

(12) **Österreichische Patentanmeldung**

(21) Anmeldenummer: A 50282/2021
(22) Anmeldetag: 15.04.2021
(43) Veröffentlicht am: 15.11.2022

(51) Int. Cl.: **G08G 1/01** (2006.01)
H04W 12/02 (2009.01)
H04W 4/38 (2018.01)
G06F 21/62 (2013.01)
H04L 9/32 (2006.01)

(56) Entgegenhaltungen:
US 2020312047 A1
DE 102019201530 B3

(71) Patentanmelder:
AVL List GmbH
8020 Graz (AT)
(72) Erfinder:
Priller Peter Dipl.-Ing.
8111 Gratwein-Straßengel (AT)
(74) Vertreter:
Patentanwälte Pinter & Weiss OG
1040 Wien (AT)

(54) **Datenerfassung im Fahrzeug**

(57) Ein Verfahren zur Datenerfassung in einem Fahrzeug (2) bestehend aus zumindest einer Datenerfassungseinheit (3) und zumindest einer Verarbeitungseinheit (4), wobei die zumindest eine Datenerfassungseinheit (3) zumindest einen Fahrzeugdatensatz (10a) aufzeichnet, der von zumindest einem geschützten Fahrzeugdatensatz (8a) geprägt wird. Die Fahrzeugdaten (10) werden auf Basis eines Anonymitätsgrads (14) in einer Verarbeitungseinheit (4) über eine Vorverarbeitung (17) verändert und als gesicherte Fahrzeugdaten (12) abgespeichert, sodass kein Rückschluss auf die geschützten Fahrzeugdaten (8) möglich ist.

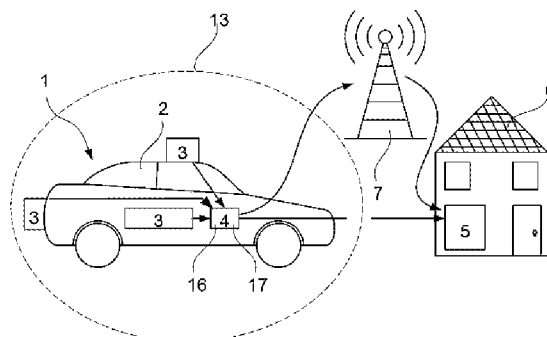


Fig. 1

Zusammenfassung

Ein Verfahren zur Datenerfassung in einem Fahrzeug (2) bestehend aus zumindest einer Datenerfassungseinheit (3) und zumindest einer Verarbeitungseinheit (4), wobei die zumindest eine Datenerfassungseinheit (3) zumindest einen Fahrzeugdatensatz (10a) aufzeichnet, der von zumindest einem geschützten Fahrzeugdatensatz (8a) geprägt wird. Die Fahrzeugdaten (10) werden auf Basis eines Anonymitätsgrads (14) in einer Verarbeitungseinheit (4) über eine Vorverarbeitung (17) verändert und als gesicherte Fahrzeugdaten (12) abgespeichert, sodass kein Rückschluss auf die geschützten Fahrzeugdaten (8) möglich ist.

Fig. 1

Datenerfassung im Fahrzeug

Verfahren zur Datenerfassung in einem Fahrzeug bestehend aus zumindest einer Datenerfassungseinheit und zumindest einer Verarbeitungseinheit, wobei die zumindest eine Datenerfassungseinheit zumindest einen Fahrzeugdatensatz aufzeichnet, der von zumindest einem geschützten Datensatz geprägt wird.

In den letzten Jahren wird der Bedarf nach Datenerfassung in Fahrzeugen immer höher. Das ist zumal durch den Wunsch nach autonomen bzw. automatisierten Fahren – „autonomous driving“ (AD) - begünstigt. Unter autonomen Fahren versteht man ein quasi „Autopilot-System“, welches beispielsweise Lenk-, Blink-, Beschleunigungs- und Bremsmanöver längs und quer der Fahrspur ohne menschliches Eingreifen durchführen kann. Während solche Autopilot-Systeme in der Industrie in begrenzten Bereichen (Werksgelände) schon durchaus realisiert sind, ist der Einsatz in der breiten Öffentlichkeit noch entfernt, unter anderem weil komplexe ethische Fragen der Einführung im Wege stehen. Es besteht dahingehend der Wunsch nach besserer Datenerfassung, um bessere und sicherere Systeme entwickeln zu können.

Datenerfassung in Fahrzeugen ist aber nicht nur für die Entwicklung und Verbesserung von Fahrerassistenzsystemen (ADAS) bzw. autonomen Fahren von höchster Wichtigkeit. Beispielsweise besteht in der Fahrzeugentwicklung, -optimierung, -verifizierung, -validierung, und -zertifizierung der Bedarf, verschiedenste Komponenten und Systeme des Fahrzeuges unter realen Fahrbedingungen zu testen. Hierfür wird das Fahrzeug im realen Straßenverkehr bewegt und dabei werden benötigte Daten erfasst. Speziell die Emissionen im Realbetrieb – „real driving emission“ (RDE) – sind aufgrund strengerer gesetzlicher Vorgaben zu ermitteln.

Bei der Datenerfassung in Fahrzeugen werden Daten für verschiedene Fahrzeugparameter, z.B. Motorleistung, Drehzahl, Drehmoment, Beschleunigung, Position, Batteriespannung bei (teil)elektrischen Antriebssträngen, Emissionswerte etc., im Testfahrzeug aufgezeichnet, um später ausgewertet zu werden. Die Daten werden entweder im Fahrzeug gesammelt und gespeichert und nach der Testfahrt ausgewertet (offline Testfahrt), oder unmittelbar an eine Testzentrale übertragen und dort ausgewertet (online Testfahrt).

Bei der Datenerfassung in Fahrzeugen sind vor allem personenbezogene Daten problematisch, beispielsweise aufgrund der Datenschutzgrundverordnung (DSGVO) der EU, nach der personenbezogene Daten nur in einer Weise verarbeitet werden dürfen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Per Definition sind personenbezogene Daten Angaben über eine bestimmte oder eine bestimmbare Person. Die Datenerfassung im Fahrzeug hat primär das Ziel, nur Daten des Fahrzeugs und keine personenbezogenen

Daten zu erfassen. Allerdings entsteht in bestimmten Fällen zwangsläufig auch eine ungewollte Zuordenbarkeit der Daten zu Personen, beispielsweise ist die aktuelle Position des Fahrzeugs gleichzeitig auch die Position von Fahrer und Insassen. Auch lassen sich ggf. aus Fahrzeugdaten die Aktionen bzw. Eigenschaften des Fahrers ablesen (z.B. aus Beschleunigungs- und Bremsverhalten lässt sich auf Aufmerksamkeit, Emotionen, Einfluss bestimmter Substanzen auf den Fahrer usw. schließen).

Fahrzeuge mit Fahrerassistenzsystemen sind manchmal mit Sensoren ausgestattet, deren Aufgabe es ist, andere Verkehrsteilnehmer, beispielsweise Fußgeher im Umfeld des Fahrzeugs und ihre Absicht zu erkennen und zu kategorisieren. Damit ergeben sich „indirekt“ personenbezogenen Daten (Daten zum Fahrer, Beifahrer, Passanten im Umfeld des Fahrzeugs). So ergeben sich beispielsweise Informationen aus dem Verhalten von Fahrer und anderer Verkehrsteilnehmer, aber auch, Positionsdaten, und bedürfen daher eines besonderen Schutzes.

Problematischer ist dementsprechend der „indirekte Zugriff/Rückschluss“ auf geschützte Daten, insbesondere personenbezogene Daten. Darunter versteht man, dass man aufgrund von anderen erfassten Daten im Fahrzeug, z.B. die Positionslokalisierung, Kameraaufnahmen, Motordaten (wie Leistung, Drehzahl, Drehmoment), Dynamikdaten (wie Beschleunigung, Geschwindigkeit) usw., Rückschlüsse auf Personen, deren Eigenschaften und deren unmittelbare Tätigkeit erhalten kann (Stichwort „big data analytics“). Dabei kann es sich nicht nur um Daten zum Fahrer oder Beifahrer handeln, sondern auch um Daten über Passanten und Dritte, welche mit dem Fahrzeug während der Fahrt interagiert haben, wie Stehenbleiben vor einem Fußgängerübergang oder vor einer Ampel, andere Verkehrsteilnehmer usw.

Beispielsweise kann aus einem, während einer Fahrt mit dem Fahrzeug erfassten zeitlichen Beschleunigungsprofil nicht direkt auf geschützte Daten, insbesondere personenbezogene Daten, geschlossen werden. Indirekt ist ein solcher Rückschluss aber durchaus möglich. Aus dem Beschleunigungsverlauf kann durch zeitliche Integration ein zeitlicher Geschwindigkeitsverlauf und zeitlicher Wegverlauf ermittelt werden. Aus anderen erfassten Daten, wie beispielsweise einer Fahrzeugbezeichnung, einem Startzeitpunkt usw., können Annahmen zu Startpunkten der Fahrt vorgenommen werden (Startbedingungen). Durch Übereinanderlegen von digitalen Straßenkarten, Verkehrsdaten zu dieser Zeit, und errechnetem Geschwindigkeitsprofil können möglichen Pfade ermittelt (z.B. vor einer engen Kurve wird gebremst, beim Abbiegen mit Gegenverkehr oder bei Ampeln gewartet, bei Stopp-Schild kurz stehengeblieben usw.) und nach Wahrscheinlichkeit gereiht werden. Sofern einer der möglichen Pfade eine ausreichend hohe Übereinstimmung (Confidence-Level) erreicht, kann aus diesem die Abfolge konkreter Aufenthaltsorte des Fahrzeugs zu

jeder (Mess-)Zeit angegeben werden, wodurch die geschützten Daten (Position einer Person, Aufenthaltsdauer) kompromittiert wären.

Systeme wie ADAS erfassen zwar diese Daten im und um das Fahrzeug, und verwenden diese zur unmittelbaren Steuerung des Fahrzeugs. Die erfassten Daten werden aber im

- 5 Regelfall nicht gespeichert oder übertragen. Zusätzliche Messsystemen zur Beobachtung des Fahrzeugverhaltens können beispielsweise während der Entwicklung zur Optimierung oder Fehleranalyse des ADAS oder AD eingesetzt werden. Dazu sollten diese Daten aber nach Verwendung für die Fahrfunktion nicht sofort gelöscht werden, sondern gespeichert/übertragen werden, um die Funktion im Nachhinein analysieren zu können.

