(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
8. Oktober 2015 (08.10.2015)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2015/150534 A2

(51) Internationale Patentklassifikation: Nicht klassifiziert

(21) Internationales Aktenzeichen: PCT/EP2015/057348

(22) Internationales Anmeldedatum:
2. April 2015 (02.04.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 206 545.3 4. April 2014 (04.04.2014) DE
10 2014 219 445.8
25. September 2014 (25.09.2014) DE

(71) Anmelder: **CONTINENTAL TEVES AG & CO. OHG** [DE/DE]; Guerickestr. 7, 60488 Frankfurt (DE).

(72) Erfinder: **HECHLER, Jochen**; Heinheimer Straße 76, 64289 Darmstadt (DE). **MOLTER, Hans Gregor**; Evenaristraße 1b, 64293 Darmstadt (DE). **SÄGER, Peter**; Herrnackerstraße 7, 61381 Friedrichsdorf (DE).

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

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

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts (Regel 48 Absatz 2 Buchstabe g)*

(54) Title: SETTING DATA PROTECTION IN A VEHICLE

(54) Bezeichnung : EINSTELLUNG DES DATENSCHUTZES IM FAHRZEUG

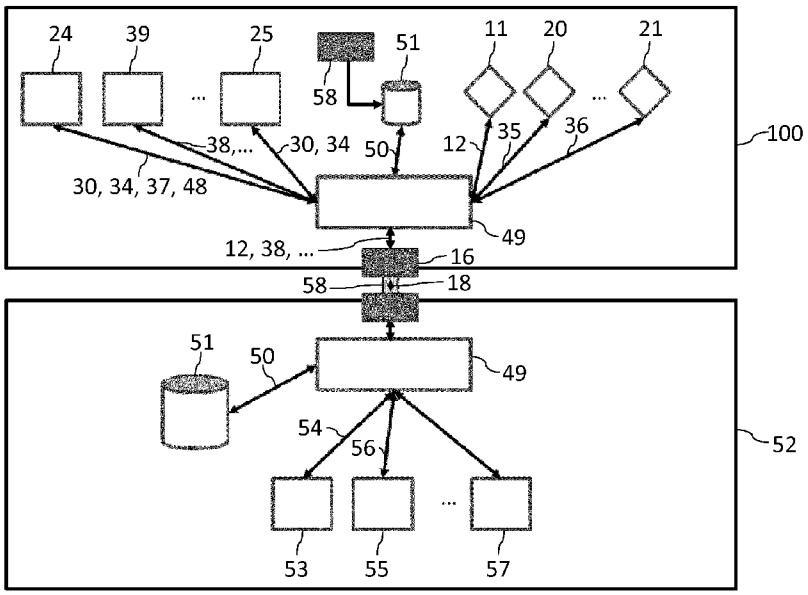


Fig. 4

(57) Abstract: The invention relates to a method for transmitting data (12, 35, 36) in a vehicle between a data source (11, 20, 21) and a signal processing device (24, 25, 39) for processing the data (12, 35, 36), said method involving: - receiving (49) the data (12, 35, 36) from the data source (11, 20, 21); - forwarding (49) the data (12, 35, 36) to the signal processing device (24, 25, 39) in accordance with an access authorization (50) that defines whether the data (12, 35, 36) is allowed to be forwarded to the signal processing device (24, 25, 39).

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Leiten von Daten (12, 35, 36) in einem Fahrzeug zwischen einer Datenquelle (11, 20, 21) und einer Signalverarbeitungseinrichtung (24, 25, 39) zur Verarbeitung der Daten (12, 35, 36), umfassend: - Empfangen (49) der Daten (12, 35, 36) aus der Datenquelle (11, 20, 21), - Weiterleiten (49) der Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) in Abhängigkeit einer Zugriffsberechtigung (50), die definiert, ob die Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) weitergeleitet werden dürfen.

WO 2015/150534 A2

Einstellung des Datenschutzes im Fahrzeug

Die Erfindung betrifft ein Verfahren zum Leiten von Daten in einem Fahrzeug zwischen einer Datenquelle und einer Signalverarbeitungseinrichtung, eine Steuervorrichtung zur Durchführung des Verfahrens und ein Fahrzeug mit der Steuervorrichtung.

Aus der DE 10 2012 112 442 A1 ist HAF genanntes hochautomatisiertes Fahren mit einem Fahrzeug bekannt. Hier werden unter anderem Daten verwendet, die aus einem Car2X-Netzwerk gennannten Fahrzeug-Ad-Hoc-Netzwerk gewonnen werden, das beispielsweise aus der WO 2010 / 139 526 A1 bekannt ist.

Es ist Aufgabe die Nutzung des hochautomatisierten Fahrens zu verbessern. Ferner ist es Aufgabe der Erfindung ist es, eine Möglichkeit aufzuzeigen, womit der Datenschutz bei Benutzung vernetzter Fahrzeuge verbessert werden kann.

Die Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Bevorzugte Weiterbildungen sind Gegenstand der abhängigen Ansprüche.

Gemäß einem ersten Aspekt der Erfindung umfasst ein Verfahren zum Leiten von Daten in einem Fahrzeug zwischen einer Datenquelle und einer Signalverarbeitungseinrichtung zur Verarbeitung der Daten die Schritte

- Empfangen der Daten aus der Datenquelle,
- Weiterleiten der Daten an die Signalverarbeitungseinrichtung in Abhängigkeit einer Zugriffsberechtigung, die definiert, ob die Daten an die Signalverarbeitungseinrichtung weitergeleitet werden dürfen.

Dem angegebenen Verfahren liegt die Überlegung zugrunde, dass das eingangs genannte hochautomatisierte Fahren technisch am besten

in dem eingangs genannten Fahrzeug-Ad-Hoc-Netzwerk realisierbar ist, weil das hochautomatisierte Fahren mit einem hohen Maß an Gefahrensicherheit realisiert werden muss. In dem Fahrzeug-Ad-Hoc-Netzwerk können die Fahrzeuge eine weitgehend ständig vernetzte Gemeinschaft bilden und sich gegenseitig oder über ein Backend bezüglich ihrer Daten aus Sensoren oder aus Applikationen beispielsweise zur Objekterkennung austauschen. Der Austausch der Daten, die grundsätzlich sowohl analog als Signale als auch digital in Form von Datenpaketen übertragen werden können, berührt jedoch auch den Datenschutz. Es wird daher mit dem angegebenen Verfahren vorgeschlagen, dem Nutzer eines Fahrzeugs grundsätzlich eine Entscheidungsmöglichkeit einzuräumen, mit der er seine persönlichen Datenschutzinteressen einerseits und den Einfluss seiner Datenschutzinteressen auf das Fahrzeug andererseits kontrollieren kann.

Hierzu wird im Rahmen des angegebenen Verfahrens eine Zugriffsberechtigung eingeführt, die beim Übertragen von Daten zwischen einer Datenquelle, wie Sensor oder einer Applikation und einer die Daten verarbeitenden Signalverarbeitungseinrichtung, wie einer Applikation, überprüft, ob die Signalverarbeitungseinrichtung zum Empfang der Daten vom Benutzer als berechtigt freigegeben wurde. Die Zugriffsberechtigung erlaubt es dem Benutzer, wie beispielsweise dem Fahrer des Fahrzeuges, sein Datenschutzbedürfnis und seinen gewünschten Funktionsumfang im Fahrzeug individuell aufeinander abzustimmen.

In einer Weiterbildung des angegebenen Verfahrens kann die Zugriffsberechtigung dabei aus einer Datenbank abgerufen werden.

In einer anderen Weiterbildung des angegebenen Verfahrens sind die Datenquelle und die Signalverarbeitungseinrichtung über eine Netzwerkverbindung getrennt. Das angegebene Verfahren sollte in diesem Zusammenhang wie eine Art gesichertes Netzwerk angewendet

werden. Hierbei können zwar alle Daten in das gesicherte Netzwerk eintreten, aber es wird sichergestellt, dass die Daten aus dem Netzwerk wieder herauskommen, die auch wirklich zur Verarbeitung freigegeben sind. Ferner wird durch das angegebene Verfahren aber auch sichergestellt, dass die aus dem gesicherten Netzwerk wieder herauskommenden Daten tatsächlich nur für die Zwecke eingesetzt werden, für die der Benutzer die Daten auch freigegeben hat.

Dabei können die Zugriffsberechtigungen an beiden Endpunkten des Netzwerkes ausgewertet werden. Auf diese Weise können die Daten ungefiltert über das Netzwerk übertragen werden, so dass auch netzwerkendseitig eine individuelle Filterung der Daten möglich ist. Dazu könnte die Zugriffsberechtigung zusammen mit den Daten übertragen werden.

Alternativ oder zusätzlich können die Zugriffsberechtigungen aber auch in mehreren, im Netzwerk verteilten Datenbanken hinterlegt werden, wobei dann sichergestellt werden sollte, dass die Zugriffsberechtigungen in den Datenbanken untereinander synchronisiert werden.

Zur Steigerung der Sicherheit umfasst das angegebene Verfahren in einer besonderen Weiterbildung den Schritt Löschen der Daten nach dem Weiterleiten in Abhängigkeit der Zugriffsberechtigung.

Gemäß einem zweiten Aspekt der Erfindung ist eine Steuervorrichtung eingerichtet, ein Verfahren nach einem der vorstehenden Ansprüche durchzuführen.

In einer Weiterbildung der angegebenen Steuervorrichtung weist die angegebene Steuervorrichtung einen Speicher und einen Prozessor auf. Dabei ist das angegebene Verfahren in Form eines Computerprogramms in dem Speicher hinterlegt und der Prozessor

zur Ausführung des Verfahrens vorgesehen, wenn das Computerprogramm aus dem Speicher in den Prozessor geladen ist.

Gemäß einem dritten Aspekt der Erfindung umfasst ein Computerprogramm Programmcodemittel, um alle Schritte eines der angegebenen Verfahren durchzuführen, wenn das Computerprogramm auf einem Computer oder einer der angegebenen Steuervorrichtungen ausgeführt wird.

Gemäß einem vierten Aspekt der Erfindung enthält ein Computerprogrammprodukt einen Programmcode, der auf einem computerlesbaren Datenträger gespeichert ist und der, wenn er auf einer Datenverarbeitungseinrichtung ausgeführt wird, eines der angegebenen Verfahren durchführt.

In einer Weiterbildung umfasst die angegebene Steuervorrichtung eine Benutzerschnittstelle zum Empfang der Zugriffsberechtigung. Auf diese Weise kann die Zugriffsberechtigung durch den Benutzer in einfacher Weise vorgegeben und auch im Nachhinein geändert werden.

Dabei kann die oben genannte Datenbank in einer besonderen Weiterbildung der angegebenen Steuervorrichtung Teil der Steuervorrichtung sein.

In einer besonders bevorzugten Weiterbildung umfasst die angegebene Steuervorrichtung eine Prüfeinrichtung zum Prüfen einer Notwendigkeit der Daten zum Betrieb der Signalverarbeitungseinrichtung, wobei die Notwendigkeit der Daten zum Betrieb der Signalverarbeitungseinrichtung auf der Benutzerschnittstelle darstellbar ist. Auf diese Weise kann der Benutzer unmittelbar sehen, welchen Einfluss seine Einstellungen und vergebenen Zugriffsberechtigungen auf das Fahrzeug haben, was Ihn bei der

Abstimmung der Datensicherheit gegenüber seinem gewünschten Funktionsumfang im Fahrzeug unterstützt.

Gemäß einem fünften Aspekt der Erfindung umfasst ein Fahrzeug einen der angegebenen Steuervorrichtungen.

Sechster Aspekt der Erfindung

Die Aufgabe wird gemäß eines sechsten Aspektes der Erfindung gelöst mit einem Verfahren zur Übermittlung von Daten zwischen einem-Kraftfahrzeug, welches zumindest einen Daten-Zugangsknoten umfasst, und wenigstens einer fahrzeugexternen Endstelle, wobei die von dem Kraftfahrzeug zu sendende Daten zumindest teilweise anonymisiert werden.

Besonders vorteilhaft sind Kombinationen aus den zur Anonymisierung der Daten genannten Verfahren mit den vorgenannten Verfahren zur Regelung der Zugriffsberechtigung. Besonders vorteilhafte Kombinationen sind unter weiteren Aspekten der Erfindung abgedeckt.

Anonymisierte Daten sind dabei Daten, welche in der Weise verändert sind, dass im Wesentlichen keine (ggf. lediglich mit erheblichem Aufwand) oder nur in begrenztem Maße Rückschlüsse auf insbesondere personen- und/oder fahrzeugbezogene Informationen möglich sind. Vorteilhafterweise kann der Datenschutz bei Benutzung vernetzter Fahrzeuge somit wesentlich verbessert werden.

Gemäß einer bevorzugten Ausführungsform der Erfindung erfolgt die Anonymisierung, bezogen auf einen Datenfluss des Kommunikationssystems, zwischen dem Daten-Zugangsknoten und einer letzten Endstelle fahrzeuginterner Daten. Ein Vorteil der dadurch erzielt wird ist, dass eine möglichst umfangreiche

Anonymisierung der Daten realisiert und die Gefahr eines Fremdzugriffs auf Daten vermindert wird.

