und **103** um einen Skalierungsfaktor n skaliert, weisen z.B. eine n-mal kleinere Fläche auf. Der Widerstand **200** ist bezüglich eines mittleren Widerstandswertes des Lastwiderstands **100** mit dem Faktor n skaliert. Im Falle eines CAN-Busses kann der Widerstand **200** beispielsweise einen Widerstandswert von n*60 Ohm aufweisen. Die Widerstände **201** und **204** sind bezüglich eines mittleren Wertes der Widerstände **101**, **104** um den Skalierungsfaktor n skaliert. Wie bereits erläutert können die Widerstände **101**, **104** zur Erzeugung von zwei Pegeln zum Modulieren des Sicherheitscodes zwei verschiedene Werte annehmen, und die Widerstände **201**, **204** sind bezüglich eines dazwischenliegenden Wertes skaliert.

[0088] Um ein Zahlenbeispiel zu geben, können bei dem Ausführungsbeispiel der **Fig. 20** die Widerstände **101**, **104** entweder auf **10** Ohm für einen hohen Pegel oder auf **20** Ohm für einen niedrigen Pegel gesetzt werden, was einem Unterschied von näherungsweise 500 mV zwischen den Pegeln für die oben bereits verwendeten Zahlenbeispiele entspricht. Die Widerstände **201**, **204** können dann einen Wert von n*15 Ohm aufweisen, oder n * einem anderer Wert, des zwischen **10** Ohm und **20** Ohm liegt, beispielsweise n*14 Ohm. Der Spannungsabfall über dem Widerstand **200** wird dann als Referenzspannung zum Wiedergewinnen des Sicherheitscodes verwendet. Bei derartigen Ausführungsbeispielen ist keine Kalibrierung des Widerstandes **200** nötig. Bei manchen Ausführungsbeispielen ist jedoch der Flächenbedarf wegen des größeren Unterschiedes der beiden Werte der Widerstände **101**, **104** höher. Zudem kann der Unterschied zwischen den Pegeln je nach verwendetem Kommunikationsprotokoll nicht beliebig hoch gewählt werden, wenn die oben erläuterte Rückwärtskompatibilität, in dem die Pegel in spezifizierten Bereichen gehalten werden, erhalten werden soll.

[0089] Die **Fig. 20** zeigt Simulationsergebnisse für eine Schaltung wie unter Bezugnahme auf **Fig. 20** erläutert. Die **Fig. 20** zeigt insbesondere Spannungen Vdiff,high und Vdiff,low über der Temperatur in Grad Celsius für verschiedene Lastwiderstände Rload und eine konstante Versorgungsspannung VCC=5 Volt. Eine Kurve **210** zeigt Vdiff,high für Rload=75 Ohm, eine Kurve **211** zeigt Vdiff,high für Rload=50 Ohm, eine Kurve **213** zeigt Vdiff,low für Rload=75 Ohm und eine Kurve **214** zeigt Vdiff,low für Rload=50 Ohm. Eine Kurve **212** zeigt die Referenzspannung an dem Widerstand **200** der **Fig. 20** für einen Widerstandwert von n*60 Ohm. Wie zu sehen ist, kann für den gesamten Bereich von Rload von **50** Ohm bis **75** Ohm mittels der Referenzspannung **212** gemäß der Kurve **212** zwischen Vdiff,high und Vdiff,low unterschieden werden.

[0090] Somit ist auch ein Ausführungsbeispiel ohne die oben erläuterte Kalibrierung möglich, beispielsweise indem wie unter Bezugnahme auf **Fig. 20** erläutert die möglichen Widerstandwerte für die Widerstände **101**, **104** so gewählt werden, dass der Abstand zwischen Vdiff,high und Vdiff,low genügend groß ist.

[0091] Wie oben erläutert ist allgemein der Unterschied zwischen Vdiff,low und Vdiff,high relativ klein, beispielsweise ungefähr 200 mV oder ungefähr 500 mV in den obigen Beispielen. Dieses Signal kann durch elektromagnetische Störungen beeinflusst werden. Um elektromagnetische Verträglichkeit (EMV) zu verbessern, können bei manchen Ausführungsbeispielen Maßnahmen ergriffen werden, um die Auswirkungen von elektromagnetischen Störungen auf das Signal zumindest zu verringern. Dies wird nun unter Bezugnahme auf die **Fig. 22** und **Fig. 23** erläutert. Die **Fig. 22** und **Fig. 23** zeigen jeweils ein Ersatzschaltbild für eine Ausgangsstufe eines CAN-Busses mit Leitungen CANH, CANL unter dem Einfluss einer elektromagnetischen Störung.

[0092] Sowohl in **Fig. 22** als auch in **Fig. 23** ist mit dem Bezugszeichen **220** der Ausgangswiderstand (entsprechend dem Widerstand **100** in vorherigen Figuren), der etwa **60** Ohm beträgt, bezeichnet. Jede Leitung CANH, CANL ist mit einem Widerstand **221**, **222** dargestellt, welcher in dem dargestellten Beispiel etwa 120 Ohm beträgt. Zusätzlich ist eine Kapazität **223** bzw. **224** mit einem Kapazitätswert von 4,7 Nanofarrad bereitgestellt. Die Widerstände **221**, **222** und die Kapazitäten **223**, **224** repräsentieren ein Einkoppelnetzwerk, über welches Störungen in die Busleitungen CANH, CANL eingekoppelt werden.

[0093] Im Falle der **Fig. 22** und **Fig. 23** wird eine elektromagnetische Störung durch eine Störungsquelle **226**, mit Wechselspannungsquelle **228** und Widerstand **227** dargestellt, über das Einkoppelnetzwerk (**221**-**224**) in die Leitungen CANH, CANL eingekoppelt. Im Falle einer derartigen Störung wird Vdiff durch einen Kurzschlussstrom, welcher einem maximalen möglichen Stromfluss entspricht, bereitgestellt, da in diesem Fall eine Strombegrenzung auf der mit CANH gekoppelten Seite oder der mit CANL gekoppelten Seite eines Treibers auftritt. Dieser Treiber ist in **Fig. 22** durch eine Stromquelle **229** und im Falle der **Fig. 23** durch eine Stromquelle **230** repräsentiert. Bei großen Spannungen (z.B. durch Störungen) verhalten sich Treiber mit Strombegrenzung wie eine Stromquelle. Die Stromquellen **229** bzw. **230** repräsentieren somit auch den Kurzschlussstrom der im Falle der **Fig. 22** zu einer positiven Spannung, wie VCC, und im Falle der **Fig. 23** zu Masse fließt. Eine derartige Strombegrenzung kann beispielsweise durch einen maximalen Stromfluss eines durch einen oder mehrere Transistoren implementierten Schalters wie der Schalter **56**, **54**, **52** der **Fig. 5** auftreten.

[0094] In beiden Fällen fließt der Kurzschlussstrom in gleicher Weise über beide Leitungen CANH, CANL, wie durch Pfeile **2210**, **2211** in den **Fig. 22** und **Fig. 23** angedeutet.

[0095] Die sich ergebende Differenzspannung Vdiff ist in diesem Fall Vdiff=Rload*ishort/2, wobei ishort der Kurzschlussstrom ist.

[0096] Durch geeignete Wahl der Strombegrenzung dieses Kurzschlussstroms kann erreicht werden, dass auch bei elektromagnetischen Störungen die Spannung Vdiff im Wesentlichen unverändert bleibt. Insbesondere kann der Kurzschlussstrom ishort so eingestellt werden, dass er zweimal der im Normalzustand fließende Strom ist (d.h. im dominanten Zustand fließende Strom). Eine derartige Strombegrenzung kann in irgendeiner herkömmlichen Weise, beispielsweise mittels eine Stromspiegels erreicht werden.

[0097] Wie oben erläutert ist (im Falle ohne elektromagnetische Störungen) Vdiff=(VCC-2Ud)*Rload/(RH+RL +Rload).

[0098] Mit der oben erwähnten Bedingung, dass der Kurzschlussstrom ishort zweimal dem unter Normalbedingungen fließenden Strom ist, erhält man

$$\text{ishort} = 2 * (\text{VCC} - 2\text{Ud}) / (\text{RH} + \text{RL} + \text{Rload}).$$

[0099] Damit ist die Spannung Vdiff,en unter dem Einfluss einer elektromagnetischen Störung

$$Vdiff,en = Rload*ishort / 2 = Rload*(VCC - 2Ud)(RH + RL + Rload)$$

und somit gleich dem obigen Wert von Vdiff ohne den Einfluss elektromagnetischer Störungen. Somit kann durch die oben beschriebene Begrenzung des Kurzschlussstromes der Einfluss von elektromagnetischen Störungen auf die Differenzspannungen Vdiff bei manchen Ausführungsbeispielen zumindest verringert, wenn nicht beseitigt werden. Dabei kann der Strombegrenzungswert ishort entsprechend der Änderung von RH und RL für die verschiedenen Pegel des zweiten Signals jeweils geändert werden. Es kann bei anderen Ausführungsbeispielen auch ein Mittelwert für ishort für die verschiedenen Werte von RH, RL gebildet werden.

[0100] Oben wurden viele Ausführungsbeispiele diskutiert, bei welchen ein erstes Signal mit einem kryptographischen Datum auf einer physikalischen Ebene auf ein Signal moduliert wird. Zusätzlich zu diesem Sicherheitscode kann auch eine Codierung in einer Logikprotokollschicht erfolgen, d.h. die zu sendende Information wird auf Basis eines (geheimen) Schlüssels verschlüsselt, welcher mit einem Schlüssel, der zur Erzeugung des kryptographischen Datums dient, identisch sein kann oder von diesem verschieden sein kann. Wie im Folgenden erläutert kann hierdurch eine Redundanz mit gleichzeitiger Diversität (verschiedene Sicherheitsverfahren, Verschlüsselung auf der Logikprotokollschicht und Überlagern mit dem zweiten Signal mit dem kryptographischen Datum) bereitgestellt werden. Eine derartige Verschlüsselung mittels Schlüsseln kann in verschiedenen Ausprägungen in herkömmlicher Weise implementiert werden.

[0101] Die **Fig. 24** zeigt eine entsprechende Kommunikationsschaltungsanordnung gemäß einem Ausführungsbeispiel mit einer ersten Kommunikationsschaltung **241**, die als Transmitter dient, und einer zweiten Kommunikationsschaltung **242**, die als Receiver dient. Das Ausführungsbeispiel der **Fig. 24** beruht dabei auf dem Ausführungsbeispiel der **Fig. 1**, und einander entsprechende Elemente tragen die gleichen Bezugszeichen. Insbesondere erfolgt die Modulation eines zweiten Signals mit kryptographischem Datum auf physikalischer Ebene, wie unter Bezugnahme auf die **Fig. 1** beschrieben, wobei hier sämtliche unter Bezugnahme auf die **Fig. 1-23** beschriebenen Varianten und Implementierungsmöglichkeiten anwendbar sind.

[0102] Daher werden im Folgenden nur die Unterschiede zwischen der Kommunikationsschaltungsanordnung **240** und der Kommunikationsschaltungsanordnung **10** der **Fig. 1** erläutert.

[0103] In der Kommunikationsschaltung **241** wird eine zu sendende Information einer Signalerzeugungs- und Codierungsschaltung **245** zugeführt. Die Signalerzeugungs- und Codierungsschaltung verschlüsselt die Information basierend auf einem Schlüssel auf einer Logikprotokollschicht, die gemäß einem Logikprotokoll arbeitet. Auf Basis der so verschlüsselten Information wird dann ein Sendesignal erzeugt, wie für die Erzeugung eines Signals durch die Signalerzeugungsschaltung **15** der **Fig. 1** beschrieben, mit dem Unterschied, dass nunmehr die verschlüsselte Information als Grundlage dient. Auf dieses Signal wird dann in der Modulationsschaltung **16** wie beschrieben das zweite Signal mit dem kryptographischen Datum **14** aufmoduliert und das Signal wird über das Kommunikationsmedium **13** übertragen.

[0104] In der Kommunikationsschaltung **242** wird zum einen durch die bereits beschrieben Codeempfangsschaltung **18** der in der Modulationsschaltung **16** aufmodulierte Sicherheitscode wiedergewonnen. Zum anderen wird in einer Signalempfangs- und Decodierungsschaltung **247** zum einen die verschlüsselte Information aus dem empfangenen Signal wiedergewonnen und dann die verschlüsselte Information in einer Logikprotokollschicht entschlüsselt. Hierzu liegt der Signalempfangs- und Decodierungsschaltung der zum Verschlüsseln verwendete Schlüssel oder ein entsprechend hierzu passender Entschlüsselungsschlüssel vor.

[0105] Diese Verschlüsselung und Entschlüsselung kann in jeder herkömmlichen Weise erfolgen.

[0106] Entspricht das durch die Codeempfangsschaltung **18** gewonnene kryptographische Datum nicht dem erwarteten Sicherheitscode, können wie beschrieben Maßnahmen ergriffen werden. Diese Maßnahmen können den bereits beschriebenen Maßnahmen entsprechen. Zudem kann, wenn die Entschlüsselung in der Signalempfangs- und Decodierungsschaltung **247** korrekt verlief, auch lediglich eine Warnung ausgegeben werden, oder es kann keine Maßnahme ergriffen werden, wenn die Authentifizierung durch die erfolgreiche Entschlüsselung allein auf der Logikprotokollschicht akzeptabel ist. Es wird also auf diese Weise eine Redundanz mit zwei verschiedenen Sicherheitsmechanismen (Verschlüsselung auf der Logikprotokollschicht und Modulierung eines zweiten Signals mit kryptographischem Datum auf der physikalischen Schicht) mit gleichzeitiger Diversität (zwei verschiedene Maßnahmen) bereitgestellt.

[0107] In der **Fig. 25** ist ein entsprechendes Verfahren gemäß mancher Ausführungsbeispiele dargestellt. Das Verfahren der **Fig. 25** kann in der Kommunikationsschaltungsanordnung **240** der **Fig. 24** implementiert werden und wird zur Vermeidung von Wiederholungen unter Bezugnahme auf diese beschrieben, und kann jedoch auch unabhängig von der Kommunikationsschaltungsanordnung **240** verwendet werden.

[0108] Wie bereits für das Verfahren der **Fig. 2** ausgeführt müssen die Verfahrensschritte der **Fig. 25** nicht notwendigerweise in der dargestellten Reihenfolge durchgeführt werden, und es können insbesondere verschiedene Vorgänge auch gleichzeitig durchgeführt werden.

[0109] Bei **250** wird eine Information verschlüsselt, beispielsweise auf Basis eines Schlüssels, wie für die Signalerzeugungs- und Codierungsschaltung **215** beschrieben. Bei **251** wir die verschlüsselte Information in ein erstes Signal umgesetzt, insbesondere basierend auf einem physikalischen Kommunikationsprotokoll, wie dem diskutierten CAN-Protokoll oder einem anderen Kommunikationsprotokoll.

[0110] Bei **252** wird das erste Signal durch ein zweites Signal mit einem kryptographischen Datum überlagert. Das kryptographische Datum kann ein von einem gleichen Schlüssel, der zum Verschlüsseln bei **250** verwendet wurde, abgeleitetes Datum oder auch ein anderes kryptographisches Datum sein.

[0111] Das so erzeugte Überlagerungssignal wird an einen Empfänger gesendet, und bei **253** wird die verschlüsselte Information aus dem Sendesginal wiedergewonnen. Bei **254** wird die verschlüsselte Information dann entschlüsselt. Bei **255** wird zudem das kryptographische Datum aus dem Überlagerungssignal wiedergewonnen. Je nachdem, ob das Entschlüsseln bei **254** und/oder das kryptographische Datum, das bei **255** gewonnen wurde, mit einem erwarteten kryptographischen Datum übereinstimmt, kann die Information als authentifiziert, d.h. von einem autorisierten Empfänger gesendet, angesehen werden, wie dies ebenfalls bereits beschrieben wurde.

[0112] Die beschriebenen Funktionalitäten können auf verschiedene Weise implementiert werden. Insbesondere können manche der Funktionalitäten, beispielsweise das Bereitstellen des Sicherheitscodes angepasst an die zu sendenden Daten, in einem Microcontroller bereitgestellt werden, wie für den Microcontroller **40** der **Fig. 19** beschrieben, der dann entsprechende Informationen an einen CAN-Transceiver wie den CAN-Transceiver **41** der **Fig. 19** gibt und von diesem empfängt. Details solcher Implementierungsmöglichkeiten werden nunmehr unter Bezugnahme auf die **Fig. 26-36** erläutert.

[0113] Die **Fig. 26** zeigt ein Blockdiagramm eines Microcontrollers **260** gemäß eines Ausführungsbeispiels.

[0114] Der Microcontroller **260** kann beispielsweise eine Steuereinheit (MCU, microcontrol unit) eines Fahrzeugs sein, beispielsweise eine Motorsteuerung, Getriebesteuerung oder andere Steuereinheit. In einem Fahrzeug sind häufig eine Vielzahl derartiger Steuereinheiten verbaut.

[0115] Neben den im Folgenden explizit dargestellten Funktionen des Microcontrollers **260** und auch nachfolgend beschriebener Microcontroller können weitere herkömmliche Funktionen in dem Microcontroller **260** implementiert sein.

[0116] Der Microcontroller **260** weist ein Hardwaresicherheitsmodul (MSM) **261** auf, in welchem Schlüssel (keys) gespeichert sind, die als kryptographisches Datum bei den oben beschriebenen Verfahren und Vorrichtungen dienen können, bzw. aus denen ein derartiges kryptographisches Datum, z.B. der beschriebene Sicherheitscode, erzeugbar ist. Das Hardwaresicherheitsmodul **261** ist durch zusätzliche, für sich genommen bekannte Maßnahmen vor Zugriff und Störungen wie Störungen durch Partikel, elektromagnetische Strahlung und dgl. geschützt. Es ist auch gegen Angriffe und Zugriffe besser als der Rest des Microcontrollers **260** geschützt. Software des Hardwaresicherheitsmoduls **261** kann z.B. in gesonderten Speicherbereichen laufen, und Algorithmen können seitenkanalresistent sein.

