(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 121 224 A1** 2017.05.18

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 121 224.5**
(22) Anmeldetag: **07.11.2016**
(43) Offenlegungstag: **18.05.2017**

(51) Int Cl.: ***B60R 25/00*** (2013.01)
B60R 16/02 (2006.01)

(30) Unionspriorität:
14/939,447 **12.11.2015** **US**

(71) Anmelder:
Ford Global Technologies, LLC, Dearborn, Mich., US

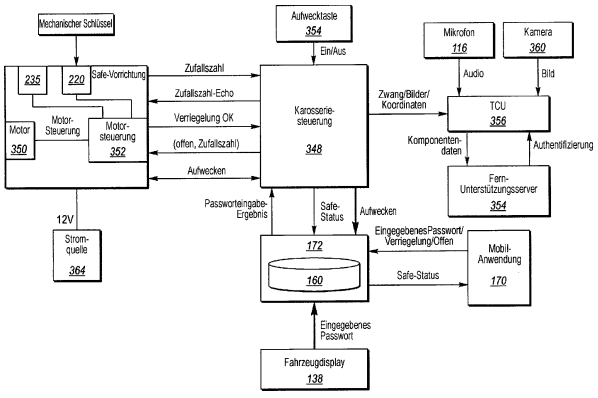
(74) Vertreter:
PATERIS Theobald Elbel Fischer, Patentanwälte, PartmbB, 10117 Berlin, DE

(72) Erfinder:
Makke, Omar, Lyon Township, Mich., US; Bowes Chowanic, Andrea, Commerce Township, Mich., US; Bajwa, Manpreet Singh, Novi, Mich., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **FAHRZEUGSAFE UND AUTHENTIFIZIERUNGSSYSTEM**

(57) Zusammenfassung: Ein Fahrzeugsafe-Authentifizierungssystem kann einen Fahrzeugsafe, eine Fahrzeugkamera und eine Steuereinheit, programmiert zum Empfangen einer Angabe von unbefugtem Zugang an dem Fahrzeugsafe, und ferner programmiert zum Aktivieren der Fahrzeugkamera als Reaktion auf die Angabe umfassen, wobei Aktivierung der Kamera Aufnehmen mindestens eines Bildes umfassen kann.



Beschreibung

TECHNISCHES GEBIET

[0001] Es werden hier Fahrzeugsafes und Authentifizierungssysteme offenbart.

STAND DER TECHNIK

[0002] Weil immer mehr Benutzer wertvolle Artikel in ihrem Fahrzeug lassen, wenn das Fahrzeug nicht benutzt wird, sind in Fahrzeugen oft während der Nichtbenutzung wertvolle Artikel untergebracht. Einige Fahrzeuge umfassen getrennte Fächer, wie etwa ein Handschuhfach, das mit einem physischen Schlüssel verriegelbar ist. Diese Systeme sind jedoch oft klein, Schlüssel werden oft verlegt und das Holen von Objekten aus dem verriegelten Fach kann einen durch einen Händler gelieferten Ersatzschlüssel erfordern. Außerdem sind diese Fächer oft das Ziel von Diebstahl.

KURZDARSTELLUNG

[0003] Ein Fahrzeugsafe-Authentifizierungssystem kann einen Fahrzeugsafe, eine Fahrzeugkamera und eine Steuereinheit, programmiert zum Empfangen einer Angabe von unbefugtem Zugang an dem Fahrzeugsafe und ferner programmiert zum Aktivieren der Fahrzeugkamera als Reaktion auf die Angabe umfassen, wobei Aktivierung der Kamera Aufnehmen mindestens eines Bildes umfassen kann.

[0004] Ein Fahrzeugsafe-Authentifizierungssystem kann einen Fahrzeugsafe, eine Fahrzeugkamera und eine Steuerung, programmiert zum Empfangen von Benutzereingaben, einschließlich eines Benutzerpassworts oder eines speziellen Passworts, und zum Senden eines Befehls für die Fahrzeugkamera zum Aufnehmen mindestens eines Bildes als Reaktion auf die das spezielle Passwort enthaltende Benutzereingabe, umfassen.

[0005] Ein Verfahren kann Folgendes umfassen: Empfangen eines Hinweissignals, das einen unbefugten Zugangsversuch zu einem fahrzeuginternen Safe angibt, Anweisen mindestens einer Fahrzeugkomponente, sich zu aktivieren, als Reaktion auf das Hinweissignal, wobei die Fahrzeugkomponente eine Kamera und/oder ein Mikrofon umfasst, Identifizieren eines Fahrzeugorts, Empfangen von Komponentendaten von der Fahrzeugkomponente und Senden der Komponentendaten und des Fahrzeugorts zu einem entfernten Server.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0006] Die Ausführungsformen der vorliegenden Offenbarung werden mit Sorgfalt in den angehängten Ansprüchen angeführt. Allerdings werden andere Merkmale der verschiedenen Ausführungsformen klarer und am besten durch Bezugnahme auf die folgende ausführliche Beschreibung in Verbindung mit den anliegenden Zeichnungen verstanden, in welchen:

[0007] die **Fig.** 1A und **Fig.** 1B ein beispielhaftes Diagramm eines Systems veranschaulichen, das verwendet werden kann, um Telematikdienste für ein Fahrzeug bereitzustellen,

[0008] **Fig.** 2 zeigt eine beispielhafte Safe-Vorrichtung für einen Fahrzeugkofferraumsafe;

[0009] **Fig.** 3 zeigt eine beispielhafte Blockdarstellung eines Teils eines Safe-Authentifizierungssystems;

[0010] **Fig.** 4 zeigt einen beispielhaften Prozess für das Safe-Authentifizierungssystem;

[0011] **Fig.** 5 zeigt einen beispielhaften Prozess zum Verriegeln der Safe-Vorrichtung über eine Mobil-Anwendung;

[0012] **Fig.** 6 zeigt einen beispielhaften Prozess zum Entriegeln der Safe-Vorrichtung über eine Schnittstelle;

[0013] **Fig.** 7 zeigt einen beispielhaften Prozess zum Entriegeln der Safe-Vorrichtung im Fall eines vergessenen Passworts; und

[0014] **Fig.** 8 zeigt einen beispielhaften Prozessfluss zum Aktivieren verschiedener Komponenten als Reaktion auf eine Authentifizierungsbedrohung.

AUSFÜHRLICHE BESCHREIBUNG

[0015] Wie erforderlich, werden hier detaillierte Ausführungsformen der vorliegenden Erfindung offenbart; es versteht sich jedoch, dass die offenbarten Ausführungsformen für die Erfindung, die in diversen und alternativen Formen verkörpert werden kann, rein beispielhaft sind. Die Figuren sind nicht notwendigerweise maßstabsgetreu; einige Merkmale können übertrieben oder minimiert sein, um Einzelheiten bestimmter Bauteile darzustellen. Daher sollen hier offenbarte spezielle strukturelle und funktionale Einzelheiten nicht als einschränkend interpretiert werden, sondern lediglich als eine repräsentative Basis, um einen Fachmann zu lehren, wie die vorliegende Erfindung auf verschiedene Art und Weise einzusetzen ist.

[0016] Es wird hier ein Safe-Authentifizierungssystem offenbart, das einen fahrzeuginternen Safe umfasst, der dafür ausgelegt ist, mit verschiedenen Fahrzeugschnittstellen und Mobil-Anwendungen zu kommunizieren, um sichere Mechanismen zum Ver-

riegeln und Entriegeln des Fahrzeugsafes bereitzustellen. Wenn eine Angabe empfangen wird, dass möglicherweise gerade ein unbefugter Zugangsversuch abläuft, kann eine Telematiksteuereinheit verschiedene Fahrzeugkomponenten, wie etwa Fahrzeugkameras, aktivieren, um zu versuchen, Bilder des potentiellen unbefugten Zugangs aufzunehmen. Die Steuereinheit kann diese Bilder zusammen mit einem Fahrzeugort zu den entsprechenden Behörden senden. Die Steuereinheit kann auch Benutzer authentifizieren, falls ein Passwort vergessen wurde.

[0017] Die **Fig.** 1A und **Fig.** 1B veranschaulichen ein beispielhaftes Diagramm eines Systems **100**, das verwendet werden kann, um Telematikdienste für ein Fahrzeug **102** bereitzustellen. Das Fahrzeug **102** kann eines von verschiedenen Typen von Personenfahrzeugen, wie etwa ein Crossover-Utility-Vehicle (CUV), ein Sport-Utility-Vehicle (SUV), ein Lastwagen, ein Freizeitfahrzeug (RV), ein Boot, ein Flugzeug oder eine andere mobile Maschine zum Transportieren von Personen oder Gütern sein. Telematikdienste können, als einige nicht einschränkende Möglichkeiten, Navigation, Turn-by-Turn-Wegbeschreibungen, Fahrzeugzustandsberichte, Suche nach lokalen Unternehmen, Unfallberichtswesen und Freisprechen beinhalten. Bei einem Beispiel kann das System **100** das SYNC-System, das von The Ford Motor Company in Dearborn, MI, USA hergestellt wird, beinhalten. Es versteht sich, dass das veranschaulichte System **100** lediglich ein Beispiel darstellt und dass mehr, weniger und/oder anders gelegene Elemente verwendet werden können.

[0018] Die Rechnerplattform **104** kann einen oder mehrere Prozessoren **106** und Steuervorrichtungen aufweisen, die dazu konfiguriert sind, Anweisungen, Befehle und andere Routinen als Unterstützung der hier beschriebenen Prozesse durchzuführen. Zum Beispiel kann die Rechnerplattform **104** dazu ausgelegt sein, Anweisungen von Fahrzeuganwendungen **110** auszuführen, um Merkmale, wie zum Beispiel Navigation, Unfallberichtswesen, Satellitenfunkdecodierung, Freisprechen und Einparkhilfe bereitzustellen. Derartige Anweisungen und andere Daten können auf eine nichtflüchtige Weise unter Verwendung einer Vielzahl von Arten computerlesbarer Speichermedien **112** geführt werden. Das computerlesbare Medium **112** (auch als ein prozessorlesbares Medium oder Speicher bezeichnet) beinhaltet ein beliebiges nicht vergängliches Medium (z. B. ein greifbares Medium), das an einer Bereitstellung von Anweisungen oder anderen Daten beteiligt ist, die von dem Prozessor **106** der Rechnerplattform **104** gelesen werden können. Computerausführbare Anweisungen können von Computerprogrammen kompiliert oder interpretiert werden, die unter Verwendung einer Vielzahl von Programmiersprachen und/oder -technologien erstellt werden, darunter, aber ohne Beschränkung, und entweder allein oder in Kombination Java, C, C++, C#, Objective C, Fortran, Pascal, Java Script, Python, Perl und PL/SQL.

[0019] Die Rechnerplattform **104** kann mit verschiedenen Merkmalen versehen sein, die es den Fahrzeuginsassen ermöglichen, an die Rechnerplattform **104** anzukoppeln. Die Rechnerplattform **104** kann zum Beispiel einen Audioeingang **114**, der dazu konfiguriert ist, gesprochene Befehle von Fahrzeuginsassen über ein verbundenes Mikrofon **116** zu empfangen, und einen Hilfsaudioeingang **118**, der dazu konfiguriert ist, Audiosignale von verbundenen Vorrichtungen zu empfangen, beinhalten. Der Hilfsaudioeingang **118** kann eine physische Verbindung, wie etwa ein elektrischer Draht oder ein Glasfaserkabel, oder ein drahtloser Eingang, wie etwa eine BLUETOOTH-Audioverbindung, sein. Bei einigen Beispielen kann der Audioeingang **114** dazu konfiguriert sein, Audioverarbeitungsfähigkeiten, wie etwa die Vorverstärkung von Niederpegelsignalen, und eine Umwandlung analoger Eingaben in digitale Daten zur Verarbeitung durch den Prozessor **106** bereitzustellen.

[0020] Die Rechnerplattform **104** kann auch einen oder mehrere Audioausgänge **120** zu einem Eingang eines Audiomoduls **122** bereitstellen, das über Audiowiedergabefunktionalität verfügt. Bei anderen Beispielen kann die Rechnerplattform **104** die Audioausgabe für einen Insassen durch Verwendung eines oder mehrerer (nicht veranschaulichter) dedizierter Lautsprecher bereitstellen. Das Audiomodul **122** kann einen Eingangswahlschalter **124** aufweisen, der dazu konfiguriert ist, Audioinhalt aus einer ausgewählten Audioquelle **126** für einen Audioverstärker **128** zur Wiedergabe über die Fahrzeuglautsprecher **130** oder (nicht veranschaulichte) Kopfhörer bereitzustellen. Die Audioquellen **126** können, als einige Beispiele, decodierte amplitudenmodulierte (AM) oder frequenzmodulierte (FM) Funksignale und Audiosignale aus der Audiowiedergabe von Compact Disc (CD) oder Digital Versatile Disk (DVD) beinhalten. Die Audioquellen **126** können auch Audio beinhalten, das von der Rechnerplattform **104** empfangen wird, wie zum Beispiel Audioinhalt, der durch die Rechnerplattform **104** erzeugt wird, Audioinhalt, der aus Flash-Speicherlaufwerken decodiert wird, die mit einem USB(Universal Serial Bus)-Subsystem **132** der Rechnerplattform **104** verbunden sind, und Audioinhalt, der vom Hilfsaudioeingang **118** über die Rechnerplattform **104** weitergeleitet wird.

