

DIRECCIÓN DE NUEVAS CREACIONES

SOLICITUD FASE NACIONAL - PCT

1 Título de la Invención(200 caracteres o espacios máximos)

MÉTODOS, APARATOS Y SISTEMAS ANTIRROBO DE CARGA

2 Datos del Solicitante

Nombre:	NUVE, INC.	Dirección Electrónica:	patents@olartemoure.com
Dirección:	7320 North Mopac Expressway, Suite 100 Austin, Texas 78731	Domicilio/País de constitución:	ESTADOS UNIDOS DE AMERICA - TEXAS - AUSTIN

Identificación:

☐ CEDULA DE CIUDADANIA	☐ CEDULA DE EXTRANJERIA
☒ EMPRESA EXTRANJERA	☐ NIT
☐ PASAPORTE	

Número: 900043060-

3 Solicitantes

Apellidos - Nombres o Razón Social	Tipo	Identificación
1. NUVE, INC.	NN	900043060

4 Datos del Inventor

	Nombre:	Elom TSOGBE	Dirección Electrónica:	patents@olartemoure.com
	Dirección:	Suite 100 7320 North Mopac Expressway Austin, Texas 78731	Domicilio/País de constitución:	ESTADOS UNIDOS DE AMERICA - TEXAS - AUSTIN
	Identificación: ☐ CEDULA DE CIUDADANIA ☐ EMPRESA EXTRANJERA ☐ PASAPORTE ☐ CEDULA DE EXTRANJERIA ☐ NIT ☒ No Aplica			
	Número:	-		
5	Inventor(es)			
	Apellidos - Nombres		Domicilio	
	1. TSOGBE Elom		ESTADOS UNIDOS DE AMERICA	
	2. AROCHA Antonio		ESTADOS UNIDOS DE AMERICA	
6	Datos Inventor(es)			
	País de Residencia	Departamento/Estado	Ciudad	Dirección
	1. ESTADOS UNIDOS DE AMERICA	TEXAS	AUSTIN	Suite 100 7320 North Mopac Expressway Austin, Texas 78731
	2. ESTADOS UNIDOS DE AMERICA	TEXAS	AUSTIN	Suite 100 7320 North Mopac Expressway Austin, Texas 78731
7	Datos del Representante Legal / Apoderado			
	Nombre:	CARLOS R. OLARTE GARCIA	Dirección Electrónica:	patents@olartemoure.com

Dirección:		patents@olartemoure.com	Domicilio/País de constitución:	COLOMBIA - BOGOTA D.C. - BOGOTA D.C.
Identificación: ☒ CEDULA DE CIUDADANIA ☐ CEDULA DE EXTRANJERIA ☐ EMPRESA EXTRANJERA ☐ NIT ☐ PASAPORTE Número: 79782747-				
Presentación de Poder				
Año de Radicación				
Número de Radicación				
8	Datos Solicitud: PCT / WO			
Número Solicitud:		PCT/US2015/026169	Fecha Solicitud:	16/04/2015
Número Publicacion:		WO2015/161073	Fecha Publicacion:	22/10/2015
9	Declaraciones de prioridad		☒ SI ☐ NO	
	(33) País de origen	Codigo del país	(31) No. Solicitud	(32) Fecha
1.	ESTADOS UNIDOS DE AMERICA	US	61/980,470	16/04/2014
2.	ESTADOS UNIDOS DE AMERICA	US	PCT/US2014/054796	09/09/2014
10	Reivindicaciones			
Número reivindicaciones:		20	Pago Reivindicaciones:	No
11	Reducción de tasas.			
<i>Declaro que carezco de medios económicos para presentar la solicitud de patente.</i> ☐ SI ☒ NO Nota: En caso de ser persona natural y carecer de medios económicos, y por lo tanto, aplique la reducción de tasas a que se refiere la resolución vigente en tarifas, debe firmar la presente solicitud bajo la gravedad de juramento.				
☐ Micro, pequeñas y medianas empresas ☐ Universidades públicas o privadas				

☐ Entidades sin ánimo de lucro

Debe aportar los documentos que se indican en el numeral 17 de anexos

12	Documentos Anexos
-----------	--------------------------

- | |
|--|
| <ul style="list-style-type: none">☒ Reivindicaciones☒ Descripción☒ Dibujos y/o Figuras☒ Resumen☐ Certificado Depósito Material Biológico☐ Uso de Conocimiento tradicional☐ Listado de secuencias☐ Artes finales 12 x 12 cm☐ Poderes, si fuere el caso☐ Copia de la primera solicitud si se reivindica prioridad☐ Traducción simple de la primera solicitud, si se reivindica prioridad☒ Otros Anexos |
|--|

MÉTODOS, APARATOS Y SISTEMAS ANTIRROBO DE CARGA

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

5

Esta solicitud reclama prioridad a la solicitud de patente del Tratado de cooperación en materia de patentes No. PCT/US 14/54796, titulada MÉTODOS, APARATOS Y SISTEMAS ANTIRROBO DE COMBUSTIBLE, presentada por Elom Tsogbe el 9 de septiembre de 2014 la cual reclama prioridad a la solicitud de patente provisional de los Estados Unidos No. 61/883,431 titulada MÉTODOS, APARATOS Y SISTEMAS ANTIRROBO DE COMBUSTIBLE, presentada por Elom Tsogbe el 27 de septiembre de 2013, las cuales se incorporan en el presente documento en su totalidad como si se establecen en su totalidad. Esta solicitud también reclama prioridad a y es una solicitud no provisional de la solicitud de patente provisional de los Estados Unidos No. 61/980,470 titulada MÉTODOS, APARATOS Y SISTEMAS DE PROTECCIÓN PARA CARGA, presentada por Elom Tsogbe el 16 de abril de 2015 de la cual se incorpora en el presente documento en su totalidad como si se establece en su totalidad.