[0117] Der Microcontroller **260** enthält zudem ein oder mehrere als SPAD (safe physical anomaly detection) bezeichnete Schaltungsteile **263A-263D**, welche die beschriebenen Techniken implementieren. Insbesondere kann jede SPAD **263A-263D** (im Folgenden zusammenfassend als SPAD **263** bezeichnet) einen aufzumodulierenden Sicherheitscode für einen Transceiver wie einen CAN-Transceiver bereitstellen, wie dies unter Bezugnahme auf die **Fig. 4** erläutert worden ist. Die Anzahl von vier SPADs **263** in **Fig. 26** dient dabei lediglich als Beispiel, und es kann jede benötigte Anzahl von SPADs gewählt werden.

[0118] Die SPADs **263** empfangen Steuer- und Dateninformationen über einen internen Bus **262** des Microcontrollers. Beispielsweise können so die zu sendenden Daten und Informationen hinsichtlich einer Position von Sende- und Empfangsbits wie unter Bezugnahme auf die **Fig. 3** erläutert bereitgestellt werden. Zusätzlich erhalten die SPADs **263** Schlüssel von dem Hardwaresicherheitsmodul **261**. Dies kann entweder auch über den Steuer- und Datenbus **262** oder auch über eine separate Verbindung wie durch gestrichelte Linien angezeigt erfolgen. Diese Schlüssel können dann als kryptographisches Datum bei den oben beschriebenen Techniken verwendet werden, oder es kann aus den Schlüsseln gemäß einem vorgegebenen Algorithmus ein kryptographisches Datum, wie der diskutierte Sicherheitscode, erzeugt werden.

[0119] Die SPADs können jeweils Kommunikationsschnittstellen zugeordnet sein. Dies ist schematisch in der **Fig. 27** dargestellt. Hier umfasst ein Microcontroller **270** SPADs **273A**-274D und das Hardwaresicherheitsmodul **261** der **Fig. 27**. Die SPADs **273A-273D** werden im Folgenden zusammenfassend als SPADs **273** bezeichnet, wobei die Anzahl von vier SPADs **273** wiederum nur als nicht einschränkendes Beispiel zu verstehen ist. Jeder der SPADs **273** ist einer jeweiligen Kommunikationsschnittstelle **274A**, **274B**, **274C** bzw. **274C** (zusammenfassend als Kommunikationsschnittstellen **274** bezeichnet) zugeordnet. Die Kommunikationsschnittstellen **274** können beispielsweise mit CAN-Transceivern wie beschrieben oder mit Transceivern für andere Arten von Bussen gekoppelt werden, sind jedoch nicht hierauf beschränkt.

[0120] Bei dem Ausführungsbeispiel der **Fig. 27** ist jedes SPAD **273** einer jeweiligen Kommunikationsschnittstelle **274** zugeordnet. Bei anderen Ausführungsbeispielen kann ein SPAD mehreren Kommunikationsschnittstellen zugeordnet sein. Ein entsprechendes Ausführungsbeispiel ist als Microcontroller **280** in **Fig. 28** dargestellt. Die **Fig. 28** zeigt einen Microcontroller **280** mit dem bereits beschriebenen Hardwaresicherheitsmodul **261** und dem internen Bus **262**. Mit dem Bus sind Kommunikationsschnittstellen **262A**-**262C**, zusammenfassend als Kommunikationsschnittstellen **282** bezeichnet, angeordnet. Die Kommunikationsschnittstellen **282** können als Submodule einer einzigen Kommunikationsschnittstelle gesehen sein, die einem einzigen SPAD **281** zugeordnet ist. Der SPAD **281** führt die beschriebenen Techniken für alle Kommunikationsschnittstellen **282A-282C** aus. Die Anzahl von drei dargestellten Kommunikationsschnittstellen **282** in **Fig. 28** ist dabei wiederum lediglich ein Beispiel. Somit zeigen die **Fig. 27** und **Fig. 28**, dass SPADs auf verschiedene Weise Kommunikationsschnittstellen zugeordnet sein können. Auch Mischformen zwischen **Fig. 27** und **Fig. 28** sind möglich, bei denen manche SPAD mehreren Kommunikationsschnittstellen zugeordnet sind und andere SPADs nur einer einzigen Kommunikationsschnittstelle zugeordnet sind.

[0121] Die **Fig. 29** zeigt ein Blockdiagramm eines SPADs **290**, wie er beispielsweise als SPAD in den **Fig. 26**, **Fig. 27** und **Fig. 28** verwendbar ist.

[0122] Der SPAD **290** umfasst ein Modul **291** zum Schlüsselaustausch mit einem Hardwaresicherheitsmodul wie dem beschriebenen Hardwaresicherheitsmodul **261** der **Fig. 26-28**. Basierend auf einem empfangenen Schlüssel stellt ein Modul **293** einen Sicherheitscode zum Modulieren auf ein Signal auf einer physikalischen Ebene bereit, wie beschrieben. Ein Modul **294** empfängt einen aus einem empfangenen Signal gewonnenen Sicherheitscode und führt in einem Modul **292** eine Authentifizierung auf Basis eines empfangenen Schlüssels, welcher einen erwarteten Sicherheitscode angibt, wie beschrieben aus. Die Authentifizierung bei **292** kann dabei redundant erfolgen. Beispielsweise kann zudem wie beschrieben eine Codierung der gesendeten Informationen auf einer Logikprotokollschicht, oder die Überprüfung des empfangenen Sicherheitscodes kann redundant in mehreren Schaltungsteilen durchgeführt werden. Je nach Erfolg der Authentifizierung kann dann ein Signal ausgegeben werden, welches eine erfolgreiche oder eine fehlgeschlagene Authentifizierung anzeigt, und bei einer fehlgeschlagenen Authentifizierung können Maßnahmen wie beschrieben ergriffen werden.

[0123] Wie bereits oben erläutert können in einer Vorrichtung wie einem Fahrzeug eine Vielzahl von Microcontrollern angeordnet sein. Bei manchen Ausführungsbeispielen können Informationen über erfolgreiche oder fehlgeschlagene Authentifizierungen von mehreren Microcontrollern gesammelt werden, und basierend auf dieser Sammlung können dann Maßnahmen ergriffen werden. Dies ist in **Fig. 30** schematisch dargestellt.

[0124] **Fig. 30** zeigt eine Vielzahl von Microcontrollern **300A**, **300B**, **300C** (die Anzahl von drei Microcontrollern ist wiederum nur als Beispiel zu verstehen), welche jeweils eine SPAD wie oben beschrieben zur Authentifizierung beinhalten und welche mit einem Kommunikationsmedium, beispielsweise einem gemeinsamen Bus, verbunden sind. Jede der Microcontroller **300** führt Authentifizierungsmessungen (z.B. die beschriebenen Überprüfungen eines empfangenen kryptographischen Datums) auf dem Bus durch und meldet Informationen über die Authentifizierungen (beispielsweise über fehlgeschlagene Authentifizierungen) an eine Aggregationseinheit **301**. Die Aggregationseinheit **301** wertet die empfangenen Informationen aus und verursacht weitere Maßnahmen. Beispielsweise kann, wenn nur eine MCU ein Signal nicht authentifizieren kann, bei manchen

Ausführungsbeispielen noch keine Maßnahme ergriffen werden, da dies beispielsweise auch auf einem Übertragungsfehler beruhen könnte. Empfangen mehrere Microcontroller nicht authentifizierbare Nachrichten, kann dies beispielsweise als Eindringversuch gewertet werden, und wie beschrieben eine Maßnahme ergriffen werden. Dies stellt ebenso eine Redundanz bei der Detektion von unerlaubt angekoppelten Kommunikationsvorrichtungen bereit und kann somit dazu beitragen, Sicherheitserfordernisse zu erfüllen.

[0125] Eine SPAD kann Signale von einem Übertragungsmedium wie dem Übertragungsmedium **13** der **Fig. 1** auf verschiedene Weise empfangen. Dies wird nunmehr unter Bezugnahme auf die **Fig. 31**-**Fig. 35** näher erläutert.

[0126] In der **Fig. 31** sind ein SPAD **312** und eine zugehörige Kommunikationsschnittstelle **311** in einem Microcontroller **310** angeordnet. Weitere Elemente wie bereits oben beschrieben können in dem Microcontroller vorhanden sein, insbesondere ein Hardwaresicherheitsmodul und weitere Kommunikationsschnittstellen und/oder weitere SPADs. Die Kommunikationsschnittstelle **311** ist mit einem Transceiver **313**, welcher eine physikalische Schicht einer Kommunikation implementiert, verbunden, beispielsweise mit einem CAN-Transceiver wie beschrieben. Der Transceiver **313** kommuniziert dann über ein physikalisches Medium **315**, beispielsweise einen CAN-Bus.

[0127] Bei der Anordnung der **Fig. 31** erhält die SPAD **312** direkt Signale von dem physikalischen Medium **315** über eine dazwischen geschaltete Schutzschaltung **314**, beispielsweise um den Sicherheitscode wiederzugewinnen. Die Schutzschaltung **314** kann übliche Schutzelemente wie Schutzelemente vor elektrostatischen Entladungen (ESD-Schutzelemente, vom Englischen „electrostatic discharge“), Überstromschutzelemente oder Überspannungsschutzelemente umfassen. Das Ausführungsbeispiel der **Fig. 31** kann einen herkömmlichen Transceiver nutzen, benötigt aber eine zusätzliche Schutzschaltung **314**.

[0128] Eine andere Anordnung ist in der **Fig. 32** gezeigt. Hier ist wiederum eine Kommunikationsschnittstelle **321** und eine SPAD **322** in einem Microcontroller **322** angeordnet. Die Kommunikationsschnittstelle **321** kommuniziert mit einem Transceiver **322**, der im Falle der **Fig. 32** etwas detaillierter mit einer Treiberschaltung **327**, einem Sender **326**, einem Empfänger **325** und einer Schutzschaltung **324** dargestellt ist. Im Gegensatz zur **Fig. 31** benutzt die SPAD hier die Schutzschaltung **324** des Transceivers **323** mit, d.h. sie erhält von der Schutzschaltung **324** gefilterte Signale. Das Ausführungsbeispiel der **Fig. 32** benötigt keine zusätzliche Schutzschaltung, benötigt aber einen entsprechend ausgestalteten Transceiver **323**, der von der Schutzschaltung **324** das Signal direkt zur SPAD gibt.

[0129] Eine weitere Anordnung ist in **Fig. 33** dargestellt. Ein Microcontroller **330** enthält eine Kommunikationsschnittstelle **331** und eine SPAD **332**. Die Kommunikationsschnittstelle **331** ist mit einem Transceiver **334** verbunden, welcher wie der Transceiver der **Fig. 32** eine Treiberschaltung **335**, einen Sender **336**, einen Empfänger **337** und eine Schutzschaltung **338** enthält. Von der Schutzschaltung **338** werden Signale einer Messschaltung **339** zugeführt, welche beispielsweise den Sicherheitscode wiedergewinnen kann und den wiedergewonnenen Sicherheitscode über eine Schnittstelle **3310** zu einer entsprechenden Schnittstelle **333** in dem Microcontroller **330** und von dort zur SPAD **332** sendet. Hier erfolgt die Wiedergewinnung also - wie auch beispielsweise in **Fig. 4** gezeigt - in dem Transceiver.

[0130] Das Ausführungsbeispiel der **Fig. 33** benötigt einen komplexeren Transceiver **334** mit der Messschaltung **339**, ermöglicht jedoch auf der anderen Seite präzisere Messungen.

[0131] Bei einem anderen Ausführungsbeispiel, welches in **Fig. 34** gezeigt ist, kann eine Messeinheit **349** entsprechend der Messeinheit **339** außerhalb eines Transceivers **344** und außerhalb eines Microcontrollers **340** zusammen mit einer Schnittstelle **3410** angeordnet sein, beispielsweise in einem eigenen Baustein, um direkt an dem Medium **315** Messungen durchzuführen. Der Transceiver **344** enthält eine Treiberschaltung **345**, einen Sender **346**, einen Empfänger **347** und eine Schutzschaltung **348**. Der Microcontroller **340** enthält eine SPAD **342**, eine Kommunikationsschnittstelle **341** und eine Schnittstelle **343**. Hier ist dann noch eine zusätzliche Einheit mit der Messeinheit **349** und der Schnittstelle **3410** nötig, welche ggf. eine eigene Schutzschaltung benötigt. Ansonsten ist die Funktionsweise wie bei dem Ausführungsbeispiel der **Fig. 33**.

[0132] Die **Fig. 31-34** zeigen also, dass verschiedene Aufteilungen und Implementierungen der diskutierten Funktionalitäten möglich sind.

[0133] Die Funktionalitäten einer SPAD können auch zentral in einem geschalteten Netzwerk bereitgestellt werden. Die **Fig. 35** zeigt ein derartiges Netzwerk mit einem Switch **352**, welcher verschiedene Kommunika-

tionsteilnehmer, im Beispiel der **Fig. 35** einen ersten Microcontroller **350** mit einem ersten Transceiver **351**, einen zweiten Microcontroller **3511** mit einem zweiten Transceiver **359** und einen dritten Microcontroller **3512** mit einem dritten Transceiver **3510** wahlweise miteinander verbindet. Hierfür weist der Switch **352** Transceiver **353**, **358** und **357** auf, um wie dargestellt mit den Transceivern **351**, **359** und **3510** zu kommunizieren. Des Weiteren verfügt der Switch **352** über eine Prozessoreinheit **355** mit einer SPAD **356**, womit die von den Microcontrollern **350**, **3511**, **3512** über die jeweiligen Transceiver **351**, **359**, **3510** gesendeten Signale authentifiziert werden müssen. In diesem Fall muss also nicht jeder Microcontroller über eine SPAD verfügen, sondern die Authentifizierung (Überprüfung des aufmodulierten kryptographischen Datums und/oder einer zusätzlichen Verschlüsselung auf Logikprotokollschicht) kann zentral im Switch überprüft werden.

[0134] Auch bei einem Transceiver, der mehrere Kanäle bedient, beispielsweise mehrere Kanäle auf einem oder mehreren CAN-Bussen, kann die Bereitstellung und Überprüfung eines Sicherheitscodes für alle Kanäle in einer Einheit erfolgen. Ein Beispiel ist in **Fig. 36** schematisch dargestellt.

[0135] Bei dem Ausführungsbeispiel der **Fig. 36** stellen Sende/Empfangsknoten **361A**, **361B**, **361C** ein Sendesignal **TX** für einen jeweiligen zugeordneten CAN-Bus **362A**, **362B** oder **362C** bereit und empfangen ein entsprechendes empfangenes Signal RX. Diesbezüglich entspricht die Funktion der CAN-Knoten **361A**, **361B**, **361C** den Elementen **33**, **34**, **39** und **38** der **Fig. 3**.

[0136] Das Bereitstellen eines Sicherheitscodes wird in zeitmultiplexter Art und Weise auf Basis einer Zeitsteuerung durch einen Zeitmultiplexer bereitgestellt, welcher wie durch einen Pfeil **356** angedeutet den Sicherheitscode für einen Mehrkanaltransceiver **364** bereitstellt und steuert, welcher CAN-Bus **362A**, **362B**, **362C** jeweils bedient wird. Die Knoten **361A**, **361B**, **361D** liefern dabei wie ebenfalls unter Bezugnahme auf **Fig. 3** beschrieben Daten und die Bitpositionen an den Zeitmultiplexer **360**, sodass dieser einen geeigneten Sicherheitscode zum Modulieren auf dominante Bits des jeweiligen CAN-Busses erstellen kann. Der Transceiver **364** moduliert dann den Sicherheitscode grundsätzlich wie bereits beschrieben auf die Signale auf dem jeweiligen CAN-Bus, mit dem Unterschied, dass es in einem Zeitmultiplexverfahren alternierend für die CAN-Busse geschieht. Auf diese Weise können bei manchen Ausführungsbeispielen eine Implementierung für mehrere CAN-Busse mit vergleichsweise wenig Komponenten realisiert werden.

[0137] Wie somit aus den vorstehend beschriebenen Figuren ersichtlich gibt es eine Vielzahl verschiedener Möglichkeiten, die beschriebenen Techniken zu implementieren. Somit ist die Anwendung der beschriebenen Techniken nicht auf eine spezifische Art der Implementierung beschränkt.

[0138] Die folgenden Beispiele definieren wenigstens einige der Ausführungsbeispiele.

[0139] Beispiel 1. Transceiver aufweisend:

einen Transmitter, der dazu ausgebildet ist,

- an einem Ausgang ein erstes Signal gemäß eines physikalischen Kommunikationsprotokolls bereitzustellen, und

- an dem Ausgang ein zweites Signal bereitzustellen, das mindestens ein kryptographisches Datum umfasst, wobei das erste und das zweite Signal als ein Überlagerungssignal an dem Ausgang einander überlagert sind, und wobei das Überlagerungssignal das physikalische Kommunikationsprotokoll erfüllt.

[0140] Beispiel 2. Transceiver nach Beispiel 1,
wobei das zweite Signal ein pulsförmiges Signal oder ein wechselstromförmiges Signal ist.

[0141] Beispiel 3. Transceiver nach einem der Beispiele 1 bis 2, wobei das zweite Signal dem ersten Signal nur auf einem von mindestens zwei Pegeln des ersten Signals gemäß des physikalischen Kommunikationsprotokolls überlagert wird.

[0142] Beispiel 4. Transceiver nach einem der Beispiele 1 bis 3, wobei das zweite Signal überlagert wird, wenn für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgte oder für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgen wird.

[0143] Beispiel 5. Transceiver nach einem der Beispiele 1 bis 4, wobei eine Logikprotokollschicht, die dem physikalischen Kommunikationsprotokoll übergeordnet ist, ein Logiksignal bereitstellt, und das Logiksignal zur Erzeugung des ersten Signals verwendet wird.

[0144] Beispiel 6. Transceiver nach Beispiel 5, wobei die Logikprotokollschicht ausgebildet ist, zu sendende Daten zu verschlüsseln, um das Logiksignal bereitzustellen.