[0021] Die Rechnerplattform **104** kann eine Sprachschnittstelle **134** nutzen, um eine Freisprechschnittstelle zur Rechnerplattform **104** bereitzustellen. Die Sprachschnittstelle **134** kann Spracherkennung von Audiosignalen, die über das Mikrofon **116** empfangen werden, gemäß Grammatik, die mit verfügbaren Befehlen assoziiert ist, und Erzeugung von Sprachaufforderungen für die Ausgabe über das Audiomodul **122** unterstützen. In manchen Fällen kann das

System dazu konfiguriert sein, die vom Eingangswahlschalter **124** ausgewählte Audioquelle zeitweise stumm zu schalten oder anders außer Kraft zu setzen, wenn eine Audioaufforderung zur Darstellung durch die Rechnerplattform **104** bereitsteht und eine andere Audioquelle **126** zur Wiedergabe ausgewählt ist.

[0022] Die Rechnerplattform **104** kann auch eine Eingabe aus Mensch-Maschine-Schnittstellen(MMS)-Steuerungen **136** empfangen, die dazu konfiguriert sind, eine Interaktion der Insassen mit dem Fahrzeug **102** bereitzustellen. Beispielsweise kann sich die Rechnerplattform **104** an eine oder mehrere Tasten oder andere MMS-Steuerelemente ankoppeln, die dazu konfiguriert sind, Funktionen auf der Rechnerplattform **104** aufzurufen (z. B. Lenkrad-Audiotasten, eine Push-to-Talk-Taste, Armaturenbrettsteuerungen usw.). Die Rechnerplattform **104** kann auch eine oder mehrere Anzeigen **138**, die dazu konfiguriert sind, mittels einer Videosteuerung **140** visuelle Ausgaben für die Fahrzeuginsassen bereitzustellen, ansteuern oder anderweitig mit diesen kommunizieren. In manchen Fällen kann das Display **138** ein Touchscreen sein, der ferner dazu konfiguriert ist, Berührungseingaben des Benutzers über die Videosteuerung **140** zu empfangen, während das Display **138** in anderen Fällen lediglich ein Display ohne Berührungseingabefähigkeiten sein kann.

[0023] Die Rechnerplattform **104** kann ferner dazu konfiguriert sein, über ein oder mehrere fahrzeuginterne Netzwerke **142** mit anderen Komponenten des Fahrzeugs **102** zu kommunizieren. Die fahrzeuginternen Netzwerke **142** können unter anderem ein Fahrzeugsteuerungsbereichsnetzwerk (CAN) und/oder ein Ethernet-Netzwerk und/oder eine medienorientierte Systemübertragung (MOST) beinhalten. Die fahrzeuginternen Netzwerke **142** können es der Rechnerplattform **104** ermöglichen, mit anderen Systemen des Fahrzeugs **102** zu kommunizieren, wie etwa mit einem Fahrzeugmodem **144** (das bei manchen Konfigurationen eventuell nicht vorhanden ist), einem globalen Positionierungssystem(GPS)-Modul **146**, das dazu konfiguriert ist, gegenwärtige Positions- und Richtungsinformationen des Fahrzeugs **102** bereitzustellen, und verschiedenen Fahrzeug-ECUs **148**, die dazu konfiguriert sind, mit der Rechnerplattform **104** zusammenzuarbeiten. Als einige nicht einschränkende Möglichkeiten können die Fahrzeug-ECUs **148** Folgendes umfassen: ein Kraftübertragungs-Steuermodul, ausgelegt zum Bereitstellen von Steuerung von Motorbetriebskomponenten (z. B. Leerlaufsteuerkomponenten, Kraftstoffablieferungskomponenten, Emissionssteuerungskomponenten usw.) und Überwachen von Motorbetriebskomponenten (z. B. Status von Motordiagknostikcodes); ein Karosseriesteuermodul (wie in **Fig.** 3 als Karosseriesteuerung **348** gezeigt), ausgelegt zum Verwalten verschiedener Leistungssteuerfunktionen wie Außenbeleuchtung, Innenbeleuchtung, schlüsselloser Zutritt, Fernstarten und Zugangspunkt-Statusverifikation; ein Funksendeempfängermodul, ausgelegt zum Kommunizieren mit Schlüsselanhängern oder anderen lokalen Vorrichtungen des Fahrzeugs **102**; und ein Klimatisierungs-Verwaltungsmodul, ausgelegt zum Bereitstellen von Steuerung und Überwachung von Heiz- und Kühlsystemkomponenten (z. B. Kompressorkupplungs- und Lüftersteuerung, Temperatursensorinformationen usw.).

[0024] Wie gezeigt wird, können das Audiomodul **122** und die MMS-Steuerungen **136** mit der Rechnerplattform **104** über ein erstes fahrzeuginternes Netzwerk **142-A** kommunizieren, und das Fahrzeugmodem **144**, das GPS-Modul **146** und die Fahrzeug-ECUs **148** können mit der Rechnerplattform **104** über ein zweites fahrzeuginternes Netzwerk **142-B** kommunizieren. Bei anderen Beispielen kann die Rechnerplattform **104** mit mehr oder weniger fahrzeuginternen Netzwerken **142** verbunden sein. Zusätzlich oder alternativ dazu können eine oder mehrere MMS-Steuerungen **136** oder andere Komponenten mit der Rechnerplattform **104** über andere als die dargestellten fahrzeuginternen Netzwerke **142** oder direkt ohne eine Verbindung mit einem fahrzeuginternen Netzwerk **142** verbunden sein.

[0025] Die Rechnerplattform **104** kann auch dazu konfiguriert sein, mit mobilen Vorrichtungen **152** der Fahrzeuginsassen zu kommunizieren. Die mobilen Vorrichtungen **152** können beliebige verschiedener Arten tragbarer Rechnervorrichtungen sein, wie etwa Mobiltelefone, Tablet-Computer, Smartwatches, Laptop-Computer, tragbare Musik-Player oder andere Vorrichtungen, die zur Kommunikation mit der Rechnerplattform **104** fähig sind. In vielen Beispielen kann die Rechnerplattform **104** einen drahtlosen Transceiver **150** enthalten (z. B. ein BLUETOOTH-Modul, einen ZIGBEE-Transceiver, einen WiFi-Transceiver, einen IrDA-Transceiver, einen RFID-Transceiver usw.), der dazu ausgelegt ist, mit einem kompatiblen drahtlosen Transceiver **154** der mobilen Vorrichtung **152** zu kommunizieren. Zusätzlich oder alternativ dazu kann die Rechnerplattform **104** mit der mobilen Vorrichtung **152** über eine verdrahtete Verbindung kommunizieren, wie etwa über eine USB-Verbindung zwischen der mobilen Vorrichtung **152** und dem USB-Subsystem **132**.

[0026] Das Kommunikationsnetzwerk **156** kann Kommunikationsdienste, wie etwa paketvermittelte Netzwerkdienste (z. B. Internetzugang, VoIP-Kommunikationsdienste), für Vorrichtungen, die mit dem Kommunikationsnetzwerk **156** verbunden sind, bereitstellen. Ein Beispiel eines Kommunikationsnetzwerks **156** kann ein zellulares Telefonnetzwerk beinhalten. Mobile Vorrichtungen **152** können eine Netzwerkkonnektivität zum Kommunikationsnetzwerk **156** über ein Vorrichtungsmodem **158** der mobi-

len Vorrichtung **152** bereitstellen. Um die Kommunikationen über das Kommunikationsnetzwerk **156** zu ermöglichen, können die mobilen Vorrichtungen **152** mit eindeutigen Vorrichtungskennungen (z. B. Mobilvorrichtungsnummern (MDNs), Internetprotokoll(IP)-Adressen usw.) assoziiert sein, um die Kommunikationen der mobilen Vorrichtungen **152** über das Kommunikationsnetzwerk **156** zu identifizieren. In manchen Fällen können Insassen des Fahrzeugs **102** oder Vorrichtungen, die eine Erlaubnis besitzen, sich mit der Rechnerplattform **104** zu verbinden, durch die Rechnerplattform **104** gemäß Daten **160** gepaarter Vorrichtungen identifiziert werden, die im Speichermedium **112** geführt werden. Die Daten **160** gepaarter Vorrichtungen können zum Beispiel die einzigartigen Vorrichtungskennungen mobiler Vorrichtungen **152**, die früher mit der Datenverarbeitungsplattform **104** des Fahrzeugs **102** gepaart waren, derart anzeigen, dass sich die Datenverarbeitungsplattform **104** automatisch, ohne Benutzereingriff, wieder mit den mobilen Vorrichtungen **152**, die in den Daten **160** gepaarter Vorrichtungen referenziert sind, verbindet.

[0027] Wenn eine mobile Vorrichtung **152**, die Netzwerkkonnektivität unterstützt, mit der Rechnerplattform **104** gekoppelt ist, kann die mobile Vorrichtung **152** der Rechnerplattform **104** ermöglichen, die Netzwerkkonnektivität des Vorrichtungsmodems **158** zu verwenden, um über das Kommunikationsnetzwerk **156** mit den entfernten Telematikdiensten **162** zu kommunizieren. Bei einem Beispiel kann die Rechnerplattform **104** einen Data-Over-Voice-Plan oder Datenplan der mobilen Vorrichtung **152** verwenden, um Informationen zwischen der Rechnerplattform **104** und dem Kommunikationsnetzwerk **156** zu kommunizieren. Zusätzlich oder alternativ dazu kann die Rechnerplattform **104** das Fahrzeugmodem **144** nutzen, um ohne Verwendung der Kommunikationsausstattung der mobilen Vorrichtung **152** Informationen zwischen der Rechnerplattform **104** und dem Kommunikationsnetzwerk **156** zu kommunizieren.

[0028] Ähnlich der Rechnerplattform **104** kann die mobile Vorrichtung **152** einen oder mehrere Prozessoren **164** beinhalten, die dazu konfiguriert sind, Anweisungen von mobilen Anwendungen **170** auszuführen, die von einem Speichermedium **168** der mobilen Vorrichtung **152** in einen Speicher **166** der mobilen Vorrichtung **152** geladen werden. Bei einigen Beispielen können die mobilen Anwendungen **170** konfiguriert sein, um mit der Rechnerplattform **104** über den drahtlosen Transceiver **154** und mit den entfernten Telematikdiensten **162** oder anderen Netzdiensten über das Vorrichtungsmodem **158** zu kommunizieren. Die Rechnerplattform **104** kann auch eine Vorrichtungsverbindungsschnittstelle **172** beinhalten, um die Integration von Funktionalität der mobilen Anwendungen **170** in die Grammatik von Befehlen, die über die Sprachschnittstelle **134** verfügbar sind, sowie in die Anzeige **138** der Rechnerplattform **104** zu ermöglichen. Die Vorrichtungsverbindungsschnittstelle **172** kann den mobilen Anwendungen **170** auch Zugang zu Fahrzeuginformationen bereitstellen, die der Rechnerplattform **104** über die fahrzeuginternen Netzwerke **142** zur Verfügung stehen. Einige Beispiele von Vorrichtungsverbindungsschnittstellen **172** weisen die SYNC APPLINK-Komponente des SYNC-Systems, das von The Ford Motor Company in Dearborn, MI, bereitgestellt wird, das CarPlay-Protokoll, das von der Apple Inc. in Cupertino, Kalifornien, bereitgestellt wird, oder das Android Auto-Protokoll, das von Google, Inc. in Mountain View, Kalifornien, bereitgestellt wird, auf. Die Fahrzeugkomponenten-Schnittstellenanwendung **174** kann eine derartige, in der mobilen Vorrichtung **152** installierte Anwendung sein.

[0029] Die Fahrzeugkomponenten-Schnittstellenanwendung **174** der mobilen Vorrichtung **152** kann dazu konfiguriert sein, Zugang zu einem oder mehreren Merkmalen des Fahrzeugs **102**, die durch das Fahrzeug **102** für eine Vorrichtungskonfiguration zur Verfügung gestellt werden, zu ermöglichen. In einigen Fällen kann auf die verfügbaren Merkmale des Fahrzeugs **102** von einer einzelnen Fahrzeugkomponenten-Schnittstellenanwendung **174** zugegriffen werden, wobei in einem solchen Falle die Fahrzeugkomponenten-Schnittstellenanwendung **174** konfiguriert sein kann, um anpassbar zu sein oder Konfigurationen, die die spezielle Marke, das spezielle Modell und Optionspakete des Fahrzeugs **102** unterstützen, aufrecht zu erhalten. Bei einem Beispiel kann die Fahrzeugkomponenten-Schnittstellenanwendung **174** dazu konfiguriert sein, eine Definition der Merkmale, die zum Steuern verfügbar sind, von dem Fahrzeug **102** zu empfangen, eine Benutzerschnittstelle anzuzeigen, die die verfügbaren Merkmale beschreibt, und dem Fahrzeug **102** Benutzereingaben von der Benutzerschnittstelle bereitzustellen, um dem Benutzer zu ermöglichen, die angezeigten Merkmale zu steuern. Wie unten ausführlich beispielhaft ausgeführt wird, kann eine passende mobile Vorrichtung **152** zum Anzeigen der Fahrzeugkomponenten-Schnittstellenanwendung **174** (zum Beispiel des mobilen Displays **176**) identifiziert werden, und eine Definition der anzuzeigenden Benutzerschnittstelle kann zu der identifizierten Fahrzeugkomponenten-Schnittstellenanwendung **174** zwecks Anzeige für den Benutzer zugeführt werden.