- 10 Eine Verschlüsselung der geschützten Daten wäre eine Möglichkeit, um diese zumindest bei der Übertragung und Verarbeitung vor unerlaubten Zugriff zu schützen. Allerdings bleiben die zu schützenden Daten dabei erhalten, womit nachträgliche (nach einem Entschlüsseln der Daten) Rückschlüsse auf geschützte Daten, insbesondere personenbezogene Daten, trotzdem möglich sind.

- 15 DE 10 2006 043 363 A1 offenbart eine Datenerfassung, wobei die erfassten Daten in zwei Gruppen aufgeteilt werden. Davon besitzt eine Gruppe personenbezogene Daten, die andere nicht. Die personenbezogene Gruppe wird von einer Zwischenstelle geprüft und entfernt. Die zweite Gruppe ist per Annahme unkritisch und kann verarbeitet werden. Dieser Ansatz bedingt aber, dass die erfassten Daten tatsächlich in diese zwei Gruppen aufgeteilt
20 werden können. In der Praxis ist das allerdings in der Regel nicht möglich.

Während einer Fahrt mit einem Fahrzeug erfasste Daten werden nämlich üblicherweise von geschützten Daten, wie beispielsweise persönlich zuordenbaren Merkmalen des Fahrers, Ort der Fahrt usw., geprägt. Beispielsweise beeinflusst der Fahrertyp (z.B. konservativ, sportlich, aggressiv) ein Beschleunigungsprofil des Fahrzeugs und damit einen zeitlichen Verlauf der

- 25 Motorleistung, genauso beeinflusst die Topologie der Straße (Straßenneigung, Kurven usw.) oder die Beladung des Fahrzeugs (Masse) einen zeitlichen Verlauf der Motorleistung. Eine während der Fahrt erfasste Motorleistung kann damit nicht einfach als unkritische Information betrachtet werden, weil diese von geschützten Daten geprägt wird und sich daraus bis zu einem bestimmten Maß Rückschlüsse auf personenbezogene Daten ziehen
30 lassen.

Im Stand der Technik sind somit zwar Methoden zur Datenverarbeitung von mit einem Fahrzeug während einer Fahrt erfassten Daten offenbart, welche den direkten Zugriff auf geschützte Daten verhindert, jedoch bleibt der indirekte Zugriff auf solche geschützten Daten weiterhin möglich.

Es ist daher eine Aufgabe der gegenständlichen Erfindung den indirekten Zugriff auf geschützte Daten anhand von mit einem Fahrzeug während einer Fahrt erfassten Fahrzeugdaten zu verhindern.

Die gegenständliche Aufgabe wird dadurch gelöst, dass in der zumindest einen
 5 Verarbeitungseinheit eine Vorverarbeitung des zumindest einen Fahrzeugdatensatzes durchgeführt wird, wobei die Vorverarbeitung unter Berücksichtigung eines vorgegebenen Anonymitätsgrads folgende Schritte ausführt, nämlich Laden des zumindest einen Fahrzeugdatensatzes in die Vorverarbeitung, Anwenden von zumindest einer Methode auf den zumindest einen Fahrzeugdatensatz, um den zumindest einen Fahrzeugdatensatz zu
 10 verändern, Analyse, ob mit dem veränderten Fahrzeugdatensatz der Anonymitätsgrad erfüllt ist, und Speichern des zumindest einen veränderten Fahrzeugdatensatzes, der den Anonymitätsgrad erfüllt, als zumindest einen gesicherten Fahrzeugdatensatz, um einen indirekten Rückschluss auf zumindest einen geschützten Datensatz zu verhindern.

In einer vorteilhaften Ausführung werden während einer Testfahrt mit einem Fahrzeug
 15 Fahrzeugdaten gesammelt. Diese Fahrzeugdaten können unterschiedliche Qualität haben, z.B. Leistungsdaten eines Motors, visuelle Daten von einer Videokamera, Abgasdaten von einer Emissionsanalyseeinheit, Positionsdaten eines GPS-Sensors, persönlich vom Fahrer eingetragene Daten etc.

Bevorzugterweise werden Fahrzeugdaten bei einer Testfahrt ausgewählt, welche für eine
 20 gewisse Messkampagne relevant sind. Das könnte beispielsweise RDE Daten eines Dieselmotors sein, welche beispielsweise abhängig von Motortemperatur, Motorleistung, Außentemperatur etc. sind. Bevorzugte Fahrzeugdaten wären dann Stickoxidgehalt, Aerosolpartikel, Motorleistung und Motortemperatur. Die Datenerfassungseinheiten sind dann beispielsweise an unterschiedlichen Stellen angebracht, z.B. am Motor und entlang der
 25 Abgasanlage. Auch Kameras am Fahrzeugdach, oder GPS-Positionsermittlung können Datenerfassungseinheiten sein. Diese Fahrzeugdaten werden während der Testfahrt aufgezeichnet. Solche Fahrzeugdaten können beispielsweise von einer Laufvariable, wie Zeit, Geoposition, Motordrehzahl, Geschwindigkeit und ähnliches sein. Alle Laufvariablen, die der Fachmann für die Auswertung benötigt, können benutzt werden um
 30 Fahrzeugdatensätze zu indizieren.

Bevorzugterweise werden Testfahrten zur Datenaufzeichnung mit Testfahrzeugen durchgeführt, höchst bevorzugt mit vorinstallierten Datenerfassungsmodulen. Testautos stehen bevorzugterweise auf einem Unternehmensparkplatz, welches die Testungen durchführt und werden von geschultem Personal gefahren. So ergeben sich beispielsweise
 35 im Regelfall Testfahrten mit gleichem Start und Endpunkt und mit begrenzter Anzahl an Fahrern. Es können aber auch Standard-Fahrzeuge aus der laufenden Produktion

instrumentiert werden, beispielsweise für Fahrzeugflotten (Lieferfahrzeuge, Taxis, Mietwagen, etc.), oder Einzelfahrzeuge für Stichprobenanalysen.

Solchen geschützten Daten, wie Fahrer und Bewegungsprofil, werden während Testfahrten noch weitere geschützte Daten hinzugefügt. Beispielsweise interagieren Testfahrzeuge mit anderen Verkehrsteilnehmern, wie anderen Fahrzeugen oder Passanten. Verschiedene Interaktionen mit dem Testfahrzeug prägen die erfassten Fahrzeugdaten der Datenerfassung. Beispielsweise sind daher Rückschlüsse auf Autokennzeichen von anderen Verkehrsteilnehmern oder die Identität von Passanten mittels Fahrzeugdaten aus einer Videokamera oder auch aus einer GPS-Positionsermittlung möglich.

Erfindungsgemäß wird eine Verarbeitungseinheit im Fahrzeug integriert, welche über eine Vorverarbeitung verfügt, die, durch die Testfahrt aufgenommenen Fahrzeugdaten, mittels zumindest einer Datenerfassungseinheit, in gesicherte Fahrzeugdaten überführt, und somit kein indirekter Rückschluss auf die geschützten Daten möglich ist.

Die Vorverarbeitung erfolgt über eine Vorgabe der Wahrscheinlichkeit, einem Anonymitätsgrad („Degree of anonymity“), geschützte Daten identifizieren zu können. Definitionen für den Anonymitätsgrad sind in einschlägigen Publikationen gegeben, wie „Diaz, C., Seys, S., Claessens, J., & Preneel, B. (2002, April). Towards measuring anonymity. In *International Workshop on Privacy Enhancing Technologies* (pp. 54-68). Springer, Berlin, Heidelberg“ oder „Edman, M., Sivrikaya, F., & Yener, B. (2007, May). A combinatorial approach to measuring anonymity. In *2007 IEEE Intelligence and Security Informatics* (pp. 356-363). IEEE“. Wenn ein Fahrzeugdatensatz einen vorgegebenen Anonymitätsgrad erfüllt, wird er als gesicherter Fahrzeugdatensatz gespeichert und kann bedarfsweise einer weiteren Verarbeitung zugeführt werden. Bevorzugterweise kann nach Speicherung als gesicherter Fahrzeugsatz nichtmehr auf die geschützten Daten zugegriffen werden.

Der Anonymitätsgrad kann auch an einen Kostenfaktor gekoppelt sein und eine Kategorisierung enthalten. Ein Kostenfaktor beschreibt den Aufwand für einen Zugriff auf geschützte Daten. Eine solche Kategorisierung wird vom Anwender vorgegeben und beschreibt das Risiko, dass auf geschützte Daten zugegriffen werden kann. Je nach Kategorisierung kann der Wert des Anonymitätsgrads angepasst werden, und so die Stärke der Veränderung der Fahrzeugdaten in der Vorverarbeitung angepasst werden. Bei einem geringen Risiko, kann ein Fahrzeugdatensatz nur wenig verändert werden und als gesicherter Fahrzeugdatensatz gespeichert werden und damit sehr nahe am ursprünglichen Fahrzeugdatensatz sein.

In einer höchst bevorzugten Ausführung modelliert die Vorverarbeitung den Einfluss der geschützten Daten. Das kann mittels einer Korrelationsfunktionen erfolgen, welche eine

Prägung des ungeprägten Fahrzeugdatensatzes mittels geschützter Daten beschreibt, und in einem Fahrzeugdatensatz aufgeht. Die Prägung unterschiedlicher Fahrzeugdatensätze kann über unterschiedliche Korrelationsfunktionen abgebildet werden. Wenn ein Fahrzeugdatensatz keine Prägung durch geschützte Daten aufweist, kann dieser
 5 beispielsweise direkt als gesicherter Fahrzeugdatensatz gespeichert werden. Ein Fahrzeugdatensatz kann auch durch mehrere geschützte Daten geprägt sein, was durch eine Korrelationsfunktion oder auch durch mehrere Korrelationsfunktionen abgebildet sein kann.

Es kann auch vorkommen, dass ein Fahrzeugdatensatz den Anonymitätsgrad nach einer
 10 Vorverarbeitung nicht erfüllt und verworfen wird.

Es kann auch ein Kontext verwendet werden um ein Modell der Vorverarbeitung abhängig von der Fahrzeugumgebung verändern zu können. Bevorzugterweise wird der Kontext über eine Datenerfassungseinheit erzeugt, welcher Einflüsse der Umgebung an die Vorverarbeitung weiterleitet. Solche Einflüsse können beispielsweise das
 15 Verkehrsaufkommen, die Wetterlage, Straßenverkäufe, Motorleistungskennzahlen und ähnliches sein. Die Vorverarbeitung kann dann auf diesen Kontext reagieren und beispielsweise auswählen welche Methoden in welcher Stärke angewendet werden.