[0145] Beispiel 7. Transceiver nach einem der vorhergehenden Beispiele, wobei das kryptographische Datum ein Sicherheitscode des Transceivers ist.

[0146] Beispiel 8. Transceiver nach einem der vorhergehenden Beispiele, wobei dem Transceiver ein Schlüssel zum Erzeugen des kryptographischen Datums, bereitgestellt wird.

[0147] Beispiel 9. Transceiver nach Beispiel 8, wobei der Schlüssel durch eine dem Transceiver übergeordnete Schlüsselinstanz bereitgestellt wird.

[0148] Beispiel 10. Transceiver nach einem der vorhergehenden Beispiele, wobei der Transmitter eine Treiberschaltung umfasst, die eingerichtet ist, das Überlagerungssignal bereitzustellen, und wobei der Transmitter eingerichtet ist, die Treiberschaltung zu kalibrieren.

[0149] Beispiel 11. Transceiver nach Beispiel 10, wobei die Treiberschaltung eine erste Reihenschaltung aus einem ersten Schalter und einem ersten Widerstand umfasst, die zwischen eine Versorgungsspannung und dem Ausgang gekoppelt ist, wobei der erste Schalter in Abhängigkeit von dem ersten Signal ansteuerbar ist, und die Treiberschaltung eine zweite Reihenschaltung aus einem zweiten Schalter und einen zweiten Widerstand aufweist, die zwischen die Versorgungsspannung und dem Ausgang gekoppelt ist, wobei der zweite Schalter in Abhängigkeit von dem kryptographischen Datum ansteuerbar ist.

[0150] Beispiel 12. Transceiver aufweisend:

einen Receiver, der dazu ausgebildet ist,

- ein Empfangssignal, welches eine Überlagerung eines ersten Signals gemäß einem physikalischen Kommunikationsprotokoll mit einem zweiten Signal, das ein kryptographisches Datum umfasst, ist, zu empfangen,

- das Empfangssignal gemäß dem physikalischen Kommunikationsprotokoll zu verarbeiten, um in dem ersten Signal übertragene Informationen zu gewinnen, und

- aus dem Empfangssignal das kryptographische Datum zu gewinnen.

[0151] Beispiel 13. Transceiver nach Beispiel 12, wobei das zweite Signal ein pulsförmiges Signal oder ein wechselstromförmiges Signal ist.

[0152] Beispiel 14. Transceiver nach einem der Beispiele 12 oder 13,
wobei der Receiver ausgebildet ist, das kryptographische Datum aus der Überlagerung des zweiten Signals über dem ersten Signal nur auf einem von mindestens zwei Pegeln des ersten Signals gemäß des physikalischen Kommunikationsprotokolls zu gewinnen.

[0153] Beispiel 15. Transceiver nach einem der Beispiele 1 bis 3, wobei der Receiver ausgebildet ist, das kryptographische Datum aus der Überlagerung des zweiten Signal über dem ersten Signal zu gewinnen, wenn für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgte oder für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgen wird.

[0154] Beispiel 16. Transceiver nach einem der Beispiele 12 bis 15, wobei die aus dem ersten Signal gewonnenen Informationen einer Logikprotokollschicht, die dem physikalischen Kommunikationsprotokoll übergeordnet ist, als Logiksignal bereitstellt wird.

[0155] Beispiel 17. Transceiver nach Beispiel 16, wobei die Logikprotokollschicht ausgebildet ist, aus dem Logiksignal durch Entschlüsselung gesendete Daten zu gewinnen.

[0156] Beispiel 18. Transceiver nach einem der vorhergehenden Beispiele, wobei das kryptographische Datum ein Sicherheitscode eines weiteren Transceivers ist, von dem das Empfangssignal empfangen wird, und wobei der Transceiver eingerichtet ist, das kryptographische Datum mit einem erwarteten kryptographischen Datum zu vergleichen, um den weiteren Transceiver zu authentifizieren.

[0157] Beispiel 19. Transceiver nach Beispiel 18, wobei dem Transceiver ein Schlüssel zum Erzeugen des erwarteten kryptographischen Datums bereitgestellt wird.

[0158] Beispiel 20. Transceiver nach Beispiel 19, wobei der Schlüssel durch eine dem Transceiver übergeordnete Schlüsselinstanz bereitgestellt wird.

[0159] Beispiel 21. Transceiver nach einem der Beispiele 12-20, wobei der Receiver eine Empfangsschaltung umfasst, die eingerichtet ist, das kryptographische Datum zu gewinnen, und wobei der Receiver eingerichtet ist, die Empfangsschaltung zu kalibrieren.

[0160] Beispiel 22. Transceiver nach Beispiel 21, wobei das Kalibrieren ein Bestimmen einer Referenzspannung zum Gewinnen des kryptographischen Datums umfasst.

[0161] Beispiel 23. Transceiver nach Beispiel 22, wobei die Kommunikationsschaltung eine Kalibrierungsschaltung umfasst, die eingerichtet ist, die Referenzspannung in Abhängigkeit von einer Versorgungsspannung und/oder einer Temperatur zu bestimmen.

[0162] Beispiel 24. Transceiver nach Beispiel 23, wobei die Kalibrierungsschaltung eine skalierte Nachbildung zumindest eines Teils eines Sendepfades zum Senden des Empfangssignals umfasst, wobei die Kalibrierungsschaltung eingerichtet ist, die Referenzspannung auf Basis eines Spannungsabfalls über einem Teil der Nachbildung zu bestimmen.

[0163] Beispiel 25. Transceiver nach Beispiel 24, wobei der Teil der Nachbildung einen Widerstand umfasst, der einen mit mindestens einer Übertragungsleitung, über die das Empfangssignal empfangbar ist, gekoppelten Widerstand nachbildet.

[0164] Beispiel 26. Transceiver nach Beispiel 24 oder 25, wobei der Teil der Nachbildung einstellbar ist, wobei die Kalibrierungsschaltung eingerichtet ist, den Teil der Nachbildung zur Anpassung an einen entsprechenden Teil des Sendepfades einzustellen.

[0165] Beispiel 27. Transceiver nach Beispiel 26, wobei die Kalibrierungsschaltung eingerichtet ist, den Teil der Nachbildung auf Basis von Variationen der mindestens zwei Signalpegel während einer Kalibrierungsphase einzustellen.

[0166] Beispiel 28. Transceiver nach Beispiel 26 oder 28, wobei die Kalibrierungsschaltung eingerichtet ist, die Einstellung des Teils der Nachbildung zu validieren.

[0167] Beispiel 29. Transceiver nach einem der Beispiele 12-28, wobei der Receiver eingerichtet ist, nur das Empfangssignal gemäß dem physikalischen Kommunikationsprotokoll zu verarbeiten, um in dem ersten Signal übertragene Informationen zu gewinnen, wenn das Empfangssignal kein zweites Signal enthält und/oder das kryptographische Datum nicht aus dem Empfangssignal gewinnbar ist.

[0168] Beispiel 30. System, umfassend:

einen ersten Transceiver nach einem der Beispiele 1-11, und

einen mit dem ersten Transceiver über ein Kommunikationsmedium gekoppelten zweiten Transceiver nach einem der Beispiele 12-29.

[0169] Beispiel 31. System nach Beispiel 30, wobei der erste Transceiver und/oder der zweite Transceiver ein Teil einer Steuereinheit eines Fahrzeugs ist.

[0170] Beispiel 32. Signal, umfassend eine Überlagerung aus:

- einem erstes Signal gemäß eines physikalischen Kommunikationsprotokolls, und

-einem zweites Signal, das mindestens ein kryptographisches Datum umfasst,

wobei das Signal das physikalische Kommunikationsprotokoll erfüllt.

[0171] Beispiel 33. Signal nach Beispiel 32,
wobei das zweite Signal ein pulsförmiges Signal oder ein wechselstromförmiges Signal ist.

[0172] Beispiel 34. Signal nach einem der Beispiele 32 oder 33, wobei das zweite Signal dem ersten Signal nur auf einem von mindestens zwei Pegeln des ersten Signals gemäß des physikalischen Kommunikationsprotokolls überlagert ist.

[0173] Beispiel 35. Signal nach einem der Beispiele 32 und 33, wobei das zweite Signal dem ersten Signal überlagert ist, wenn für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgte oder für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgen wird.

[0174] Beispiel 36. Signal nach einem der Beispiel 32 bis 35, wobei das erste Signal logisch verschlüsselte Daten umfasst.

[0175] Obgleich in dieser Beschreibung spezifische Ausführungsbeispiele illustriert und beschrieben wurden, werden Personen mit üblichem Fachwissen erkennen, dass eine Vielzahl von alternativen und/oder äquivalenten Implementierung als Substitution für die spezifischen Ausführungsbeispiele, die in dieser Beschreibung gezeigt und beschrieben sind, ohne von dem Umfang der gezeigten Erfindung abzuweichen, gewählt werden können. Es ist die Intention, dass diese Anmeldung alle Adaptionen oder Variationen der spezifischen Ausführungsbeispiele, die hier diskutiert werden, abdeckt. Daher ist es beabsichtigt, dass diese Erfindung nur durch die Ansprüche und die Äquivalente der Ansprüche beschränkt ist.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Nicht-Patentliteratur

- ISO 11898 [0003]
- ISO 17458-1 [0003]
- ISO 17458-4 [0003]

Patentansprüche

1. Transceiver (41) aufweisend:
einen Transmitter (42), der dazu ausgebildet ist,
- an einem Ausgang ein erstes Signal (s1) gemäß eines physikalischen Kommunikationsprotokolls bereitzustellen, und
- an dem Ausgang ein zweites Signal (s2) bereitzustellen, das mindestens ein kryptographisches Datum (14) umfasst, wobei das erste (s1) und das zweite (s2) Signal als ein Überlagerungssignal (s) an dem Ausgang einander überlagert sind, und wobei das Überlagerungssignal das physikalische Kommunikationsprotokoll erfüllt.

2. Transceiver (41) nach Anspruch 1, wobei das zweite Signal (s2) ein pulsförmiges Signal oder ein wechselstromförmiges Signal ist.

3. Transceiver nach einem der Ansprüche 1 bis 2, wobei das zweite Signal (s2) dem ersten Signal (s1) nur auf einem von mindestens zwei Pegeln des ersten Signals gemäß des physikalischen Kommunikationsprotokolls überlagert wird.

4. Transceiver nach einem der Ansprüche 1 bis 3, wobei das zweite Signal (s2) überlagert wird, wenn für eine bestimmte Zeit kein Pegelwechsel des ersten Signals (s1) erfolgte oder für eine bestimmte Zeit kein Pegelwechsel des ersten Signals (s1) erfolgen wird.

5. Transceiver nach einem der Ansprüche 1 bis 4, wobei eine Logikprotokollschicht, die dem physikalischen Kommunikationsprotokoll übergeordnet ist, ein Logiksignal bereitstellt, und das Logiksignal zur Erzeugung des ersten Signals (s1) verwendet wird.

6. Transceiver nach Anspruch 5, wobei die Logikprotokollschicht ausgebildet ist, zu sendende Daten zu verschlüsseln, um das Logiksignal bereitzustellen.

7. Transceiver nach einem der vorhergehenden Ansprüche, wobei das kryptographische Datum (14) ein Sicherheitscode des Transceivers ist.

8. Transceiver nach einem der vorhergehenden Ansprüche, wobei dem Transceiver ein Schlüssel zum Erzeugen des kryptographischen Datums (14), bereitgestellt wird.

9. Transceiver nach Anspruch 8, wobei der Schlüssel durch eine dem Transceiver (41) übergeordnete Schlüsselinstanz (261) bereitgestellt wird.

10. Transceiver nach einem der vorhergehenden Ansprüche, wobei der Transmitter (42) eine Treiberschaltung (50) umfasst, die eingerichtet ist, das Überlagerungssignal bereitzustellen, und wobei der Transmitter (42) eingerichtet ist, die Treiberschaltung zu kalibrieren.

11. Transceiver nach Anspruch 10, wobei die Treiberschaltung (50) eine erste Reihenschaltung aus einem ersten Schalter (56, 54) und einem ersten Widerstand (55, 53) umfasst, die zwischen eine Versorgungsspannung und dem Ausgang gekoppelt ist, wobei der erste Schalter (56, 54) in Abhängigkeit von dem ersten Signal (s1) ansteuerbar ist, und die Treiberschaltung eine zweite Reihenschaltung aus einem zweiten Schalter (52) und einen zweiten Widerstand (51) aufweist, die zwischen die Versorgungsspannung und dem Ausgang gekoppelt ist, wobei der zweite Schalter (52) in Abhängigkeit von dem kryptographischen Datum ansteuerbar ist.

12. Transceiver (41) aufweisend:
einen Receiver (43), der dazu ausgebildet ist,
- ein Empfangssignal (s), welches eine Überlagerung eines ersten Signals gemäß einem physikalischen Kommunikationsprotokoll mit einem zweiten Signal, das ein kryptographisches Datum (14) umfasst, ist, zu empfangen,
- das Empfangssignal gemäß dem physikalischen Kommunikationsprotokoll zu verarbeiten, um in dem ersten Signal übertragene Informationen zu gewinnen, und
- aus dem Empfangssignal das kryptographische Datum zu gewinnen.

13. Transceiver nach Anspruch 12, wobei das zweite Signal ein pulsförmiges Signal oder ein wechselstromförmiges Signal ist.

14. Transceiver nach einem der Ansprüche 12 oder 13, wobei der Receiver (43) ausgebildet ist, das kryptographische Datum aus der Überlagerung des zweiten Signals über dem ersten Signal nur auf einem von mindestens zwei Pegeln des ersten Signals gemäß des physikalischen Kommunikationsprotokolls zu gewinnen.

15. Transceiver nach einem der Ansprüche 1 bis 3, wobei der Receiver (43) ausgebildet ist, das kryptographische Datum aus der Überlagerung des zweiten Signal über dem ersten Signal zu gewinnen, wenn für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgte oder für eine bestimmte Zeit kein Pegelwechsel des ersten Signals erfolgen wird.

16. Transceiver (41) nach einem der Ansprüche 12 bis 15, wobei die aus dem ersten Signal gewonnenen Informationen einer Logikprotokollschicht, die dem physikalischen Kommunikationsprotokoll übergeordnet ist, als Logiksignal bereitstellt wird.

17. Transceiver (41) nach Anspruch 16, wobei die Logikprotokollschicht ausgebildet ist, aus dem Logiksignal durch Entschlüsselung gesendete Daten zu gewinnen.

18. Transceiver (41) nach einem der vorhergehenden Ansprüche, wobei das kryptographische Datum ein Sicherheitscode eines weiteren Transceivers ist, von dem das Empfangssignal empfangen wird, und wobei der Transceiver (41) eingerichtet ist, das kryptographische Datum mit einem erwarteten kryptographischen Datum zu vergleichen, um den weiteren Transceiver zu authentifizieren.

19. Transceiver (41) nach Anspruch 18, wobei dem Transceiver (41) ein Schlüssel zum Erzeugen des erwarteten kryptographischen Datums bereitgestellt wird.

20. Transceiver (41) nach Anspruch 19, wobei der Schlüssel durch eine dem Transceiver (41) übergeordnete Schlüsselinstanz (261) bereitgestellt wird.

21. Transceiver (41) nach einem der Ansprüche 12-20, wobei der Receiver (43) eine Empfangsschaltung (44) umfasst, die eingerichtet ist, das kryptographische Datum zu gewinnen, und wobei der Receiver (43) eingerichtet ist, die Empfangsschaltung zu kalibrieren.

22. Transceiver nach Anspruch 21, wobei das Kalibrieren ein Bestimmen einer Referenzspannung zum Gewinnen des kryptographischen Datums umfasst.

23. Transceiver (41) nach einem der Ansprüche 12-21, wobei der Receiver (43) eingerichtet ist, nur das Empfangssignal gemäß dem physikalischen Kommunikationsprotokoll zu verarbeiten, um in dem ersten Signal übertragene Informationen zu gewinnen, wenn das Empfangssignal kein zweites Signal enthält und/oder das kryptographische Datum nicht aus dem Empfangssignal gewinnbar ist.

24. System (10), umfassend:
einen ersten Transceiver nach einem der Ansprüche 1-11, und
einen mit dem ersten Transceiver über ein Kommunikationsmedium (13) gekoppelten zweiten Transceiver nach einem der Ansprüche 12-23.

25. System nach Anspruch 24, wobei der erste Transceiver und/oder der zweite Transceiver ein Teil einer Steuereinheit eines Fahrzeugs ist.

26. Signal, umfassend eine Überlagerung aus:
- einem erstes Signal (s1) gemäß eines physikalischen Kommunikationsprotokolls, und
-einem zweites Signal (s2), das mindestens ein kryptographisches Datum umfasst, wobei das Signal das physikalische Kommunikationsprotokoll erfüllt.

27. Signal nach Anspruch 26, wobei das zweite Signal (s2) ein pulsförmiges Signal oder ein wechselstromförmiges Signal ist.

28. Signal nach einem der Ansprüche 26 oder 27, wobei das zweite Signal (s2) dem ersten Signal (s1) nur auf einem von mindestens zwei Pegeln des ersten Signals (s1) gemäß des physikalischen Kommunikationsprotokolls überlagert ist.

29. Signal nach einem der Ansprüche 26 bis 28, wobei das zweite Signal (s2) dem ersten Signal(s1) überlagert ist, wenn für eine bestimmte Zeit kein Pegelwechsel des ersten Signals (s1) erfolgte oder für eine bestimmte Zeit kein Pegelwechsel des ersten Signals (s1) erfolgen wird.