[0030] Systeme wie das System **100** können das Paaren der mobilen Vorrichtung **152** mit der Rechnerplattform **104** und/oder andere Einrichtvorgänge erfordern. Allerdings kann, wie unten ausführlich erläutert wird, ein System konzipiert sein, um es Fahrzeuginsassen zu ermöglichen, nahtlos mit Benutzerschnittstellenelementen in ihrem Fahrzeug oder irgendeinem anderen frameworkfähigen Fahrzeug zu interagieren, ohne dass es erforderlich ist, dass die mobile Vorrichtung **152** oder die tragbare Vorrichtung

mit der Rechnerplattform **104** gepaart wurde oder in Kommunikation mit dieser steht.

[0031] Zusätzlich kann der drahtlose Transceiver **150** Daten in Zusammenhang mit der Position des Fahrzeugs zu anderen Fahrzeugen in Fahrzeug-zu-Fahrzeug-Kommunikation empfangen und übertragen. Solche Kommunikation von Fahrzeug zu Fahrzeug kann verschiedene drahtlose Kommunikationsprotokolle umfassen, darunter drahtlose Nahfeldkommunikation, Wi-Fi, Bluetooth™ usw.

[0032] Der entfernte Server **162** und das Kommunikationsnetzwerk **156** können auch die Übertragung anderer Fahrzeug-zu-Fahrzeug-Daten erleichtern, wie zum Beispiel Daten, die von anderen mobilen Anwendungen und Websites erfasst werden, wie zum Beispiel Google Maps™, Waze™, usw. Bei diesen Beispielen können Daten zwischen Nutzern gemeinsam verwendet werden, um die Lage anderer Fahrzeuge, Notsituationen usw. zu bestimmen.

[0033] **Fig.** 2 zeigt eine perspektivische Ansicht einer beispielhaften Safe-Vorrichtung **200**. Die Safe-Vorrichtung **200** kann einen Safe-Container **205** umfassen, der dafür ausgelegt ist, Artikel auf zubewahren, einschließlich Wertgegenstände oder potentiell gefährliche Gegenstände wie Waffen und Medikamente. Der Container **205** kann aus feuerfesten Materialien bestehen, um Beschädigung des Innenraums des Containers **205** während eines Feuers zu verhindern. Ferner kann der Container **205** aus belastbaren Materialien bestehen, um extremer Abnutzung zu widerstehen. Im Fall eines Fahrzeugunfalls kann der Safe-Container **205** dafür ausgelegt sein, darin befindliche Inhalte zu schützen.

[0034] Die Safe-Vorrichtung **200** kann eine Safe-Tür **210** umfassen, die dafür ausgelegt ist, sich zu öffnen und zu schließen, wodurch Benutzer Zugang zum Innenraum des Safe-Containers **205** erhalten können. Die Safe-Vorrichtung **200** kann einen Verriegelungsmechanismus **220** umfassen, der dafür ausgelegt ist, die Tür **210** in einer geschlossenen Position zu verriegeln. Der Verriegelungsmechanismus **220** kann eine mechanische, elektronische, elektromechanische Befestigungsvorrichtung usw. umfassen. Speziell kann der Verriegelungsmechanismus **220** einen röhrenförmigen Riegel, einen Stiftriegel, einen Klinkenriegel usw. umfassen. Der Safe-Container **205** kann ein mechanisches Schlüsselloch **230** umfassen, das dafür ausgelegt ist, einen mechanischen Schlüssel zum Entriegeln und Verriegeln des Verriegelungsmechanismus **220** aufzunehmen. Der Safe-Container **205** kann auch eine elektronische Schlüsselschnittstelle **235** umfassen. Der Verriegelungsmechanismus **220** kann über einen mechanischen Schlüssel in dem mechanischen Schlüsselloch **230** oder die elektronische Schlüsselschnittstelle **235** verriegelt und entriegelt werden.

[0035] Die elektronische Schlüsselschnittstelle **235** kann ein Display **240** umfassen, das dafür ausgelegt ist, Benutzereingaben zu empfangen. Das Display **240** kann eine Flüssigkristallanzeige (LCD), ein Touchscreen usw. sein. Auf dem Display **240** kann ein Benutzer den Verriegelungsmechanismus **220** entriegeln und verriegeln, indem er bestimmte Berechtigungsnachweise auf dem Display **240** eingibt. Das Display **240** kann auch dafür ausgelegt sein, dem Benutzer verschiedene Bildschirmanzeigen zu präsentieren, wie etwa Zugang-Verweigert-Bildschirmanzeigen, Zugang-Gewährt-Bildschirmanzeigen sowie Bildschirmanzeigen, die den Verriegelungsmechanismusstatus (z. B. ”verriegelt”, ”entriegelt”, ”angelehnt” usw.) angeben.

[0036] Die Safe-Vorrichtung **200** kann über das Display **240** und/oder einen mechanischen Schlüssel in dem mechanischen Schlüsselloch **230** entriegelt werden. Zusätzlich oder als Alternative kann die Safe-Vorrichtung **200** durch eine Fernschnittstelle entriegelt werden. Die Fernschnittstelle kann über das Fahrzeugdisplay **138** oder die mobile Vorrichtung **152** präsentiert werden. An diesen Schnittstellen können Benutzereingaben empfangen werden, darunter Benutzerberechtigungsnachweise wie Benutzernamen, Passwörter usw.

[0037] Die Safe-Vorrichtung **200** kann im Fahrzeug **102** befestigt sein. In dem in **Fig.** 2 gezeigten Beispiel kann die Safe-Vorrichtung **200** im Fahrzeugkofferraum befestigt sein. Die Safe-Vorrichtung **200** kann während der Montage des Fahrzeugs installiert werden. Sie kann auch nach der Montage installiert werden, kann aber immer noch permanent oder halbpermanent im Fahrzeug befestigt werden, als Versuch, zu verhindern, dass unbefugte Benutzer mit dem Safe weggehen.

[0038] **Fig.** 3 zeigt eine beispielhafte Blockdarstellung eines Teils eines Safe-Authentifizierungssystems **300**. Das Safe-Authentifizierungssystem **300** kann die Safe-Vorrichtung **200** umfassen. Wie in **Fig.** 3 gezeigt, kann das mechanische Schlüsselloch **230** an den Verriegelungsmechanismus **220** angrenzen, so dass Zugang zu der Safe-Vorrichtung **200** gewährt werden kann, indem ein mechanischer Schlüssel in das mechanische Schlüsselloch **230** eingeführt und gedreht wird. Der Verriegelungsmechanismus **220** kann elektronisch mit einer Motorsteuerung **352** verbunden sein. Der Verriegelungsmechanismus **220** kann dafür ausgelegt sein, einen Verriegelungsmechanismusstatus oder Verriegelungsstatus zu der Motorsteuerung **352** zu senden. Der Verriegelungsmechanismusstatus kann anzeigen, ob der Safe verriegelt oder entriegelt ist. Das Display **235** kann sich in elektronischer Kommunikation mit einer Motorsteuerung **352** befinden.

[0039] Die Motorsteuerung **352** kann sich in elektronischer Kommunikation mit einem Motor **350** befinden, der dafür ausgelegt ist, einen Teil des Verriegelungsmechanismus **220** anzutreiben. Das heißt, der Motor **350** kann einen Teil des Verriegelungsmechanismus **220** in eine Verriegelungs- oder Entriegelungsstellung drehen. Die Motorsteuerung **352** kann dem Motor **350** auf der Basis von Benutzereingaben auf dem Display **235** oder an anderen Schnittstellen, wie etwa auf der mobilen Vorrichtung **152** und dem Fahrzeugdisplay **138**, Anweisungen geben. Zum Beispiel kann die Motorsteuerung **352** einen Riegel-Öffnen-Befehl zum Motor **350** senden, wenn ein gültiger Benutzername und eine gültige Geheimzahl auf dem Display **235** eingegeben werden. Der Motor **350** kann seinerseits den Verriegelungsmechanismus **220** entriegeln. Die Motorsteuerung **352** kann ein CAN-Bus (Controller Area Network) sein, der dafür ausgelegt ist, mit einer Karosseriesteuerung **348** zu kommunizieren. Die Motorsteuerung **352** kann durch die Karosseriesteuerung **348** aufgeweckt werden, wenn Zugang zu der Safe-Vorrichtung **200** von einem Ferndisplay aus, wie etwa dem Fahrzeugdisplay **138** oder der mobilen Vorrichtung **152**, versucht wird.

[0040] Die Safe-Vorrichtung **200** kann durch eine Stromquelle **364** mit Strom versorgt werden. Die Stromquelle **364** kann der Vorrichtung **200** ungefähr 12 Volt bereitstellen und kann mit einer Fahrzeugbatterie verbunden sein. Zusätzlich oder als Alternative kann die Stromquelle **364** eine selbständige Stromquelle sein, die dafür ausgelegt ist, die Safe-Vorrichtung **200** mit Strom zu versorgen.

[0041] Das Safe-Authentifizierungssystem **300** kann die Karosseriesteuerung **348** umfassen. Die Karosseriesteuerung **348** kann Teil der elektronischen Steuereinheit (ECU) **148** sein, wie als Teil von **Fig.** 1A gezeigt. Die Karosseriesteuerung **348** kann sich mit einer Aufwecktaste **366** in Kommunikation befinden. Die Aufwecktaste **366** kann eine physische Taste sein, die auf oder nahe dem Armaturenbrett des Fahrzeugs **102** angeordnet ist, die dafür ausgelegt ist, Authentifizierung des Benutzers zum Zwecke des Entriegelns der Safe-Vorrichtung **200** einzuleiten. Bei Betätigung kann die Aufwecktaste **366** dafür ausgelegt sein, Signale zu jeder der Steuerungen zu senden, darunter, aber ohne Beschränkung darauf, die Karosseriesteuerung **348**, das Fahrzeugdisplay **138**, die Motorsteuerung **352** und die TCU **356**.

[0042] Die Karosseriesteuerung **348** kann sich mit einem Teil der Datenverarbeitungsplattform **104**, insbesondere der Vorrichtungsverbindungsschnittstelle **172**, in Kommunikation befinden. Wie erläutert, kann die Vorrichtungsverbindungsschnittstelle **172** die Komponente SYNC APPLINK des von The Ford Motor Company bereitgestellten SYNC-Systems umfassen. Die Verbindungsschnittstelle **172** kann Daten **160** gepaarter Vorrichtungen umfassen. Diese Daten **160** gepaarter Vorrichtungen können eindeutige Vorrichtungskennungen, Benutzeridentifikation und zugeordnete Passwörter oder Berechtigungsnachweise damit unterhalten. Die Passwörter können benutzerspezifische eindeutige Identifikationscodes oder -wörter bei Paarung mit der Benutzeridentifikation umfassen und können benutzt werden, um Zugang zu der Safe-Vorrichtung **200** zu erhalten. Solche Passwörter können über das Safe-Display **235**, das Fahrzeugdisplay **138**, wie etwa ein Heads-Up-Display oder Konsolendisplay und/oder ein Mobil-Display **176** empfangen werden.

[0043] Die Vorrichtungsverbindungsschnittstelle **172** kann über drahtlose Kommunikation wie oben besprochen mit der mobilen Vorrichtung **152** eine Schnittstelle bilden. Die mobile Vorrichtung **152** kann eine Mobil-Anwendung **170** umfassen, die dafür ausgelegt ist, für die Safe-Vorrichtung **200** relevante Informationen anzuzeigen. In einem Beispiel kann die Mobil-Anwendung **170** einen Safe-Status anzeigen, wie etwa ”verriegelt”, ”entriegelt”, ”angelehnt” usw. In einem anderen Beispiel kann die Mobil-Anwendung **170** dafür ausgelegt sein, eine Anmeldebildschirmanzeige oder Zugangsbildschirmanzeige anzuzeigen, die dafür ausgelegt ist, Benutzereingaben zu empfangen, um Zugang zu der Safe-Vorrichtung **200** zu erhalten.

[0044] Die Karosseriesteuerung **348** kann sich auch mit einer Telematiksteuereinheit (TCU) **356** in Kommunikation befinden. Die TCU **356** kann das GPS-Modul **146** umfassen oder sich mit diesem in Kommunikation befinden. Die TCU **356** kann sich mit einer Fahrzeugkamera **360** in Kommunikation befinden. Die Fahrzeugkamera **360** kann eine oder mehrere existierende Fahrzeugkameras sein, wie etwa Fahrzeugkameras, die von anderen Systemen verwendet werden, darunter, aber ohne Beschränkung darauf, ein aktives Parkhilfesystem. Als Reaktion auf Anzeichen für unbefugten Zugang an der Safe-Vorrichtung **200** kann die TCU **356** die Kamera **360** anweisen, Bilder aufzunehmen. Dies wird hier ausführlicher beschrieben.