In einer bevorzugten Ausführung werden diese gesicherten Fahrzeugdaten im Fahrzeug gespeichert und später am Auswertestandort ausgelesen. Höchst bevorzugt werden aber die
 20 gesicherten Fahrzeugdaten online an den Auswertestandort übermittelt, um die Testfahrt und die Testergebnisse in einer Auswerteeinheit direkt analysieren zu können. Bevorzugt kann die Testfahrt bei genügend Daten abgeschlossen oder bei ungenügender Datenlage verlängert werden.

Bevorzugterweise wird die Vorverarbeitung mittels mikroprozessorbasierter Hardware
 25 ausgeführt sein, auf der die Datenverarbeitungssoftware läuft, beispielsweise ein Computer oder eine speicherprogrammierbare Datenverarbeitung. Auch eine Implementierung als integrierter Schaltkreis (IC), beispielsweise als anwendungsspezifische integrierte Schaltung (ASIC) oder Field Programmable Gate Array (FPGA), ist denkbar. Ebenso sind Mischformen möglich.

Die Vorverarbeitung benutzt Methoden wie beispielsweise Normalisieren,
 30 Auflösungsreduktion, Anonymisieren, De-referenzieren oder Überlagern aus einer Methodenbibliothek. Die Methoden können permanent auf einen Fahrzeugdatensatz angewendet werden, es können Methoden aber auch abhängig vom Modell der Vorverarbeitung angewandt werden. Dann kann es sein, dass Methoden parallel oder
 35 sequentiell, oder in Kombinationen davon angewandt werden. Die Anwendung der Methoden kann auch abhängig von Korrelationsfunktionen und vom Kontext sein. Bevorzugterweise,

werden die Methoden soweit angewandt, dass ein vorgegebener Anonymitätsgrad gerade erfüllt ist.

Es können aber auch neue, alternative oder zusätzliche Methoden je nach Bedarf in die Vorverarbeitung geladen werden. In einer bevorzugten Ausführungsform kann ein
 5 Hinzufügen neuer, alternativer oder zusätzlicher Methoden auf Abo-Basis laufen. Solche Formen können beispielsweise auf Subscription Basis funktionieren. Damit können neue Methoden über regelmäßige Software Updates hinzugefügt werden, oder bei der Routineuntersuchung in einer Werkstatt. Das kann nötig sein, falls neue Entwicklungen Zugriffe auf geschützte Daten ermöglichen, die bislang nicht möglich waren.

10 Die gegenständliche Erfindung wird nachfolgend unter Bezugnahme auf die Figuren 1 bis 5 näher erläutert, die beispielhaft, schematisch und nicht einschränkend vorteilhafte Ausgestaltungen der Erfindung zeigen. Dabei zeigt

Fig.1 eine schematische Darstellung der Ausführung einer Messkampagne,

15 Fig.2 Prägung der Fahrzeugdaten durch geschützte Daten und Verarbeitung in gesicherte Fahrzeugdaten,

Fig.3 Verarbeitungseinheit mit Vorverarbeitung gemäß der Erfindung und

Fig.4 Flowchart mit Wirkungsweise der Vorverarbeitung und

Fig.5 eine beispielhafte Positionsverarbeitung.

20 Fig.1 zeigt eine mögliche Anordnung 1 für eine Messkampagne mit einem Fahrzeug 2 laut gegenständlicher Erfindung. Im oder am Fahrzeug 2 befindet sich zumindest eine Datenerfassungseinheit 3 und zumindest eine Verarbeitungseinheit 4, welche für eine Messkampagne verwendet werden. Eine Messkampagne beschreibt eine Testfahrt (auch im Sinne mehrerer Testfahrten, auch über einen längeren Zeitraum) mit den im Fahrzeug 2 ermittelten Fahrzeugdaten 10, um diese Kampagne erfolgreich abzuschließen.

25 Eine Datenerfassungseinheit 3 kann ein beliebiger Messsensor sein, der eine bestimmte Größe misst oder erfasst. Eine Datenerfassungseinheit 3 kann auch Daten aus einem fest im Fahrzeug verbauten Steuergerät erfassen. Solche Steuergeräte arbeiten nach dem EVA Prinzip (Eingabe – Verarbeitung – Ausgabe), wobei eine physikalische Kenngröße wie z. B. Drehzahl, Druck, Temperatur usw. gemessen wird und dieser Wert mit einer im Steuergerät
 30 eingegebenen oder berechneten Sollgröße verglichen wird. Sollte der gemessene Wert mit dem eingespeicherten Wert nicht übereinstimmen, regelt das Steuergerät mittels Aktoren den physikalischen Prozess nach, so dass die gemessenen Istwerte wieder mit Sollgrößen übereinstimmen. Die Aktoren greifen also korrigierend in einen laufenden Prozess ein. Solche Steuergeräte im Fahrzeug sind beispielsweise ein Motor-Steuergerät, ein Getriebe-
 35 Steuergerät, ein Batteriemanagementsystem oder ein Hybridsteuergerät. Deren

Eingangssignale kommen von fest verbauten Sensoren wie Drehzahl-, Drehmoment-, Temperatur-, Druck-, Spannungs-, Stromsensoren etc. Die Steuergeräte steuern Aktoren im Fahrzeug, wie z.B. Einspritzpumpen, Einlassventile, Antriebsbatterien, Fahrhebelsteller usw., an. In einer bevorzugten Ausführungsweise sind solche Steuergeräte mittels Systembusse systemweit miteinander verbunden.

Beispielsweise kann eine solche Datenerfassungseinheit 3 auch ein GPS-Positionsermittler, eine Abgasmesseinheit, eine Umgebungskamera, ein Temperatursensor, eine Luftfeuchtmesseinheit, etc. sein. Die Erfindung ist nicht auf diese exemplarischen Messsensoren limitiert. Es können verschiedene Datenerfassungseinheiten 3 in verschiedenen Ausführungen in einem Fahrzeug verbaut sein, welche der Fachmann für die Datenauswertungen benötigen könnte. Die Datenerfassungseinheiten 3 können standardmäßig am Fahrzeug 2 verbaut sein, können aber auch speziell für die Durchführung der Messkampagne am Fahrzeug 2 angeordnet werden (beispielsweise Emissionsmesstechnik).

Die zumindest eine Datenerfassungseinheit 3 generiert Fahrzeugdaten 10 in Form zumindest eines Fahrzeugdatensatzes 10a. Unter Fahrzeugdatensatz 10a versteht man den Verlauf einer erfassten Größe x_n^* der Datenerfassungseinheit 3 in einem vorgegebenen Intervall, insbesondere während der Testfahrt oder eines Teils der Testfahrt. Die erfasste Größe x_n^* wird vorzugsweise zur weiteren Verwendung, wie Verarbeitung oder Speicherung, digitalisiert. Unter Verlauf einer erfassten Größe x_n^* wird eine Abfolge von aufeinander folgenden Messungen oder Datenpaketen verstanden. Unter Fahrzeugdaten 10 wird die Gesamtheit aller einzelnen Fahrzeugdatensätze 10a verstanden, die bei der Durchführung der Testfahrt für die Messkampagne aufgezeichnet werden. Fahrzeugdatensätze 10a können beispielsweise einzelne aufgenommen Verläufe einer Datenerfassungseinheit 3 sein. Es können aber auch mehrere Fahrzeugdatensätze 10a von einer Datenerfassungseinheit 3 erstellt werden. Diese Fahrzeugdatensätze 10a werden, bevorzugterweise als Funktion einer Laufvariable k , wie der Zeit aufgenommen ($x_n(t)$), oder auch als Funktion der Position (z.B. Geokoordinate (Länge, Breite, Höhe) $x_n(x,y,z)$ oder auch Wegstrecke $x_n(s)$), aufgenommen.

Fahrzeugdatensätze 10a können Daten sein, die den Fahrzeugzustand beschreiben und mit bekannten Messsensoren oder Steuergeräten erfasst werden, wie beispielsweise Position, Geschwindigkeit (auch im Raum), Beschleunigung (auch im Raum), Motorleistung, Motordrehzahl, Motormoment, Motortemperatur, Kühlmitteltemperatur, Raddrehzahl, Reifenschlupf usw., aber auch Daten, die die Umgebung des Fahrzeugs 2 beschreiben, wie beispielsweise mittels Radar, LIDAR, einer Kamera, eines Infrarotsensors aufgenommene Daten. Fahrzeugdatensätze 10a können aber auch Daten sein, die von anderen Datenquellen bezogen werden, beispielsweise Straßendaten aus digitalen Straßenkarten (z.B. Topologie der Straße) oder Wetterdaten von digitalen Wetterdiensten, oder

Informationen die von anderen Fahrzeugen über Fahrzeug-zu-Fahrzeug Kommunikation (z.B. Fahrzeug zu Fahrzeug Kommunikation (C2C), oder eine Kombination von Fahrzeug zu Fahrzeug und Fahrzeug zu Infrastrukturkommunikation (V2X)) übermittelt werden. Auch Daten, die vom Fahrer oder einem Beifahrer während der Fahrt manuell eingegeben oder
 5 ausgelöst werden, wie beispielsweise das Aktivieren / Deaktivieren einer Funktion im Fahrzeug, können Fahrzeugdatensätze 10a sein.

Die gegenständliche Erfindung beinhaltet auch zumindest eine Verarbeitungseinheit 4, welche ebenfalls am oder im Fahrzeug 2 vorgesehen ist. Die Verarbeitungseinheit 4 empfängt die mit der zumindest einen Datenerfassungseinheit 3 laufend während einer Fahrt
 10 mit dem Fahrzeug 2 erfassten Fahrzeugdaten 10. Eine Datenerfassungseinheit 3 kann die erfassten Fahrzeugdaten 10 direkt an die Verarbeitungseinheit 4 übermitteln, beispielsweise über eine geeignete Verkabelung oder drahtlos.

Die Verarbeitungseinheit 4 besteht aus zumindest einer Vorverarbeitung 17 (Fig.2 und 3). Die Verarbeitungseinheit 4 kann auch eine Speichereinheit 11 umfassen, in welche Daten
 15 gespeichert werden können. Die Speichereinheit 11 kann aber auch extern angeordnet sein und mit einer geeigneten Datenverbindung mit der Verarbeitungseinheit 4 verbunden sein.

Während einer Testfahrt gibt es auch geschützte Daten 8. Geschützte Daten 8 beschreiben zumindest einen geschützten Datensatz 8a, welcher als kritisch zu sehen ist und nicht weitergegeben werden soll, beispielsweise personenbezogene Daten im Sinne der DSGVO.