30. Signal nach einem der Ansprüche 26 bis 29, wobei das erste Signal (s1) logisch verschlüsselte Daten umfasst.

Es folgen 21 Seiten Zeichnungen

Anhängende Zeichnungen

FIG 1

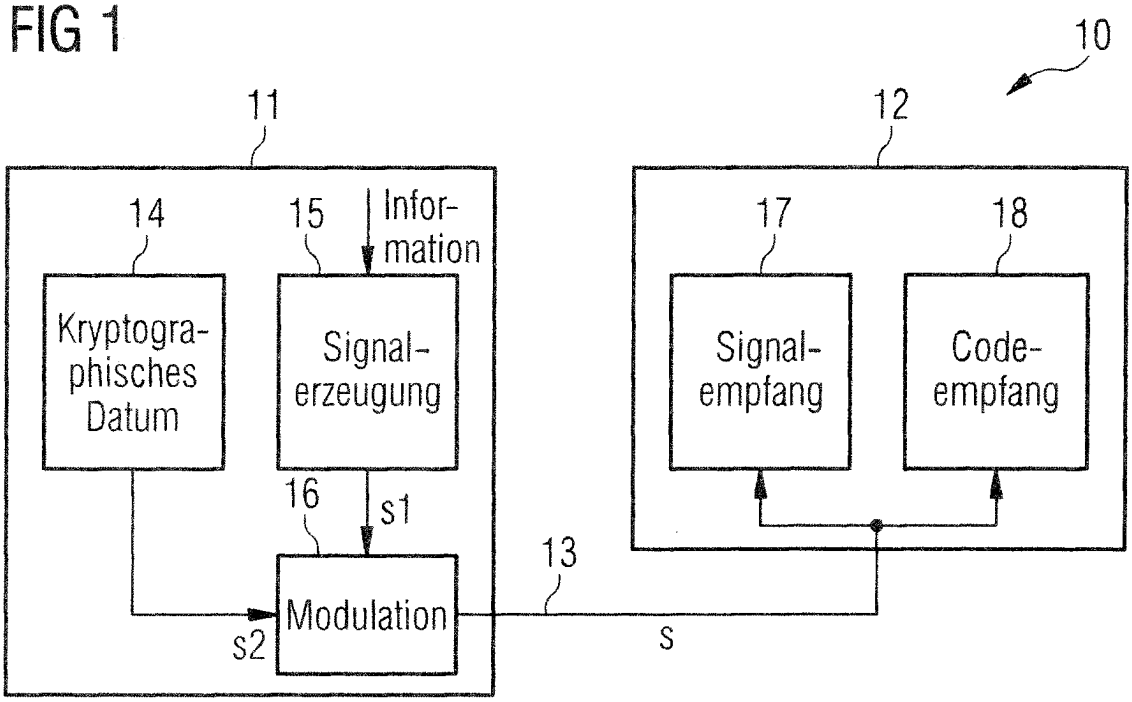


FIG 2

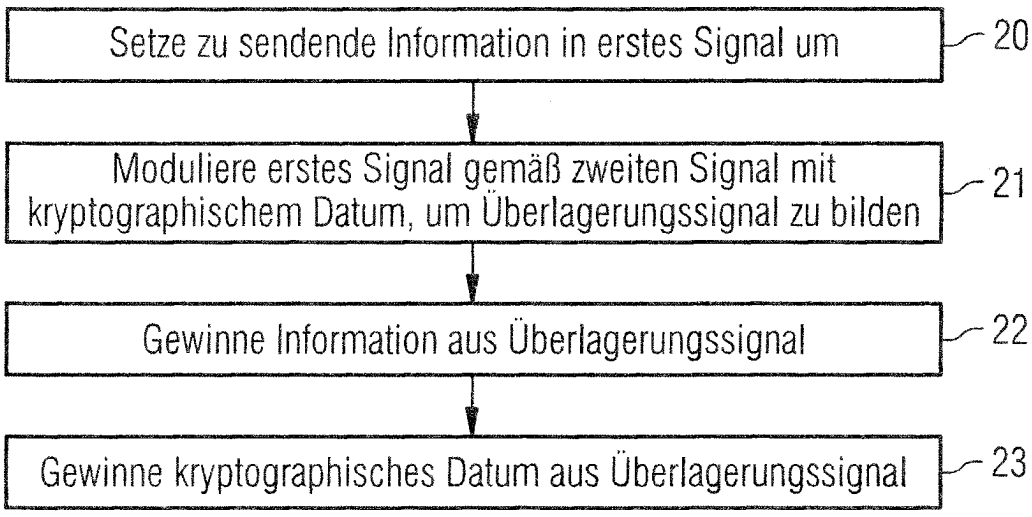


FIG 3

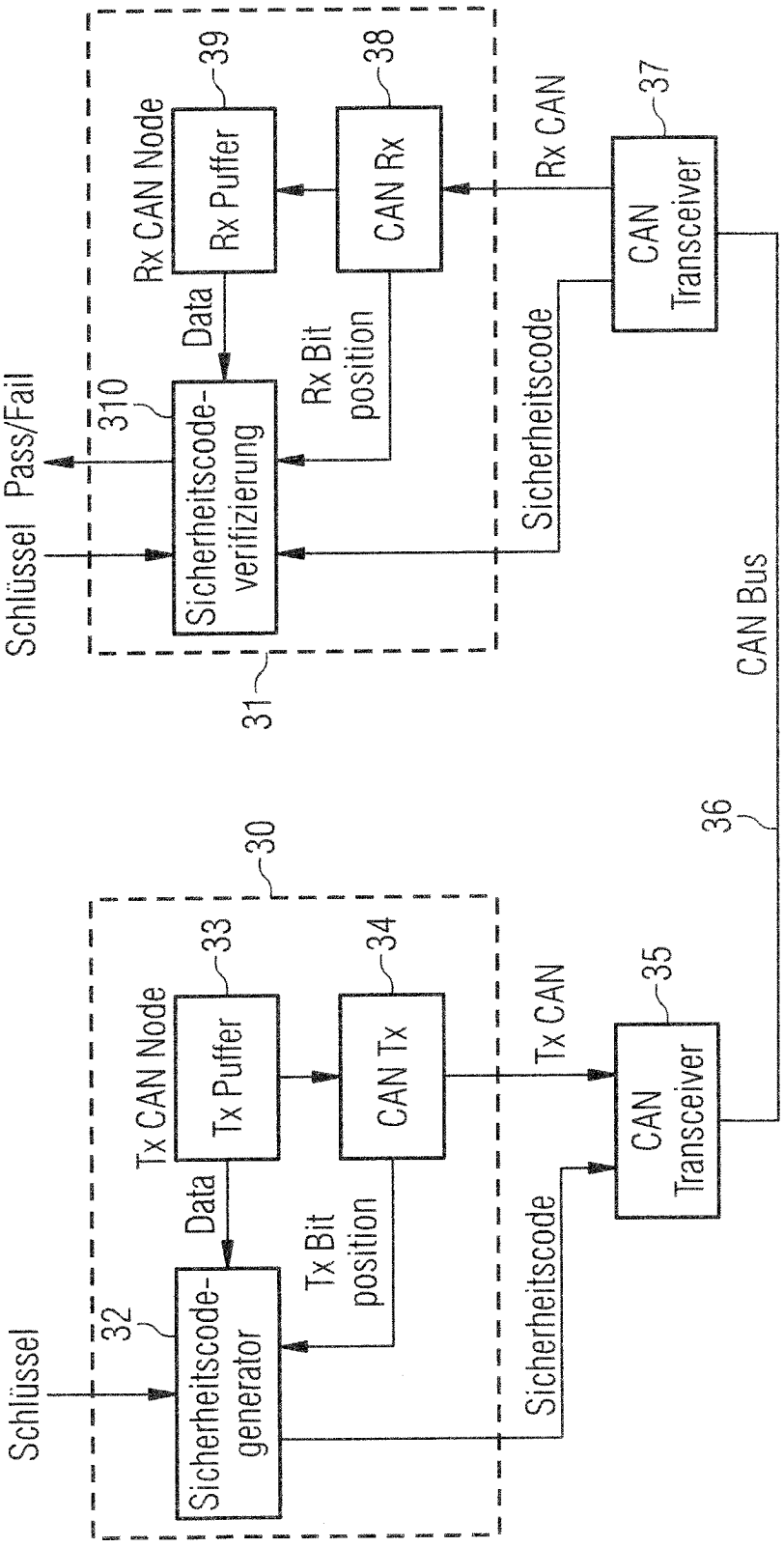

Schlüssel
32
Sicherheitscode-generator
Tx CAN Node
Tx Puffer
33
Data
Tx Bit position
CAN Tx
34
Tx CAN
CAN Transceiver
35
30
Sicherheitscode
36
CAN Bus
Schlüssel
Pass/Fail
310
Sicherheitscode-verifizierung
Rx CAN Node
Rx Puffer
39
Data
Rx Bit position
CAN Rx
38
Rx CAN
CAN Transceiver
37
Sicherheitscode
31

FIG 4

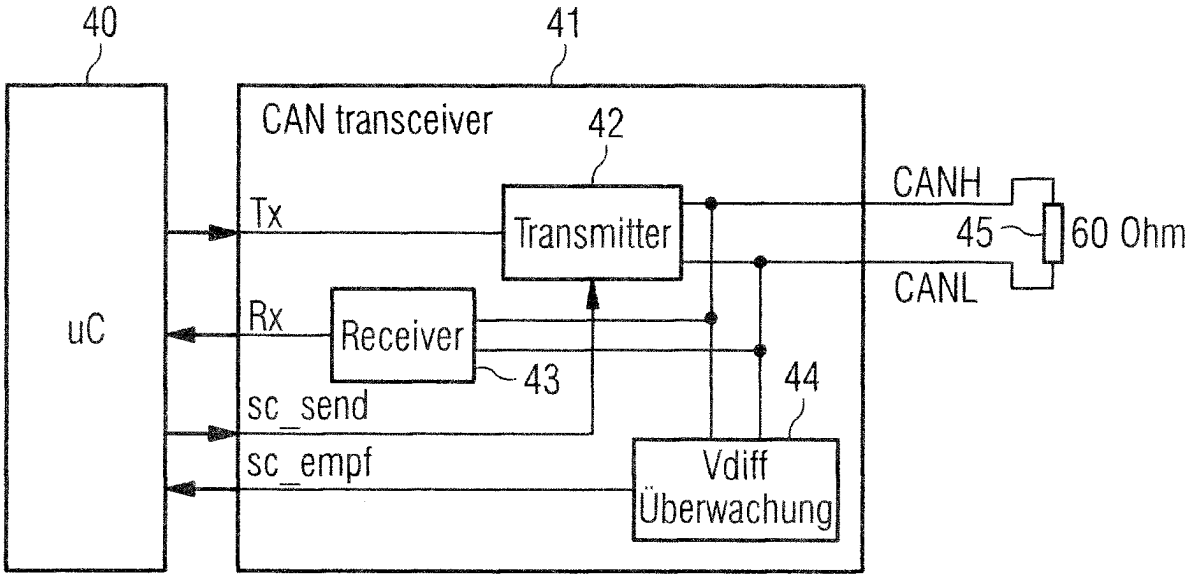

40
41
CAN transceiver
42
Tx
Transmitter
CANH
45
60 Ohm
CANL
uC
Rx
Receiver
43
44
sc_send
sc_empf
Vdiff
Überwachung

FIG 5

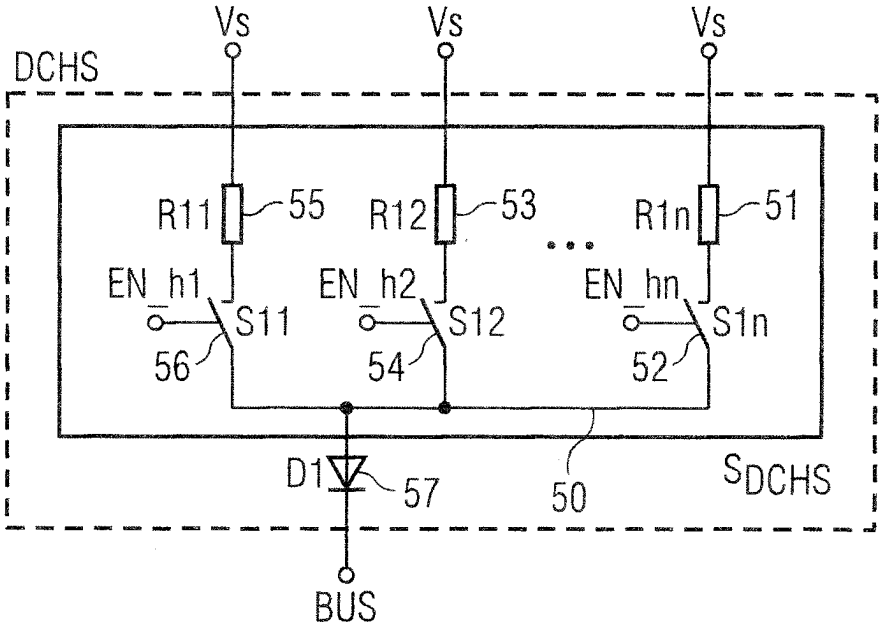

Vs
Vs
Vs
DCHS
R11
55
R12
53
R1n
51
EN_h1
EN_h2
EN_hn
S11
S12
S1n
56
54
52
D1
57
50
SDCHS
BUS