[0045] Die TCU **356** kann auch dafür ausgelegt sein, mit einem externen Unterstützungsserver **354** zu kommunizieren, der dem in **Fig.** 1B gezeigten entfernten Server **162** ähnlich ist. Diese Kommunikation kann über eine drahtlose Kommunikation erreicht werden. Als Reaktion auf Anzeichen für unbefugten Zugang an der Safe-Vorrichtung **200** kann die TCU **356** die in der Kamera **360** aufgenommenen Bilder zu dem Unterstützungsserver **354** senden. Mit den Bildern können dann Behörden oder anderes Personal Täter identifizieren. Zusätzlich oder als Alternative können die Bilder auch verwendet werden, um Benutzer auf der Basis wahrer Eigentümerschaft zu authentifizieren. Eine solche Authentifizierung kann über Gesichtserkennung oder andere biometrische

Vergleiche erreicht werden. Die Bilder kann ein über die TCU **356** beschaffter Ort begleiten.

[0046] Das Safe-Authentifizierungssystem **300** kann dafür ausgelegt sein, in einer von mehreren Betriebsarten zu arbeiten. Eine erste Betriebsart kann eine Betriebsart umfassen, die dafür ausgelegt ist, Zugang zu der Safe-Vorrichtung **200** als Reaktion auf Authentifizierung des Benutzers zu gewähren. Eine zweite Betriebsart kann eine Betriebsart umfassen, die dafür ausgelegt ist, begrenzten Zugang zu der Safe-Vorrichtung **200** zu gewähren, wenn ein Notfallpasswort zum Zugang zu der Safe-Vorrichtung **200** verwendet wird. In der zweiten Betriebsart kann die Safe-Vorrichtung **200** entriegelt werden. Als Reaktion auf die Verwendung des Notfallpassworts können jedoch andere Fahrzeugsysteme freigegeben werden, um Ereignisse und Personen, die das Fahrzeug umgeben, zu erfassen und zu melden. In einem Beispiel kann die Kamera **360** angewiesen werden, Bilder aufzunehmen. In einem anderen Beispiel kann das Mikrofon angewiesen werden, eingeschaltet zu werden. Zusätzlich zu der Freigabe dieser Fahrzeugkomponenten kann die TCU **356** den externen Unterstützungsserver **354** anweisen, Notfallpersonal zu benachrichtigen, dass gerade ein unbefugter Zugangsversuch ablaufen kann. Die TCU **356** kann den aktuellen Fahrzeugort zu den Behörden senden. Solche Sicherheitsmaßnahmen können Zugang zu der Safe-Vorrichtung **200** gestatten, falls ein Benutzer während einer Notfallsituation Zugang zu Artikeln in dem Safe-Container **205** benötigt (z. B. wenn medizinische Bestände benötigt werden). Gleichzeitig kann der entfernte Unterstützungsserver **354** als Reaktion auf Verwendung des Notfallpassworts zusätzliche Informationen über das Fahrzeug empfangen, um Missbrauch oder unbefugten Zugang zu dem Safe-Authentifizierungssystem **300** zu verhindern. Diese Prozesse werden nachfolgend ausführlicher beschrieben.

[0047] **Fig.** 4 zeigt einen beispielhaften Prozess **400** zum Verriegeln der Safe-Vorrichtung **200** unter Verwendung eines mechanischen Schlüssels. Der Prozess kann in Block **405** beginnen, in dem die Motorsteuerung **352** bestimmen kann, ob der Verriegelungsmechanismus **220** über einen mechanischen Schlüssel verriegelt wurde. Die Motorsteuerung **352** kann eine solche Angabe über ein Signal empfangen, das als Reaktion auf Verriegelung des Verriegelungsmechanismus **220** über einen mechanischen Schlüssel in dem mechanischen Loch **230** von dem Verriegelungsmechanismus **220** gesendet wird. In einem Beispiel kann der Verriegelungsmechanismus **220** einen Schalter umfassen, der dafür ausgelegt ist, als Reaktion auf Drehen eines Stifts in dem Verriegelungsmechanismus betätigt zu werden. Das heißt, sobald ein mechanischer Schlüssel in dem Schlüsselloch **230** gedreht wird, kann der Schalter betätigt werden, wodurch ein Verriegelungssignal zur Motorsteuerung **352** gesendet wird. Wenn die Motorsteuerung **352** bestimmt, dass ein mechanischer Schlüssel zum Blockieren der Safe-Vorrichtung **200** verwendet wurde, schreitet der Prozess **400** zu Block **410** voran.

[0048] In Block **410** sendet die Motorsteuerung ein Aufwecksignal zu der Karosseriesteuerung **348**.

[0049] In Block **415** empfängt die Motorsteuerung **352** einen neuen Zufallsschlüssel von der Karosseriesteuerung **348**. Es werden Zufallsschlüssel zwischen der Motorsteuerung **352** und der Karosseriesteuerung **348** ausgetauscht, um so Mittelsmannangriffe zu vermeiden.

[0050] In Block **420** sendet die Motorsteuerung **352** als Reaktion auf den Empfang des neuen Zufallsschlüssels einen alten Zufallsschlüssel zu der Karosseriesteuerung **348**.

[0051] In Block **425** bestimmt die Motorsteuerung **352**, ob der neue Zufallsschlüssel innerhalb einer vordefinierten Zeit von der Karosseriesteuerung **348** empfangen wurde. In einem Beispiel kann die vordefinierte Zeit ein annehmbarer Zeitrahmen sein, für den die Motorsteuerung **352** erwarten kann, eine Antwort auf der Karosseriesteuerung **348** zu empfangen. In einem Beispiel kann die vordefinierte Zeit ungefähr 2,0 Sekunden sein. Wenn die Motorsteuerung **352** bestimmt, dass der neue Zufallsschlüssel innerhalb der vordefinierten Zeit von der Karosseriesteuerung **348** empfangen wurde, schreitet der Prozess **400** zu Block **430** voran. Wenn nicht, schreitet der Prozess zu Block **435** voran.

[0052] In Block **430** sendet die Motorsteuerung **352** eine Bestätigungsnachricht zur Karosseriesteuerung **348**. Die Bestätigungsnachricht kann Anweisungen umfassen, dass die Karosseriesteuerung den neuen Zufallsschlüssel in Speicher abspeichern kann. Der neue Zufallsschlüssel kann dann bei einem späteren Zugangsversuch wie hier offenbart wieder aufgerufen werden.

[0053] Im Block **435** kann die Motorsteuerung **352** einen Hinweisbefehl zu dem Safe-Display **235** senden, der das Display **235** anweist, eine Hinweisnachricht zu präsentieren, die angibt, dass die Karosseriesteuerung **348** nicht antwortet. Diese Hinweisnachricht kann den Benutzer informieren, dass ein Problem mit der Kommunikation zwischen der Karosseriesteuerung **348** und der Safe-Vorrichtung **200** vorliegen kann. Die Hinweisnachricht kann auch erläutern, dass, während die Safe-Vorrichtung **200** unter Verwendung des mechanischen Schlüssels verriegelt und entriegelt werden kann, die Safe-Vorrichtung **200** ferner durch andere Mechanismen gesichert werden kann, wie etwa die Karosseriesteuerung **348** und den entfernten Unterstützungsserver **354**, wie hier besprochen.

[0054] In Block **440** kann beim Empfang des neuen Zufallsschlüssels von der Karosseriesteuerung **348** die Motorsteuerung **352** den Safe-Status auf "verriegelt" aktualisieren. Dann kann der Prozess enden.

[0055] **Fig.** 5 zeigt einen beispielhaften Prozess **500** zum Verriegeln der Safe-Vorrichtung **200** unter Verwendung der Mobil-Anwendung **170** auf dem Mobil-Display **176** und/oder dem Fahrzeugdisplay **138**. Diese Mechanismen können hier kollektiv als die Schnittstelle bezeichnet werden. Der Prozess **500** kann in Block **505** beginnen, in dem die Karosseriesteuerung **348** eine Verriegelungsanforderung von der Schnittstelle empfangen kann. Die Verriegelungsanforderung kann als Reaktion auf eine Benutzerauswahl an der Schnittstelle gesendet werden. Das heißt, der Benutzer kann anfordern, dass die Safe-Vorrichtung **200** verriegelt wird, indem eine solche Option an der Schnittstelle ausgewählt wird.

[0056] In Block **510** kann die Karosseriesteuerung **348** als Reaktion auf den Empfang der Verriegelungsanforderung einen neuen Zufallsschlüssel erzeugen.

[0057] In Block **515** kann die Karosseriesteuerung **348** den neuen Zufallsschlüssel und Speicher speichern.

[0058] In Block **520** kann die Karosseriesteuerung **348** den Safe-Status auf "verriegelt" aktualisieren. Dann kann der Prozess enden.

[0059] **Fig.** 6 zeigt einen beispielhaften Prozess **600** zum Entriegeln der Safe-Vorrichtung **200** unter Verwendung der Schnittstelle (z. B. des Fahrzeugdisplays **138** oder des Mobilvorrichtungs-Displays **176**). Der Prozess **600** beginnt in Block **605**. In Block **605** kann die Karosseriesteuerung **348** ein Aufwecksignal empfangen. In einem Beispiel kann das Aufwecksignal durch die auf oder an dem Fahrzeugarmaturenbrett angeordnete Aufwecktaste **366** eingeleitet werden. Das heißt, sobald ein Benutzer in das Fahrzeug einsteigt, kann der Benutzer die Aufwecktaste **366** betätigen. In einem anderen Beispiel kann das Aufwecksignal automatisch beim Starten der Mobil-Anwendung **170** eingeleitet werden. Die Mobil-Anwendung **170** kann das Aufwecksignal über die Vorrichtungsverbindungsschnittstelle **172** senden.

[0060] In Block **610** kann die Karosseriesteuerung **348**, sobald die Karosseriesteuerung **348** das Aufwecksignal empfängt, die Motorsteuerung **352** oder den CAN-Bus aufwecken.

[0061] Im Block **615** kann die Karosseriesteuerung **348** einen Zugangsanforderungsbefehl zu der Schnittstelle senden. Die Befehle können die Schnittstelle anweisen, eine Passwort-Bildschirmzeige anzuzeigen. Die Passwort-Bildschirmanzeige kann den Benutzer auffordern, seine Berechtigungsnachweise einzugeben. Die Berechtigungsnachweise können ein Passwort, einen Benutzernamen, biometrische Eingaben wie Daumenabdrücke, Gesichtserkennung oder Irisscans usw. umfassen. Die Berechtigungsnachweise können auch von dem gespeicherten zufällig erzeugten Schlüssel begleitet werden, so dass die Motorsteuerung **352** bestimmen kann, ob die Karosseriesteuerung **354** imitiert wird.

[0062] In Block **620** kann die Karosseriesteuerung **348** auf den Empfang von Benutzereingaben von der Schnittstelle warten. Die Benutzereingaben können ein Passwort oder andere biometrische oder Identifikationsdaten umfassen. Wenn die Karosseriesteuerung **348** Benutzereingaben empfängt, schreitet der Prozess **600** zu Block **625** voran. Wenn nicht, schreitet der Prozess zu Block **630** voran.

[0063] In Block **625** bestimmt die Karosseriesteuerung **348**, ob die Benutzereingaben gültige Berechtigungsnachweise umfassen. Das heißt, wurde das richtige Passwort eingegeben. Diese Bestimmung kann durchgeführt werden, indem man bekannte Passwörter, die mit bestimmten Benutzeridentifikationen (z. B. den in den Vorrichtungsdaten **160** gespeicherten) assoziiert sind, mit dem in den Benutzereingaben enthaltenen Passwort vergleicht. Wenn gültige Berechtigungsnachweise eingegeben wurden, schreitet der Prozess **600** zu Block **635** voran. Wenn nicht, schreitet der Prozess zu Block **640** voran.

[0064] In Block **635** bestimmt die Karosseriesteuerung **348**, ob die gültigen Berechtigungsnachweise ein spezielles Passwort umfassten. Das spezielle Passwort kann ein Notfallpasswort sein, mit dem man in einer Notfallsituation Zugang zu der Safe-Vorrichtung **200** erhält. Wenn ein spezielles oder Notfall-Passwort verwendet wurde, schreitet der Prozess zu Block **650** voran. Wenn nicht, schreitet der Prozess zu Block **655** voran.

[0065] In Block **650** kann die Karosseriesteuerung **348**, wenn die gültigen Berechtigungsnachweise ein spezielles Passwort enthalten, ein Hinweissignal zur TCU **356** senden. Das Hinweissignal kann angeben, dass ein spezielles Passwort verwendet wurde, um Zugang zu der Safe-Vorrichtung **200** zu erhalten. Als Reaktion auf den Empfang des Hinweissignals kann die TCU **356** Sicherheitsmaßnahmen einleiten, wie etwa Beschaffen von Bildern von der Kamera **360**, Beschaffen von Klängen von dem Mikrofon **116** und Melden dieser sowie des Fahrzeugorts an den entfernten Unterstützungsserver **354**. Wie oben erläutert, kann die Verwendung eines Notfallpassworts eine zweite Betriebsart auslösen, mit der unbefugter Zugang oder Missbrauch des speziellen Passworts verhindert wird. Zusätzlich oder als Alternative kann, wenn ein Notfall vorliegt, der entfernte Unterstützungsserver **354** das entsprechende Notfallpersonal kontaktieren. Wenn zum Beispiel ein Benutzer wäh-

rend einer Raubübertallsituation unter Zwang steht, kann der Benutzer das Notfallpasswort verwenden, um die Sicherheitsmaßnahmen geräuschlos auszulösen.