Bevorzugt sind zumindest zwei Betriebsmodi vorgesehen, wobei in einem ersten Betriebsmodus eine teilweise Anonymisierung erfolgt und in einem zweiten Betriebsmodus eine im Wesentlichen vollständige Anonymisierung der zu sendenden Daten vorgenommen wird. In dem ersten Betriebsmodus werden fahrzeugseitig, insbesondere abgesehen von Authentifizierungsdaten, bevorzugt im Wesentlichen keine privaten Daten und in dem zweiten Betriebsmodus keine Daten gesendet. Private Daten sind bevorzugt Daten welche insbesondere durch einen Nutzer des Fahrzeugs, den Fahrzeughalter und/oder Fahrzeughersteller vorher als solche definiert wurden. Dies können beispielsweise Daten sein, welche unmittelbar einen Rückschluss auf den oder die Nutzer des Fahrzeugs zulassen würden. Gemäß einem dritten Betriebsmodus wird bevorzugt keine Anonymisierung vorgenommen und erfolgt ein im Wesentlichen freier Austausch von Daten.

Bevorzugt erfolgt zumindest in dem ersten und in dem zweiten Betriebsmodus ein Empfang von Daten. Dadurch ist es in vorteilhafter Weise möglich weiterhin Informationen, wie beispielsweise über Verkehrsmeldungen, zu erhalten.

Eine Auswahl des jeweiligen Betriebsmodus wird vorzugsweise mittels wenigstens einer Mensch-Maschine-Schnitt¬stelle vorgenommen. Nutzer eines Fahrzeugs können in vorteilhafter Weise somit Einfluss darauf nehmen, welche insbesondere personen- und/oder fahrzeugbezogenen Informationen vom Fahrzeug gesendet werden dürfen. Damit lässt sich auch die Privatsphäre im Rahmen personenindividueller Auffassung anpassen und die Akzeptanz von Fahrzeugkommunikation, beispielsweise von Internet-Diensten, Backend-Servern und/oder Fahrzeug-zu-X Kommunikation, kann unter Umständen erhöht werden.

Entsprechend einer bevorzugten Ausführungsform der Erfindung ist unabhängig von dem jeweiligen Betriebsmodus, im Falle des Auslösens eines Fahrzeug-Notrufsystems (eCall), ein Senden entsprechend notwendiger Daten möglich. In vorteilhafter Weise werden sicherheitsrelevante Maßnahmen somit nicht blockiert.

Weiterhin beschreibt die Erfindung ein Kommunikationssystem eines Kraftfahrzeugs, welches zur Übermittlung von Daten zwischen dem Kraftfahrzeug und wenigstens einer fahrzeugexternen Endstelle geeignet ist und zumindest einen Daten-Zugangsknoten umfasst, wobei wenigstens ein Anonymisierungsmittel vorgesehen ist, welches derart ausgestaltet ist, dass von dem Kraftfahrzeug zu sendende Daten zumindest teilweise anonymisiert werden. Bevorzugt handelt es sich bei dem Daten-Zugangsknoten um eine Fahrzeugantenne.

Gemäß einer bevorzugten Ausführungsform des Kommunikationssystems sind zumindest zwei Betriebsmodi vorgesehen, wobei diese in der Weise ausgestaltet sind, dass in einem ersten Betriebsmodus eine teilweise und in einem zweiten Betriebsmodus eine im Wesentlichen vollständige Anonymisierung der zu sendenden Daten erfolgt.

Das Anonymisierungsmittel ist, bezogen auf einen Datenfluss des Kommunikationssystems, besonders bevorzugt zwischen dem Daten-Zugangsknoten und einem letzten fahrzeuginternen Datenknoten vor dem Daten-Zugangsknoten angeordnet.

Vorzugsweise ist wenigstens eine Mensch-Maschine-Schnitt-stelle zur Auswahl des jeweiligen Betriebsmodus vorgesehen.
Gemäß einer bevorzugten Ausführungsform ist ein Umschalten zwischen den Anonymisierungsstufen und/oder ein Einschalten oder Ausschalten der Anonymisierung mittels der Mensch-Maschine-Schnittstelle (HMI), insbesondere mittels

zumindest einem Fahrzeugschlüssel und/oder Umschalter, vorgesehen.

Besonders bevorzugt ist das Kommunikationssystem in der Weise ausgestaltet, dass dieses das erfindungsgemäße Verfahren ausführt.

Die Erfindung beschreibt weiterhin einen Daten-Zugangsknoten, insbesondere eine Kraftfahrzeugantenne, zur Übermittlung von Daten zwischen einem Kraftfahrzeug und wenigstens einer fahrzeugexternen Endstelle, welcher ausgestaltet ist das erfindungsgemäße Verfahren auszuführen.

Siebter Aspekt der Erfindung

Die Aufgabe wird ferner gelöst gemäß einem siebten Aspekt der Erfindung betreffend ein Verfahren zum Leiten von Daten in einem Fahrzeug,
wobei Daten in einem Fahrzeug zwischen einer Datenquelle und mindestens einer Signalverarbeitungseinrichtung zur Verarbeitung der Daten geleitet werden, umfassend:

- Empfangen der Daten aus der Datenquelle mittels einer Zugriffsregel- und Kommunikationsschnittstelle
- Weiterleiten der Daten an die Signalverarbeitungseinrichtung in Abhängigkeit einer in der Zugriffsregel- und Kommunikationsschnittstelle hinterlegten Zugriffsberechtigung, die definiert, ob die Daten an die Signalverarbeitungseinrichtung weitergeleitet werden dürfen,

wobei die zu verarbeiteten Daten mittels der Zugriffsregel- und Kommunikationsschnittstelle zumindest teilweise anonymisiert werden.

Die Erfindung beruht dabei auf der Erkenntnis, dass zusätzlich zu einer Einführung einer Zugriffsberechtigungskontrolle eine

Anonymisierung der Daten dem Fahrer gegenüber den Vorteil bietet die vollständige Funktionsfähigkeit der Signalverarbeitungseinrichtungen aufrecht halten zu können und gleichzeitig seine Privatsphäre wahren zu können.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das Verfahren durch die Schritte weitergebildet:

- Empfangen von verarbeiteten Daten von der Signalverarbeitungseinrichtung mittels der Zugriffsregel- und Kommunikationsschnittstelle, und
- Weiterleiten der verarbeiteten Daten an eine externe Endstelle. Die Anonymisierung kann auf diese Weise auf die an externe Endstellen weitergeleitete Daten eingeschränkt werden.

Auf diese Weise bleibt die Privatsphäre gegenüber dritten gewahrt und gleichzeitig kann die fahrzeuginterne Weiterleitung von Daten zumindest aus funktionaler Sicht weitestgehend unberührt bleiben.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das Verfahren dadurch weitergebildet, dass der Austausch von Daten zwischen der Datenquelle, der Signalverarbeitungseinrichtung sowie zwischen der Signalverarbeitungseinrichtung und der Endstelle ausschließlich über die Zugriffsregel- und Kommunikationsschnittstelle erfolgt. Auf diese Weise können Umgehungen des Sicherheitskonzeptes erschwert werden.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das Verfahren dadurch weitergebildet, wobei zumindest zwei Betriebsmodi vorgesehen sind, wobei in einem ersten Betriebsmodus eine teilweise Anonymisierung erfolgt und in einem zweiten Betriebsmodus eine im Wesentlichen vollständige Anonymisierung der zu sendenden Daten vorgenommen wird. Auf diese Weise wird eine flexiblere Einstellbarkeit des Datenzugriffs ermöglicht.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das Verfahren dadurch weitergebildet, dass der zu verwendende Betriebsmodus in Abhängigkeit der Endstelle ausgewählt wird. Viele Komfortfunktionen eines Fahrzeugs können auf diese Weise realisiert werden ohne auf die Privatsphäre verzichten zu müssen.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das Verfahren dadurch weitergebildet, dass die Zugriffsregel- und Kommunikationsschnittstelle ein weiterleiten von Kombinationen aus mehreren Daten der Datenquelle an eine jeweilige Signalverarbeitungseinrichtung nur teilweise zulässt oder unterbindet. Die Anonymisierung von Daten kann auf diese Weise einfach realisiert werden, indem solche Kombinationen von Daten, die einen Rückschluss auf persönliche Profile ermöglichen, unterbunden werden. Solche Kombinationen könnten beispielsweise Geschwindigkeit des Fahrzeugs und dessen Position sein, aus der ein genaues Bewegungsprofil erstellbar ist. Für einige Signalverarbeitungseinrichtungen ist es denkbar, dass zum Ausführern ihrer Funktion nur Teile der Daten obligatorisch sind, so dass in solchem Falle so wenig Daten wie möglich übermittelt werden.

Die Aufgabe wird ferner gelöst mittels eines achten Aspektes der Erfindung betreffend ein System zum Leiten von Daten in einem Fahrzeug, aufweisend

- eine Datenquelle zum Empfangen und Generieren von Fahrzeugdaten,
- mindestens eine Signalverarbeitungseinrichtung zur Verarbeitung der Daten,
- eine Zugriffsregel- und Kommunikationsschnittstelle umfassend,

wobei die Datenquelle und die Signalverarbeitungseinrichtung mittels der Zugriffsregel- und Kommunikationsschnittstelle gekoppelt sind und ein weiterleiten der Daten an die Signal-

verarbeitungseinrichtung oder an eine externe Endstelle nur in Abhängigkeit einer an der Schnittstelle hinterlegten Zugriffsberechtigung erfolgt, die definiert, ob die Daten an die Signalverarbeitungseinrichtung weitergeleitet werden dürfen.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das System dadurch weitergebildet, dass an der Schnittstelle ferner eine Identifizierungsberechtigung hinterlegt ist, wobei die Identifizierungsberechtigung zumindest zwei Betriebsmodi vorgesehen sind, wobei in einem ersten Betriebsmodus eine teilweise Anonymisierung erfolgt und in einem zweiten Betriebsmodus eine im Wesentlichen vollständige Anonymisierung der zu sendenden Daten vorgenommen wird.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das System dadurch weitergebildet, dass das Systeme eine Mensch Maschine Schnittstelle zum Einstellen der Zugriffsberechtigung und der Identifizierungsberechtigung aufweist.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird das System dadurch weitergebildet, dass die Datenquellen in einem Fahrzeug verbaute Sensoren sind und mittels der Mensch-Maschineschnittstelle eine fahrzeuginterne Verarbeitung der Sensordaten oder ein Weiterleiten der Sensordaten an eine externe Endstelle anhand der Einstellung der Zugriffsberechtigung und Identifizierungsberechtigung einstellbar ist.

Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit der folgenden Beschreibung der Ausführungsbeispiele, die im Zusammenhang mit den Zeichnungen näher erläutert werden, wobei:

Fig. 1 eine Prinzipdarstellung eines auf einer Straße fahrenden Fahrzeuges,

Fig. 2 eine Prinzipdarstellung des Fahrzeuges der Fig. 1,

Fig. 3 eine Prinzipdarstellung eines Fahrzeug-Ad-Hoc-Netzwerkes, an dem das Fahrzeug der Fig. 1 und 2 teilnehmen kann,

Fig. 4 eine Prinzipdarstellung eines Kommunikationssystems,

Fig. 5 eine Prinzipdarstellung einer Benutzerschnittstelle zur Definition von Zugriffsberechtigungen in dem Kommunikationssystem der Fig. 4 in einem ersten Zustand,

Fig. 6 eine Prinzipdarstellung einer Benutzerschnittstelle zur Definition von Zugriffsberechtigungen in dem Kommunikationssystem der Fig. 4 in einem ersten Zustand,

Fig. 7 eine Prinzipdarstellung einer Benutzerschnittstelle zur Definition von Zugriffsberechtigungen in dem Kommunikationssystem der Fig. 4 in einem ersten Zustand zeigen, und

Fig. 8 zwei bevorzugte Ausführungsbeispiele des sechsten Aspektes der Erfindung mit unterschiedlichen Anonymisierungspositionen.

In den Figuren werden gleiche technische Elemente mit gleichen Bezugszeichen versehen und nur einmal beschrieben.

Die Erfindung soll nachstehend innerhalb eines in Fig. 3 gezeigten Fahrzeug-Ad-Hoc-Netzwerkes näher erläutert werden, das nachstehend der Einfachheit halber Car2X-Netzwerk 1 genannt wird. Zur besseren Verständlichkeit des technischen Hintergrundes zu diesem Car2X-Netzwerk 1 soll zunächst ein nicht einschränkendes Anwendungsbeispiel zu diesem Car2X-Netzwerk 1 gegeben werden, bevor auf technische Einzelheiten zu diesem näher eingegangen wird.

Es wird daher auf Fig. 1 Bezug genommen, die eine Prinzipdarstellung eines auf einer Straße 2 fahrenden Fahrzeuges 3 zeigt.