FIG 6

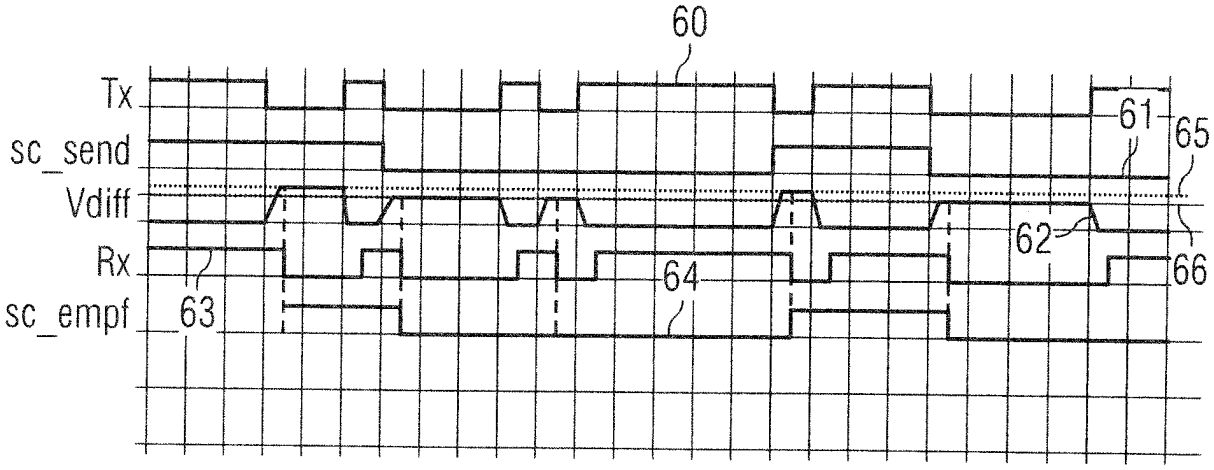


FIG 7

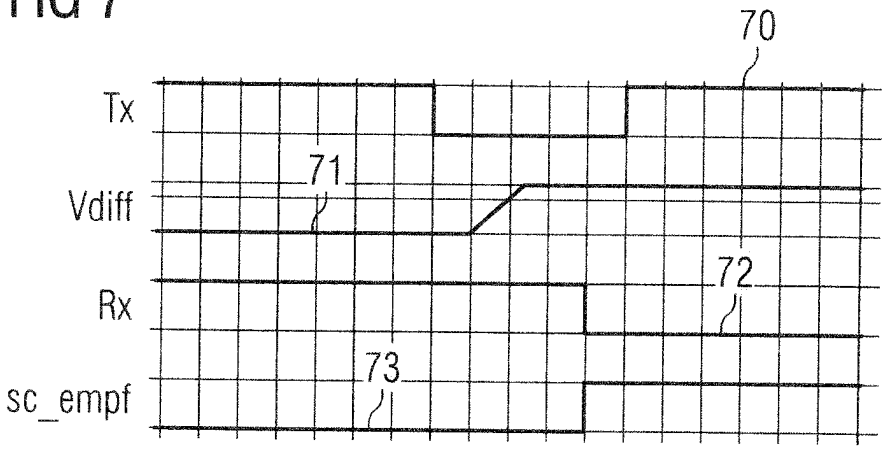


FIG 8

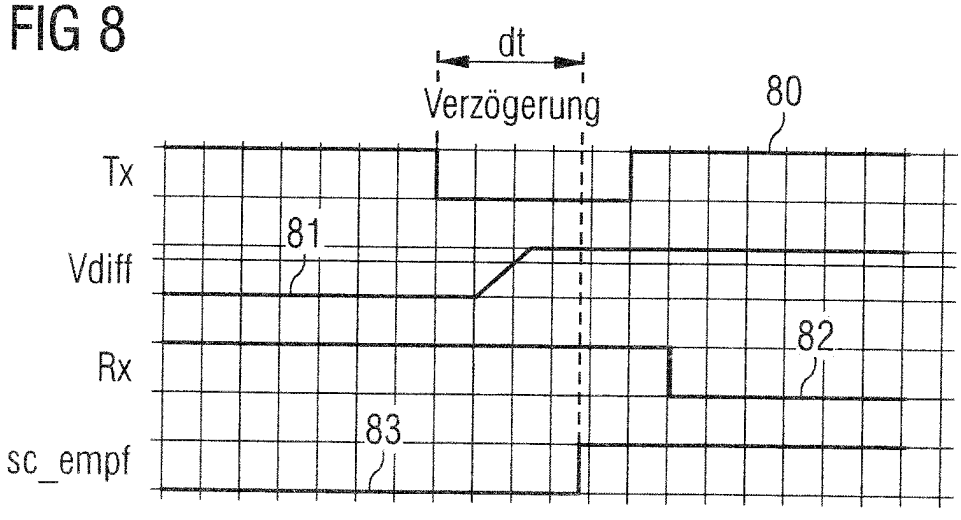


FIG 9

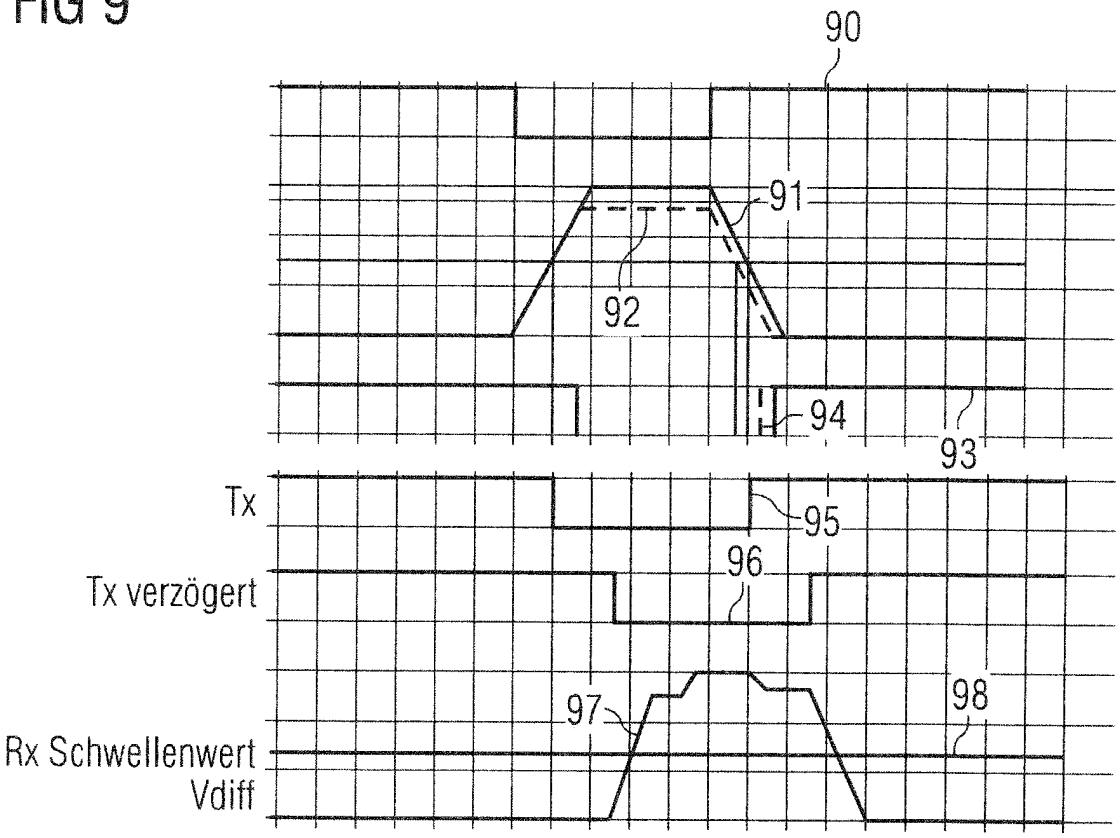

90
91
92
94
93
Tx
95
96
Tx verzögert
97
98
Rx Schwellenwert
Vdiff

FIG 10

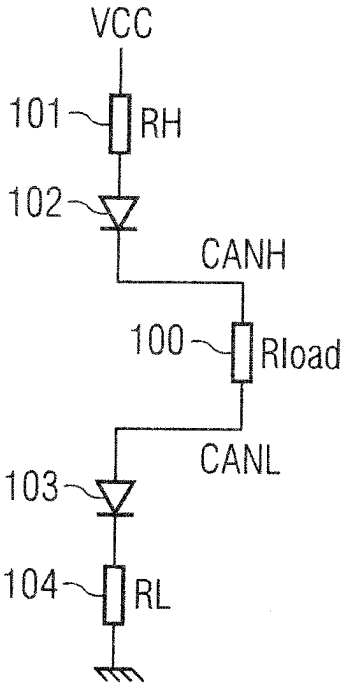

VCC
101
RH
102
CANH
100
Rload
CANL
103
104
RL

FIG 11

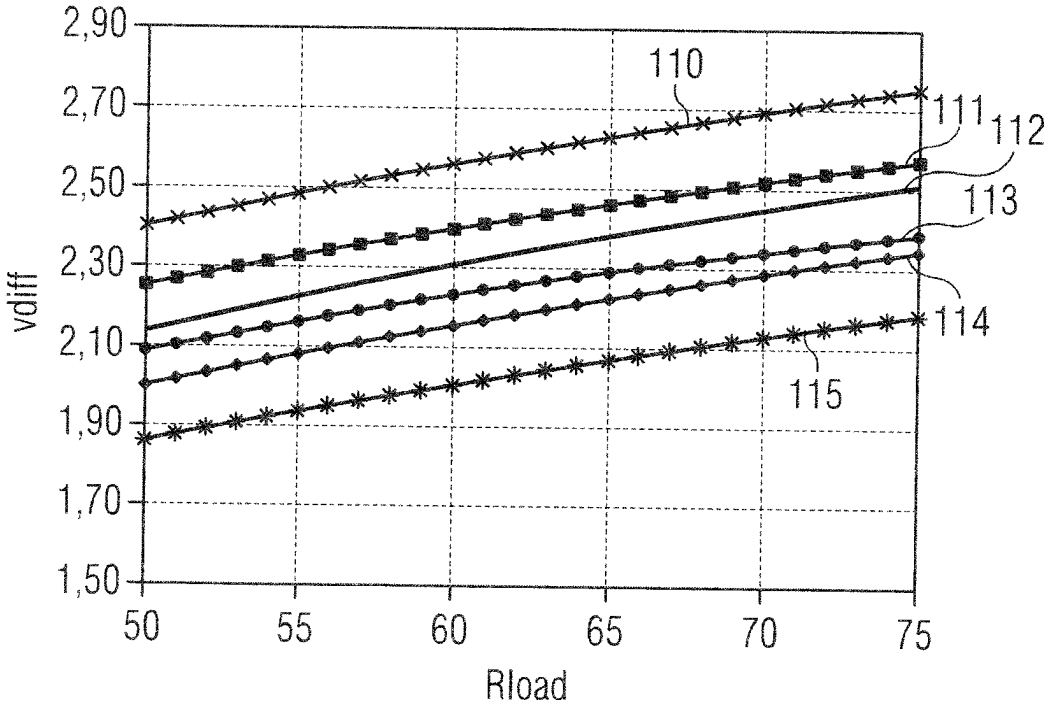

2,90
2,70
2,50
2,30
2,10
1,90
1,70
1,50
vdiff
50
55
60
65
70
75
Rload
110
111
112
113
114
115

FIG 12

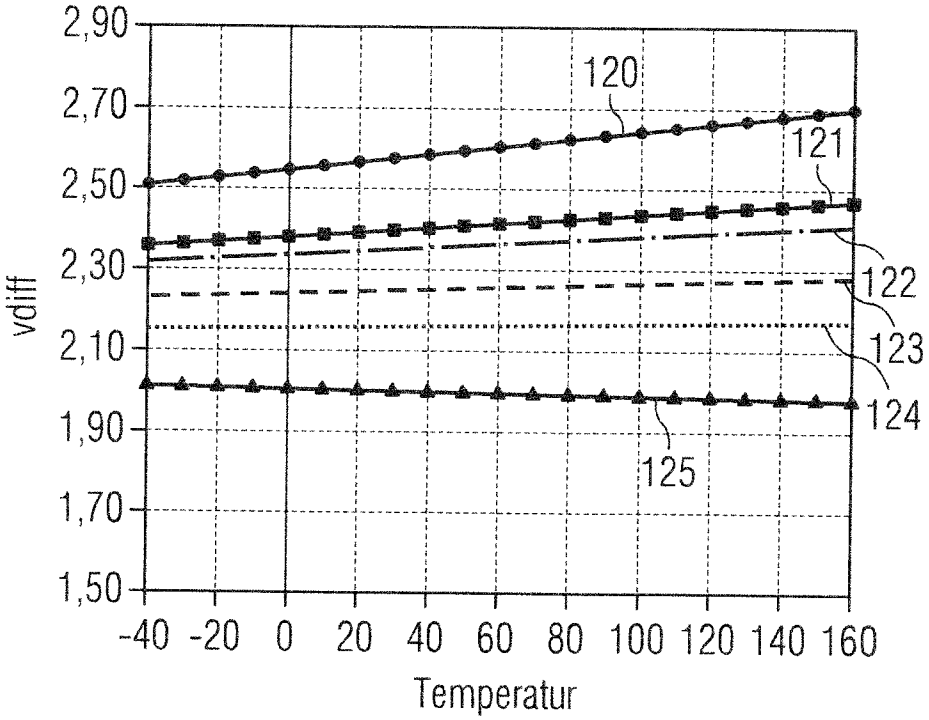

2,90
2,70
2,50
2,30
2,10
1,90
1,70
1,50
vdiff
-40 -20 0 20 40 60 80 100 120 140 160
Temperatur
120
121
122
123
124
125

FIG 13

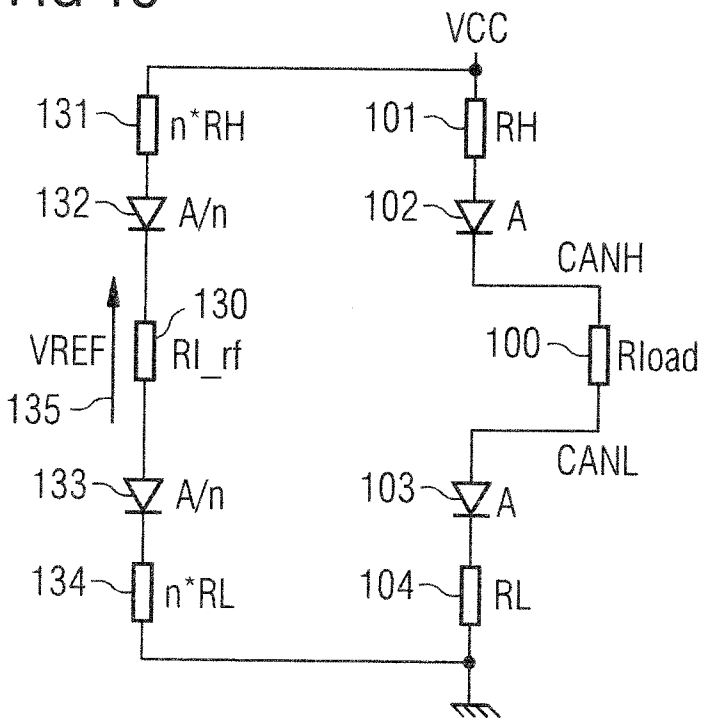

VCC
131
n*RH
132
A/n
130
VREF
RI_rf
135
133
A/n
134
n*RL
101
RH
102
A
CANH
100
Rload
CANL
103
A
104
RL

FIG 14

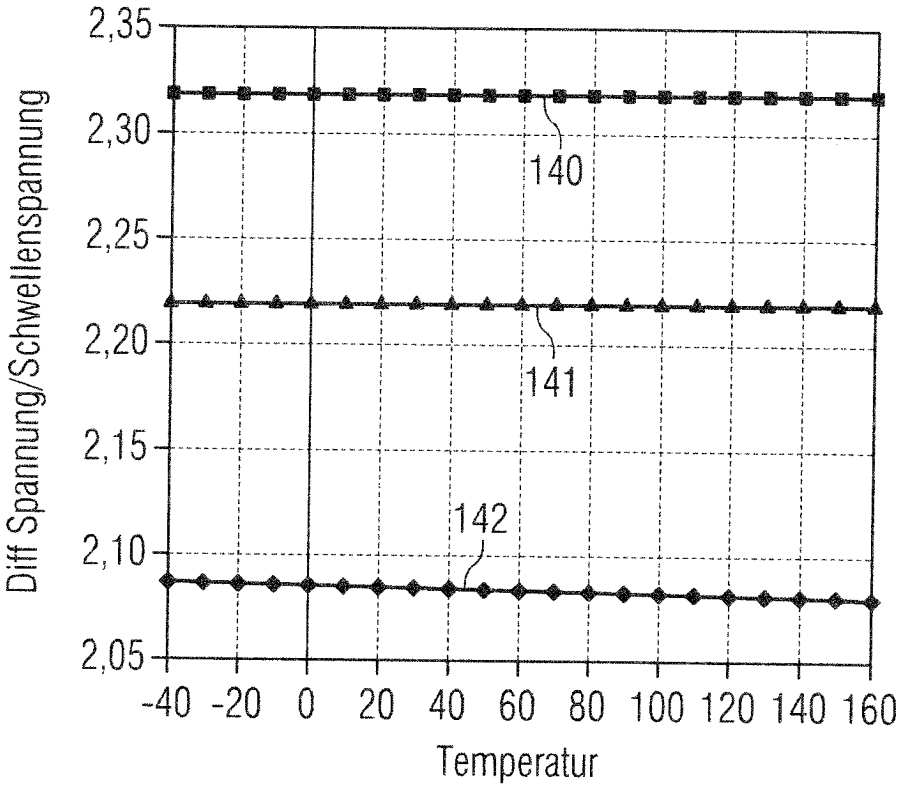

2,35
2,30
2,25
2,20
2,15
2,10
2,05
Diff Spannung/Schwellenspannung
140
141
142
-40 -20 0 20 40 60 80 100 120 140 160
Temperatur

FIG 15

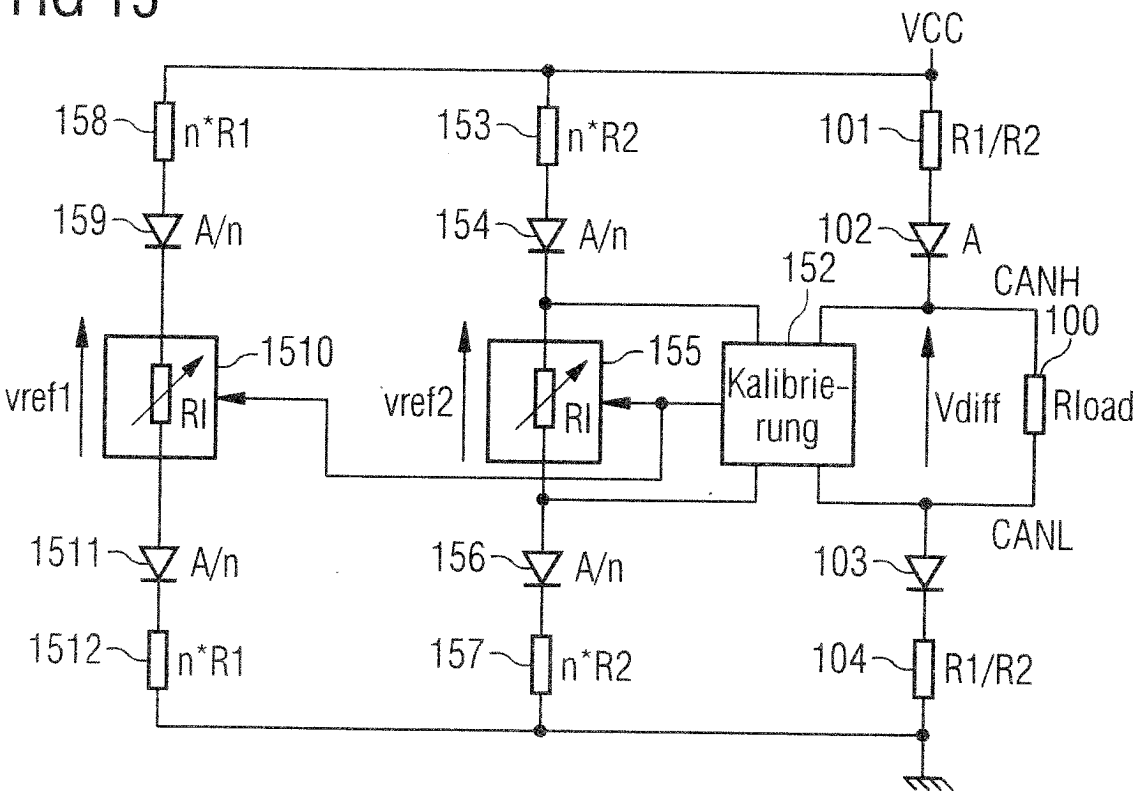

VCC
158
n*R1
153
n*R2
101
R1/R2
159
A/n
154
A/n
102
A
152
CANH
100
1510
155
vref1
Rl
vref2
Rl
Kalibrie-
rung
Vdiff
Rload
CANL
1511
A/n
156
A/n
103
1512
n*R1
157
n*R2
104
R1/R2

FIG 16

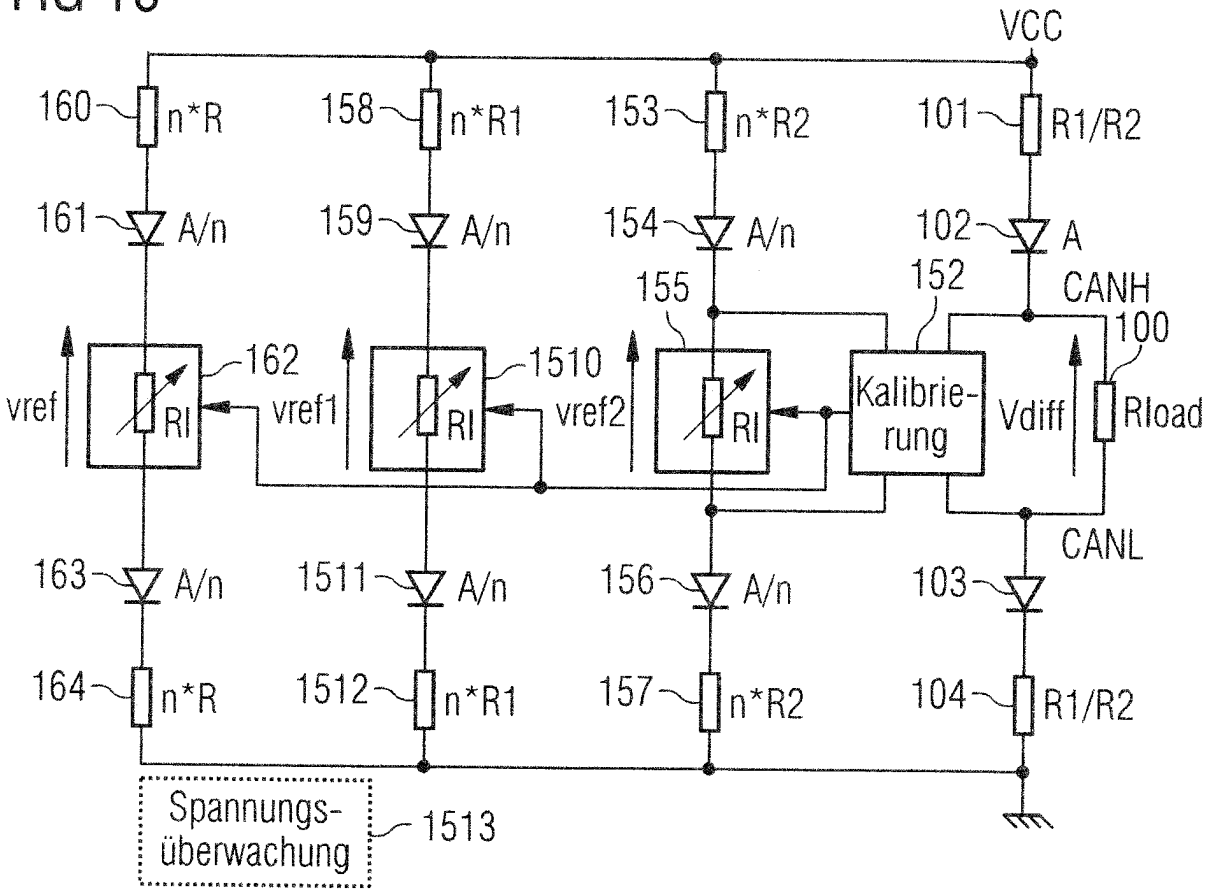

VCC
160
n*R
158
n*R1
153
n*R2
101
R1/R2
161
A/n
159
A/n
154
A/n
102
A
155
152
CANH
100
vref
162
RI
vref1
1510
RI
vref2
RI
Kalibrie-
rung
Vdiff
Rload
CANL
163
A/n
1511
A/n
156
A/n
103
164
n*R
1512
n*R1
157
n*R2
104
R1/R2
Spannungs-
überwachung
1513