20 Geschützte Daten 8 sind insbesondere solche Daten, die nur einer bestimmten Person selbst zugänglich sein sollen oder auch völlig anonym bleiben sollen. Dazu zählen z.B. personenbezogene Daten, wie die Identität des Fahrers oder des Beifahrers, eine Adresse des Startpunkts und Daten Dritter, die mit dem Fahrzeug 2 während der Testfahrt interagieren. Solche kritischen Daten können während der Testfahrt durch eine
 25 Datenerfassungseinheit 3 aufgezeichnet werden (können also auch ein Fahrzeugdatensatz 10a sein), können aber auch zu einer Testfahrt eingegeben oder vorgegeben werden, beispielsweise Daten zum Fahrer, zum Fahrzeug 2, Fahrstrecke usw.

Geschützte Daten 8 haben jedoch Einfluss auf Fahrzeugdaten 10, wie anhand von Fig.2 veranschaulicht und erläutert wird. Beispielsweise kann der Fahrstil des Fahrers die
 30 Geschwindigkeit, Beschleunigung, Stopps etc. beeinflussen. Ein bestimmter Fahrzeugdatensatz 10a kann somit bei unterschiedlichen Fahrern bei gleicher Fahrstrecke unterschiedlich sein. Auch Verkehrsaufkommen, wie Staus, oder die Position, im städtischen oder ländlichen Bereich, oder andere Verkehrsteilnehmer beeinflussen die Fahrt und den Fahrstil des Fahrers und haben Einfluss auf die Fahrzeugdaten 10. Dieser Einfluss der
 35 geschützten Daten 8 auf Fahrzeugdaten 10 wird als „Prägung“ bezeichnet.

Ein Fahrzeugdatensatz 10a kann daher durch eine Prägung beeinflusst sein. In einer Anordnung wird daher ein ungeprägter Fahrzeugdatensatz 9a, der eine Größe x_n enthält, durch die Prägung beeinflusst und zu dem durch die Datenerfassungseinheit 3 aufgezeichneten Fahrzeugdatensatz 10a gemacht. Ungeprägte Fahrzeugdaten 9 enthalten
 5 zumindest einen ungeprägten Fahrzeugdatensätze 9a. Auf ungeprägte Fahrzeugdatensätze 9a kann nicht direkt zugegriffen werden, weil diese durch die Prägung erst in Fahrzeugdatensätzen 10a aufgehen und als Fahrzeugdatensätze 10a erfasst werden. Es sei aber angemerkt, dass nicht jeder erfasste Fahrzeugdatensatz 10a durch geschützte Daten 8 geprägt sei muss.

10 Diese Prägung kann ganz unterschiedlich erfolgen. Einerseits prägen Daten, wie Fahrer, Beifahrer, Positionsdaten die Fahrzeugdaten 10, diese können aber auch von Dritten (z.B. andere Verkehrsteilnehmer) und Umweltfaktoren (Regen, Schnellfall) geprägt werden. Beispielsweise wird ein zeitlicher Verlauf einer Beschleunigung bei einer Fahrt entlang einer bestimmten Strecke vom Fahrzeugtyp und der Nutzlast, vom Fahrverhalten des Fahrers, von
 15 der Umgebung (z.B. Passanten), vom Zeitpunkt der Fahrt usw. abhängig sein. Ein zeitlicher Verlauf einer Beschleunigung wird andererseits auch von der Strecke selbst abhängig sein.

Der Einfluss der Prägung auf einen Fahrzeugdatensatz 10a kann beispielsweise mittels zumindest einer Korrelationsfunktion C beschrieben werden (Fig.2). Die Korrelationsfunktion C beschreibt, wie geschützte Daten 8 den ungeprägten Fahrzeugdatensatz 9a prägen und in
 20 einem Fahrzeugdatensatz 10a aufgehen. Die Korrelationsfunktion C ist abhängig von den geschützten Daten 8 und beispielsweise eine bekannte Funktion, welche den Einfluss von geschützten Daten 8 auf Fahrzeugdaten 10 beschreibt. Die Korrelationsfunktionen C für verschiedene ungeprägte Fahrzeugdatensätze 9a und/oder geschützte Daten 8 sind in der Regel nicht gleich, da verschiedene ungeprägte Fahrzeugdatensätze 9a unterschiedlich von
 25 geschützte Daten 8 geprägt werden können. Eine Korrelationsfunktion C kann beispielsweise aus der Literatur bekannt sein, oder über Testreihen bestimmt worden sein. Die Korrelationsfunktion C kann von der Anzahl der generierten Fahrzeugdatensätze 10a abhängig sein. Beispielsweise, kann bei wiederholter Fahrt durch einen identen Fahrer das Beschleunigungsprofil immer ähnlich oder sogar gleich sein. Durch eine größere Menge an
 30 gleichen Fahrzeugdatensätzen 10a wird daher die Identifikation des Fahrers immer wahrscheinlicher. So eine Korrelationsfunktion C kann daher benutzt werden um den Einfluss der Prägung auf die Fahrzeugdaten 10a zu beschreiben und möglicherweise auch zu gewichten.

Nicht jeder geschützte Datensatz 8a muss mit jedem Fahrzeugdatensatz 10a eine
 35 Korrelationsfunktion C aufweisen. Beispielsweise, kann das Fahrerverhalten auf Beschleunigung und abgerufene Motorleistung Einfluss haben, nicht aber auf Außentemperatur oder Luftfeuchte. Die gewählte Fahrstrecke kann beispielsweise die

dadurch erlebten Umweltbedingungen beeinflussen, wie Gewitter, Schneefall und hat daher Einfluss auf Temperatur und Luftfeuchtedaten.

Die mit einer Datenerfassungseinheit 3 erfassten Fahrzeugdaten 10 erlauben aufgrund dieser Prägung einen indirekten Rückschluss auf die geschützten Daten 8. Hat man
 5 beispielsweise ein Beschleunigungsprofil in Abhängigkeit der Zeit t als Fahrzeugdatensatz 10a, kann mittels zweifacher Integration eine zurückgelegte Strecke und damit eine theoretische Position relativ zum Start ermittelt werden. Mit Kenntnis des möglichen Startpunktes, welcher aus naheliegender Überlegung gegeben sein kann, könnte die Route rückgerechnet werden. Aus den Fahrzeugdaten 10 könnte auch auf eine Fahrweise eines
 10 Fahrers rückgeschlossen werden, was letztendlich einen Rückschluss auf die Identität und weiterer Eigenschaften des Fahrers ermöglicht.

Die in der Verarbeitungseinheit 4 enthaltene Vorverarbeitung 17 dient dazu, die Fahrzeugdaten 10 vor der Weiterleitung an die Auswerteeinheit 5 so zu verändern, dass ein
 Rückschließen auf die geschützten Daten 8 anhand der Fahrzeugdaten 10

15 unwahrscheinlich, oder gar unmöglich, wird. Die Vorgabe der Wahrscheinlichkeit auf einen möglichen Rückschluss wird über einen Anonymitätsgrad 14 („Degree of Anonymity“ - DoA) beschrieben (Fig. 3). Dieser Anonymitätsgrad 14 kann in einer bevorzugten Ausführungsform als bekannte k -Anonymität ausgestaltet sein. Der Anonymitätsgrad 14 ist eine Kenngröße, die den Rückschluss auf geschützte Daten 8 darstellt und wird für die Vorverarbeitung 17 der
 20 Fahrzeugdaten 10 vorgegeben, beispielsweise von einem Anwender und ist also bekannt.

Eine Möglichkeit der Quantifizierung des Anonymitätsgrades 14 besteht in der Wahrscheinlichkeit p , dass eine bestimmte Person (über die geschützten Daten 8) in den gesicherten Fahrzeugdaten 12 identifizierbar ist. Der Anonymitätsgrad beträgt dann $1-p$. So beträgt beispielsweise bei einer Wahrscheinlichkeit eine Zuordenbarkeit von $p = 0,01$ (1%)
 25 der Anonymitätsgrad 0.99 (99%).

Eine ebenfalls mögliche Quantifizierung besteht in der Angabe der kleinstmöglichen Gruppe von N Personen, für die eine Zuordnung der geschützten Daten gleichwahrscheinlich ist. Im eben genannten Beispiel mit $p=0,01$ beträgt $N = 100$. Beispielsweise, müsste bei einem Anonymitätsgrad 14 von größer 99% für die Identifikation des Fahrers (bei gleicher
 30 Wahrscheinlichkeit der Identifikation eines Fahrers) ein Fahrzeugdatensatz 10a von der Vorverarbeitung 17 so verändert werden, dass zumindest ein resultierender gesicherter Fahrzeugdatensatz 12a entsteht. Bei der bevorzugten Verwendung einer k -Anonymität mit $k > 99$ als Anonymitätsgrad 14 wird der Fahrzeugdatensatz 10a so verändert, dass bei Datenauswertung des gesicherten Fahrzeugdatensatzes 12a ein Rückschluss auf
 35 mindestens 100 Personen ($N = 100$) gleichwahrscheinlich ist.

In einer weiteren Ausführungsform kann der Anonymitätsgrad 14 auch an einen Kostenfaktor gebunden werden, welcher den nötigen Aufwand zur Ermittlung von einem bestimmten geschützten Datensatz 8a aus einem resultierenden gesicherten Fahrzeugdatensatz 12a beschreibt. Dieser Aufwand ist über Rechenleistung, Zeitaufwand und Manpower bei einem Angriff errechenbar oder abschätzbar. Dem Angriff kann je nach verbundenem Aufwand eine Kategorisierung (Level an Security) zugeordnet werden, wie beispielsweise „niedrig“, „mittel“, „hoch“. „Niedrig“ würde sehr geringen Aufwand, wie zuvor in Rechenleistung, Zeitaufwand darstellen, während „hoch“ einen sehr hohen Aufwand charakterisiert.

Für verschiedene ungeprägte Fahrzeugdaten 9 können auch verschiedene

Anonymitätsgrade 14 verwendet werden.

Diese Kategorisierungen können für geschützte Daten 8 vom Anwender getroffen werden und sind beispielsweise abhängig von der Art der geschützten Daten 8. Dadurch, dass ein Angriff nie völlig ausgeschlossen werden kann, kann anhand dieser Kategorisierung immer nur eine Risikominimierung durchgeführt werden. Anhand der Kategorisierungen kann der Risikominimierung eine Wahrscheinlichkeit zugeordnet werden, dass ein Angreifer auf geschützte Daten 8 einen Zugriff schafft. Beispielsweise kann gefordert sein, dass die Wahrscheinlichkeit, für eine Kategorisierung von „hoch“, anhand eines Fahrzeugdatensatzes 10a auf eine bestimmte Person rückgeschlossen werden kann, kleiner als 1% gleichwahrscheinlich sein soll. Der Wert des Anonymitätsgrad 14 würde sich dann auf einen Wahrscheinlichkeitswert, wie schon oben errechnet, von größer 99% belaufen.