In der vorliegenden Ausführung soll sich auf der Straße 2 eine Fußgängerüberführung 4 befinden, an der mittels einer Ampel 5 geregelt wird, ob das Fahrzeug 3 oder gegebenenfalls die Fahrzeuge 8 und/oder 9 auf der Straße 2 die Fußgängerüberführung 4 überqueren darf oder ein nicht weiter dargestellter Fußgänger auf der Fußgängerüberführung 4 die Straße 2. Zwischen der Fußgängerüberführung 4 und der Ampel 5 befindet sich im Rahmen der vorliegenden Ausführung ein Hindernis in Form einer Kurve 9, die die Fußgängerüberführung 4 dem Fahrer des Fahrzeuges 3 sowie einer noch zu beschreibenden Umfeldsensorik des Fahrzeuges 3 gegenüber verdeckt.

In einer Fahrtrichtung 7 vor dem Fahrzeug 3 ist in Fig. 1 ein weiteres Fahrzeug 8 dargestellt, das mit einem gepunktet dargestellten Fahrzeug 9 auf der Fußgängerüberführung 4 in einen Verkehrsunfall 10 verwickelt ist und die Fahrspur in Fahrtrichtung 7 des Fahrzeuges 3 blockiert.

Die Fußgängerüberführung 4 und der Verkehrsunfall 10 stellen Gefahrensituationen auf der Straße 2 dar. Übersieht der Fahrer des Fahrzeuges 3 die Fußgängerüberführung 4 und hält vor dieser

damit regelwidrig nicht an, so könnte er einen die Fußgängerüberführung 4 überquerenden Fußgänger erfassen, der beim Überqueren der Fußgängerüberführung 4 auf das regelkonforme Verhalten des Fahrers des Fahrzeuges 3 vertraut. In beiden Gefahrensituationen muss der Fahrer des Fahrzeuges 3 das Fahrzeug 3 anhalten, um eine Kollision mit dem Gefahrenobjekt in der Gefahrensituation, also dem Fußgänger und/oder dem weiteren Fahrzeug 8 zu vermeiden. Hierzu kann das Car2X-Netzwerk 1 verwendet werden, worauf an späterer Stelle näher eingegangen wird.

Das Fahrzeug 3, wie in Figur 2 gezeigt, weist in der vorliegenden Ausführung einen Empfänger 11 für ein globales Satellitennavigationssystem, nachstehend GNSS-Empfänger 11 genannt auf, über den das Fahrzeug 3 in einer an sich bekannten Weise Positionsdaten in Form seiner absoluten geographischen Lage 12 bestimmen und beispielsweise im Rahmen eines Navigationssystems 13 nutzen kann, um diese auf einer nicht weiter dargestellten geographischen Karten anzuzeigen. Entsprechende Signale 14 des Globalen Satellitennavigationssystems, nachstehend GNSS-Signale 14 genannt, können beispielsweise über eine entsprechende GNSS-Antenne 15 empfangen und in an sich bekannter Weise an den GNSS-Empfänger 11 weitergeleitet werden.

Das Fahrzeug weist in der vorliegenden Ausführung ferner einen Transceiver 16 auf, über den das Fahrzeug 3 als Knoten am Car2X-Netzwerk 1 teilnehmen und mit anderen Knoten, wie beispielsweise dem weiteren Fahrzeug 8 und/oder der Ampel 5 nachstehend Car2X-Nachrichten 17 genannte Nachrichten austauschen kann. Dieser Transceiver 16 soll zur Abgrenzung gegenüber dem GNSS-Empfänger 11 nachstehend Car2X-Transceiver 16 genannt werden.

In den über das Car2X-Netzwerk 1 ausgetauschten Car2X-Nachrichten 17, können die einzelnen Knoten 3, 5, 8 untereinander verschiedene Informationen beschreibende Daten austauschen mit denen beispielsweise die Verkehrssicherheit auf der Straße 2 erhöht werden kann. Ein Beispiel für die Informationen, die mit den Daten in den Car2X-Nachrichten 17 ausgetauscht werden können, wäre die über den GNSS-Empfänger 11 bestimmte absolute geographische Lage 12 des jeweiligen Knotens 3, 5, 8 des Car2X-Netzwerkes 1. Derartige Daten können auch als Positionsdaten bezeichnet werden. Ist der die geographische Lage 12 empfangende Knoten 3, 5, 8 des Car2X-Netzwerkes 1 ein Fahrzeug, wie beispielsweise das nicht am Verkehrsunfall 10 beteiligte Fahrzeug 3 und das am Verkehrsunfall 10 beteiligte Fahrzeug 8 dann kann die über das Car2X-Netzwerk 1 empfangene geographische Lage 12 beispielsweise auf dem Navigationssystem 13 des empfangenden Fahrzeuges 3, 8 zur Darstellung beispielsweise der Verkehrsbewegung verwendet werden. Wird neben der absoluten geographischen Lage 12 auch der Verkehrsunfall 10 als Information mit den Daten in der Car2X-Nachricht 17 beschrieben, so können bestimmte Verkehrssituationen, wie beispielsweise der Verkehrsunfall 10 auf Navigationssystem 13 konkreter dargestellt werden. Auf weitere mögliche mit den Car2X-Nachrichten 17 austauschbare Informationen wird später im Rahmen der Fig. 2 näher eingegangen.

Zum Austausch der Car2X-Nachrichten 17 moduliert der Car2X-Transceiver 16 entweder eine Car2X-Nachricht 17 auf ein nachstehend Car2X-Signal 18 genanntes Übertragungssignal und versendet es über eine nachstehend Car2X-Antenne 19 genannte Antenne an die anderen Knoten 3, 5, 8 im Car2X-Netzwerk 1 oder er empfängt über die Car2X-Antenne 19 ein Car2X-Signal 18 und filtert aus diesem die entsprechende Car2X-Nachricht 17 heraus. Darauf wird an späterer Stelle im Rahmen der Fig. 3 näher eingegangen. In Fig. 1 ist dabei dargestellt, dass der

Car2X-Transciever 16 eine Car2X-Nachricht 17 an das Navigationssystem 13 unter der Annahme ausgibt, dass diese in der oben beschriebenen Weise Informationen enthält, die auf diesem darstellbar sind. Das ist jedoch nicht einschränkend zu verstehen. Insbesondere kann zweckmäßigerweise auch der GNSS-Empfänger 11 direkt oder, wie in Fig. 2 gezeigt, indirekt mit dem Car2X-Transceiver 16 verbunden sein, um die eigene absolute geographische Lage 12 im Car2X-Netzwerk 1 zu versenden.

Die Struktur der Car2X-Nachricht 17 sowie des Car2X-Signals 18 und damit der Aufbau des Car2X-Netzwerkes können in einem Kommunikationsprotokoll definiert werden. Es gibt bereits derartige Kommunikationsprotokolle länderspezifisch unter anderem im Rahmen der ETSI TC ITS bei ETSI in Europa und im Rahmen der IEEE 1609 bei IEEE sowie bei SAE in den Vereinigten Staaten von Amerika. Weitere Informationen hierzu lassen sich in den genannten Spezifikationen finden.

Das Fahrzeug 3 soll im Rahmen des vorliegenden Ausführungsbeispiels eine Funktion mit dem Namen hochautomatisiertes Fahren, nachstehend HAF-Funktion genannt besitzen. Hierfür ist an dem Fahrzeug 3 eine Vielzahl weiterer Sensoren, wie die oben genannte Umfeldsensorik in Form einer Kamera 20 und eines Radarsensors 21 vorhanden. Mit der Kamera 20 kann das Fahrzeug 3 innerhalb eines Bildwinkels 22 ein Bild einer Ansicht aufnehmen, die in Fahrtrichtung 7 des Fahrzeuges 3 betrachtet vor dem Fahrzeug 3 liegt. Zudem kann das Fahrzeug 3 mit dem Radarsensor 21 und entsprechenden Radarstrahlen 23 in Fahrtrichtung 7 des Fahrzeuges 3 betrachtet Objekte erkennen und in einer an sich bekannten Weise den Abstand zum Fahrzeug 3 bestimmen.

Um die HAF-Funktion zu konkretisieren, soll nachstehend zunächst auf den Aufbau des Fahrzeuges 3 beispielhaft anhand des Fahrzeuges 3 eingegangen werden. Neben dem Fahrzeug 3 können auch

die anderen Fahrzeuge 8 und9 auf der Straße 2 in dieser Weise aufgebaut sein. Das Fahrzeug 3 besitzt verschiedene die Sensorsignale verarbeitende Applikationen, von denen in Fig. 2 eine HAF-Applikation 24 und eine an sich bekannte Fahrdynamikregelung 25 gezeigt ist. Während für die HAF-Applikation 24 auf die DE 10 2012 112 442 A1 mit weiteren Nachweisen verwiesen wird, können der DE 10 2011 080 789 A1 Details zur Fahrdynamikregelung 25 entnommen werden.

Das Fahrzeug 3 umfasst ein Chassis 26 und vier Räder 27. Jedes Rad 27 kann über eine ortsfest am Chassis 26 befestigte Bremse 28 gegenüber dem Chassis 26 verlangsamt werden, um eine Bewegung des Fahrzeuges 3 auf der Straße 2 zu verlangsamen.

Dabei kann es in einer dem Fachmann bekannten Weise passieren, dass die Räder 27 des Fahrzeugs 3 ihre Bodenhaftung verlieren und sich das Fahrzeug 3 sogar von einer durch ein noch zu beschreibendes Lenksignal 48 vorgegebenen Trajektorie durch Untersteuern oder Übersteuern wegbewegt. Dies wird durch die Fahrdynamikregelung 25 vermieden.

In der vorliegenden Ausführung weist das Fahrzeug 4 dafür Drehzahlsensoren 29 an den Rädern 27 auf, die eine Drehzahl 30 der Räder 27 erfassen.

Basierend auf den erfassten Drehzahlen 30 kann ein Regler 31 in einer dem Fachmann bekannten Weise bestimmen, ob das Fahrzeug 3 auf der Fahrbahn rutscht oder sogar von der oben genannten vorgegebenen Trajektorie abweicht und entsprechend mit einem an sich bekannten Reglerausgangssignal 32 darauf reagieren. Das Reglerausgangssignal 32 kann dann von einer Stelleinrichtung 33 verwendet werden, um mittels Stellsignalen 34 Stellglieder, wie die Elektromotoren 28 anzusteuern, die auf das Rutschen und die

Abweichung von der vorgegebenen Trajektorie in an sich bekannter Weise beispielsweise im Rahmen des Torque-Vectoring reagieren.

Der HAF-Applikation 24 kann über die Kamera 20 erfasste Bilddaten 35 und über den Radarsensor 21 erfasste Abstandsdaten 36 zu Objekten wie Fahrzeugen in Fahrtrichtung 7 vor dem Fahrzeug 3, Spurstreifen auf der Straße 2 und so weiter auswerten und basierend darauf die Situationen auf der Straße 2 erfassen. Dabei soll die HAF-Applikation 24 durch die Ausgabe von Steuersignalen in das Fahrzeug 3 eingreifen und seine Bewegung auf der Straße derart regeln, dass es innerhalb der zuvor genannten Spurstreifen auf der Straße 2 fährt, Hindernissen wie dem Unfall 10 in sicherheitskonformer Weise ausweicht oder an nicht gezeigten Kreuzungen anhält. Zu den zuvor genannten Steuersignalen zählt beispielsweise ein Antriebssignal 37 mit dem die Elektromotoren 28 zum Vortrieb des Fahrzeuges 3 in Fahrtrichtung angetrieben werden, das Lenksignal 48, um das Fahrzeug 3 auf der Spur der Straße 2 zu halten und/oder Hindernissen, wie dem Unfall 10 auszuweichen sowie ein nicht gezeigtes Bremssignal, um eine nicht gezeigte Bremsanlage des Fahrzeuges 3 zum Abbremsen des Fahrzeuges 3 anzusteuern. Darüber hinaus können in der HAF-Applikation 24 auch die zuvor genannten Car2X-Botschaften 17 ausgewertet werden, die weitere wertvolle Informationen zur Steuerung des Fahrzeuges 3 auf der Straße 2 liefern.

Anders herum kann jedes Mal, die Fahrdynamikregelung 25 über die Stelleinrichtung 33 in das Fahrzeug 4 eingreift, beispielsweise die Stelleinrichtung 33 ein in Fig. 2 gepunktet dargestelltes Berichtssignal 38 ausgeben. Ein derartiges Berichtssignal 38 kann von einer beliebigen Instanz im Fahrzeug 3, also beispielsweise auch vom Regler 31 der Fahrdynamikregelung 25 erzeugt werden. Eine Nachrichtenerzeugungseinrichtung 39 könnte dann basierend auf dem Berichtssignal 38, der absoluten geo-

graphischen Lage 12 und einem in Fig.3 gezeigten aus einem Zeitgeber 40 ausgegebenen Zeitstempel 41 eine Car2X-Nachricht 17 erzeugen, mit der der Eingriff der Fahrdynamikregelung 25 als Information über das Car2X-Netzwerk 1 den anderen Knoten 5, 8 berichtet werden kann. Die so erzeugte Car2X-Nachricht 17 könnte dann über die Car2X-Antenne 19 im Car2X-Netzwerk 1 versendet werden.