FIG 17

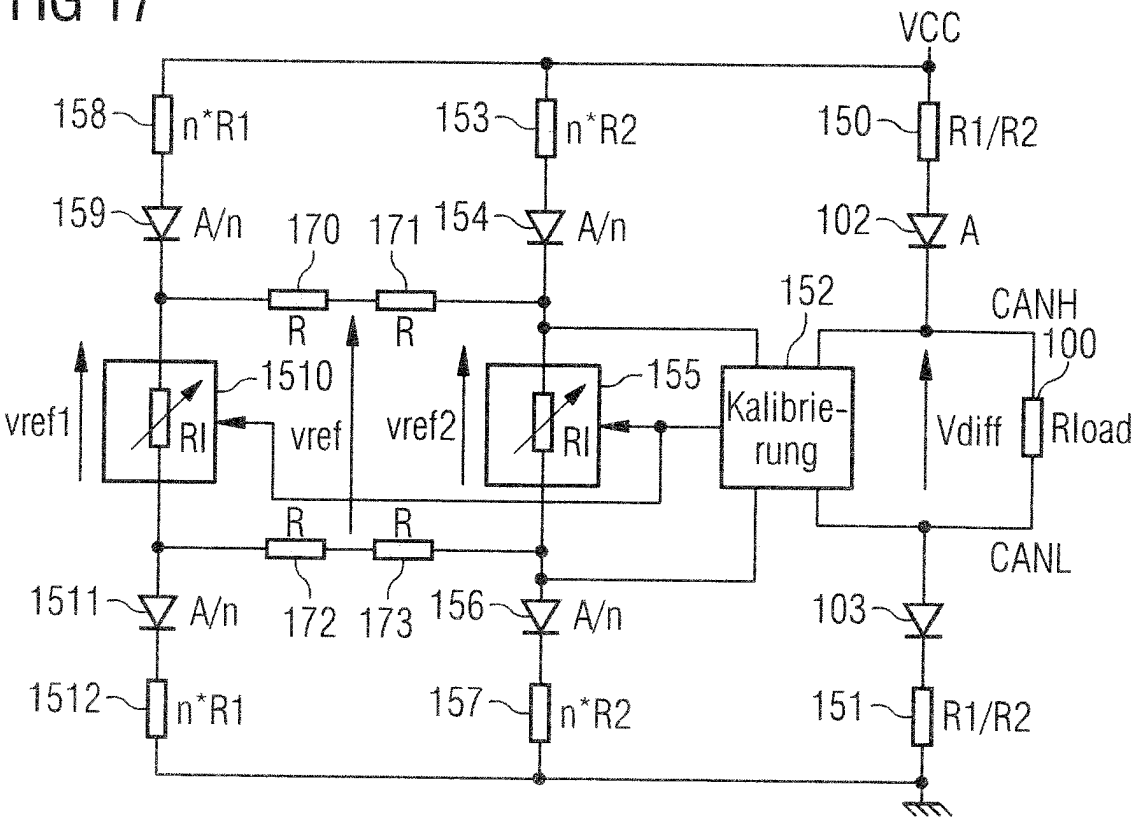

VCC
158
n*R1
153
n*R2
150
R1/R2
159
A/n
170
171
154
A/n
102
A
152
CANH
100
R
R
vref1
1510
RI
vref
vref2
155
RI
Kalibrie-
rung
Vdiff
Rload
R
R
CANL
1511
A/n
172
173
156
A/n
103
1512
n*R1
157
n*R2
151
R1/R2

FIG 18

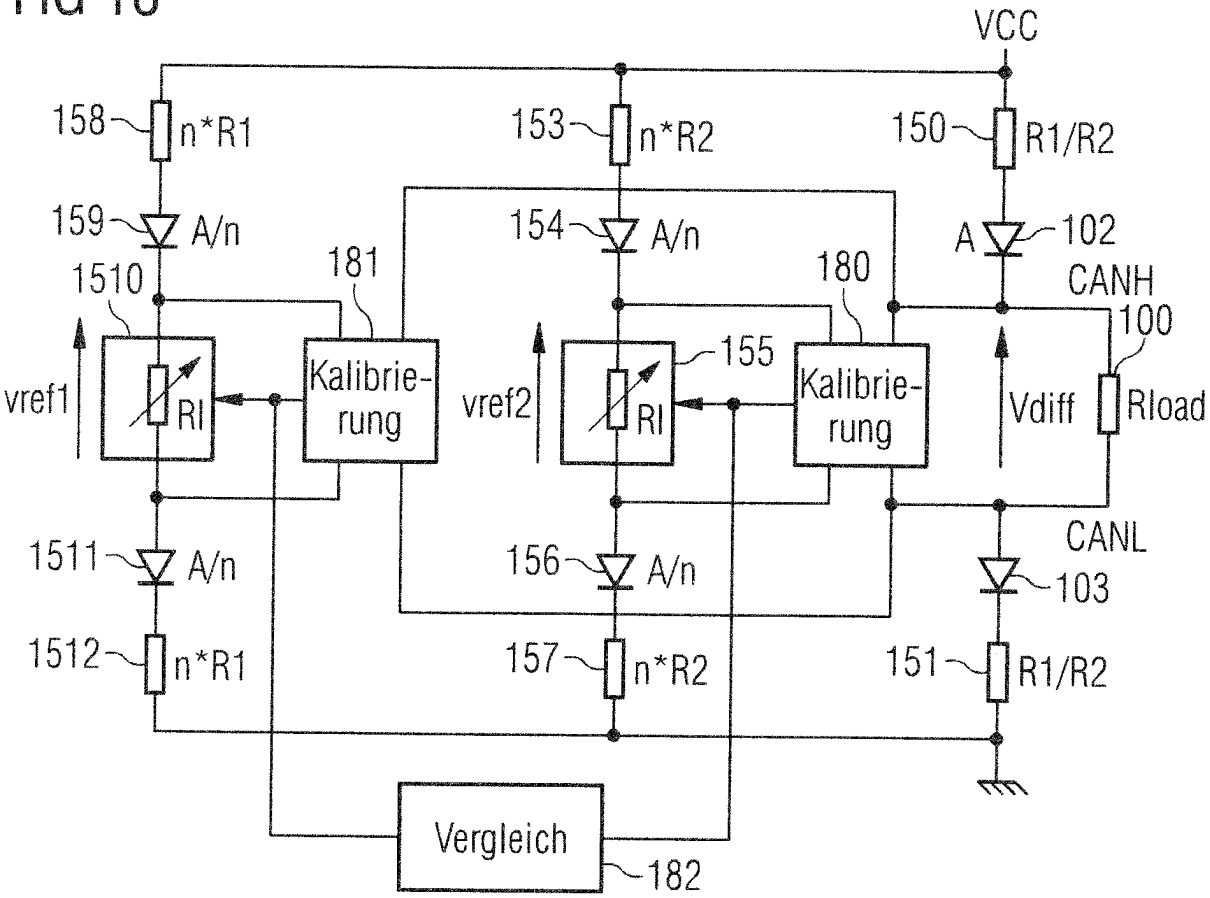

VCC
158
n*R1
153
n*R2
150
R1/R2
159
A/n
154
A/n
A
102
CANH
1510
181
180
100
vref1
RI
Kalibrie-rung
vref2
155
RI
Kalibrie-rung
Vdiff
Rload
1511
A/n
156
A/n
CANL
103
1512
n*R1
157
n*R2
151
R1/R2
Vergleich
182

FIG 19

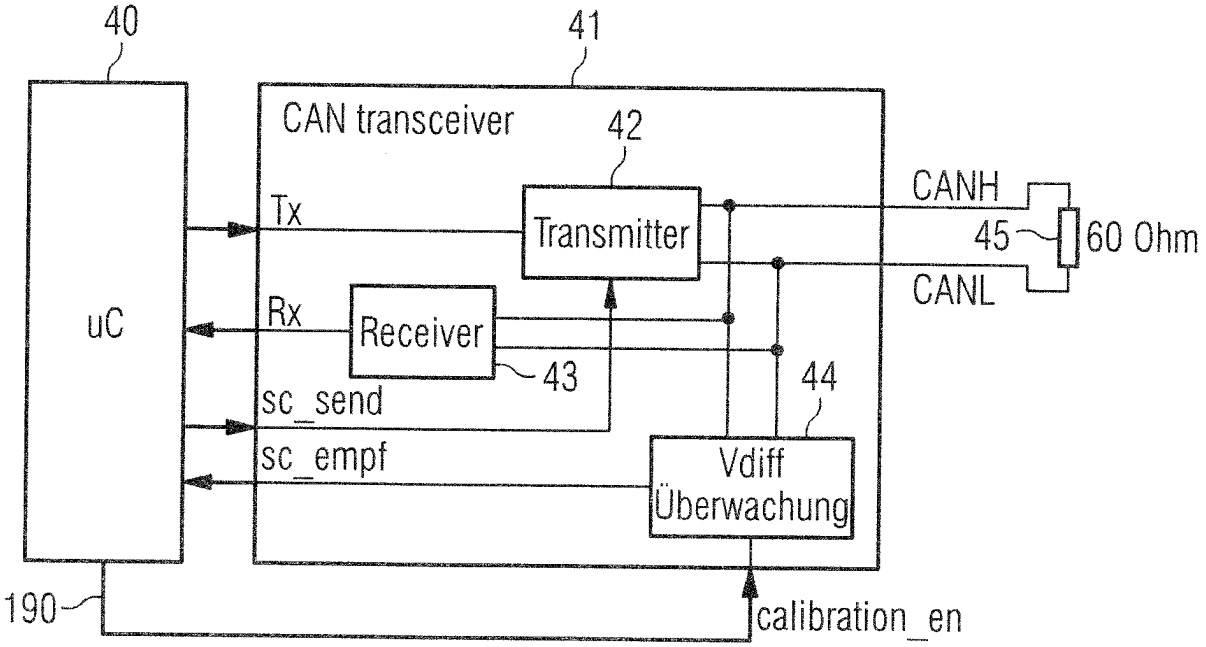

40
41
CAN transceiver
42
Tx
Transmitter
CANH
45
60 Ohm
CANL
uC
Rx
Receiver
43
44
sc_send
sc_empf
Vdiff Überwachung
190
calibration_en

FIG 20

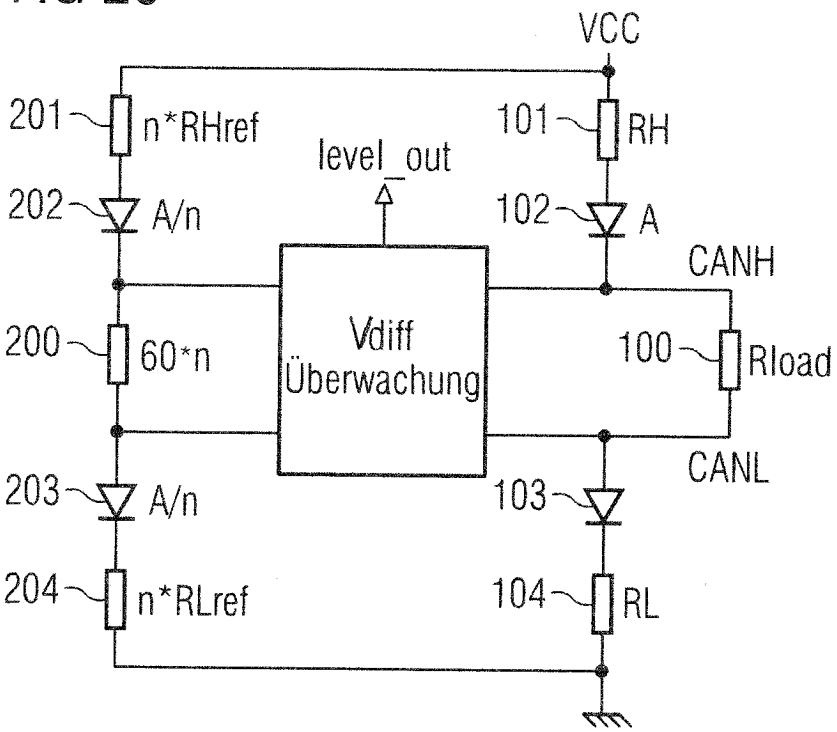

VCC
201
n*RHref
101
RH
level_out
202
A/n
102
A
CANH
200
60*n
Vdiff
Überwachung
100
Rload
CANL
203
A/n
103
204
n*RLref
104
RL

FIG 21

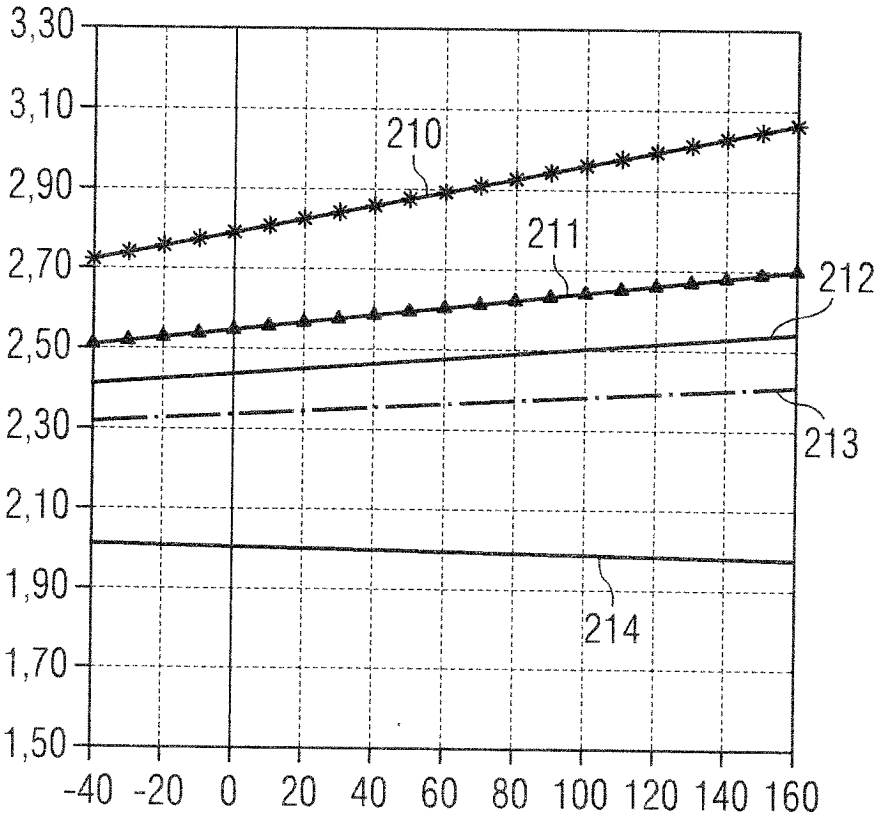

3,30
3,10
2,90
2,70
2,50
2,30
2,10
1,90
1,70
1,50
-40 -20 0 20 40 60 80 100 120 140 160
210
211
212
213
214