Der gesicherte Fahrzeugdatensatz 12a enthält dann eine aus einer erfassten Größe x_n^* durch die Vorverarbeitung 17 hervorgehende veränderte Größe y_n , die der Vorgabe des Anonymitätsgrads 14 entspricht. Der Anonymitätsgrad 14 kann vom Anwender, beispielsweise vom Fahrer selbst oder einem Entwicklungsingenieur, eingestellt werden.

Der Anonymitätsgrad 14 sollte so gewählt werden, dass der Informationsgehalt der Daten möglichst wenig, bzw. nicht mehr als benötigt, reduziert wird. Wird der Anonymitätsgrad 14 vom Anwender zu hoch angesetzt, sind die gesicherten Fahrzeugdaten 12 möglicherweise auch für einen legitimen Benutzer unbrauchbar. Beispielsweise werden bei einer RDE Messfahrt genaue Angaben über das Fahrverhalten (Beschleunigung, Fahrweise) benötigt, die aber bei einem hohen Anonymitätsgrad 14 verändert werden würden, um keine Zuordnung zu einem bestimmten Fahrer zu ermöglichen. Bevorzugterweise sind die Integrität der Fahrzeugdaten 10a zur Abgaszusammensetzung bei einer Messkampagne zur RDE für den legitimen Benutzer wichtiger, als die beispielsweise GPS-Geokoordinaten bei gleicher Messkampagne. Danach kann der Anonymitätsgrad 14 bei dieser Messkampagne für den Fahrzeugdatensatz 10a „GPS-Geokoordinaten“ wesentlich höher gewählt werden, als für die Abgaszusammensetzung.

Die Vorverarbeitung 17 kann verschiedene Methoden 16 zur Datenverarbeitung benutzen. Beispielsweise können in der Vorverarbeitung häufig genutzte Methoden 16 wie Normalisieren, Anonymisieren, Überlagern, Reduktion der Auflösung etc. erfolgen. Unter Normalisieren versteht man das Abbilden der Absolutwerte einer Größe x_n^* eines Fahrzeugdatensatzes 10a auf Werte zwischen 0 und 1 (bzw. -1 und +1). Das kann durch Division aller Werte, durch den Höchstwert der Werte erfolgen. Das ist z.B. eine geeignete Methode, um Geschwindigkeitsdaten oder Beschleunigungsdaten zu verarbeiten. Beispielsweise erschwert es durch Integration der Beschleunigung auf die Strecke der Testfahrt zurück zu schließen, wenn der Höchstwert bzw. Bezugswert nicht bekannt ist.

In einer bevorzugten Ausführungsform kann auch eine Reduktion der Auflösung angewandt werden. In anschaulicher Weise werden z.B. Ortschaftskennzahlen von durchfahrenen Orten bei einer Testfahrt vom 5 Stellen auf 2 Stellen reduziert. Testfahrer werden beispielsweise nicht mit ihren Namen gespeichert, sondern nur als „männlich“ oder „weiblich“ abstrahiert. Ein solches Maskieren wird beispielsweise auch bei digitalen Straßenkarten verwendet. Die niederwertigsten Bits von Objektkoordinaten werden beispielsweise auf null gesetzt und dadurch erfolgt ein „Verpixeln“ der digitalen Straßenkarte. Werden beispielsweise GPS-Daten auf diese Weise in der Auflösung reduziert, wird die Genauigkeit der erfassten GPS-Position reduziert. Solche Methoden werden auch oft als „Microaggregation“ bezeichnet.

Bei der Methode 16 „Anonymisierung“ werden Personen-zuordenbare Daten entfernt oder durch nicht-zuordenbare Daten ersetzt. Als Beispiel kann der Aufmerksamkeitsassistent genannt werden, der in manchen Fahrzeugen mit Hilfe einer, dem Fahrer zugewandten, Videokamera implementiert ist, um die Pupillenaktivität des Fahrers zu überwachen. Üblicherweise werden diese Videodaten sofort nach der Auswertung gelöscht; könnte aber für Entwicklung oder Fehlersuche in einer späteren Analyse erforderlich sein. Diese

Fahrzeugdaten (10a) könnten in diesem Fall biometrische Personenmerkmale (beispielsweise Augenfarbe und Iris-Muster) enthalten. Diese werden mit der Kamera zwar miterfasst, sind aber für die Erkennung der Aufmerksamkeit durch Überwachung der Pupillenaktivität nicht unbedingt erforderlich. In diesem Fall wäre eine Methode 16, die tatsächliche Augenfarbe durch eine zufällig gewählte zu ersetzen (Anonymisierung). Eine weitere Methode 16 könnte den Bereich der Iris im Bild mit einem Bildrauschen überlagern, und somit genaue Zuordenbarkeit erschweren bzw. verunmöglichen.

Die Methoden 16 der Datenverarbeitung sind nur Beispiele zur Verdeutlichung der Funktionsweise und nicht auf die genannten limitiert, sondern alle Methoden 16, welche für einen Fachmann ersichtlich sind, können angewandt werden.

Alle möglichen Formen der Datenverarbeitung werden nachfolgend als Methoden 16 bezeichnet. Die Vorverarbeitung 17 verwendet zumindest eine Methode 16, welche in der

Vorverarbeitung 17 benutzt wird, und abhängig vom Fahrzeugdatensatz 10a gewählt ist. Es ist aber natürlich möglich, dass auf einen Fahrzeugdatensatz 10a auch mehrere Methoden 16 angewendet werden. Die Auswahl der geeigneten oder benötigten Methoden 16 kann beispielsweise vom Anwender für eine gegenständliche Messkampagne vorgeben sein oder von der Vorverarbeitung 17, automatisiert erfolgen. Bevorzugterweise verändert eine Methode 16 einen Fahrzeugdatensatz 10a zu zumindest einem gesicherten Fahrzeugdatensatz 12a. Höchst bevorzugt, wird der Fahrzeugdatensatz 10a durch ein Vorverarbeitung 17 analysiert und nur verändert, wenn ein Rückschluss auf geschützte Daten 8 möglich ist.

In einer bevorzugten Ausführung kann eine Methode 16 einen Fahrzeugdatensatz 10a unabhängig von einer Laufvariablen k, wie Zeit oder Geokoordinaten, verarbeiten. Beispielsweise wird die gleiche Methode 16 permanent auf einen Fahrzeugdatensatz 10a angewandt und erzeugt dabei einen gesicherten Fahrzeugdatensatz 12a. Dabei kann die Methode 16 unverändert bleiben und immer in gleicher Weise auf einen Fahrzeugdatensatz 10a angewandt werden.

In einer bevorzugten Ausführung enthält die Vorverarbeitung 17 einen Ablauf wie in Fig.4 dargestellt. Eine Vorverarbeitung 17 ist vorzugsweise eine softwareimplementierte Lösung die beispielsweise nach dem Flusschema in Fig.4 funktioniert. Nach einem Starten der Routine S, wird ein Fahrzeugdatensatz 10a von der Vorverarbeitung 17 analysiert. Entspricht der Fahrzeugdatensatz 10a dem vorgegebenen Anonymitätsgrad 14 (yes) wird er als gesicherter Fahrzeugdatensatz 12a gespeichert, beispielsweise in der Speichereinheit 11, und die Vorverarbeitung ist beendet (Arbeitsschritt E). Ein gesicherter Fahrzeugdatensatz 12 kann dann an eine Auswerteeinheit 5 zur weiteren Verarbeitung übermittelt werden. Falls der Fahrzeugdatensatz 10a nicht dem Anonymitätsgrad 14 entspricht (no), wird dieser über eine erste Methode 16 (Arbeitsschritt A) verändert. Dadurch entsteht ein veränderter Fahrzeugdatensatz 10a'. Wenn der veränderte Fahrzeugdatensatz 10a' dem Anonymitätsgrad 14 entspricht, wird dieser als gesicherter Fahrzeugdatensatz 12a gespeichert und die Vorverarbeitung 17 ist beendet (Arbeitsschritt E). Bei Nichtentsprechen kann die Vorverarbeitung 17 wählen, ob sie den ursprünglichen Fahrzeugdatensatz 10a oder den veränderten Fahrzeugdatensatz 10a' als Input für eine zweite Methode 16 (Arbeitsschritt B) wählt. Das kann abhängig von den angewandten Methoden 16 und/oder kann vom Anwender vorgegeben sein. Falls nach Anwenden der zweiten Methode 16 der Anonymitätsgrad 14 erfüllt ist (yes), wird der veränderte Fahrzeugdatensatz 10a' wieder als gesicherter Fahrzeugdatensatz 12a gespeichert. Diese Schleife kann, unter Anwendung verschiedener Methoden 16, solange wiederholt werden, bis der Anonymitätsgrad 14 erfüllt ist. Fig. 4 kennzeichnet diese Schleife mit Arbeitsschritt X.

Alternativ könnte ein Fahrzeugdatensatz 10a auch verworfen werden, wenn der Anonymitätsgrad 14 nach einer vorgegebenen Anzahl an Methoden 16 nicht erfüllt werden kann. Hierbei können die anzuwendenden Methoden 16 und auch deren Reihenfolge vorab festgelegt (z.B. durch Konfiguration durch einen Anwender) oder vorgegeben sein.

5 Vorzugsweise wird der oben genannte Ablauf für einen Fahrzeugdatensatz 10a in regelmäßigen Intervallen abhängig von der Laufvariable k wiederholt, beispielsweise als Funktion der Zeit. Beispielsweise können analog zu obiger Beschreibung auch nur Teile eines von der Laufvariable k abhängigen Fahrzeugdatensatzes 10a gespeichert werden und andere bei Nichterfüllen des Anonymitätsgrades 14 verworfen werden.

10 Beispielsweise können in die Vorverarbeitung 17 auch Korrelationsfunktionen C einfließen, oder auch der Kontext 13 (Fig. 1). Der Kontext 13 beschreibt die Umgebung des Fahrzeugs 2, welche über verschiedene Datenerfassungseinheiten 3 aufgenommen werden kann. In einer bevorzugten Ausführungsform können Korrelationsfunktionen C und Kontext 13 auf die Auswahl der Methoden 16 Einfluss haben, in einer höchst bevorzugten Ausführungsform
15 können Korrelationsfunktionen C und Kontext 13 auch Einfluss auf die Wirkung einer einzelnen Methode 16 haben. Beispielsweise, kann diese Methode 16 verschieden stark auf einen Fahrzeugdatensatz 10a angewandt werden, und beispielsweise eine unterschiedliche Reduktion der Auflösung in einem Fahrzeugdatensatz 10a bewirken.