[0066] In Block **630** kann die Karosseriesteuerung **348**, wenn keine Benutzereingaben empfangen wurden, Bestimmen, ob eine vordefinierte Zeit überschritten wurde. Das heißt, hat der Prozess **600** eine Zeitgrenze erreicht. In einem Beispiel kann der Prozess **600** eine Zeitgrenze erreichen, wenn innerhalb von 30 Sekunden des Sendes der Zugangsanforderung keine Benutzereingaben empfangen werden. Wenn innerhalb der vordefinierten Zeit keine Benutzereingaben empfangen wurden, endet der Prozess **600**. Wenn die vordefinierte Zeit nicht überschritten wurde, wartet die Karosseriesteuerung **348** weiter auf Benutzereingaben, und der Prozess **600** schreitet zu Block **620** zurück.

[0067] In Block **640** kann die Karosseriesteuerung **348**, wenn die Benutzereingaben keine gültigen Berechtigungsnachweise umfassen, einen Zugangsversuchszähler vergrößern.

[0068] In Block **645** kann die Karosseriesteuerung **348** bestimmen, ob der Zugangsversuchszähler einen vordefinierten Versuchsbetrag überschreitet. Der vordefinierte Versuchsbetrag kann fünf Versuche umfassen. Wenn die Karosseriesteuerung **348** bestimmt, dass der Zugangsversuchszähler den vordefinierten Versuchsbetrag nicht überschreitet, kann der Prozess zu Block **620** zurückschreiten. Wenn die Karosseriesteuerung **348** bestimmt, dass der Zugangsversuchszähler tatsächlich den vordefinierten Versuchsbetrag überschreitet, kann der Prozess **600** zu Block **650** voranschreiten.

[0069] In Block **655** kann die Karosseriesteuerung **348**, wenn die gültigen Berechtigungsnachweise kein spezielles Passwort umfassen, ein Entriegelt-Signal zu der Motorsteuerung **352** der Safe-Vorrichtung **200** senden. Die Motorsteuerung **352** kann ihrerseits den Motor anweisen, den Verriegelungsmechanismus **220** zu entriegeln. Dann kann der Prozess enden.

[0070] **Fig.** 7 zeigt einen beispielhaften Prozess **700**, der die Safe-Vorrichtung **200** entriegelt, wenn Berechtigungsnachweise eines Benutzers vergessen oder verlegt wurden. Der Prozess beginnt in Block **705**, indem die TCU **356** ein Authentifizierungsanforderungssignal von der Karosseriesteuerung **348** empfängt. Das Authentifizierungsanforderungssignal kann auf der Basis von Benutzereingaben an der Schnittstelle eingeleitet werden. In einem Beispiel kann die Schnittstelle dem Benutzer eine Authentifizierungsanforderungsoption bereitstellen. Die Authentifizierungsanforderungsoption kann es dem Benutzer gestatten, über einen anderen Mechanismus, wie etwa biometrische Authentifizierung, seine Berechtigungsnachweise anzufordern und/oder authentifiziert zu werden.

[0071] In Block **710** kann die TCU **356** Fahrzeugkomponenten, wie etwa die Kamera **360** und/oder das Mikrofon **116**, einleiten. Einleiten der Fahrzeugkomponenten kann Aufwecken der Komponenten und/oder Anweisen der Komponenten, Daten (z. B. Bilder und/oder Ton) zu beschaffen oder aufzunehmen.

[0072] In Block **715** kann die TCU **356** die Fahrzeugkomponentendaten zu dem entfernten Unterstützungsserver **354** senden. Der Unterstützungsserver **354** kann die empfangenen Komponentendaten mit zuvor beschafften anderen Benutzerdaten vergleichen. Zum Beispiel kann der entfernte Unterstützungsserver **354** Gesichtserkennungssoftware verwenden, um ein zuvor aufgenommenes Bild des Benutzers mit dem mit den Fahrzeugkomponentendaten gesendeten aktuellen Bild zu vergleichen. Es kann auch Spracherkennung verwendet werden. Andere Daten, darunter biometrische Daten wie Fingerabdrücke, können auch zum Authentifizieren des Benutzers verwendet werden. In einem anderen Beispiel kann die TCU **356** einen Authentifizierungs-Link zum Benutzer senden. In einem Beispiel kann der Authentifizierungs-Link per E-Mail zum Benutzer gesendet werden. Bei Auswahl des Authentifizierungs-Links kann der entfernte Unterstützungsserver **354** die TCU **356** über die Passwort-Ändern-Anforderung anweisen.

[0073] In Block **720** kann die TCU eine Passwort-Ändern-Anforderung empfangen. Die Passwort-Ändern-Anforderung kann durch den entfernten Server **354** als Reaktion auf die den Benutzer authentifizierenden Komponentendaten gesendet werden.

[0074] In Block **725** kann die TCU **356** die Passwort-Ändern-Anforderung zur Karosseriesteuerung **348** senden. Die Karosseriesteuerung **348** kann dann Anweisungen zu der Schnittstelle senden, um den Benutzer zur Eingabe eines neuen Passworts aufzufordern. Die Karosseriesteuerung **348** kann somit Benutzereingaben empfangen, die das neue Passwort angeben. Die Karosseriesteuerung **348** kann dieses neue Passwort und Speicher abspeichern. Die Karosseriesteuerung **348** kann dann ein Bestätigungssignal zur TCU **356** senden, das angibt, dass ein neues Passwort abgespeichert wurde. Die Karosseriesteuerung **348** kann dann weiter die Motorsteuerung **352** anweisen, den Verriegelungsmechanismus **220** zu entriegeln.

[0075] In Block **730** kann die TCU **356** das Bestätigungssignal von der Karosseriesteuerung **348** empfangen. Beim Empfang des Bestätigungssignals kann die TCU **356** auch ein Signal zu dem entfern-

ten Server **354** senden, das angibt, dass die Passwort-Ändern-Anforderung abgeschlossen wurde. In einem Beispiel kann der entfernte Server **354** wählen, dem Benutzer eine Gebühr für das Anfordern eines Passwortrücksetzens zu berechnen, um somit routinemäßigen Gebrauch des Authentifizierungsanforderungsmerkmals zu demotivieren. Dann kann der Prozess enden.

[0076] **Fig.** 8 ist ein beispielhafter Prozessfluss **800** für das Safe-Authentifizierungssystem **300** zum Aktivieren verschiedener Fahrzeugkomponenten (z. B. der Kamera **360** und des Mikrofons **116**) als Reaktion auf eine Authentifizierungsbedrohung. In Schritt **805** kann die Karosseriesteuerung **348** das Hinweissignal zur TCU **356** senden. Wie oben erläutert kann die Karosseriesteuerung **348** das Hinweissignal als Reaktion darauf zu der TCU senden, dass eine vordefinierte Anzahl von Zugangsversuchen überschritten wurde, oder als Reaktion auf den Empfang eines Authentifizierungsanforderungssignals zum Abrufen eines vergessenen Passworts. Als Reaktion auf den Empfang des Hinweissignals kann die TCU **356** verschiedene Sicherheitsmaßnahmen einleiten, um zu versuchen, vor dem möglichen unbefugten Zugang an der Safe-Vorrichtung **200** zu schützen. In Schritt **810** kann die TCU **356** einen durch das GPS-Modul **146** erkannten Fahrzeugort zu dem entfernten Unterstützungsserver **354** senden.

[0077] In Schritt **815** kann die TCU **356** Aufwecksignale zu den Fahrzeugkomponenten senden. Die Aufwecksignale können Anweisungen für die Komponenten zum Beschaffen von Daten, wie etwa Bildern oder Klängen, umfassen. Die Bilder oder Klänge können potentiell einen potentiellen Täter (z. B. einen unbefugten Benutzer) erfassen. Die durch die Kamera **360** aufgenommenen Bilder können mindestens einen Teil des unbefugten Benutzers zeigen. Die durch das Mikrofon **116** aufgenommene Ton kann die Stimme des unbefugten Benutzers erfassen. Obwohl es in **Fig.** 3 nicht gezeigt ist, können auch andere Komponenten freigegeben werden, wie etwa biometrische Sensoren.

[0078] In Schritt **820** können die Fahrzeugkomponenten dann Komponentendaten zur TCU **356** zurücksenden. In Schritt **825** kann die TCU **356** ihrerseits die Komponentendaten zum Unterstützungsserver **354** senden. Der Unterstützungsserver **354** kann die Komponentendaten mit zuvor beschafften Daten vergleichen. In einem Beispiel kann Gesichtserkennung verwendet werden, um Bilder eines bekannten Benutzerraums mit denen der vor kurzem beschafften Komponentendaten zu vergleichen. Wenn ein autorisierter Benutzer erkannt wird, kann der Unterstützungsserver **354** ein Authentifizierungssignal zur TCU **356** zurücksenden, das angibt, dass der Benutzer tatsächlich authentifiziert ist. Dies kann in dem Beispiel eines verlorenen oder vergessenen Passworts der Fall sein. In einem anderen Beispiel kann der Unterstützungsserver **354** die Komponentendaten sowie den Fahrzeugort zu den entsprechenden Behörden oder Notfallpersonal senden. Zum Beispiel kann der Unterstützungsserver **354** ein Bild, das einen unbefugten Benutzer erfasst, der versucht, auf die Safe-Vorrichtung **200** zuzugreifen, zusammen mit dem Fahrzeugort senden. Bei Empfang der Informationen können die Behörden oder das Notfallpersonal mit einem Foto eines vermutlichen Diebs am Fahrzeugort ankommen.

[0079] Dementsprechend wird hier ein Safe-Authentifizierungssystem für einen fahrzeuginternen Safe beschrieben, das mehrere Sicherheitsmechanismen unterhält. In einem Beispiel kann das Fahrzeug, wenn ein potentiell unbefugter Benutzer auf die Safe-Vorrichtung zugreift, bestimmte Fahrzeugkomponenten, wie etwa die Kamera, freigeben, um Bilder der potentiell unbefugten Person zu beschaffen.

[0080] Datenverarbeitungsvorrichtungen, wie etwa die Steuerungen, Steuereinheiten, Datenverarbeitungsplattformen, mobilen Vorrichtungen, Server usw. umfassen im Allgemeinen computerausführbare Anweisungen, wobei die Anweisungen durch eine oder mehrere Datenverarbeitungsvorrichtungen wie die oben aufgelisteten ausführbar sein können. Computerausführbare Anweisungen können aus Computerprogrammen kompiliert oder interpretiert werden, die unter Verwendung vielfältiger Programmiersprachen und/oder -technologien erstellt werden, darunter, aber ohne Beschränkung, und entweder alleine oder in Kombination Java™, C, C++, Visual Basic, Java Script, Perl usw. Im Allgemeinen empfängt ein Prozessor (z. B. ein Mikroprozessor) Anweisungen z. B. aus einem Speicher, einem computerlesbaren Medium usw. und führt diese Anweisungen aus, um dadurch einen oder mehrere Prozesse, einschließlich eines oder mehrerer der hier beschriebenen Prozesse, auszuführen. Derartige Anweisungen und andere Daten können unter Verwendung einer Vielfalt von computerlesbaren Medien gespeichert und übertragen werden.

[0081] Datenbanken, Datensammlungen oder andere Datenspeicher, die hier beschrieben sind, können diverse Arten von Mechanismen zum Speichern und Abrufen diverser Arten von Daten sowie Zugreifen auf diese aufweisen, einschließlich einer hierarchischen Datenbank, eines Dateisatzes in einem Dateisystem, einer Anwendungsdatenbank in einem proprietären Format, eines relationalen Datenbankverwaltungssystems (Relational Database Management System, RDBMS) usw. Jeder derartige Datenspeicher ist im Allgemeinen in einer Rechenvorrichtung enthalten, die ein Computerbetriebssystem einsetzt, wie eines der oben erwähnten, und auf ihn wird mittels eines Netzwerks auf eine beliebige oder mehrere beliebige einer Vielfalt von Methoden zugegriffen.

Ein Dateisystem kann für ein Computerbetriebssystem zugänglich sein und die gespeicherten Dateien in diversen Formaten herstellen. Ein RDBMS wendet Im Allgemeinen die Structured Query Language (SQL), zusätzlich zu Sprache zum Erstellen, Speichern, Bearbeiten und Ausführen gespeicherter Vorgehensweisen, wie etwa die oben erwähnte PL/SQL-Sprache, an.

[0082] In einigen Beispielen können Systemelemente als computerlesbare Anweisungen (z. B. Software) auf einer oder mehreren Datenverarbeitungsvorrichtungen (z. B. Servern, PCs usw.) implementiert werden, die auf computerlesbaren Medien gespeichert sind, die damit assoziiert sind (z. B. Datenträgern, Speichern, usw.). Ein Computerprogrammprodukt kann derartige auf computerlesbaren Medien gespeicherte Anweisungen zum Ausführen der hier beschriebenen Funktionen umfassen.