Es wird an dieser Stelle noch einmal darauf verwiesen, dass die in den Car2X-Nachrichten 17 ausgetauschten Information über die absolute geographische Lage 12 der einzelnen Knoten 3, 5, 8 und/oder über Ereignisse wie der Verkehrsunfall 10 und/oder wie ein Eingriff der Fahrdynamikregelung 25 auf dem Navigationssystem 13 wie bereits in Fig. 1 ausgeführt auch zu anderen Zwecken verwendet werden können. Beispielsweise könnten sie zur Orientierung des Fahrers dargestellt werden oder beispielsweise im Rahmen von Verkehrskontrollen durch die Polizei ausgewertet werden, die dann ein nicht regelkonformes durch den Fahrer des Fahrzeuges 3 feststellen kann. Die in den Car2X-Nachrichten 17 versendeten Informationen sind daher grundsätzlich für jedermann zugänglich, auch wenn es sich um Informationen handelt, die der Fahrer des Fahrzeuges 3 eigentlich nicht mit anderen Verkehrsteilnehmern oder anderen potentiellen Empfängern teilen möchte. Darauf wird an späterer Stelle näher eingegangen.

Nachstehend soll anhand der Fig. 3 die Übertragung einer Car2X-Nachricht 17 über das Car2X-Netzwerk 1 erläutert werden, das in Fig. 3 der Übersichtlichkeit halber mit einer Wolke angedeutet ist. Als Inhalt der Car2X-Nachricht 17 kann beispielsweise eine Auslösung eines Insassenschutzmittels, wie beispielsweise ein Airbag im am Verkehrsunfall 10 beteiligten Unfall-Fahrzeug 8 angenommen werden.
Wie bereits erläutert kann die Nachrichtenerzeugungseinrichtung 39 basierend auf dem Berichtssignal 38, der absoluten

geographischen Lage 12 und dem Zeitstempel 41 die Car2X-Nachricht 17 gemäß dem oben erwähnten Kommunikationsprotokoll erzeugen. Grundsätzlich können in einer Car2X-Nachricht 17 jedoch beliebige Signale und damit Daten aus dem Fahrzeug 2 berichtet werden, wobei der oben genannte Standard das Format vorgibt, wie diese Signale und damit Daten berichtet werden. Die Nachrichtenerzeugungseinrichtung 39 kann dabei prinzipiell auch Teil des Car2X-Transceivers 16 sein.

Aus der Car2X-Nachricht 17 werden in dem Car2X-Transceiver 16 des Unfall-Fahrzeuges 8 in einer Datenpaketerzeugungseinrichtung 42 Datenpakete 43 erzeugt. Durch das Erzeugen von Datenpaketen 43 können Car2X-Nachrichten 17 aus verschiedenen Anwendungen in dem Unfall-Fahrzeug 8 zu einem einzigen Datenstrom zusammengefasst werden, um das Car2X-Signal 18 zu erzeugen. Die Datenpaketerzeugungseinrichtung 42 entspricht daher einer Netzwerk- und Transportschicht (eng. network and transport layer), deren Aufgabe es bekanntlich ist die Netzwerkdaten aus verschiedenen Anwendungen zu routen. Der Aufbau der Datenpaketerzeugungseinrichtung 42 ist von der oben genannten Spezifikation des Kommunikationsprotokolls für das Car2X-Netzwerk 1 abhängig.

Die generierten Datenpakete 43 werden in einer Modulationseinrichtung 44 auf das Car2X-Signal 18 aufmoduliert und im Car2X-Netzwerk 1 drahtlos versendet. Die Modulationseinrichtung 44 entspricht daher einer Schnittstellenschicht, deren Aufgabe es ist, das Unfall-Fahrzeug 8 physikalisch an das Car2X-Netzwerk 1 anzubinden. Auch der Aufbau der Modulationseinrichtung 44 ist von der oben genannten Spezifikation des Kommunikationsprotokolls für das Car2X-Netzwerk 1 abhängig.

Auf Seiten des nicht am Verkehrsunfall 10 beteiligten Fahrzeuges 3 kann das vom Unfall-Fahrzeug 8 versendete Car2X-Signal 18 dann über die Car2X-Antenne 19 empfangen werden.

Um die Car2X-Nachricht 17 aus dem Car2X-Signal 18 zu extrahieren weist der Car2X-Transceiver 16 des Fahrzeuges 3 eine Demodulationseinrichtung 45 auf, die die senderseitige Modulation der Datenpakete 43 in an sich bekannter Weise rückgängig macht. Entsprechend kann eine Nachrichtenextraktionseinrichtung 46 die Car2X-Nachrichten 17 aus den Datenpaketen 43 extrahieren und den Anwendungen im Fahrzeug 3, wie dem Navigationssystem 13 oder auch der Stelleinrichtung 33 zur Verfügung stellen. Letztendlich stellen die Demodulationseinrichtung 45 und die Nachrichtenextraktionseinrichtung 46 die empfangsseitigen Gegenstücke entsprechend der oben genannten Netzwerk und Transportschicht und der Schnittstellenschicht dar und sind ebenfalls von der oben genannten Spezifikation des Kommunikationsprotokolls für das Car2X-Netzwerk 1 abhängig.

Zu Details der einzelnen Netzwerkschichten wird daher auf die einschlägigen Spezifikationen verwiesen.

Wie aus den zuvor erläuterten Ausführungen ersichtlich, sind die an dem Car2X-Netzwerk 1 teilnehmenden Fahrzeuge 3, 8 für alle Teilnehmerknoten in dem Car2X-Netzwerk 1 transparent. Möchte der Fahrer einer der Fahrzeuge 3, 8 jedoch nicht, dass bestimmte Daten übertragen werden so hat er grundsätzlich nur die Möglichkeit, sein Fahrzeug 3 vom Car2X-Netzwerk 1 zu trennen. Die Trennung vom Car2X-Netzwerk könnte aber die Funktion der HAF-Applikation 24 einschränken, wenn nicht sogar vollständig blockieren.

Zur Figur 4

Hier greift das vorliegende Ausführungsbeispiel mit dem Vorschlag an, für die einzelnen Sensoren 11, 20, 21 und Anwendungen 16, 24, 25 in dem Fahrzeug 3 der Fig. 2 sogenannte Privacy Box 49 zu schaffen, über die der Datenaustausch innerhalb des Fahrzeuges 3 zwischen den einzelnen Komponenten und auch der Datenaustausch über das Car2X-Netzwerk geregelt wird. Dies soll nachstehend anhand von Fig. 4 näher erläutert werden.

Figur 4 zeigt dabei ein Kommunikationssystem 100 umfassend mehrere Datenquellen, die als Sensoren 11, 20, 21 ausgeführt sind, und mehrere Signalverarbeitungseinrichtungen 24, 25, 39, die als Applikationen ausgeführt sind.

Vorzugsweise handelt es sich bei der Privacy Box 49 um eine Zugriffsregel- und Kommunikationsschnittstelle. Dieser kann beispielsweise mit einem persistenten Datenspeicher ausgestattet sein, in dem die festgelegten Zugriffsregeln bzw. Datenschutzeinstellungen verschlüsselt gespeichert sind. Nachfolgend wird hierfür der einfachkeitshalber der Begriff Privacy Box verwendet.

Innerhalb des Fahrzeuges 3 kann grundsätzlich zwischen Applikationen 24, 25, 39 und Sensoren 11, 20, 21 unterschieden werden.

Unter Sensoren 11, 20, 21 sollen nachstehend technische Elemente im Fahrzeug 3 verstanden werden, die eine beliebige physikalische Größe oder eine andere Zustandsgröße im oder außerhalb des Fahrzeuges 3 aufnehmen und durch Sensordaten 12, 35, 36 beispielsweise in Form eines Sensorsignals beschreiben. In Fig. 4 sind derartige Sensoren durch auf die Spitze gestellte Quadrate angedeutet.

Demgegenüber sollen unter Applikationen 24, 25, 39 technische Einrichtungen im Fahrzeug 3 verstanden werden, die Sensordaten 12, 35, 36 und andere Daten im Fahrzeug 3 aufnehmen, verarbeiten und auf die Verarbeitung in einer bestimmten Weise reagieren. Die HAF-Applikation 24 steuert beispielsweise als Reaktion auf die Sensorsignale 30, 34 das Fahrzeug 3, während die Fahrdynamikregelung 25 als Applikation das Fahrzeug 3 in Reaktion auf die Raddrehzahlsignale 30 stabilisiert und die Nachrichtenerzeugungseinrichtung 39 bestimmte Zustände im Fahrzeug basierend auf dem Berichtssignal 38 ins Car2X-Netzwerk 1 meldet. Die Reaktion erfolgt in der Regel durch Ausgabedaten aus den einzelnen Applikationen 24, 25, 39 mit denen entweder in die Aktoren des Fahrzeuges 3 eingegriffen wird und/oder mit denen andere Applikationen des Fahrzeuges 3 ansteuerbar sind. In Fig. 4 sind Applikationen durch auf der Seite liegende Quadrate angedeutet. Weitere Beispiele für Applikationen im Fahrzeug 3 können ein Stauassistent, eine Schildererkennung, eine automatische Geschwindigkeitsübertretungs-Verwarngebühr-Abbuchung sein, die im Falle einer durch die Polizei erkannten Geschwindigkeitsübertretung automatisch eine fällige Verwarngebühr vom Konto des Fahrers abbucht.

Eine eindeutige Trennung zwischen Sensoren und Applikationen ist nicht immer möglich, denn der Car2X-Transceiver 16 kann sowohl als Sensor angesehen werden, der ein Car2X-Signal 18 im Car2X-Netzwerk 1 erfasst und als Sensordaten die Car2X-Botschaften 17 ausgibt. Er kann aber auch als Applikation angesehen werden, die auf im Fahrzeug 3 generierte Car2X-Botschaften 17 mit der Generierung der Datenpakete 41 als Ausgangsdaten und der Versendung der Ausgangsdaten in dem Car2X-Signal 18 im Car2X-Netzwerk 1 reagiert. Betont werden soll an dieser Stelle, dass die Ausgangsdaten aus Applikationen in anderen Applikationen weiterverwendet werden können, wie beispielsweise im Fall der zuvor genannten Schildererkennung.

Gibt die Schildererkennung ein erkanntes Verkehrsschild auf der Straße in seinen Ausgangsdaten aus, können diese Ausgangsdaten in der HAF-Applikation 24 der Steuerung des Fahrzeuges 3 zugrunde gelegt werden.

Die oben genannte Privacy Box 49 filtert nun den Datenverkehr zwischen den Sensoren 11, 20, 21 und den Applikationen 24, 25, 39 im Fahrzeug 3 untereinander. Hierbei kann der Benutzer beispielsweise vorgeben, welche Daten aus den einzelnen, an die PrivacyBox 49 angeschlossenen Sensoren und Applikationen wohin weitergeleitet werden dürfen oder nicht bzw. welche Applikationen auf Daten der Sensoren zugreifen dürfen oder nicht. Das Weiterleiten wird mit sogenannten Zugriffberechtigungen 50 gesteuert, die in einer noch zu beschreibenden Weise in einer Datenbank 51 hinterlegt werden können. Prinzipiell könnten Daten auch an Sensoren weitergeleitet werden. Der Übersichtlichkeit halber soll nachstehend aber von einem Szenario ausgegangen werden, in dem Daten aus Sensoren und/oder Applikationen nur an andere Applikationen weitergeleitet werden.

Zugriffsberechtigungen 50 können dabei grundsätzlich in zwei verschiedenen Weisen vergeben werden. Einerseits kann die Weiterleitung von Daten aus einem Sensor 24, 25, 39 und/oder einer Applikation 11, 20, 21 grundsätzlich abgelehnt werden. Aus Sicht des Systems wird der jeweilige Sensor und/oder die jeweilige Applikation faktisch abgeschaltet. Andererseits kann die Weiterleitung von Daten aber auch dediziert zugelassen werden, so dass die Weiterleitung von Daten innerhalb des Fahrzeuges 3 und/oder innerhalb des Car2X-Netzwerkes 1 nur an bestimmte Applikationen im Fahrzeug 3 zugelassen wird.

Darüber hinaus kann die Privacy Box auch eine Identifikationsberechtigung umfassen, womit einstellbar ist, ob über die

Privacy Box weitergeleitete Daten zumindest teilweise anonymisiert werden oder nicht.

So kann ein Fahrer beispielsweise grundsätzlich einer Weiterleitung seiner Geschwindigkeit aus einem in Fig. 2 nicht zu sehenden Geschwindigkeitssensor des Fahrzeuges 3 beispielsweise an die HAF-Applikation 24 zustimmen. Er kann aber dediziert die Weiterleitung der Geschwindigkeit als Daten an die automatische Geschwindigkeitsübertretungs-Verwarngebühr- Abbuchungsapplikation blockieren. Hier zeigt sich das grundsätzliche Potential PrivacyBox 49, denn wäre der Fahrer gezwungen, den Geschwindigkeitssensor des Fahrzeuges 3 vollständig abzuschalten, so dass damit auch die HAF-Applikation 24 nicht mehr funktionieren würde.