Beispielsweise kann die Vorverarbeitung 17 in einer Weise funktionieren, dass bei niedrigem
20 Verkehrsaufkommen, gemessen durch den Kontext 13 anhand von GPS-Geokoordinaten, eine Methode 16 angewandt wird, welche eine hohe Reduktion der Auflösung der Position des Fahrzeuges 2 vornimmt um einen Anonymitätsgrad 14 zu erfüllen. Bei hohem Verkehrsaufkommen kann die Vorverarbeitung 17 mit der Methode 16 nur eine geringe Reduktion der Auflösung vornehmen oder sogar mit dem ursprünglichen Fahrzeugdatensatz
25 10a weiterverfahren und sofort einen gesicherten Fahrzeugdatensatz 12a erzeugen, welcher den vorgegeben Anonymitätsgrad 14 erfüllt. Der Kontext 13 könnte beispielsweise die Anwendung der Methode 16 (hohe Reduktion, niedrige Reduktion, gar keine Reduktion) im obigen Beispiel durch Übersenden der GPS-Geokoordinaten steuern, und so in die Vorverarbeitung 17 integriert werden.

30 In einer weiteren bevorzugten Ausführungsmethode können Korrelationsfunktionen C und Kontext 13 auch Einfluss auf den Anonymitätsgrad 14 haben und so die Anwendung von Methoden 16 in der Vorverarbeitung 17 indirekt beeinflussen.

Die Summe aller Methoden 16, welche in der Vorverarbeitung 17 genutzt werden, heißt die Methodenbibliothek 15. In einer bevorzugten Ausführung werden nach Vorgabe des
35 Anwenders die Methoden 16 aus der Methodenbibliothek 15 für jeden Fahrzeugdatensatz 10a einzeln gewählt. In einer höchst bevorzugten Ausführungsform kann die Vorverarbeitung

17 selbstständig die Methoden 16 aus der Methodenbibliothek 15 auswählen, um einen gesicherten Fahrzeugdatensatz 12a zu erhalten. Die Anwendung der Methoden 16 kann wie in Fig.4 gegeben sequentiell erfolgen, aber auch eine parallele Anwendung von Methoden 16 wäre denkbar. Eine Methodenbibliothek 15 kann aus einer Anzahl an vorgespeicherten Methoden 16, welche oben beschrieben worden sind, bestehen. Es können vom Anwender auch neue Methoden 16 in die Methodenbibliothek eingespeist werden, um die Sicherheit der geschützten Daten 8 zu gewährleisten. Die geschützten Daten 8 können beispielsweise durch neue Arten von Angriffen erkannt werden und von Analysemethoden aus den gesicherten Fahrzeugdaten 12 ermittelt werden, oder neue Messmethoden im Fahrzeug 2 erfordern neue Methoden 16a zu Gewährleistung der Sicherheit der geschützten Daten 8. In einer bevorzugten Ausführungsform wird die Methodenbibliothek 15 auf Subscription-Basis in regelmäßigen Zeitintervallen upgedatet und dabei neue Methoden 16a eingespeist. Neue Methoden 16a können beispielsweise erst in Entwicklung sein und auf Methoden 16 basieren, oder einen völlig anderen Ansatz verfolgen. Bevorzugt können neue Methoden 16a über „Big data“ Analyse von durchgeführten Testfahrten des Fahrzeugs 2 entwickelt werden. Solch ein Update kann über drahtlose Übertragungsprotokolle wie Nahkommunikationsprotokollen wie beispielsweise Bluetooth, oder über Fernkommunikationsprotokolle wie 4G und 5G zeitnah erfolgen. In einer bevorzugten Ausführungsform kann ein Update aber auch bei einem planmäßigen Werkstätten-Aufenthalt des Fahrzeuges 2 über einen Fahrzeugbus oder Nahkommunikationsprotokollen wie Bluetooth aufgespielt werden.

Die Vorverarbeitung 17 erzeugt mittels Methoden 16 gesicherte Fahrzeugdaten 12 mit zumindest einem gesicherten Fahrzeugdatensatz 12a ($y_1(t)$ bis $y_n(t)$). Diese gesicherten Fahrzeugdaten 12 werden erst nach Vorverarbeitung 17 im Fahrzeug 2 gespeichert oder gesendet. Fahrzeugdaten 10 werden daher nicht gespeichert. So ist es nicht möglich auf Fahrzeugdaten 10 und geschützte Daten 8 zuzugreifen.

Dabei können die gesicherten Fahrzeugdaten 12 im Nachhinein am Ort einer Datenauswertung 6 ausgelesen werden. Dieses Auslesen kann bevorzugt kabelgebunden über eine Steckverbindung zum Datentransfer erfolgen, aber auch kabellos, wie über WLAN oder Bluetooth, ausgelesen werden. Die gesicherten Fahrzeugdaten 12 können einer Auswerteeinheit 5 zugefügt werden. Die gesicherten Fahrzeugdaten 12 können aber auch während der Testfahrt über eine Übertragungseinheit mittels einem Übertragungsprotokoll wie beispielsweise 5G (wie in Fig.1 mit dem Sendemast 7 angedeutet) gesendet werden und kann dann am Auswerteort 6 einer Auswerteeinheit 5 direkt (online) zugeführt werden.

Bevorzugterweise können die gesicherten Fahrzeugdaten 12 nach Verarbeitung auch in Fahrzeug 2 ausgelesen werden.

In einer beispielhaften Ausführung in Fig.5 wird demonstrativ aber nicht abschließend die Funktionsweise der Vorverarbeitung 17 in der Verarbeitungseinheit 4 beschrieben. Ein Fahrzeug 2 macht eine Testfahrt in ländlichem Gebiet 19 mit wenig anderen Verkehrsteilnehmern 18; neben anderen Fahrzeugdaten 10a wird auch die Fahrzeugposition über GPS zyklisch, beispielsweise mit 10 Hz, erfasst und als Fahrzeugdatensatz 10a aufgezeichnet.

Durch Fahrer und Straßennetz und andere Verkehrsteilnehmer 18 werden Fahrzeugdaten 10 geprägt, beispielsweise durch den Fahrstil des Fahrers, der den zeitlichen Verlauf der Positionsdaten prägt. Aus einer Zeitserie der Fahrzeugpositionsdaten kann nach einer ersten Ableitung nach der Zeit die Fahrzeuggeschwindigkeit ermittelt und beispielsweise die Einhaltung geltender Verkehrsregeln überprüft werden. Durch nochmaliges Ableiten entsteht daraus die Fahrzeugbeschleunigung, welche zur Abschätzung der Fahrweise (z.B. Bremsen vor Kreuzungen oder Kurven etc.) dienen kann.

Gleichzeitig sind während der Fahrt die Positionsdaten des Fahrzeugs 2 identisch mit den Positionsdaten des Fahrers. So kann durch einen Abgleich einer Zeitreihe der Fahrzeugpositionsdaten mit einer dritten Datenquelle der Fahrer des Fahrzeugs 2 identifiziert und damit die ermittelten Fahrzeugdaten 10 von Fahrverhalten als personenbezogene Daten zugeordnet werden. Als solche dritte Datenquelle können beispielsweise einzelne Positionsmessungen des Smartphones des Fahrers, die den Betreiber des Funknetzes vorliegen, oder Positionsdaten, die diverse Applikationen am Smartphone erfassen, verwendet werden. Lassen sich ein oder mehrere Messungen von (Position, Zeit) aus dem Smartphone durch Überprüfung einer Übereinstimmung von Ort und Zeit mit Messpunkten in der Zeitserie der Fahrzeugdaten 10a des Fahrzeugs finden, so kann auf eine Abhängigkeit geschlossen werden. Damit wird die hochaufgelöste Zeitserie der Positionsdaten des Fahrzeugs einer Person zuordenbar, ebenso wie die daraus abgeleiteten Erkenntnisse (Fahrstil, Beachtung der Verkehrsregeln, Verhalten gegenüber anderen Verkehrsteilnehmern etc.)

Um den Anonymitätsgrad 14 zu erfüllen und keine Rückschlüsse auf geschützte Daten 8, hier beispielsweise (a) der Fahrstil und (b) der genaue Aufenthaltsort des Fahrers zu ermöglichen, kann in der Vorverarbeitung 17 eine der folgenden Methoden 16 angewendet werden:

a. Reduktion der Auflösung

Dies kann entweder die zeitliche oder die räumliche Auflösung betreffen oder auch beides. Damit ergibt sich ein Bereich (zeitlich und räumlich), innerhalb dessen eine eindeutige Zuordenbarkeit nicht mehr möglich ist. Abhängig von der Anzahl von Smartphones mit verfügbaren Positionsdaten in diesem Bereich entsteht also eine

Mehrdeutigkeit in einer Zuordnung und damit ein gewünschter Anonymitätsgrad 14 (z.B. k-Anonymität).

Es ergibt sich in diesem Fall auch ein zweiter Effekt: Abhängig von der Straßendichte an der Position wird damit eine eindeutige Zuordnung zu einer bestimmten Fahrbahn schwieriger und auch die durch zeitliche Ableitung errechnete Geschwindigkeit bzw. Beschleunigung ungenauer. Damit kann die Bestimmung des Fahrstils erschwert oder verunmöglicht werden.

b. Normalisieren

Die Positionsdaten können auch als relative Position zu einem (nicht bekannt gegebenen) Startpunkt aufgezeichnet werden. Damit kann zwar Geschwindigkeit und Beschleunigung genau errechnet werden, aber eine Zuordnung zu einer bestimmten Verkehrsfläche und Bestimmung des Fahrverhaltens ist schwer bis gar nicht möglich. Zusätzlich ist auch ein Abgleich mit einer dritten Datenquelle wie oben beschrieben schwieriger.