FIG 22

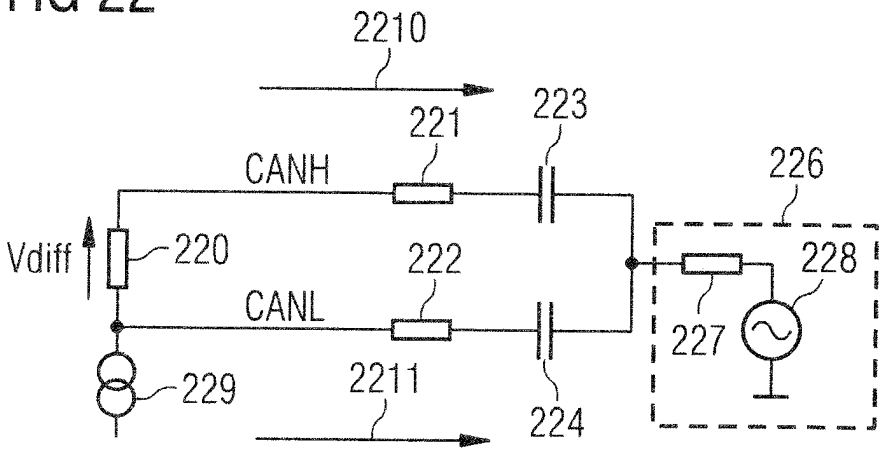

2210
221
223
CANH
226
Vdiff
220
222
228
CANL
227
229
2211
224

FIG 23

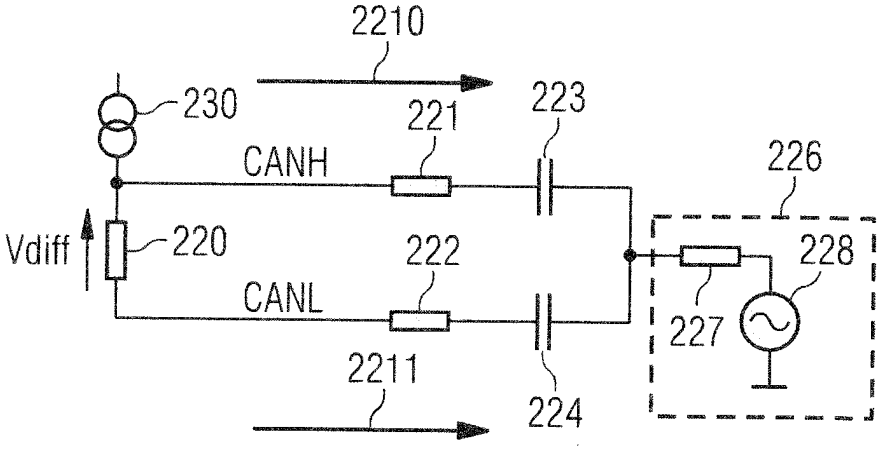

2210
230
221
223
CANH
226
Vdiff
220
222
228
CANL
227
2211
224

FIG 24

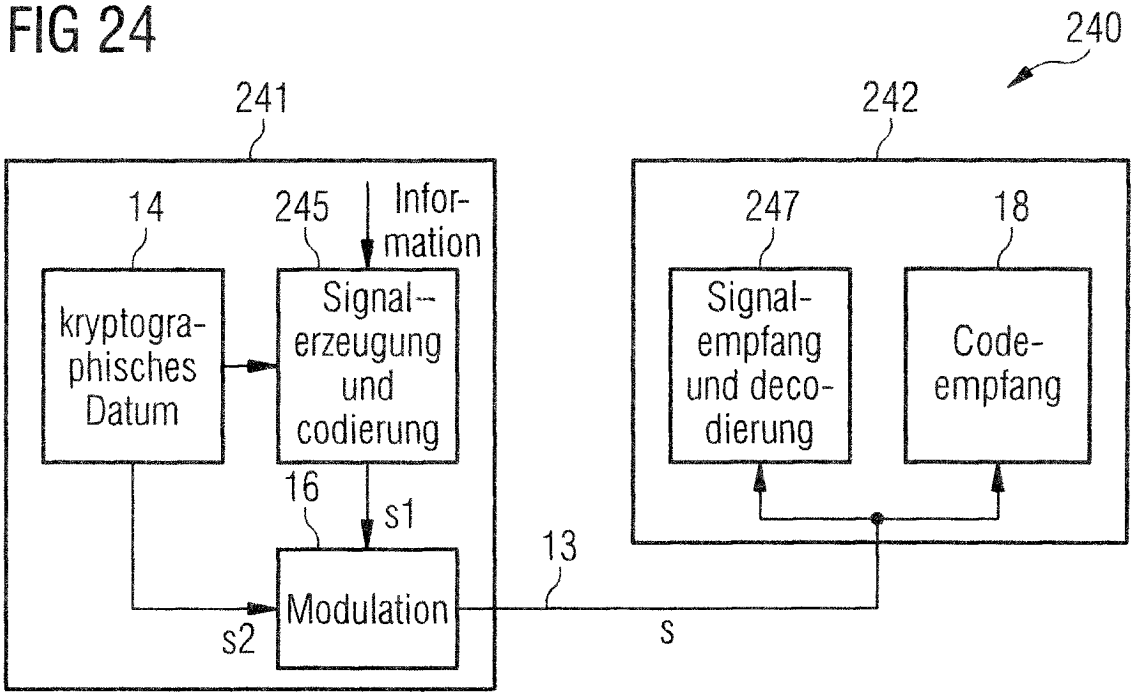

240
241
242
14
245
Infor-
mation
247
18
kryptogra-
phisches
Datum
Signal--
erzeugung
und
codierung
Signal-
empfang
und deco-
dierung
Code-
empfang
16
s1
13
Modulation
s2
s

FIG 25

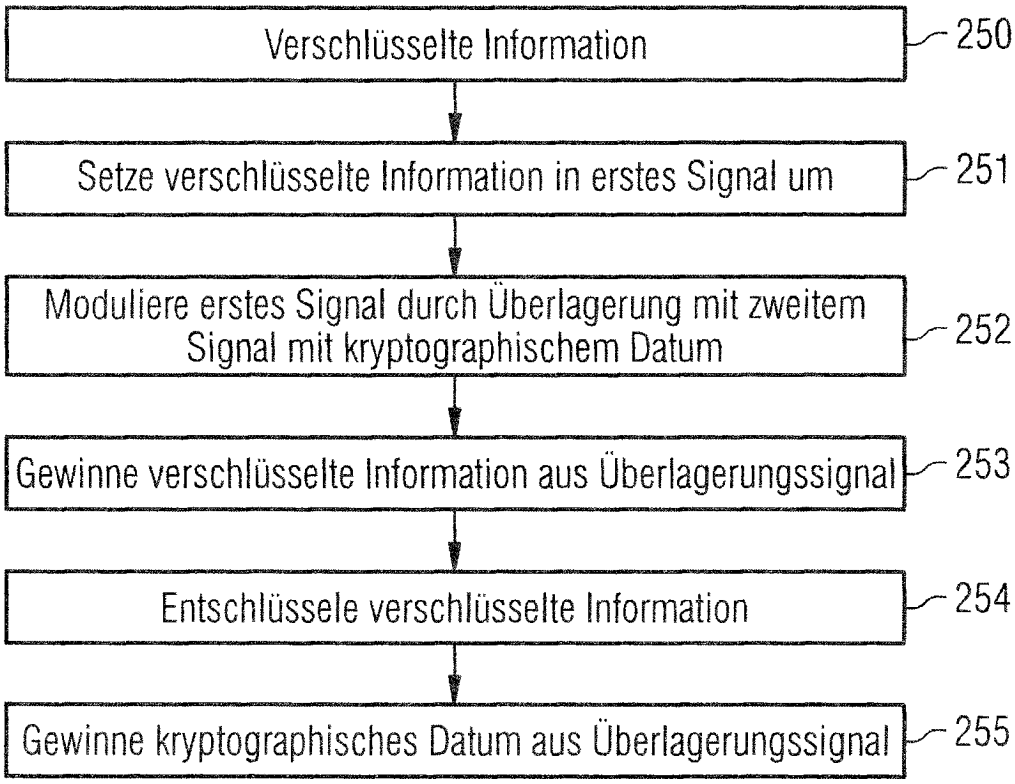

Verschlüsselte Information
250
Setze verschlüsselte Information in erstes Signal um
251
Moduliere erstes Signal durch Überlagerung mit zweitem Signal mit kryptographischem Datum
252
Gewinne verschlüsselte Information aus Überlagerungssignal
253
Entschlüssele verschlüsselte Information
254
Gewinne kryptographisches Datum aus Überlagerungssignal
255

FIG 26

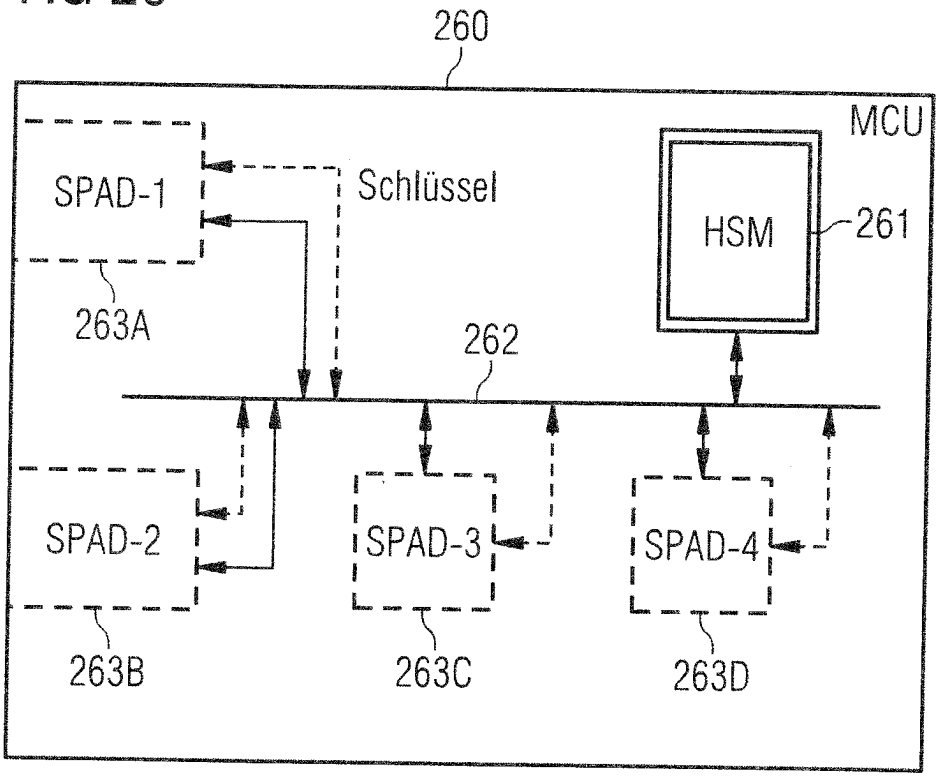

260
MCU
SPAD-1
Schlüssel
HSM
261
263A
262
SPAD-2
SPAD-3
SPAD-4
263B
263C
263D

FIG 27

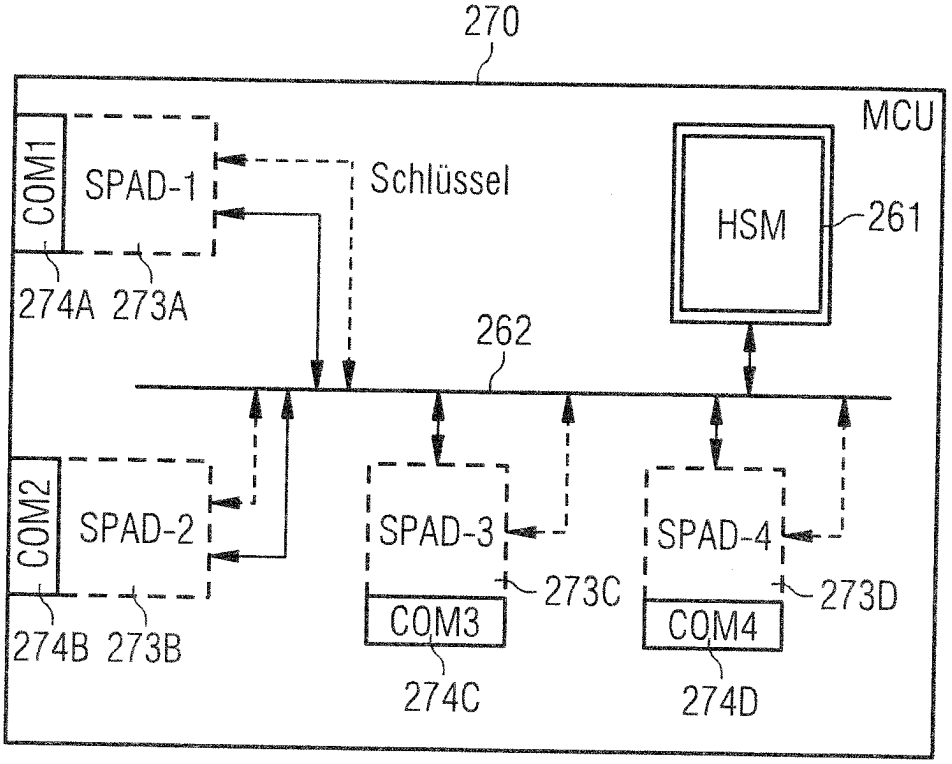

270
MCU
COM1
SPAD-1
Schlüssel
HSM
261
274A 273A
262
COM2
SPAD-2
SPAD-3
SPAD-4
273C
273D
274B 273B
COM3
COM4
274C
274D

FIG 28

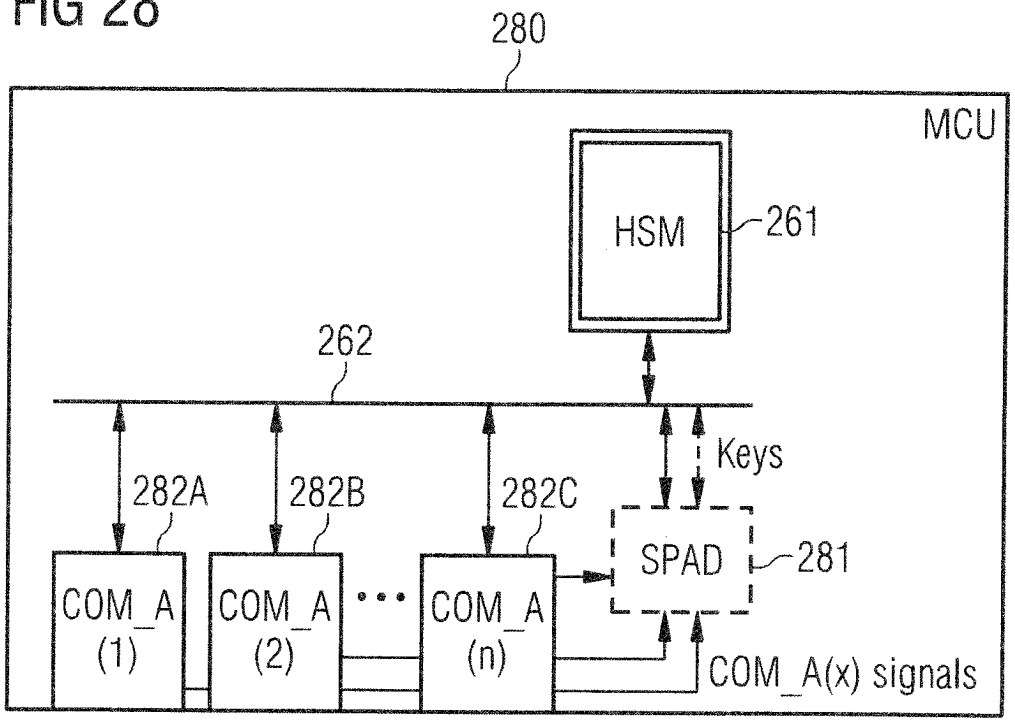

280
MCU
HSM
261
262
Keys
282A
282B
282C
SPAD
281
COM_A (1)
COM_A (2)
COM_A (n)
COM_A(x) signals

FIG 29

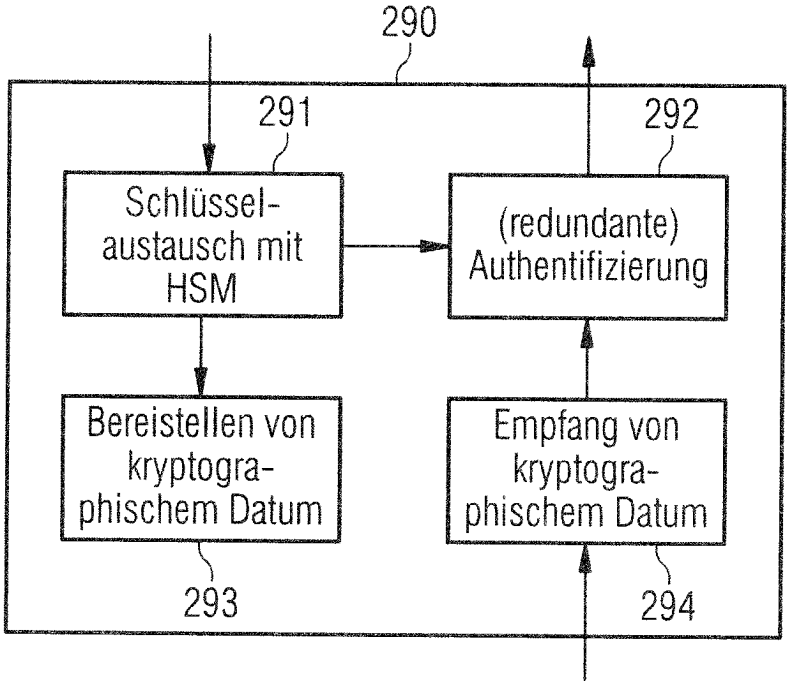

290
291
292
Schlüssel-austausch mit HSM
(redundante) Authentifizierung
Bereistellen von kryptogra-phischem Datum
Empfang von kryptogra-phischem Datum
293
294