[0083] Obgleich oben beispielhafte Ausführungsformen beschrieben werden, ist nicht beabsichtigt, dass diese Ausführungsformen alle möglichen Formen der Erfindung beschreiben. Stattdessen sind die in der Beschreibung verwendeten Wörter nicht Wörter der Beschränkung, sondern der Beschreibung, und es versteht sich, dass verschiedene Änderungen vorgenommen werden können, ohne vom Gedanken und Schutzumfang der Erfindung abzuweichen. Zusätzlich können die Merkmale verschiedener implementierender Ausführungsformen kombiniert werden, um weitere Ausführungsformen der Erfindung zu bilden.

Patentansprüche

1. Fahrzeugsafe-Authentifizierungssystem, umfassend:
einen Fahrzeugsafe;
eine Fahrzeugkamera; und
eine Steuereinheit, programmiert zum Empfangen einer Angabe von unbefugtem Zugang an dem Fahrzeugsafe und ferner programmiert zum Aktivieren der Fahrzeugkamera als Reaktion auf die Angabe, wobei Aktivierung der Kamera Aufnehmen mindestens eines Bildes umfasst.

2. System nach Anspruch 1, wobei die Steuereinheit eine GPS-Einheit (Global Positioning System) umfasst, die dafür ausgelegt ist, einen Ort des Safes zu identifizieren.

3. System nach Anspruch 2, wobei die Steuereinheit ferner programmiert ist zum Senden des Bildes und des Orts des Safes zu einem externen Server als Reaktion auf die Angabe von unbefugtem Zugang.

4. System nach einem der Ansprüche 1 bis 3, wobei die Steuereinheit ferner programmiert ist zum Empfangen der Angabe von unbefugtem Zugang von einer Karosseriesteuerung als Reaktion darauf, dass eine vordefinierte Anzahl von Versuchen, auf den Safe zuzugreifen, überschritten wird.

5. System nach einem der Ansprüche 1 bis 4, wobei die Steuereinheit ferner programmiert ist zum Empfangen der Angabe von unbefugtem Zugang von einer Karosseriesteuerung als Reaktion darauf, dass ein Benutzer ein vergessenes Passwort anfordert.

6. System nach einem der Ansprüche 1 bis 5, wobei die Steuereinheit ferner programmiert ist zum Empfangen der Angabe von unbefugtem Zugang von einer Karosseriesteuerung als Reaktion darauf, dass die Karosseriesteuerung Benutzereingaben empfängt, die ein spezielles Passwort angeben.

7. Fahrzeugsafe-Authentifizierungssystem, umfassend:
einen Fahrzeugsafe;
eine Fahrzeugkamera; und
eine Steuerung, programmiert zum Empfangen von Benutzereingaben, die ein Benutzerpasswort oder ein spezielles Passwort umfassen, und zum Senden eines Befehls für die Fahrzeugkamera, mindestens ein Bild aufzunehmen, als Reaktion darauf, dass die Benutzereingaben das spezielle Passwort umfassen.

8. System nach Anspruch 7, wobei die Steuerung ferner programmiert ist zum Senden eines Entriegelungsbefehls zu dem Fahrzeugsafe als Reaktion darauf, dass die Benutzereingaben das Benutzerpasswort umfassen.

9. Verfahren, das Folgendes umfasst:
Empfangen eines Hinweissignals, das einen unbefugten Zugangsversuch zu einem fahrzeuginternen Safe angibt;
Anweisen mindestens einer Fahrzeugkomponente, sich zu aktivieren, als Reaktion auf das Hinweissignal, wobei die Fahrzeugkomponente eine Kamera und/oder ein Mikrofon umfasst;
Identifizieren eines Fahrzeugorts;
Empfangen von Komponentendaten von der Fahrzeugkomponente; und
Senden der Komponentendaten und des Fahrzeugorts zu einem entfernten Server.

10. Verfahren nach Anspruch 9, wobei das Hinweissignal als Reaktion darauf empfangen wird, dass eine vordefinierte Anzahl von Versuchen, auf den Safe zuzugreifen, überschritten wird.

11. Verfahren nach Anspruch 9 oder Anspruch 10, wobei das Hinweissignal als Reaktion darauf empfangen wird, dass ein Benutzer ein vergessenes Passwort anfordert.

12. Verfahren nach einem der Ansprüche 9 bis 11, wobei das Hinweissignal als Reaktion darauf empfan-

gen wird, dass Benutzereingaben empfangen werden, die ein spezielles Passwort angeben.

Es folgen 9 Seiten Zeichnungen

Anhängende Zeichnungen

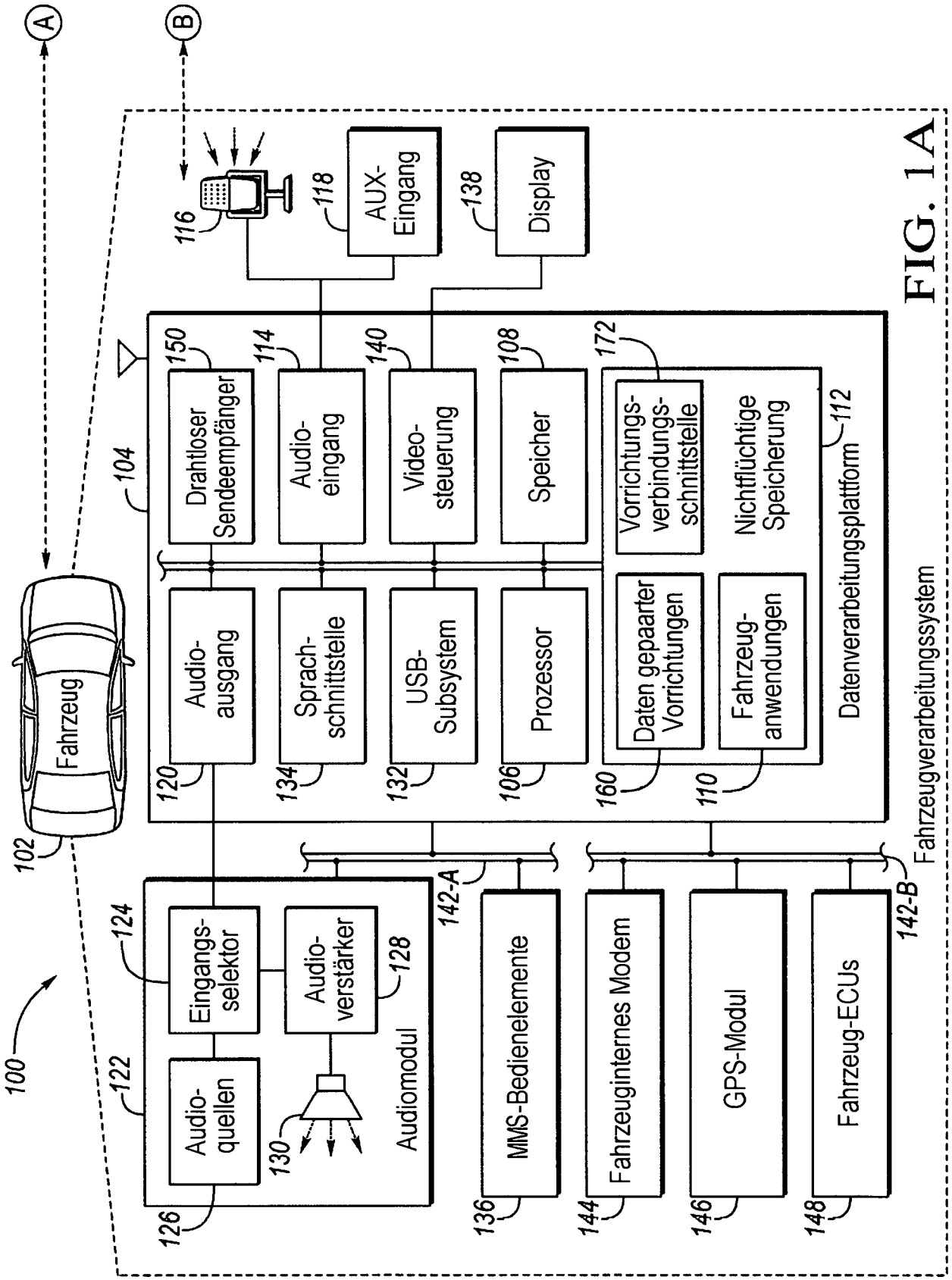


FIG. 1A

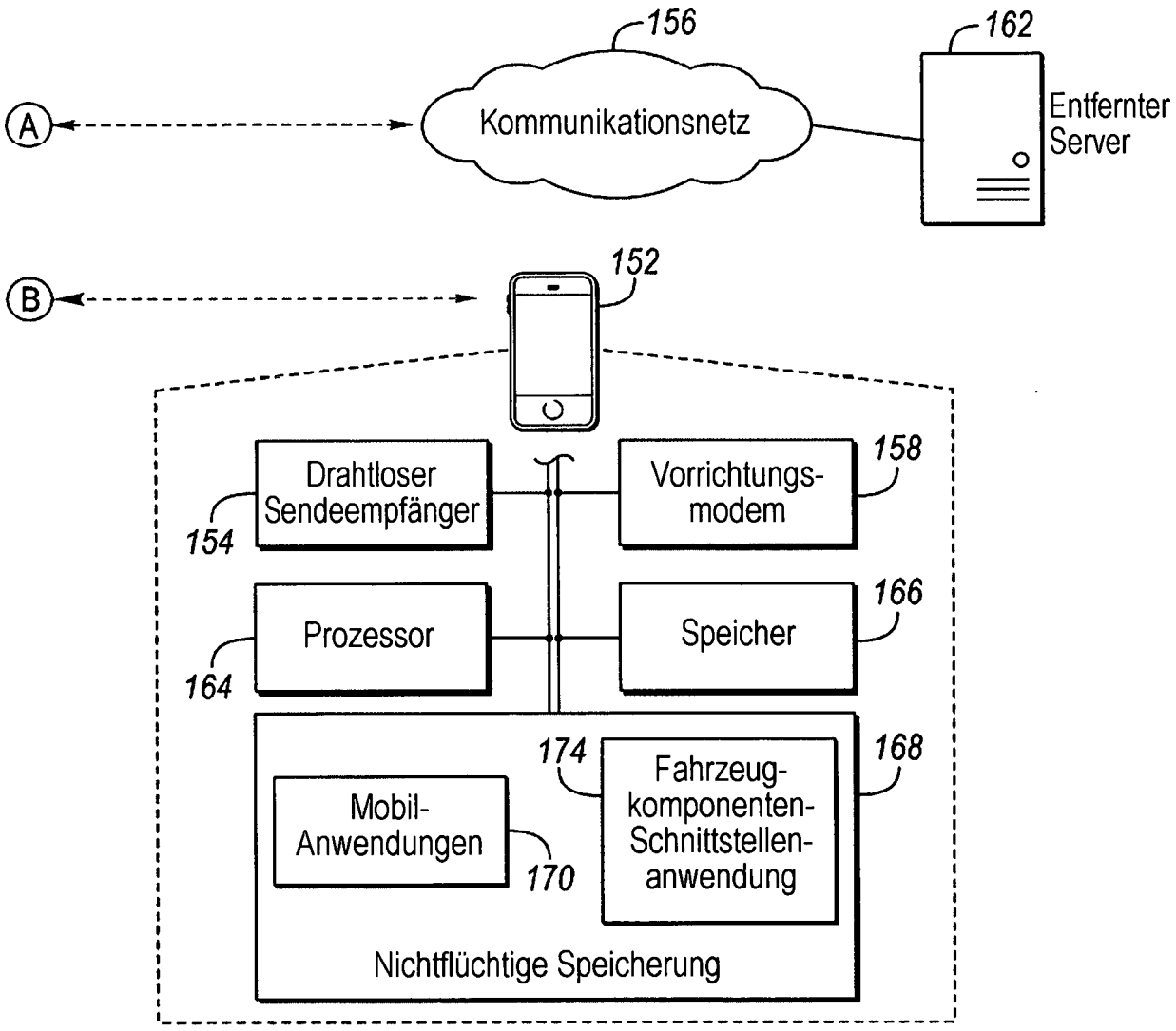

156
162
A
Kommunikationsnetz
Entfernter Server
152
B
Drahtloser Sendeempfänger
154
Vorrichtungs-modem
158
Prozessor
164
Speicher
166
174
Fahrzeug-komponenten-Schnittstellen-anwendung
168
Mobil-Anwendungen
170
Nichtflüchtige Speicherung