Die Wirksamkeit von Variante a) ist also abhängig von der aktuellen Position bzw. der gegebenen vorherrschenden Dichte an Straßen und anderen Verkehrsteilnehmern (Kontext 13) sowie verfügbaren Positionsdaten von Smartphones. Sind wenige Verkehrsteilnehmer 18 in der Nähe wird die Auflösung stark reduziert. Der Durchmesser d wird also groß gewählt, was einer Testfahrt im ländlichen Gebiet 19 entspricht. Der durch die Vorverarbeitung 17 gesicherte Fahrzeugdatensatz 12a erlaubt nun weder Rückschluss auf Fahrer noch auf das Fahrzeug. Zum Kontrast kann bei einer Testfahrt eines Fahrzeugs 2 im städtischen Gebiet 20 die Methode der Auflösungsreduktion gering ausfallen. Der Radius d wird klein gewählt, da viele andere Verkehrsteilnehmer 18 in der Nähe sind und daher den vergebenen Anonymitätsgrad 14 mit kleiner Unschärfe in der Positionsbestimmung erfüllt werden kann.

Patentansprüche

1. Verfahren zur Datenerfassung in einem Fahrzeug (2) bestehend aus zumindest einer Datenerfassungseinheit (3) und zumindest einer Verarbeitungseinheit (4), wobei die
 - 5 zumindest eine Datenerfassungseinheit (3) zumindest einen Fahrzeugdatensatz (10a) aufzeichnet, der von zumindest einem geschützten Datensatz (8a) geprägt wird, **dadurch gekennzeichnet, dass** in der zumindest einen Verarbeitungseinheit (4) eine Vorverarbeitung (17) des zumindest einen Fahrzeugdatensatzes (10a) durchgeführt wird, wobei die Vorverarbeitung (17) unter Berücksichtigung eines vorgegebenen Anonymitätsgrads (14)
 - 10 folgende Schritte ausführt:
 - Laden des zumindest einen Fahrzeugdatensatzes (10a) in die Vorverarbeitung,
 - Anwenden von zumindest einer Methode (16) auf den zumindest einen Fahrzeugdatensatz (10a), um den zumindest einen Fahrzeugdatensatz (10a) zu verändern,
 - 15 • Analyse, ob mit dem veränderten Fahrzeugdatensatz (10a') der Anonymitätsgrad (14) erfüllt ist,
 - Speichern des zumindest einen veränderten Fahrzeugdatensatzes (10a'), der den Anonymitätsgrad (14) erfüllt, als zumindest einen gesicherten Fahrzeugdatensatz (12a), um einen indirekten Rückschluss auf den zumindest einen geschützten
 - 20 Datensatz (8a) aus dem gesicherten Fahrzeugdatensatz (12a) zu verhindern.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Vorverarbeitung (17) auf zumindest eine Methode (16) aus einer Methodenbibliothek (15) zugreifen kann.
3. Verfahren nach Ansprüchen 1 und 2 **dadurch gekennzeichnet, dass** die Vorverarbeitung (17) zumindest eine Methode (16) permanent auf einen Fahrzeugdatensatz
 - 25 (10a) anwendet und dabei zumindest ein gesicherter Fahrzeugdatensatz (12a) entsteht.
4. Verfahren nach Ansprüchen 1 und 2 **dadurch gekennzeichnet, dass** die Vorverarbeitung (17) abhängig von zumindest eine Laufvariable k zumindest eine Methode (16) auf den zumindest einen Fahrzeugdatensatz (10a) anwendet und dabei zumindest ein gesicherter Fahrzeugdatensatz (12a) entsteht.
- 30 5. Verfahren nach Ansprüchen 1 bis 4 **dadurch gekennzeichnet, dass** die Vorverarbeitung (17) von zumindest einer Korrelationsfunktion C und von einem Kontext (13) abhängt.
6. Verfahren nach Ansprüchen 1 bis 5 **dadurch gekennzeichnet, dass** die Vorverarbeitung (17) zumindest zwei Methoden (16) sequentiell oder parallel anwendet.

7. Verfahren nach Ansprüchen 1 bis 6 **dadurch gekennzeichnet, dass** die Methodenbibliothek (15) auf Subscription-Basis funktioniert und neue Methoden (16a) in die Methodenbibliothek (15) hinzugefügt werden.
8. Verfahren nach Ansprüchen 1 bis 7 **dadurch gekennzeichnet, dass** der Anonymitätsgrad (14) an einen Kostenfaktor gebunden wird und eine Kategorisierung erhält.
9. Vorrichtung zur Datenerfassung in einem Fahrzeug (2) bestehend aus zumindest einer Datenerfassungseinheit (3) und zumindest einer Verarbeitungseinheit (4), wobei die zumindest eine Datenerfassungseinheit (3) zumindest einen Fahrzeugdatensatz (10a) aufzeichnet, der von zumindest einem geschützten Datensatz (8a) geprägt ist, **dadurch gekennzeichnet, dass** in der die zumindest eine Verarbeitungseinheit (4) eine Vorverarbeitung (17) vorgesehen ist, wobei die Vorverarbeitung (17) unter Berücksichtigung eines Anonymitätsgrads (14) zumindest einen Fahrzeugdatensatz (10a) verändert, indem die Vorverarbeitung (17) zumindest eine Methode (16) verwendet, um den zumindest einen Fahrzeugdatensatz (10a) in einen veränderten Fahrzeugdatensatz (10a') umzuwandeln, und **dass** eine Speichereinheit (11) vorgesehen ist, die den veränderten Fahrzeugdatensatz (10a'), der den Anonymitätsgrad (14) erfüllt, als gesicherten Fahrzeugdatensatz (12a) speichert, sodass ein indirekter Rückschluss auf zumindest einen geschützten Datensatz (8a) aus dem gesicherten Fahrzeugdatensatz (12a) verhindert ist.