Alternativ könnte der Fahrer des Fahrzeuges 3 auch eine anonyme Fahrt mit dem Fahrzeug 3 machen wollen. Hierfür kann er die Weiterleitung seiner geographischen Lage 12 als Daten aus dem GNSS-Empfänger 11 grundsätzlich ausstellen. Die PrivacyBox 49 verhindert dann die Weiterleitung. Im Gegenzug, würden dann aber eine Reihe von Applikationen nur noch eingeschränkt oder nicht mehr zur Verfügung stehen, wie beispielsweise die Nachrichtenerzeugungseinrichtung 39, die zur Erzeugung von Car2X-Nachrichten 38 die geographische Lage 12 benötigt, oder das Navigationssystem, das die geographische Lage 12 zur Darstellung auf einer Karte benötigt.

Das zweite genannte Beispiel ist in der PrivacyBox 49 leicht zu realisieren, indem die Daten der betreffenden Sensoren und/oder Applikationen grundsätzlich blockiert werden.

Das erste Beispiel ist aber der Hauptanwendungsfall, der zudem geregelt werden muss, wenn Daten oder Reaktionen enthaltende Signale an einem Teilnehmerknoten im Car2X-Netzwerk 2, wie einem

anderen Fahrzeug 8, 9 oder einem anderen Backend 52, wie beispielsweise einem Datenserver dediziert weitergeleitet werden sollen. Der Datenserver 52 kann beispielsweise ein Server sein, auf dem verschiedene Applikationen laufen, wie beispielsweise eine Kartenupdateapplikation 53, über die das Navigationssystem 13 aktualisierte Kartendaten 54 abrufen kann. Eine weitere Applikation wäre eine Protokollupdateapplikation 55, mit dessen Updatedaten 56 der der Car2X-Transceiver 16 im Fahrzeug 3 sein Netzwerkprotokoll aktualisieren kann. Es können zahlreiche weitere Updateapplikationen 57 vorhanden sein, auf die nachstehend nicht weiter eingegangen werden soll.

Möchte der Fahrer des Fahrzeuges 3, dass seine Daten aus dem Fahrzeug 3 nur an bestimmte Applikationen 53, 55, 57 im Backend 52 weitergeleitet werden, müssen grundsätzlich alle Daten über eine gesicherte Verbindung 58 zum Backend 52 geleitet werden. Das Backend 52 muss dann intern in einer eigenen PrivacyBox 49 über die dedizierte Weiterleitung entscheiden. Würde das Fahrzeug 3 die Weiterleitung der Daten über die gesicherte Verbindung 58 grundsätzlich ablehnen, wäre eine dedizierte Weiterleitung im Backend 52 prinzipbedingt nicht möglich.

Hierzu kann das Fahrzeug 3 die Zugriffsberechtigungen 50 zusammen mit dem entsprechenden, dediziert weiterzuleitenden Daten übertragen. Alternativ oder zusätzlich könnte auch eine eigene Datenbank 51 im Backend 52 geführt werden die mit der Datenbank 51 im Fahrzeug 3 synchronisiert sein sollte. Auf diese Weise könnte der Datenverkehr zum Austausch der Zugriffsberechtigungen 50 reduziert werden.

Nach dem Aufteilen der Daten auf die einzelnen Applikationen im Fahrzeug 3 und/oder im Backend 52 können die Daten dann gelöscht werden.

Nachstehend soll anhand der Fig. 5 bis 7 eine in Fig. 4 angedeutete Benutzerschnittstelle 63 erläutert werden, mit denen die Zugriffsberechtigungen grundlegend eingestellt werden können.

Die Benutzerschnittstelle 63 umfasst verschiedene Tasten 59, auf denen Leuchtindikatoren 60 angeordnet sind. Mit jeder Taste 59 kann für die Daten aus einer bestimmten Applikationen des Fahrzeuges 3 oder einem bestimmten Sensor des Fahrzeuges 3 eine Zugriffsberechtigung 50 gesetzt beziehungsweise gelöscht werden. Dabei ist auf jeder Taste ein Leuchtindikator 60 vorhanden, der anzeigt, ob für die Daten eines Sensors oder einer Applikation eine Zugriffsberechtigung 50 gesetzt ist, oder nicht. Ein grüner oder schwarzer Leuchtindikator 60 steht dabei für eine Zugriffsberechtigung 50 auf die Daten, während ein roter oder gestrichelter Leuchtindikator 60 dafür steht, dass die Daten nicht freigegeben sind.

Der Übersichtlichkeit halber können die Tasten 59 für Applikationen in einem ersten Bereich 61 und die Tasten für Sensoren in einem zweiten Bereich 62 der Benutzerschnittstelle 58 angeordnet werden.

Um die Daten aus einem Sensor oder einer Applikation für andere Applikationen freizugeben, wird eine dem entsprechenden Sensor oder der entsprechenden Applikation zugeordnete Taste 59 gedrückt. Basierend auf dem Tastendruck wird in der Datenbank 51 dann die entsprechende Zugriffsberechtigung 50 für die Daten gespeichert, wobei der Leuchtindikator 60 den Zustand der entsprechenden Zugriffsberechtigung 50 anzeigen kann. In Fig. 6 ist beispielshaft ein Zustand dargestellt, in dem auf die Daten der HAF-Applikation 24 und die Daten der Fahrdynamikregelung 25 keine Zugriffsberechtigung 50 vergeben wurde.

Ferner kann in der Benutzerschnittstelle 63 auch geprüft werden, inwieweit sich eine nicht vergebene Zugriffsberechtigung 50 auf Daten aus einem Sensor oder einer Applikation auf andere Applikationen im Fahrzeug 3 oder gegebenenfalls sogar im Car2X-Netzwerk 1 auswirkt. Hierzu kann der Leuchtindikator 60 mit einem dritten Signalzustand versehen werden, der in Fig. 7 gelb dargestellt ist.

In Fig. 7 ist beispielsweise ein Zustand dargestellt, in dem keine Zugriffsberechtigung 50 auf die Daten des GNSS-Empfängers 11 vergeben wurde. Das hat zur Folge, dass die HAF-Applikation 24 nicht mehr funktioniert, weil die geographische Lage 12 essentiell für die Funktion der HAF-Applikation ist. In diesem Fall wird der Leuchtindikator 60 ebenfalls auf Rot oder Gestrichelt gesetzt, denn eine nicht funktionierende Applikation kann gleichgesetzt werden mit einer Applikation auf die kein Zugriff besteht. In beiden Fällen stehen keine Daten aus dieser Applikation oder Funktionen für diese Applikation mehr zur Verfügung. Der gleiche Zustand kann für die Nachrichtenerzeugungseinrichtung 39 angedeutete werden, die ohne die geographische Lage 12 keine Car2X-Nachrichten 17 erzeugen kann. Unter Umständen kann eine betroffene Applikation noch teilweise zur Verfügung stehen, wie beispielsweise das Navigationssystem, das zwar noch Kartendaten, aber nicht mehr die geographische Lage 12 des Fahrzeuges 3 darin anzeigen kann. Diese eingeschränkte Funktion als Konsequenz auf eine verweigerte Zugriffsberechtigung 50 kann durch einen gelb oder gepunktet dargestellten Leuchtindikator 60 angezeigt werden.

Es wäre auch möglich zunächst mit einer Taste 59 eine bestimmte Applikation auf der Benutzerschnittstelle 63 auszuwählen. Dann könnte auf den Tasten 59 der Sensoren über die Leuchtindikatoren 60 angezeigt werden, auf welche Daten aus welchen Sensoren die ausgewählte Applikation eine Zugriffsberechtigung 50 be-

sitzt. Dann könnte der Benutzer in diesem Zustand die Zugriffsberechtigungen 50 für diese Sensoren und gegebenenfalls anderen Applikationen durch Betätigen der entsprechenden Tasten 59 individuell einstellen und damit programmieren. Gegebenenfalls könnte noch eine weitere Taste eingeführt werden, um die Programmierung die Auswahl der zu programmierenden Applikation zu beenden.

Das beschriebene Car2X-Netzwerk 1 ist nur ein Beispiel für ein Netzwerk. Alternativ oder zusätzlich kann das Fahrzeug 3 an andere Netzwerke, wie beispielsweise einem beliebigen Mobilfunknetzwerk angeschlossen sein.

Zur Figur 8

In Figur 8 wird auf den Teil der Anonymisierung der Erfindung gesondert eingegangen. Die Ausführungen sollen jedoch auch in Kombination mit den vorgenannten Ausführungen verstanden werden. So wird das ein hiernach beschriebenes Ausführungsbeispiel des Kommunikationssystems 100 der Einfachheit halber auf die Funktionen der Anonymisierung der Daten beschränkt beschrieben. Insbesondere ist das hiernach beschriebene zentrale Netzwerk-Zugangsknoten auch analog zur zuvor beschriebenen Zugriffsregel- und Kommunikationsschnittstelle 49 zu verstehen.

Entsprechend der Erfindung hat ein Nutzer eines Fahrzeugs eine Möglichkeit der direkten Beeinflussung der mittels Kommunikationssystem 100 von einem Fahrzeug versendeten Daten, wodurch der Nutzer einen gewünschten Grad der Anonymisierung insbesondere personenbezogener Informationen selbst bestimmen kann. Die Auswahl erfolgt dabei mittels Mensch-Maschine-Schnittstelle 105, wie beispielsweise einem Umschalter im Fahrzeug oder am Fahrzeugschlüssel bzw. durch entsprechende Einstellung in einem Fahrzeugmenü.

Die Fig. 8a) zeigt eine Prinzipdarstellung eines Ausführungsbeispiels des erfindungsgemäßen Kommunikationssystems 100, bei dem mittels Anonymisierungsmittel 102 eine Anonymisierung der vom Fahrzeug zu versendenden Daten, bezogen auf den Datenfluss, unmittelbar vor dem zentralen Netzwerk-Zugangsknoten 103 (Endstelle), wie zum Beispiel einer Fahrzeugantenne, vorgenommen wird. Eine Umgehung von Anonymisierungsmittel 102 mittels des Fahrzeugkommunikationsnetzes (z.B. CAN-Netzwerk) von extern und/oder intern ist somit zumindest erschwert. Eine weitere Endstelle mit welcher die Kommunikation stattfindet, z.B. einen Netzwerk-Zugangsknoten eines Dienstanbieters, ist in Fig. 8 nicht dargestellt. Gemäß dem Ausführungsbeispiel der Fig. 8b) erfolgt die Anonymisierung zu sendender Daten mittels Anonymisierungsmittel 102 zwischen Zugangsknoten 103 und einem letzten fahrzeuginternen Datenknoten - im Beispiel Gateway 104. Für die Ausführungsbeispiele der Fig. 8 dient Gateway 104 dabei als Schnittstelle zwischen Zugangsknoten 103 und Mensch-Maschine-Schnittstelle 105. Im Allgemeinen stellt ein Gateway eine Schnittstelle zwischen unterschiedlichen Kommunikationsnetzen des Fahrzeugs dar, wobei unterschiedliche Netzwerkprotokolle zugrunde gelegt sein können. Kommunikationssystem 100 ist daher insbesondere durch Verwendung von Gateway 104 bevorzugt Teil eines Fahrzeugkommunikationssystems, wie beispielsweise eines CAN-Netzwerks (nicht dargestellt). Ausgehend von Gateway 104 kann eine Kommunikation, z.B. mit Mensch-Maschine-Schnitt-stelle 105, somit mittels des Fahrzeugkommunikationssystems erfolgen. Alternativ dazu kann ein eigenständiges und im Wesentlichen lediglich auf diesen Zweck ausgerichtetes Kommunikationsmittel zur Realisierung der Erfindung vorgesehen sein, was insbesondere die Möglichkeit eines Fremdzugriffs (direkt und fern) auf die Funktionsfähigkeit der Anonymisierung einschränkt. Die erfindungsgemäße Funktion kann dabei sowohl durch ein dafür vorgesehenes Steuergerät und/oder als zusätzliche Implementierung des die Funktion von Zu-

gangsknoten 103 ausführenden Geräts und/oder von Gateway 104 vorgenommen werden.

Bei der Anonymisierung wird beispielsgemäß zwischen zwei Betriebsarten unterschieden, wobei erfindungsgemäß weitere Abstufungen der Anonymisierung der Daten vorgesehen sein können. Diese sind jeweils in der Weise ausgestaltet, dass weitere Funktionen des Fahrzeugs so wenig wie möglich beeinträchtigt werden. Entsprechend einer weiteren Betriebsart von Kommunikationssystem 100 erfolgt keine Anonymisierung der Daten des Fahrzeugs.