FIG. 1B

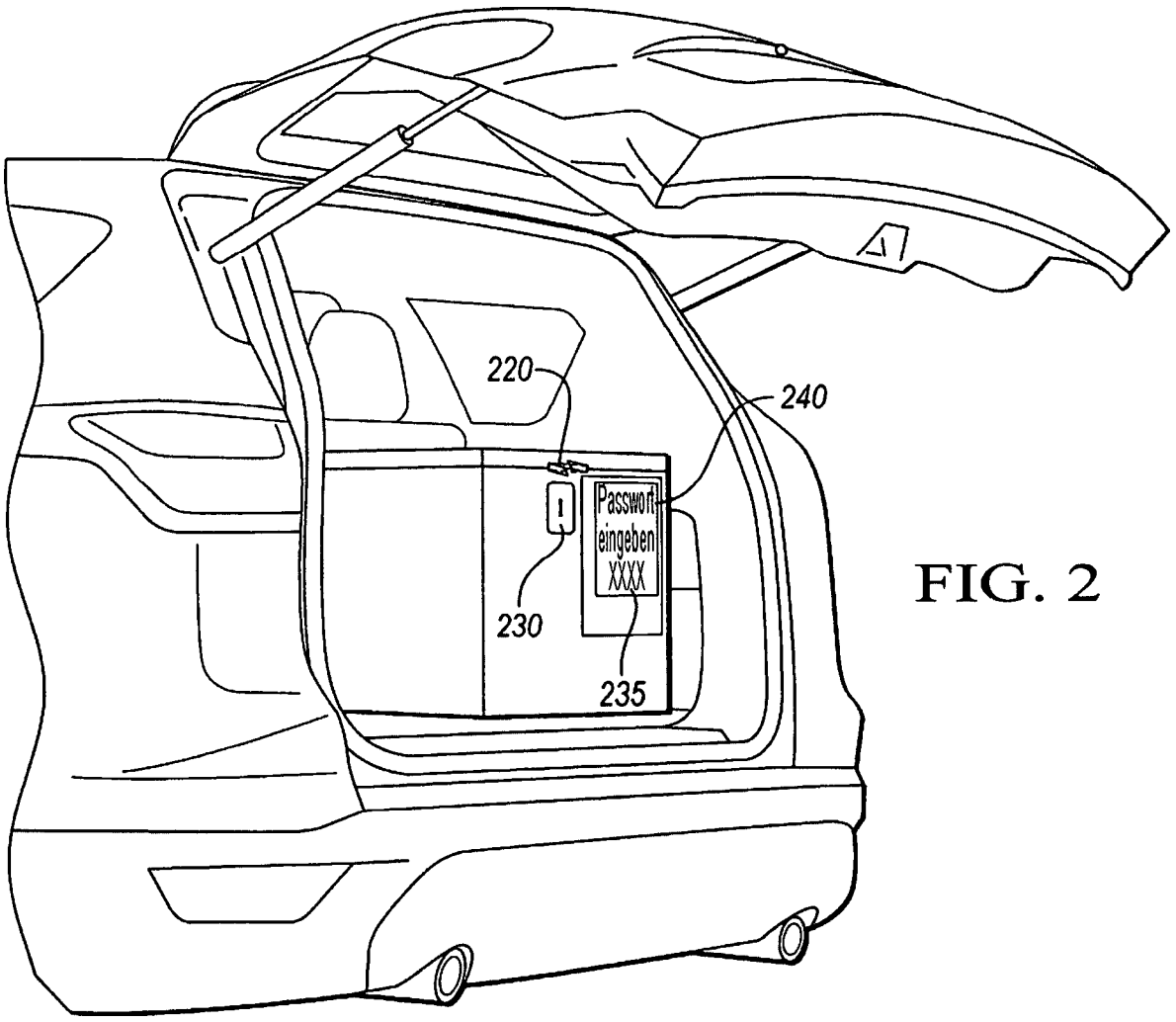


FIG. 2

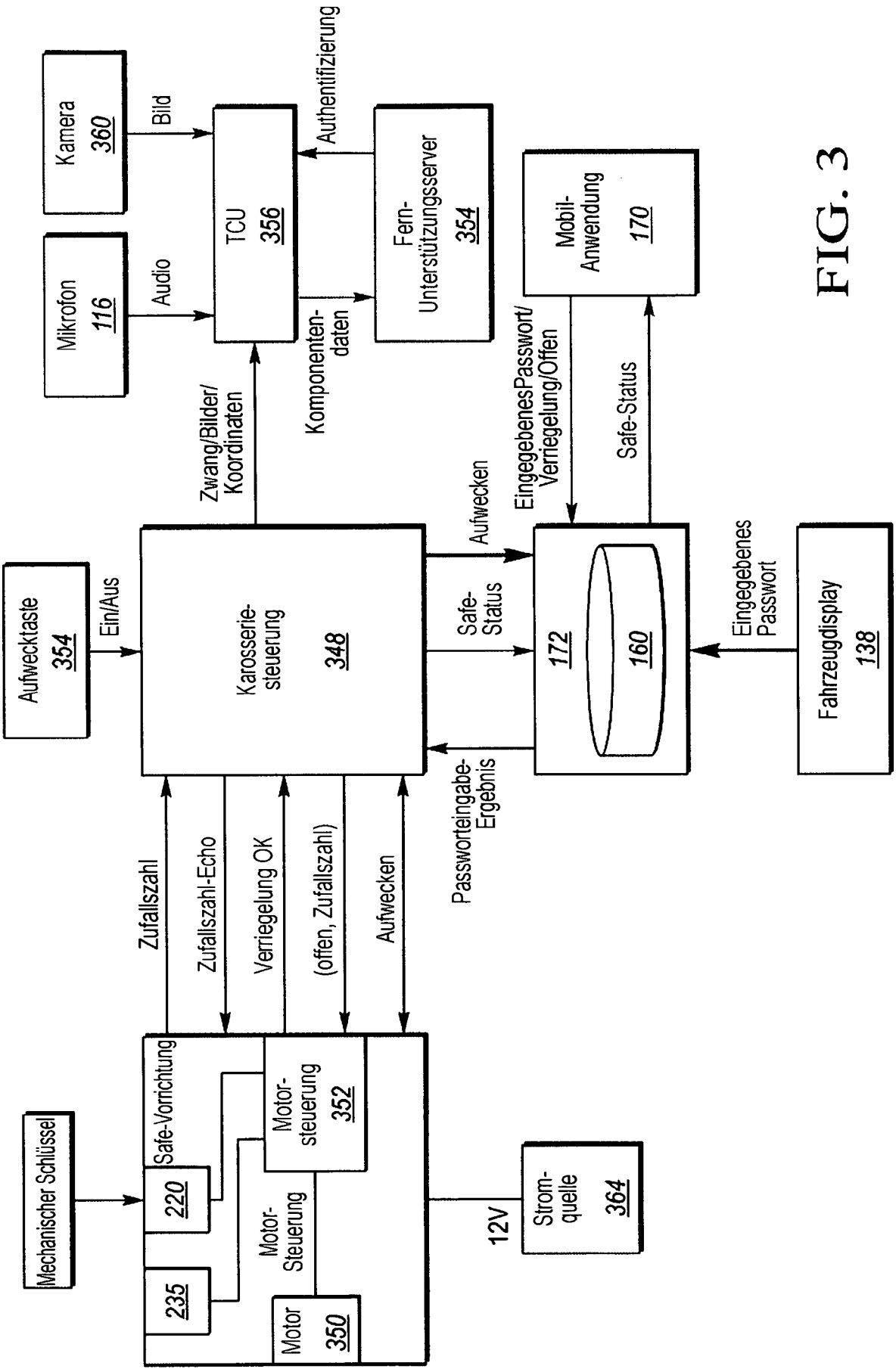

Kamera 360
Bild
Authentifizierung
Mikrofon 116
Audio
TCU 356
Fern-Unterstützungsserver 354
Komponenten-daten
Mobil-Anwendung 170
Zwang/Bilder/Koordinaten
EingegebenesPasswort/Verriegelung/Offen
Safe-Status
Aufwecken
Aufwecktaste 354
Ein/Aus
Karosserie-steuerung 348
Safe-Status
172
160
Eingegebenes Passwort
Fahrzeugdisplay 138
Passworteingabe-Ergebnis
Zufallszahl
Zufallszahl-Echo
Verriegelung OK
(offen, Zufallszahl)
Aufwecken
Mechanischer Schlüssel
Safe-Vorrichtung
220
235
Motor-Steuerung
Motor-steuerung 352
Motor 350
12V
Strom-quelle 364

FIG. 3

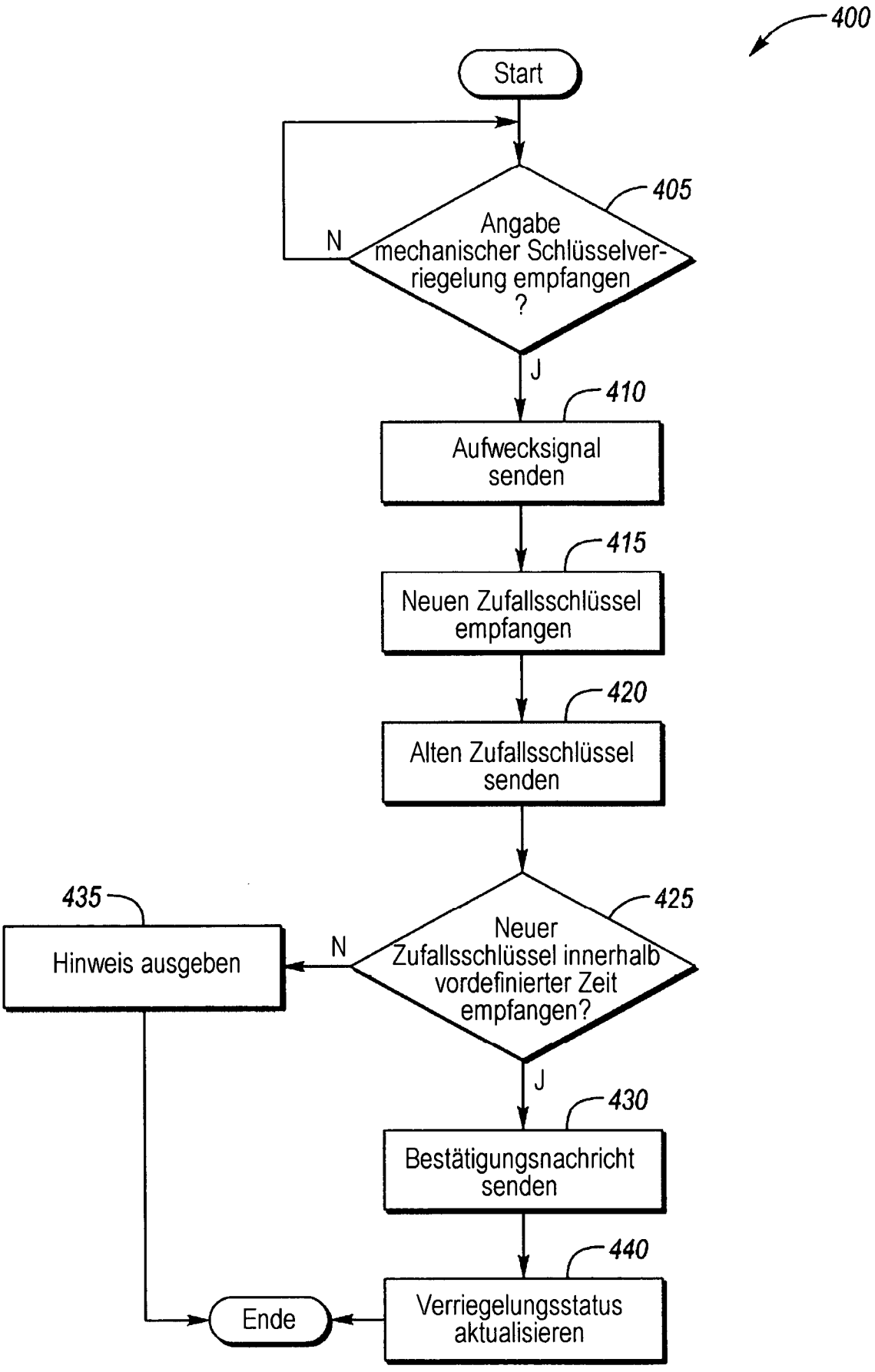

400
Start
405
Angabe mechanischer Schlüsselverriegelung empfangen ?
N
J
410
Aufwecksignal senden
415
Neuen Zufallsschlüssel empfangen
420
Alten Zufallsschlüssel senden
425
Neuer Zufallsschlüssel innerhalb vordefinierter Zeit empfangen?
N
435
Hinweis ausgeben
J
430
Bestätigungsnachricht senden
440
Verriegelungsstatus aktualisieren
Ende