1/3

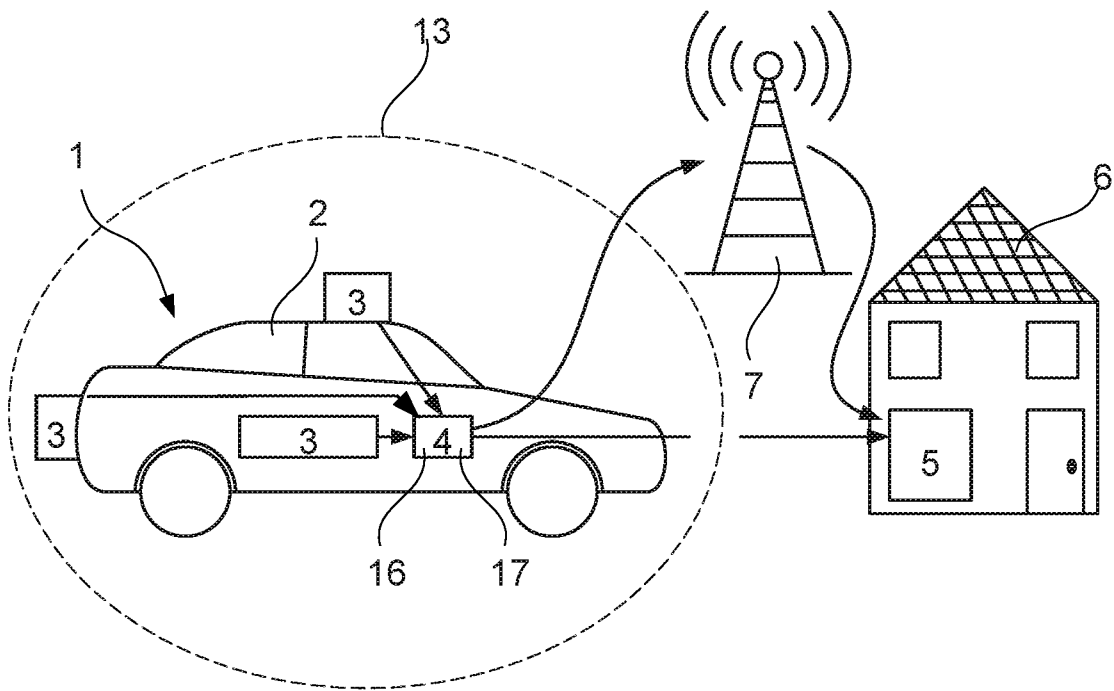


Fig. 1

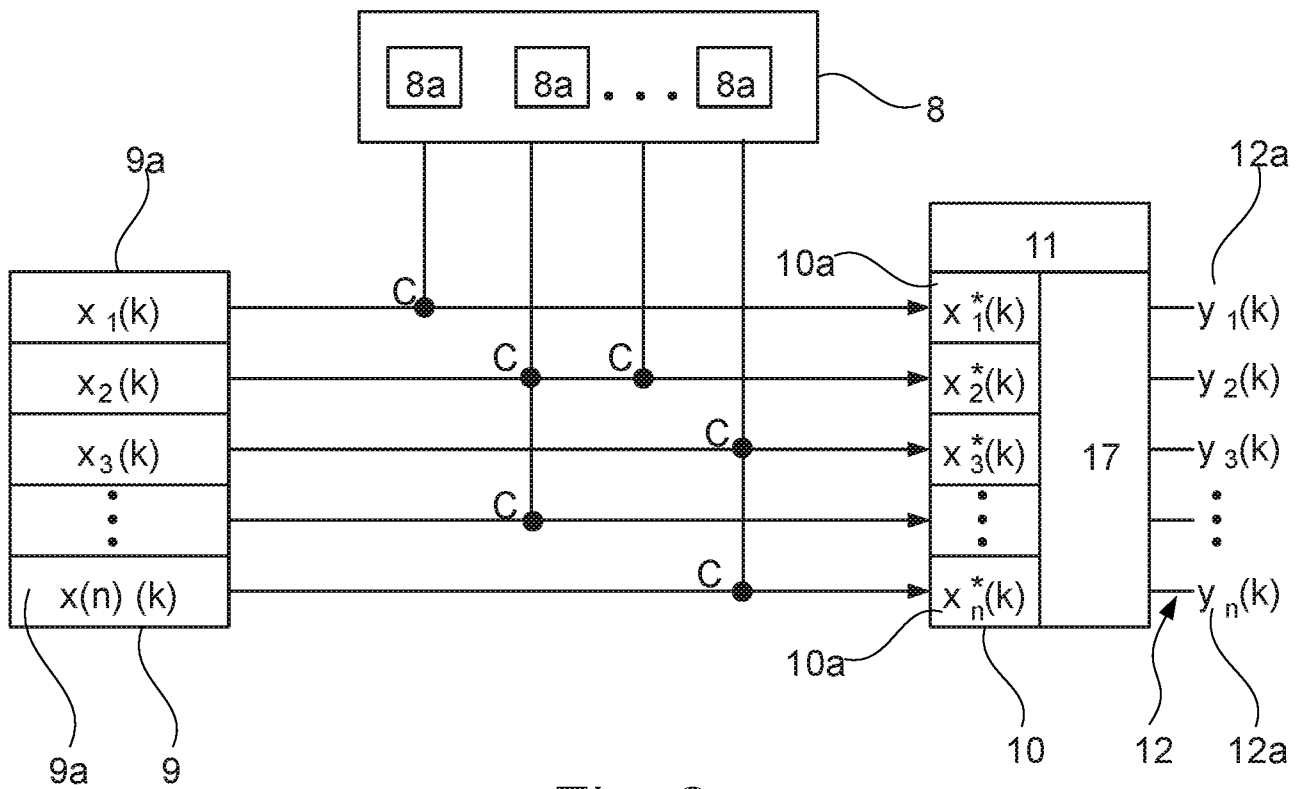
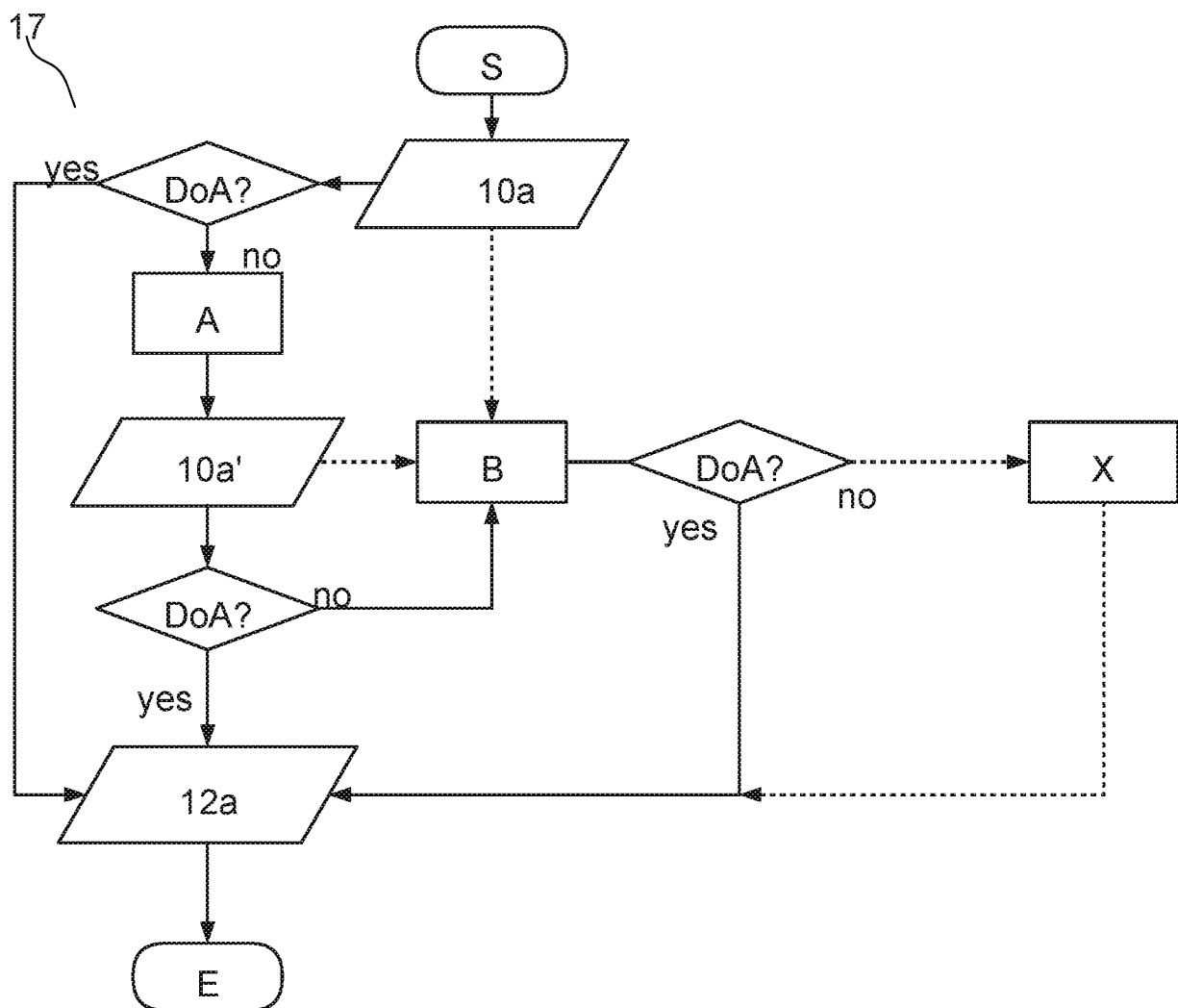
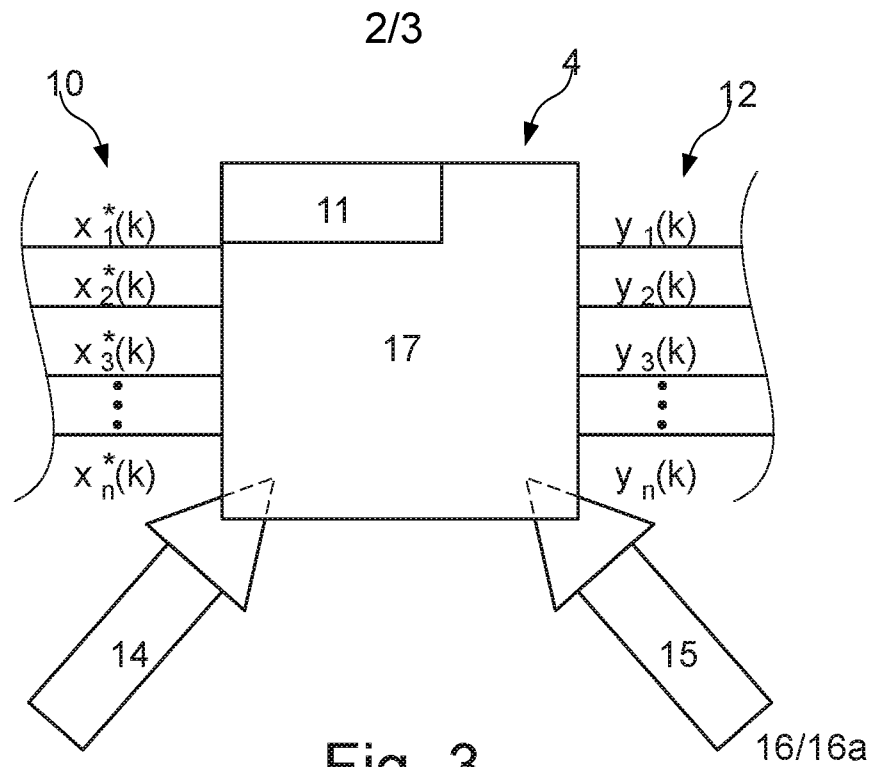


Fig. 2



3/3

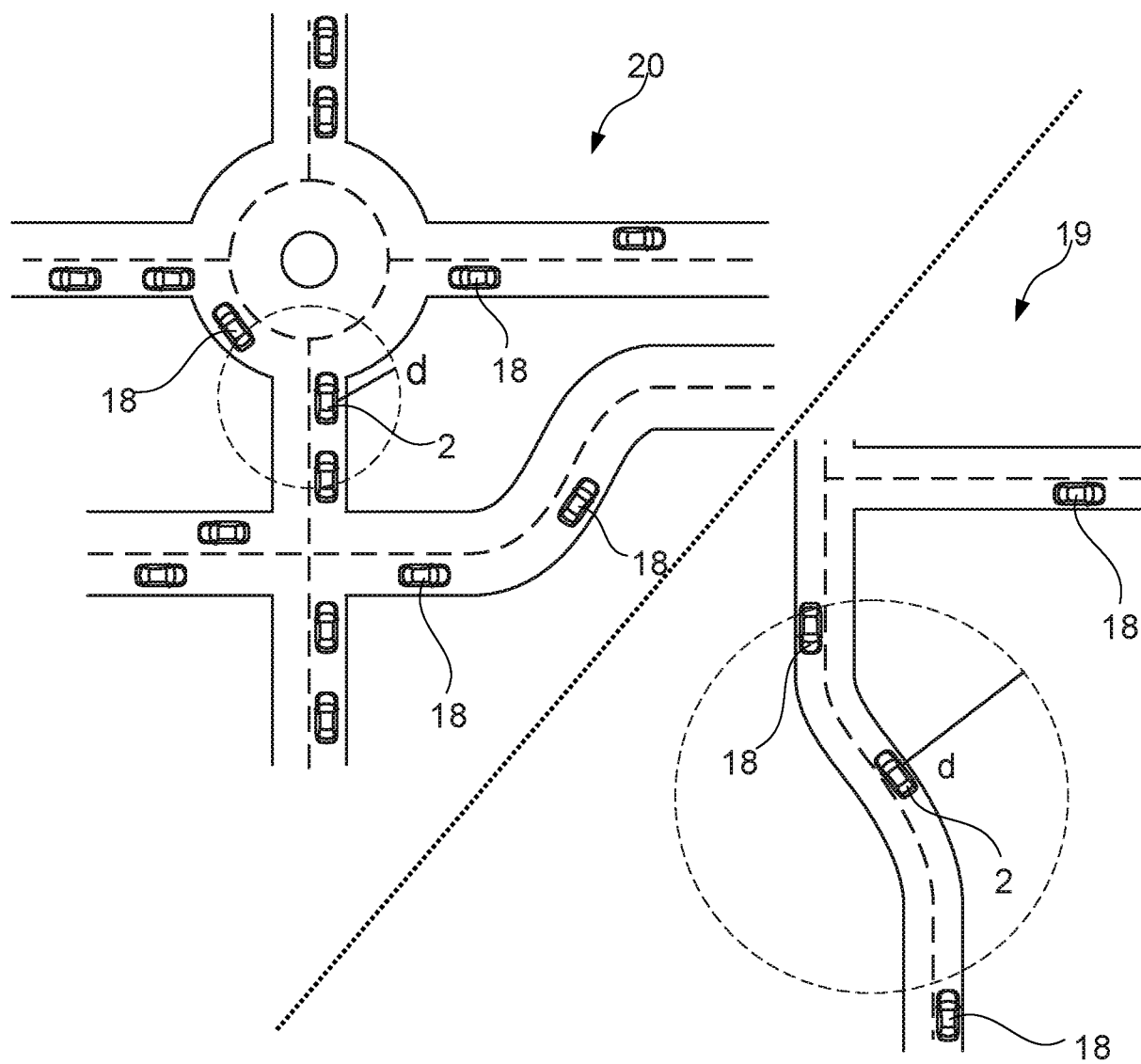


Fig. 5