Gemäß einer ersten Betriebsart erfolgt eine teilweise Anonymisierung der zu sendenden Daten, wobei ein Datenaustausch beispielsweise mit einem Backend-Server eines Dienstanbieters und/oder Sicherheitsbetreibers möglich ist, jedoch keine privaten Daten gesendet werden. Eine Ausnahme können bevorzugt Daten bilden, welche einer Authentifizierung der Netzwerkteilnehmer, z.B. des Fahrzeugs bzw. Dienstanbieters, dienen. Eine Definition, welche Daten als privat angesehen werden, kann dabei insbesondere durch einen Nutzer des Fahrzeugs und/oder durch Herstellervorgaben erfolgen.

Ein mögliche Anwendung für diese Anonymisierungsstufe ist eine Fahrt von einem Geldtransporter, bei welcher dieser zwar nicht geortet werden, trotzdem jedoch aktuelle Verkehrsdienste, wie z.B. Staumeldungen, über einen Back-End-Server beziehen soll.

Eine zweite Betriebsart ermöglicht eine möglichst vollständige Anonymisierung. Dabei sendet Zugangsknoten 103 keine Daten, kann diese jedoch weiterhin empfangen.

Ein Anwendungsbeispiel für diese zweite Betriebsart ist die Verfolgung eines Flüchtigen durch die Polizei, bei der es

notwendig sein kann, dem Flüchtigen die technische Möglichkeit einer Ortung der Polizeikräfte zu erschweren oder zu blockieren.

Zur Realisierung der Anonymisierung und um zugleich ein Umgehen dieser durch interne Funktionen oder Fremdeinwirkung („Hacker-Angriff") zu vermeiden, erfolgt eine Implementierung der diese Aufgabe ausführenden Funktion mit einer entsprechend sicheren Methodik. Die nachfolgend aufgeführten Implementierungsmöglichkeiten sind ohne Beschränkung auf diese beispielsgemäß zu verstehen und können diesbezüglich eigenständig und/oder in Kombination miteinander verwendet werden.

- Implementierung in einem geschützten Speicherbereich mit entsprechender Zugriffskontrolle,
- Implementierung einer Firewall,
- Implementierung als gesonderter Sicherheitschip,
- Implementierung parallel zur normalen Steuergeräte Applikation per Virtualisierung und/oder
- Implementierung mit Hilfe eines Hardware Sicherheitsmoduls (HSM), z.B. „Secure Hardware Extension" (SHE), „EVITA HSM", „Trusted Platform Module" (TPM), „Cloud Trusted Platform Module" CTPM usw.

Patentansprüche

1. Verfahren zum Leiten von Daten (12, 35, 36) in einem Fahrzeug zwischen einer Datenquelle (11, 20, 21) und einer Signalverarbeitungseinrichtung (24, 25, 39) zur Verarbeitung der Daten (12, 35, 36), umfassend:
   - Empfangen (49) der Daten (12, 35, 36) aus der Datenquelle (11, 20, 21),
   - Weiterleiten (49) der Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) in Abhängigkeit einer Zugriffsberechtigung (50), die definiert, ob die Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) weitergeleitet werden dürfen.

2. Verfahren nach Anspruch 1, umfassend:
   - Abrufen der Zugriffsberechtigung (50) aus einer Datenbank (51).

3. Verfahren nach Anspruch 1 oder 2, wobei die Datenquelle (11, 20, 21) und die Signalverarbeitungseinrichtung (24, 25, 39) über eine Netzwerkverbindung (59) getrennt sind.

4. Verfahren nach Anspruch 3, umfassend Übertragen der Daten (12, 35, 36) gemeinsam mit der Zugriffsberechtigung (50) über die Netzwerkverbindung.

5. Verfahren nach Anspruch 3 oder 4, wobei die Datenbank (51) auf einer Seite der Netzwerkverbindung (58) und eine weitere Datenbank (51) auf der anderen Seite der Netzwerkverbindung (58) vorhanden sind, und wobei die Zugriffsberechtigungen (50) in den Datenbanken (51) synchronisiert werden.

6. Verfahren nach einem der vorstehenden Ansprüche, umfassend:

- Löschen der Daten (12, 35, 36) nach dem Weiterleiten in Abhängigkeit der Zugriffsberechtigung (50).

7. Verfahren Leiten von Daten (12, 35, 36) in einem Fahrzeug, wobei Daten (12, 35, 36) in einem Fahrzeug zwischen einer Datenquelle (11, 20, 21) und mindestens einer Signalverarbeitungseinrichtung (24, 25, 39) zur Verarbeitung der Daten (12, 35, 36) geleitet werden, umfassend:

- Empfangen (49) der Daten (12, 35, 36) aus der Datenquelle (11, 20, 21) mittels einer Zugriffsregel- und Kommunikationsschnittstelle (49),
- Weiterleiten (49) der Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) in Abhängigkeit einer in der Zugriffsregel- und Kommunikationsschnittstelle (49) hinterlegten Zugriffsberechtigung (50), die definiert, ob die Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) weitergeleitet werden dürfen,

dadurch gekennzeichnet, dass die verarbeiteten Daten mittels der Zugriffsregel- und Kommunikationsschnittstelle (49) zumindest teilweise anonymisiert werden.

8. Verfahren nach Anspruch 7, ferner aufweisend die Schritte:

- Empfangen von verarbeiteten Daten von der Signalverarbeitungseinrichtung (24, 25, 39) mittels der Zugriffsregel- und Kommunikationsschnittstelle (49), und
- Weiterleiten der verarbeiteten Daten an eine externe Endstelle.

9. Verfahren nach Anspruch 7 oder 8, wobei der Austausch von Daten zwischen der Datenquelle (11, 20, 21), der Signalverarbeitungseinrichtung (24, 25, 39) sowie zwischen der Signalverarbeitungseinrichtung (24, 25, 39) und der Endstelle ausschließlich über Zugriffsregel- und Kommunikationsschnittstelle (49) erfolgt.

10. Verfahren nach einem der Ansprüche 7 bis 9, wobei zumindest zwei Betriebsmodi vorgesehen sind, wobei in einem ersten Betriebsmodus eine teilweise Anonymisierung erfolgt und in einem zweiten Betriebsmodus eine im Wesentlichen vollständige Anonymisierung der zu sendenden Daten vorgenommen wird.

11. Verfahren nach einem der Ansprüche 7 bis 10, wobei die Zugriffsregel- und Kommunikationsschnittstelle (49) ein weiterleiten von Kombinationen aus mehreren Daten der Datenquelle (11, 20, 21) an eine jeweilige Signalverarbeitungseinrichtung (24, 25, 39) nur teilweise zulässt oder unterbindet.

12. System zum Leiten von Daten (12, 35, 36) in einem Fahrzeug, aufweisend

- eine Datenquelle (11, 20, 21) zum Empfangen und Generieren von Fahrzeugdaten,
- mindestens eine Signalverarbeitungseinrichtung (24, 25, 39) zur Verarbeitung der Daten (12, 35, 36),
- eine Zugriffsregel- und Kommunikationsschnittstelle (49) umfassend, wobei die Datenquelle (11, 20, 21) und die Signalverarbeitungseinrichtung (24, 25, 39) mittels der Zugriffsregel- und Kommunikationsschnittstelle (49) gekoppelt sind und ein weiterleiten der Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) oder an eine externe Endstelle nur in Abhängigkeit einer an der Schnittstelle (49) hinterlegten Zugriffsberechtigung (50) erfolgt, die definiert, ob die Daten (12, 35, 36) an die Signalverarbeitungseinrichtung (24, 25, 39) weitergeleitet werden dürfen.

13. System nach Anspruch 12, wobei an der Schnittstelle (49) ferner eine Identifizierungsberechtigung hinterlegt ist, wobei die Identifizierungsberechtigung zumindest zwei Betriebsmodi vorgesehen sind, wobei in einem ersten Betriebsmodus eine

teilweise Anonymisierung erfolgt und in einem zweiten Betriebsmodus eine im Wesentlichen vollständige Anonymisierung der zu sendenden Daten vorgenommen wird.

14. System nach Anspruch 12 oder 13, wobei das Systeme eine Mensch Maschine Schnittstelle zum Einstellen der Zugriffsberechtigung (50) und der Identifizierungsberechtigung aufweist.

15. System nach einem der Ansprüche 12 bis 14, wobei die Datenquellen in einem Fahrzeug verbaute Sensoren sind und mittels der Mensch-Maschineschnittstelle eine fahrzeuginterne Verarbeitung der Sensordaten oder ein Weiterleiten der Sensordaten an eine externe Endstelle anhand der Einstellung der Zugriffsberechtigung und Identifizierungsberechtigung einstellbar ist.

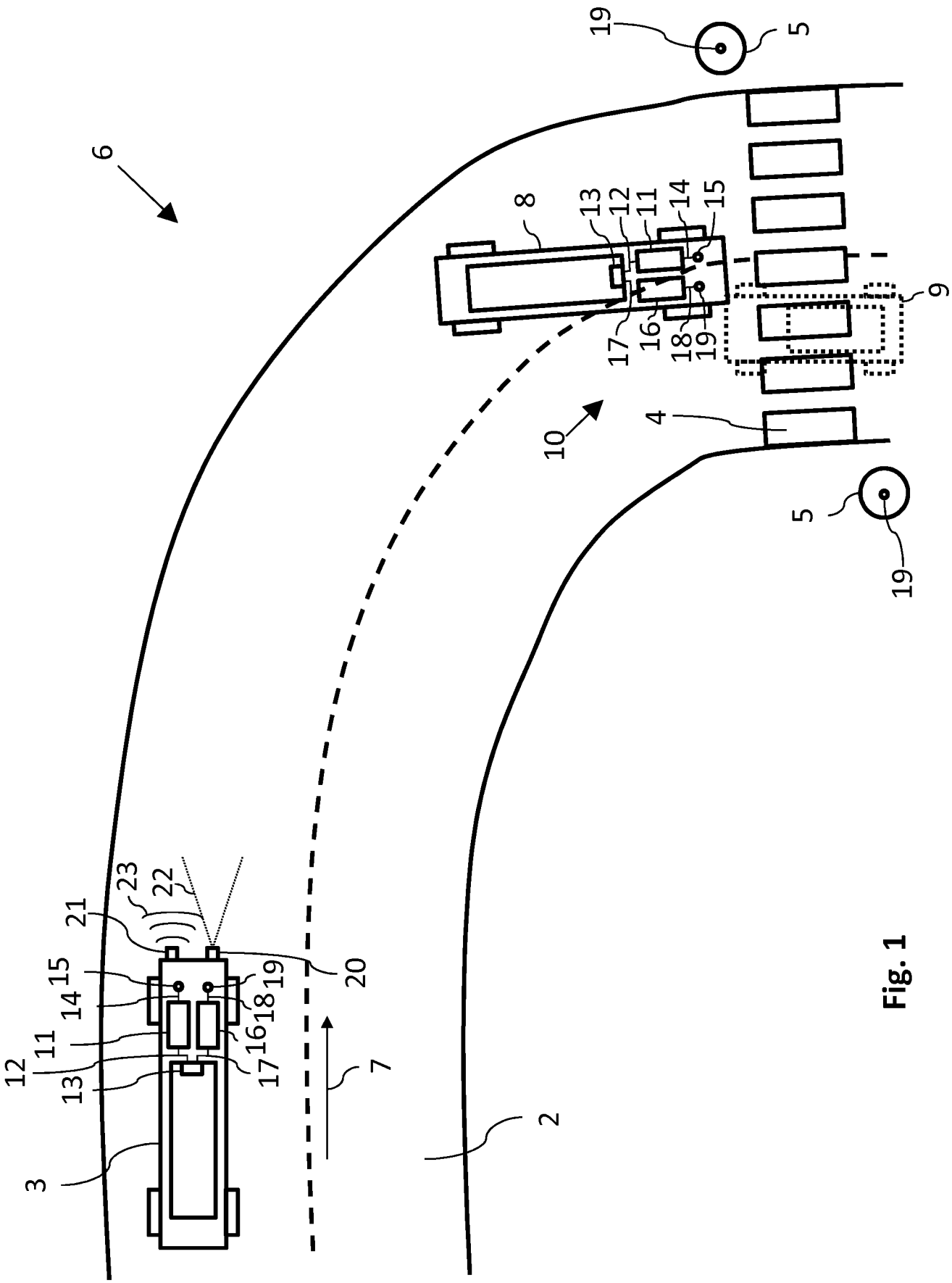

19
5
6
8
13
12
11
14
15
9
17
16
18
19
10
4
5
19
23
22
21
20
15
14
19
18
16
11
12
13
17
7
3
2