FIG. 4

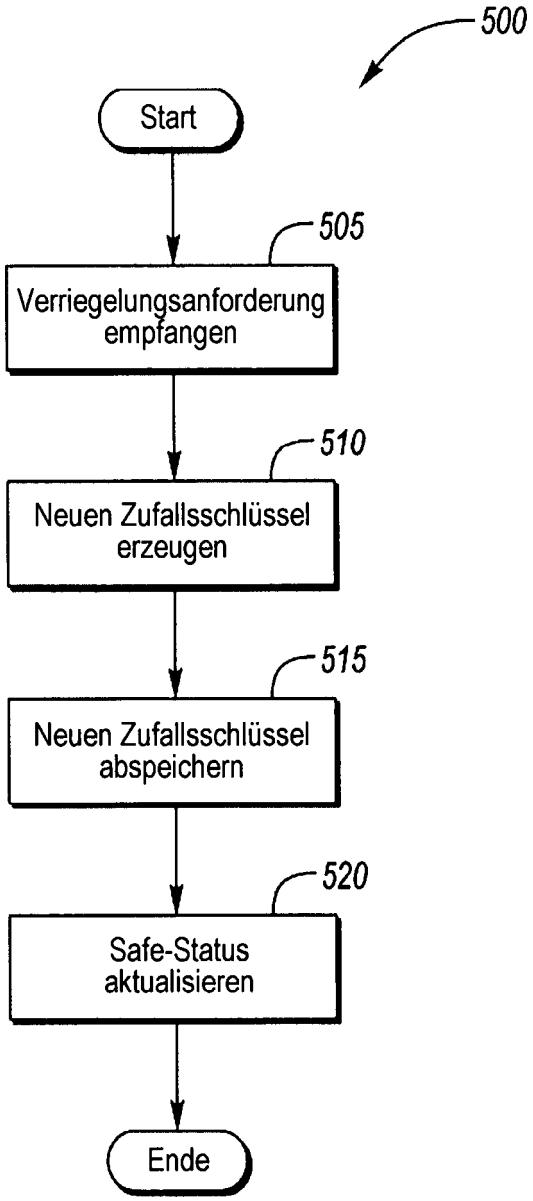

500
Start
505
Verriegelungsanforderung empfangen
510
Neuen Zufallsschlüssel erzeugen
515
Neuen Zufallsschlüssel abspeichern
520
Safe-Status aktualisieren
Ende

FIG. 5

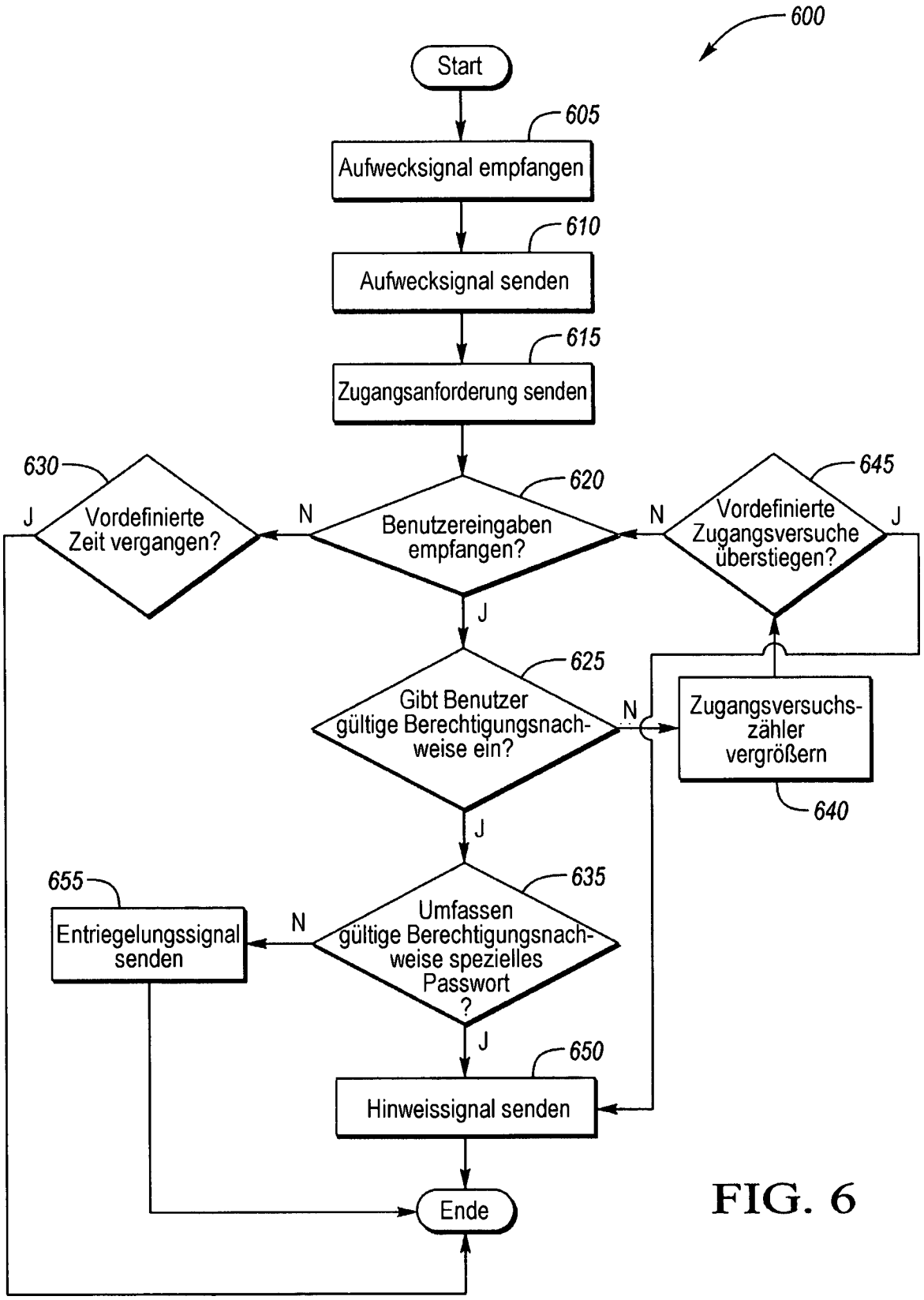

600
Start
605
Aufwecksignal empfangen
610
Aufwecksignal senden
615
Zugangsanforderung senden
620
Benutzereingaben empfangen?
630
Vordefinierte Zeit vergangen?
645
Vordefinierte Zugangsversuche überstiegen?
625
Gibt Benutzer gültige Berechtigungsnachweise ein?
640
Zugangsversuchszähler vergrößern
635
Umfassen gültige Berechtigungsnachweise spezielles Passwort ?
655
Entriegelungssignal senden
650
Hinweissignal senden
Ende
J
N

FIG. 6

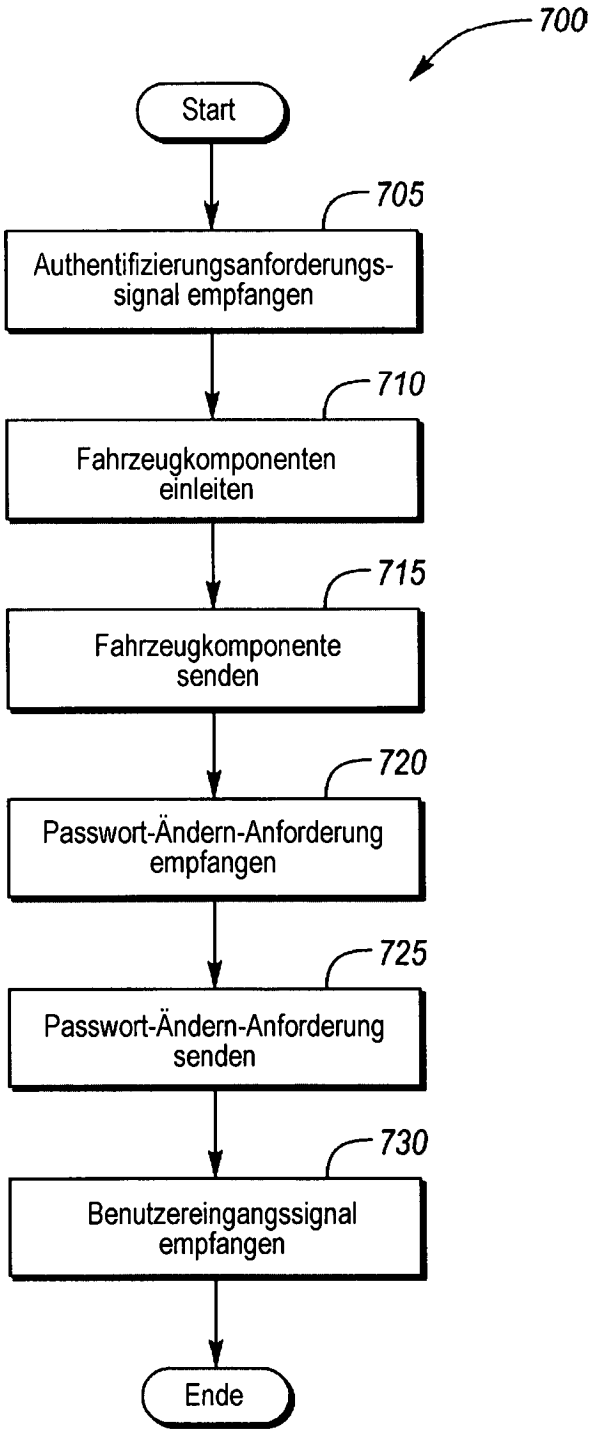

700
Start
705
Authentifizierungsanforderungs-signal empfangen
710
Fahrzeugkomponenten einleiten
715
Fahrzeugkomponente senden
720
Passwort-Ändern-Anforderung empfangen
725
Passwort-Ändern-Anforderung senden
730
Benutzereingangssignal empfangen
Ende

FIG. 7

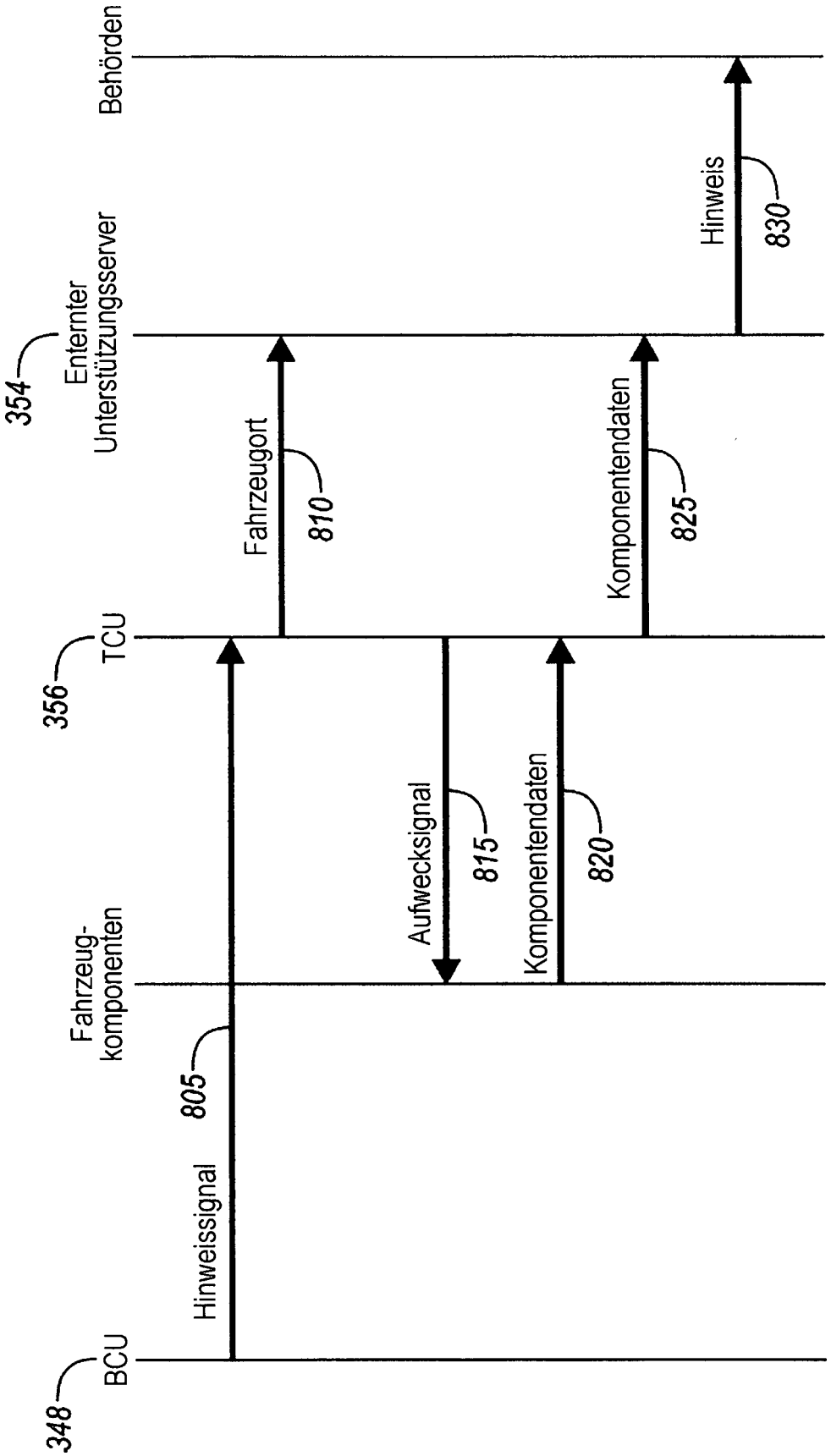

Behörden
Hinweis
830
354
Enternter Unterstützungsserver
Fahrzeugort
810
Komponentendaten
825
356
TCU
Aufwecksignal
815
Komponentendaten
820
Fahrzeug-komponenten
805
Hinweissignal
348
BCU

FIG. 8