FIG 30

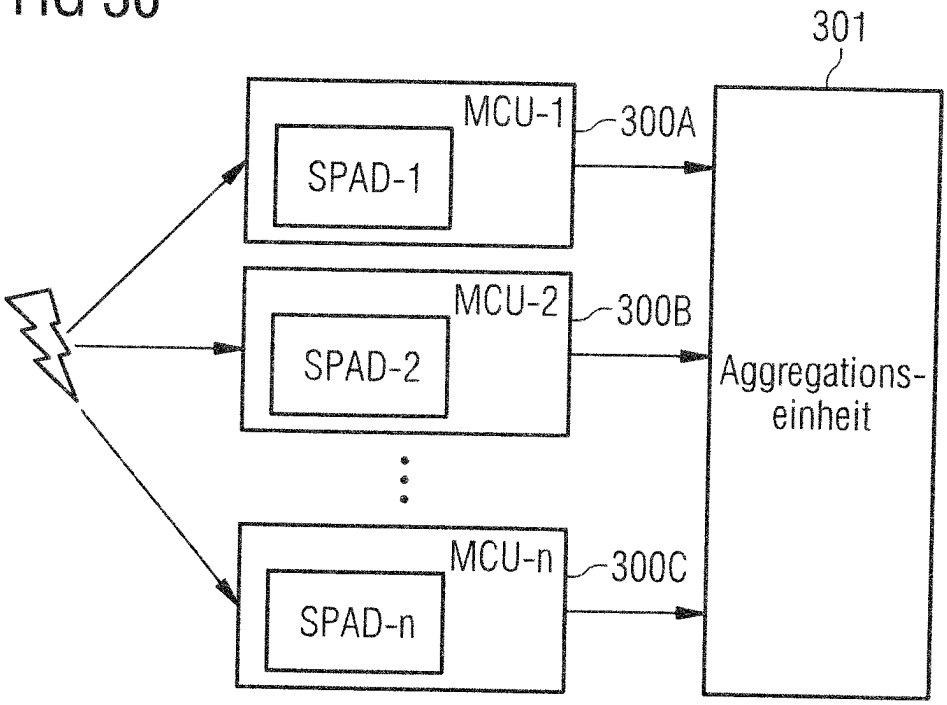

301
MCU-1
300A
SPAD-1
MCU-2
300B
SPAD-2
Aggregations-
einheit
MCU-n
300C
SPAD-n

FIG 31

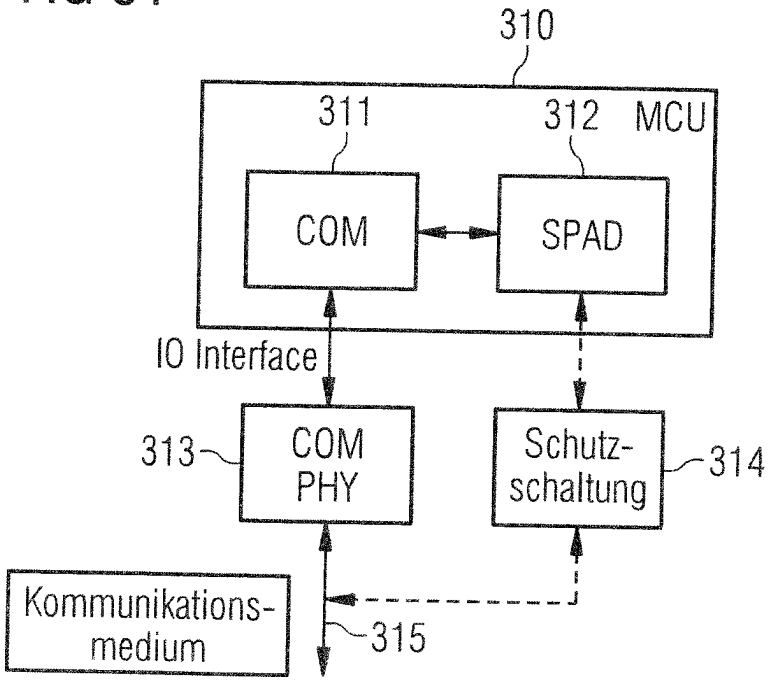

310
311
312
MCU
COM
SPAD
IO Interface
313
COM
PHY
Schutz-
schaltung
314
Kommunikations-
medium
315

FIG 32

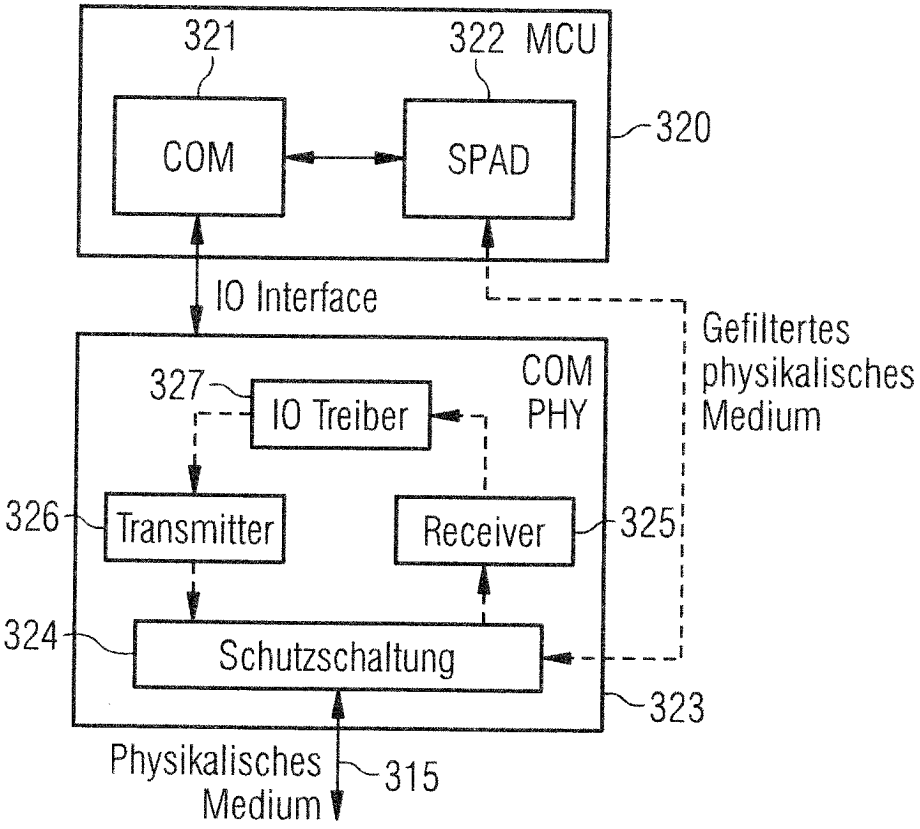

321
322 MCU
COM
SPAD
320
IO Interface
Gefiltertes physikalisches Medium
COM PHY
327
IO Treiber
326
Transmitter
Receiver
325
324
Schutzschaltung
323
Physikalisches Medium
315

FIG 33

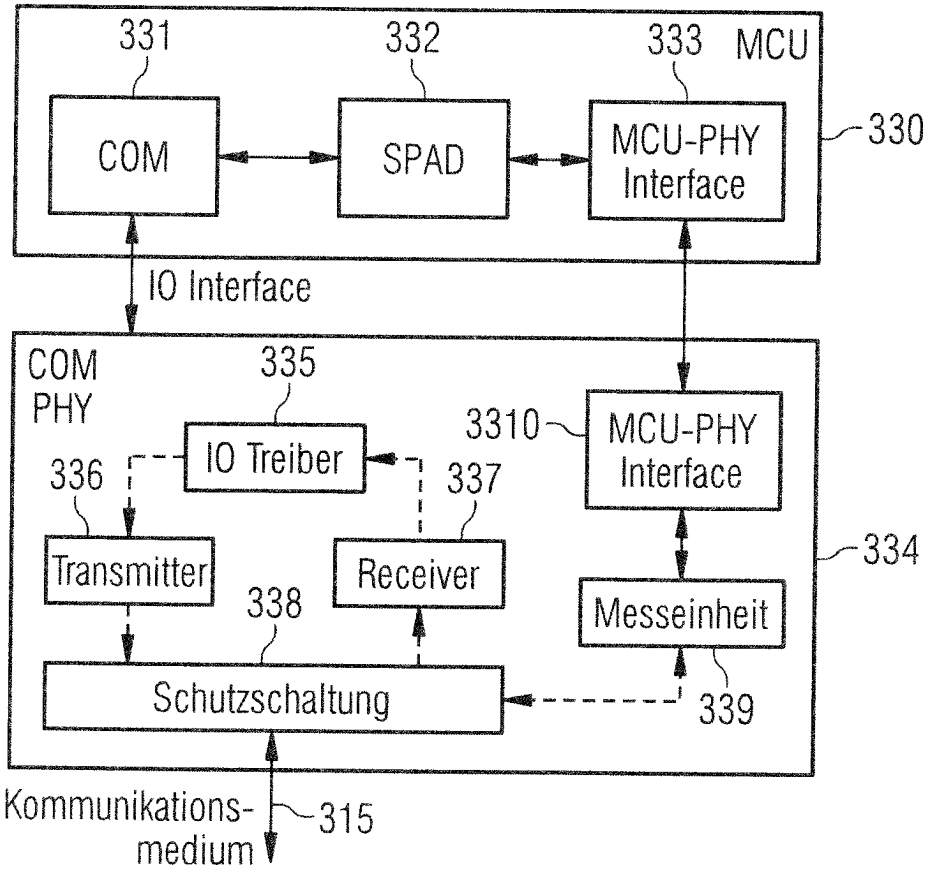

331
332
333
MCU
COM
SPAD
MCU-PHY Interface
330
IO Interface
COM PHY
335
IO Treiber
3310
MCU-PHY Interface
336
337
Transmitter
Receiver
334
338
Messeinheit
Schutzschaltung
339
Kommunikations-medium
315

FIG 34

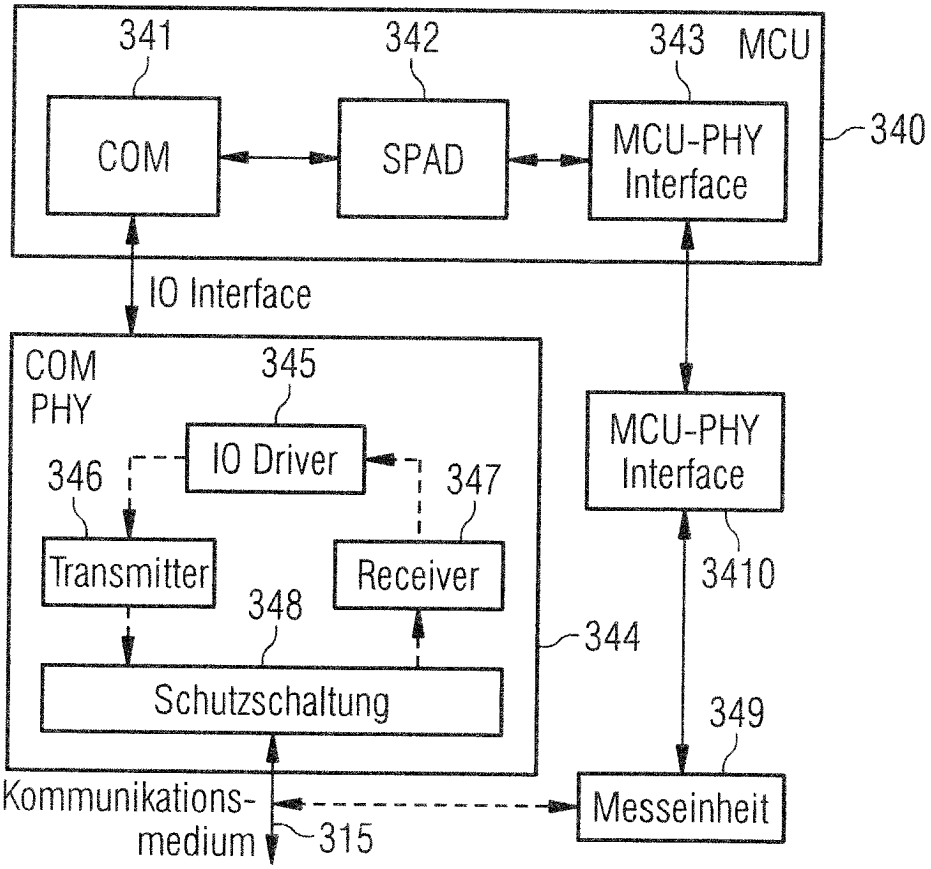

341
342
343
MCU
COM
SPAD
MCU-PHY Interface
340
IO Interface
COM PHY
345
IO Driver
346
347
Transmitter
Receiver
348
344
Schutzschaltung
MCU-PHY Interface
3410
349
Kommunikations-medium
315
Messeinheit

FIG 35

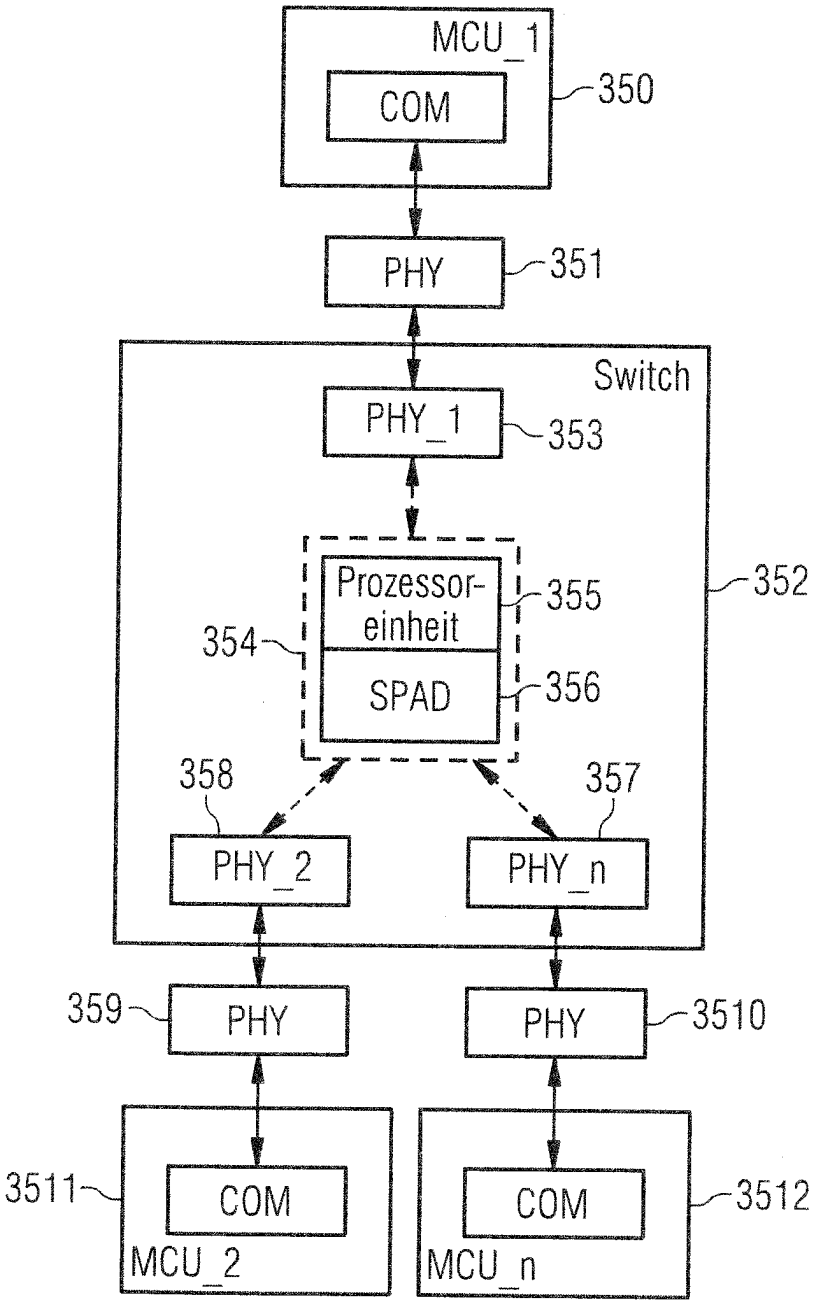

MCU_1
COM
350
PHY
351
Switch
PHY_1
353
Prozessor-
einheit
355
352
354
SPAD
356
358
357
PHY_2
PHY_n
359
PHY
PHY
3510
3511
COM
COM
3512
MCU_2
MCU_n

FIG 36

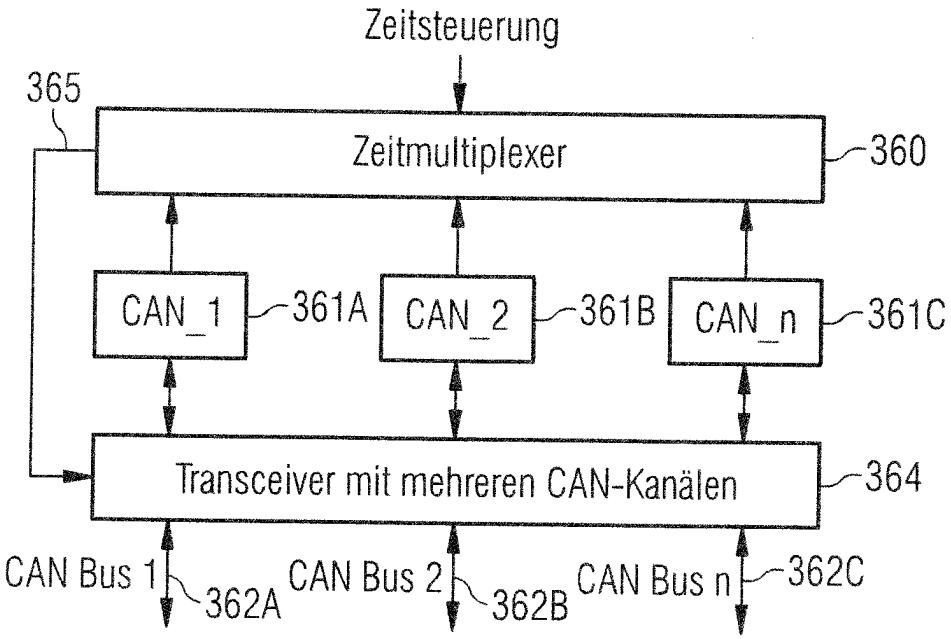
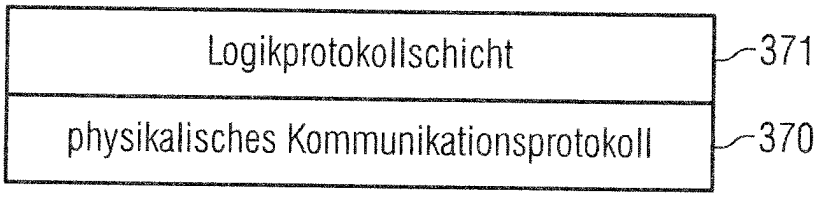

Zeitsteuerung
365
Zeitmultiplexer
360
CAN_1
361A
CAN_2
361B
CAN_n
361C
Transceiver mit mehreren CAN-Kanälen
364
CAN Bus 1
362A
CAN Bus 2
362B
CAN Bus n
362C

FIG 37


Logikprotokollschicht
371
physikalisches Kommunikationsprotokoll
370