Fig. 1

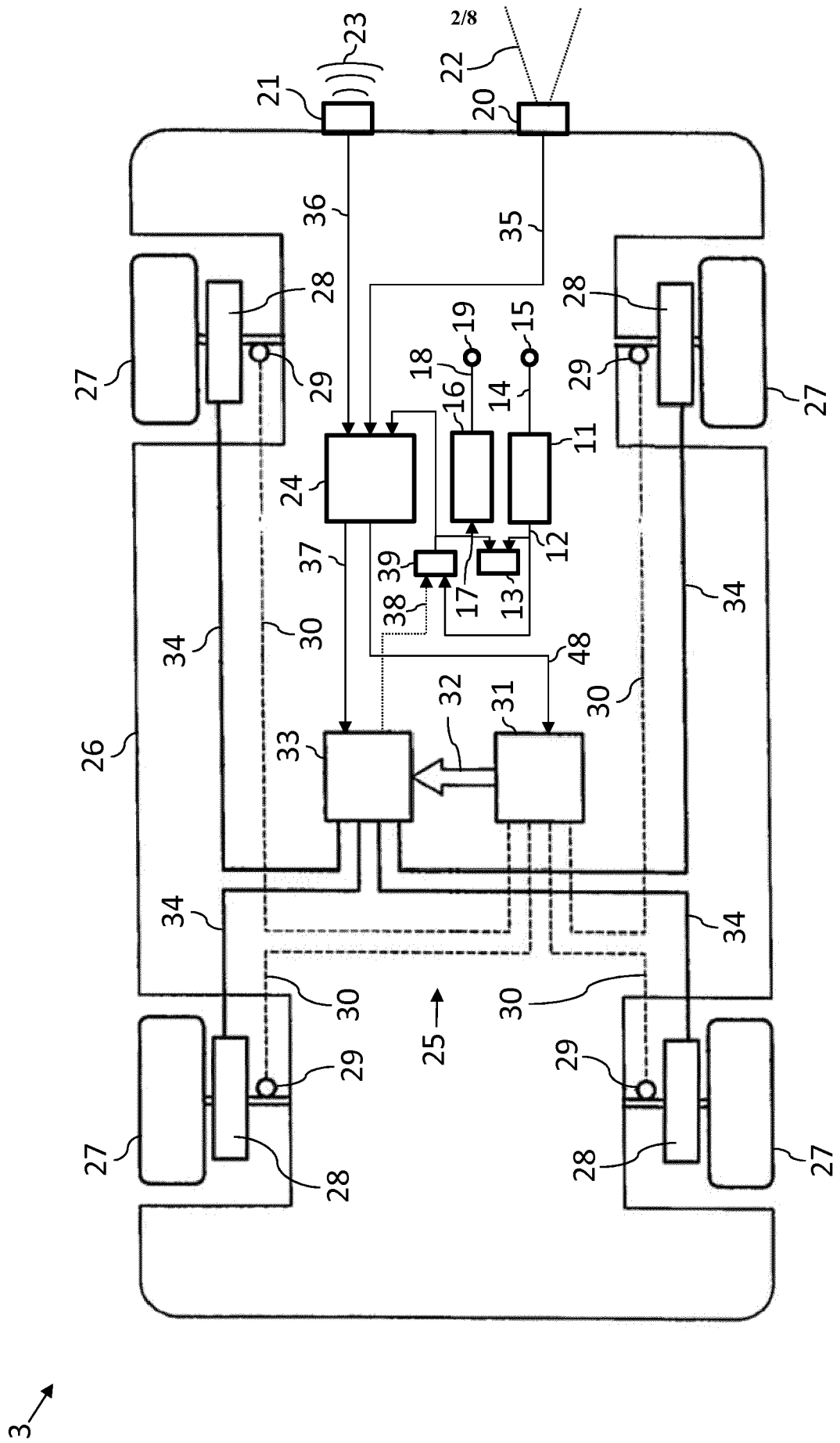

3
21
23
22
20
36
35
28
19
15
18
16
14
11
24
37
39
12
17
13
38
34
30
48
32
31
33
26
25
29
27

Fig. 2

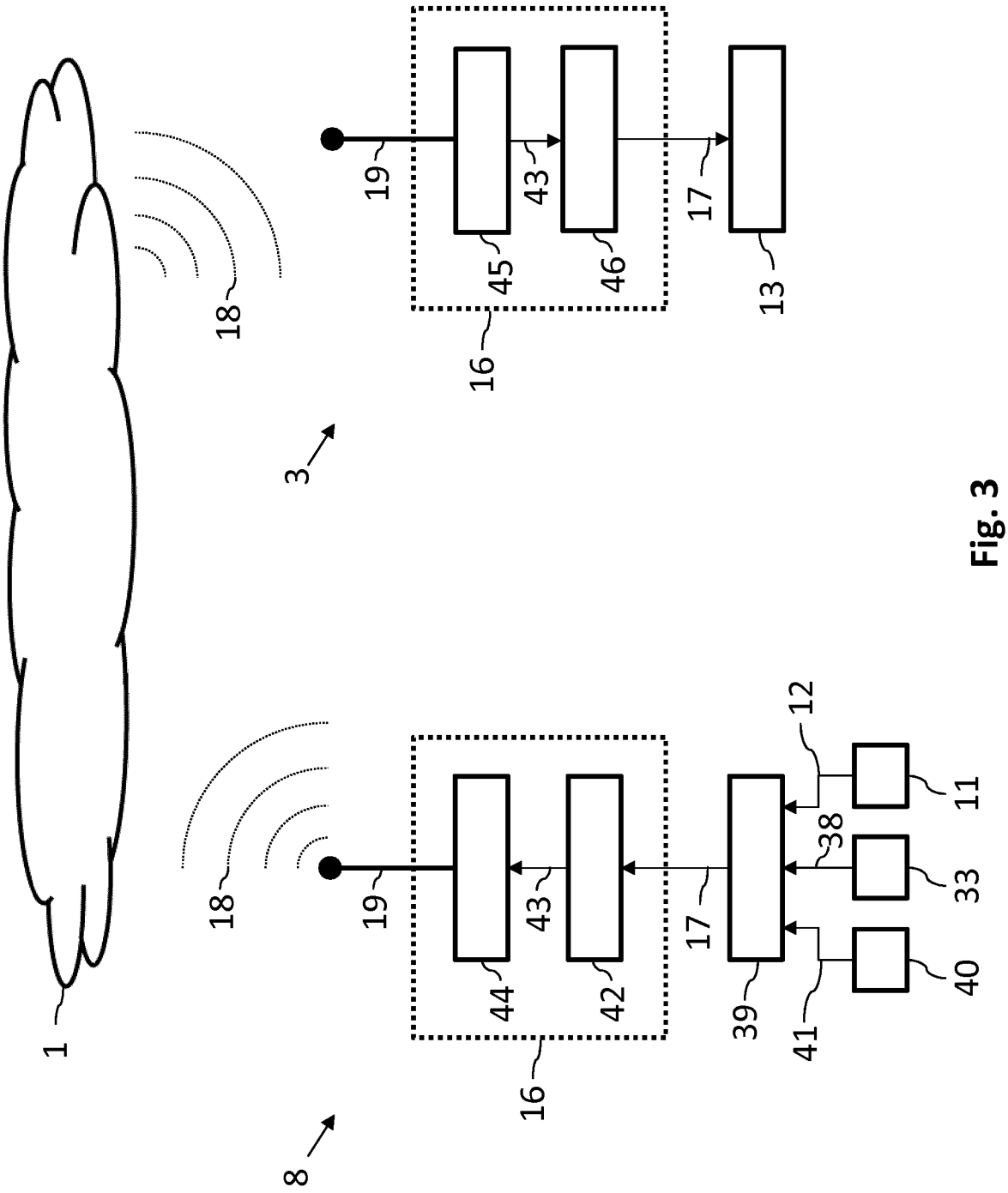


Fig. 3

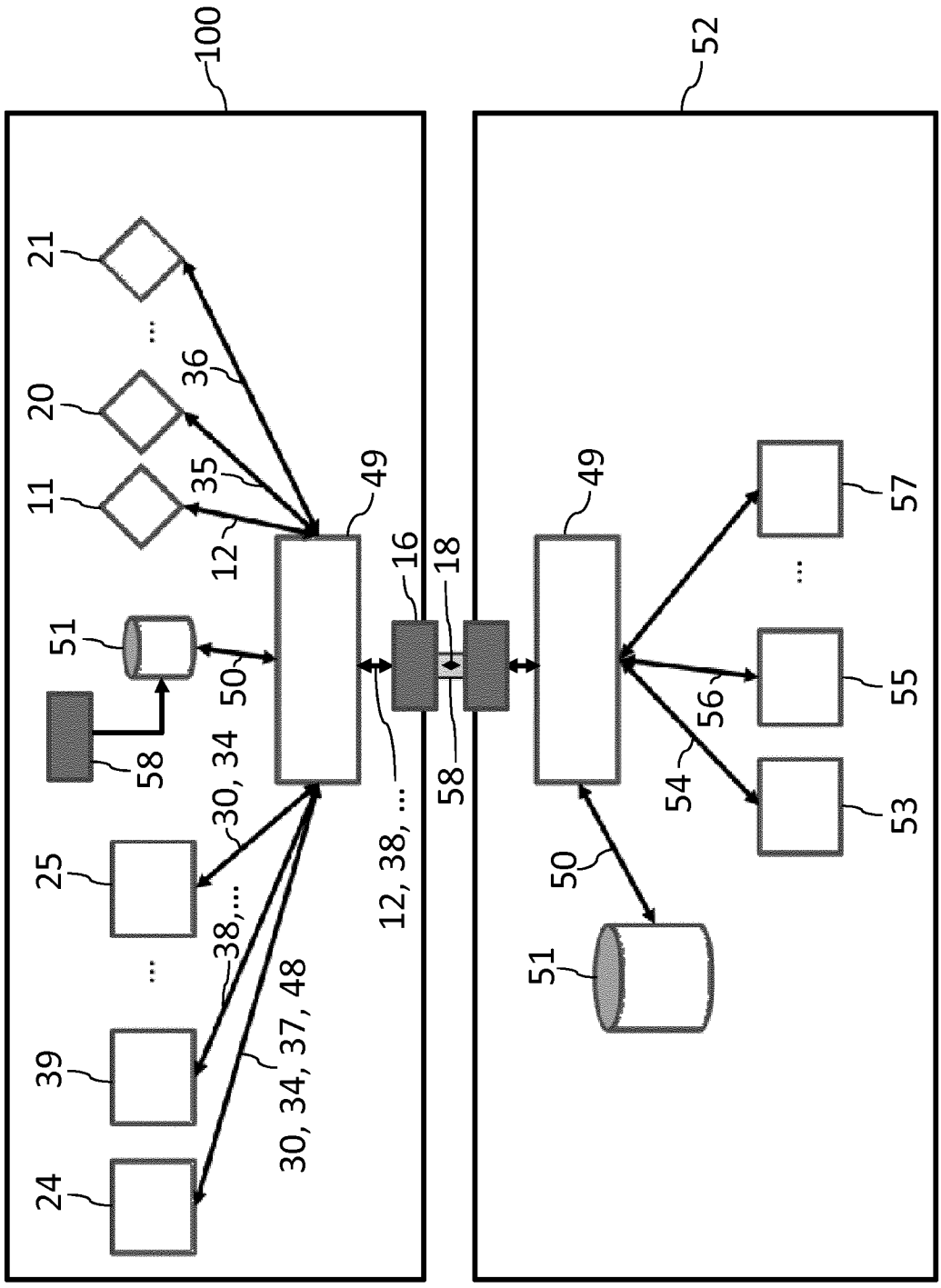

100
52
21
20
11
36
35
12
49
16
18
51
50
58
30, 34
25
38,...
39
30, 34, 37, 48
24
12, 38, ...
58
49
57
55
56
54
53
50
51

Fig. 4

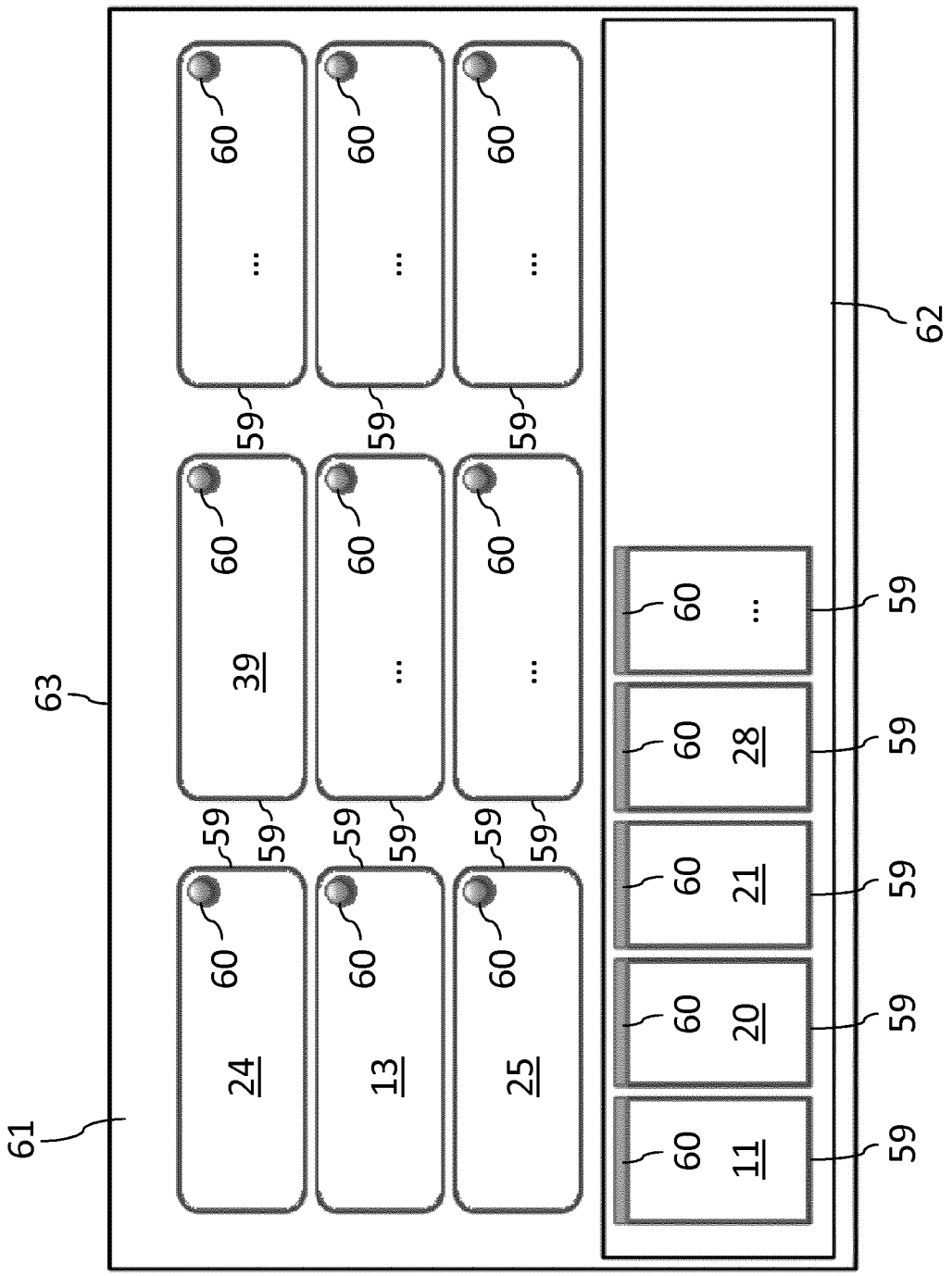


Fig. 5

Zeichner:
grün = schwarz

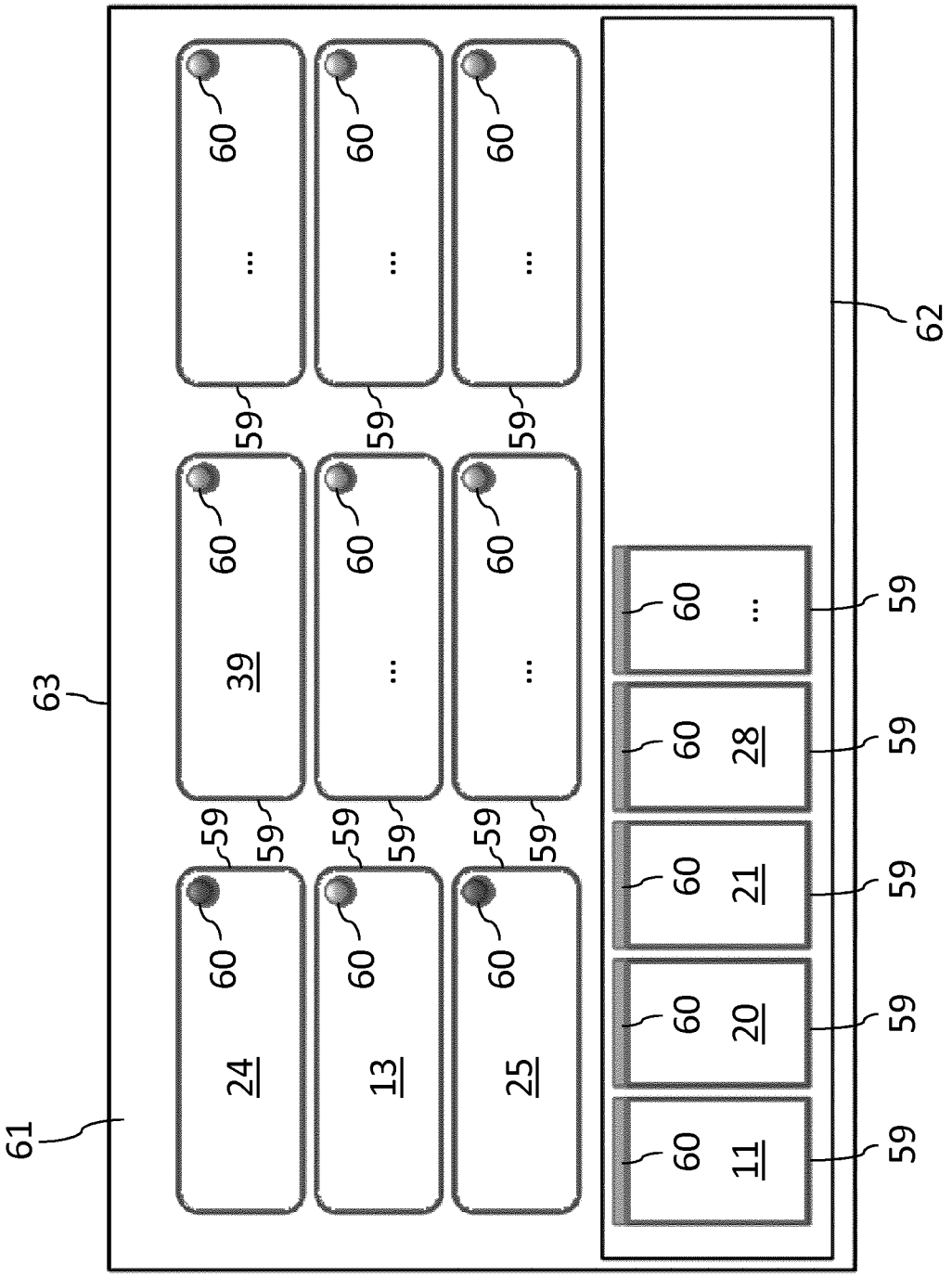


Fig. 6

Zeichner:
rot = gestrichelt

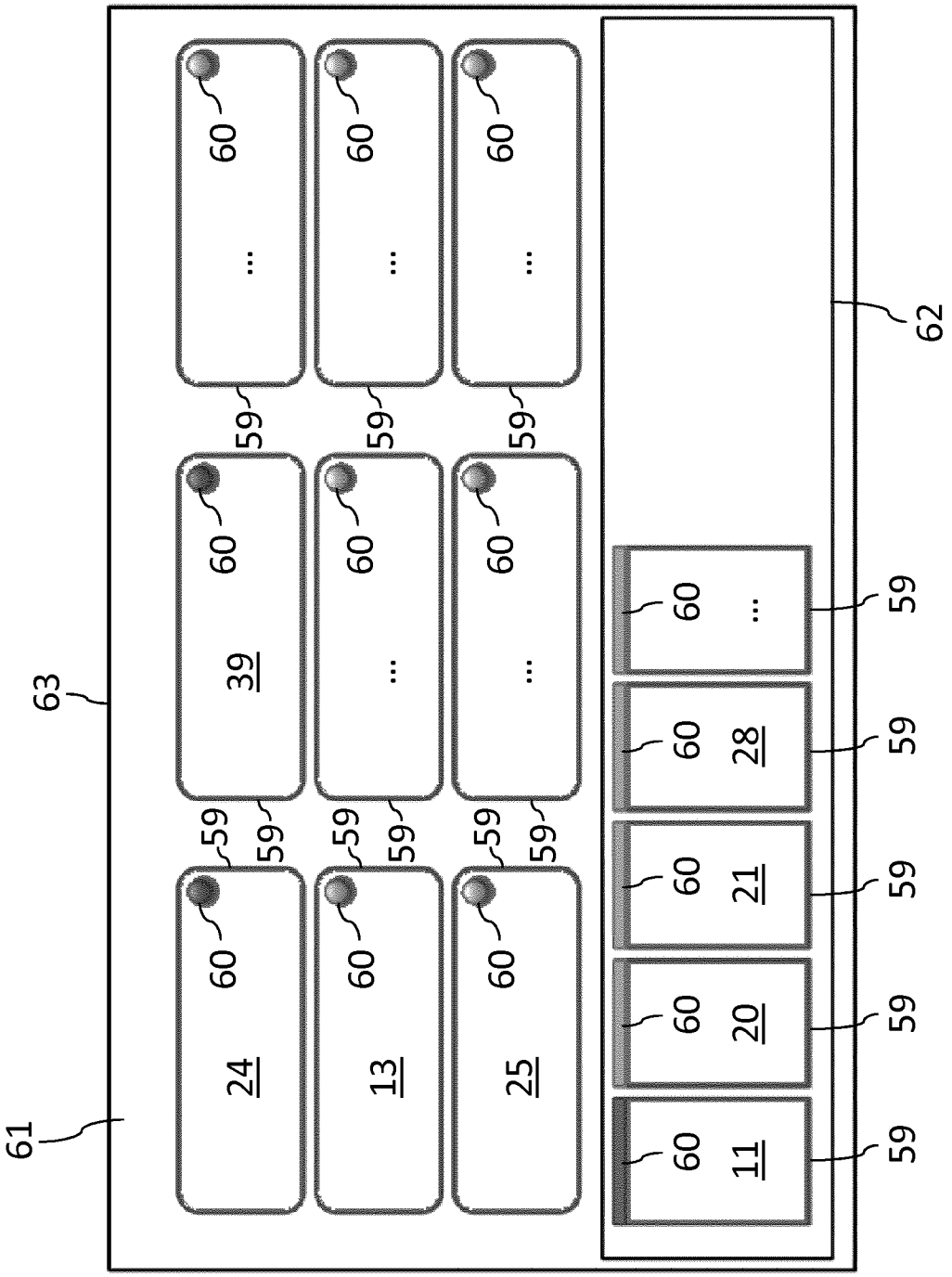
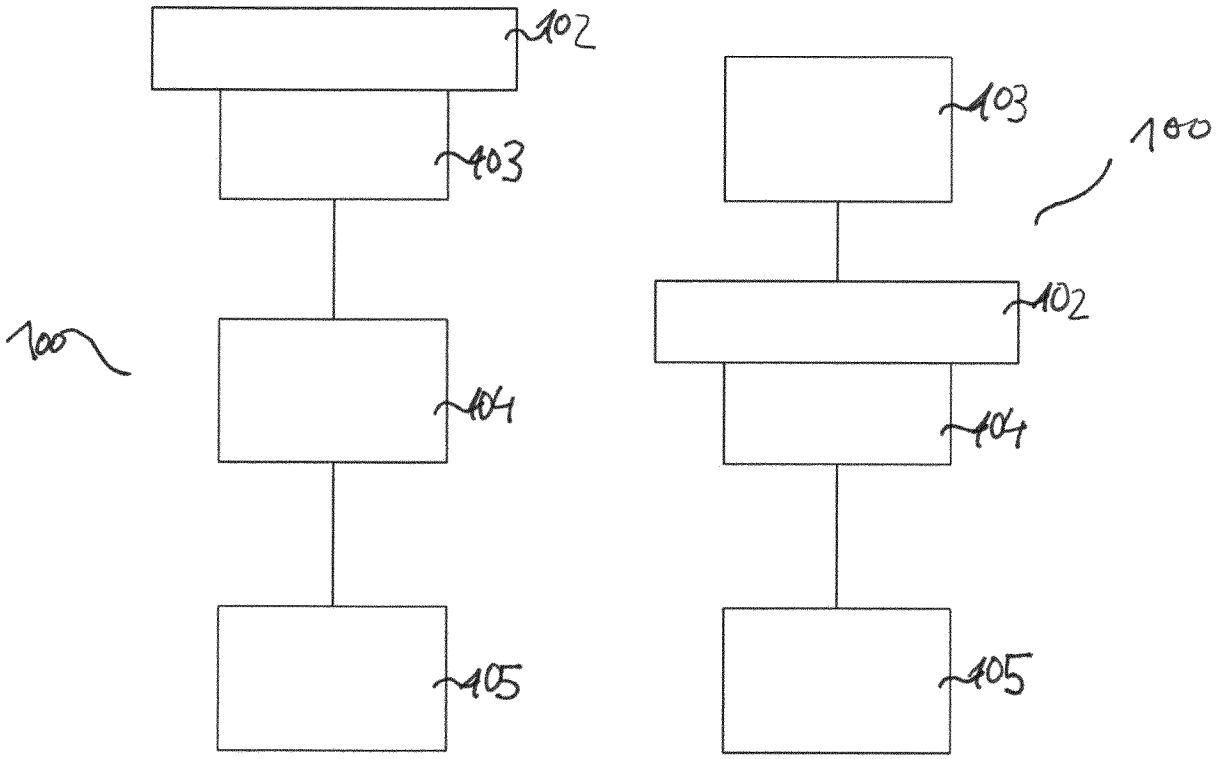


Fig. 7

Zeichner:
gelb = gepunktet



a) b)

Fig. 8