ANTECEDENTES

25

El robo de gasolina, combustible diesel y/u otros combustibles vehiculares representa una pérdida sustancial para los transportistas de carga en muchas partes del mundo. Notablemente, en muchos países en desarrollo, el combustible representa un producto de venta fácil que no puede ser rastreado y que recaba un alto beneficio en el mercado negro. Así, los vehículos estacionados se presentan como objetivos indefensos para ladrones de combustible. Incluso los vehículos custodiados, sin embargo, pueden estar en riesgo sobre todo si el conductor está "en ruta."

Por supuesto, el combustible contenido en estos vehículos se puede acceder mediante el tapón de llenado de combustible (o simplemente "tapón de combustible"). Un ladrón puede retirar el tapón de combustible, conducir un tubo o manguera a través del tubo de llenado contiguo, y succionar el combustible del tanque. Por otra parte, los sistemas de combustible vehicular normalmente presentan un número de "puntos de entrada" menos convencionales a través de los cuales un ladrón puede tener acceso al combustible contenido en el mismo. Más específicamente, los sistemas de combustible vehicular normales incluyen un tanque de combustible (a veces con un accesorio/función de drenaje), una bomba de combustible (a menudo sumergida, pero a veces externa al tanque), un filtro de combustible, varias válvulas, una línea de recirculación, puertos de prueba,

sensores de velocidad de flujo y/o una conexión a un carburador (en vehículos más antiguos), o los inyectores de combustible (la mayoría en vehículos último modelo), y/o un "riel" del combustible que alimenta los inyectores de combustible. Esa lista, por cierto, no es exclusiva pero sirve para ilustrar que cada componente del sistema tiene por lo menos un acoplamiento fluido/mecánico que puede ser manipulado para acceder al combustible. Adicionalmente, puede haber algunos de dichos acoplamientos fluidos entre tubos de otra manera separados, tuberías, mangueras, etc. que transportan combustible a través del vehículo. Todos estos acoplamientos, componentes, etc. representan el sistema de combustible "puntos de entrada" y dan el combustible en el mismo sujeto a robo.

Dichos riesgos, por otra parte, no existen con vehículos terrestres solos. Más bien los carros, camionetas, camiones, furgonetas, etc. que existen en las carreteras representan sólo una categoría de vehículo susceptible. Las aeronaves (por ejemplo, helicópteros, aviones de hélice, aviones a reacción, etc.), vehículos marinos (por ejemplo, barcos, aerodeslizadores, remolcadores, barcos grúa, etc.) y otras categorías de vehículos también están en riesgo de robo de combustible. El combustible de aviación (*av-gas*, *jet A*, *mogas*) que se vende en sobreprecio en comparación incluso con la gasolina

de automóvil, sin mencionar el diesel representa un objetivo particularmente "rico" en aeropuertos no custodiados, campos de aviación y similares. Por supuesto, los precios elevados y/o escasez (ya sea local, regional o lo contrario) agrava la amenaza.

Consideraciones similares se aplican a la carga que pueden llevar los camiones y/u otros vehículos. Por ejemplo, en zonas pobres, el alimento, agua, bebidas, etc. pueden ser altamente apreciados y considerados dignos de tentativa de robo y/u otros tipos de apropiación indebida. Una carga más valiosa tal como dispositivos electrónicos de consumo podría ser buscada con personajes menos éticos dispuestos a robar estos productos de sus empleadores, otros, etc. Y, por supuesto, mercancía más rara tal como el oro, joyería, dinero en sí (transportados en vehículos blindados) podría ser objetivos para robo.

Además, se necesita que se roben cargamentos enteros para que el exportador sufra pérdidas significativas, particularmente si se ve con el tiempo. Por ejemplo, incluso clientes legítimos del exportador pueden estar tentados a tomar ventaja de la falta de seguridad normalmente presente cuando un camión llega a sus instalaciones. En dichas situaciones, algunas personas podrían retirar su carga ordenada de forma legítima y después proceder a tomar más carga de la que ordenaron o de

otra manera están autorizados para tomar. En la alternativa, o además, dichas personas podrían reclamar fraudulentamente la carga que falta de un envío cuando de hecho estaba presente. Y, por supuesto, otros escenarios demasiado numerosos para enlistarlos aquí puede dar lugar a discrepancias asociadas con envíos de carga. Estas cuestiones van más allá de los países emergentes. De acuerdo con el FBI, el robo a carga ha alcanzado una porción epidémica con un promedio de hasta 30\$ mil millones perdidos anualmente sólo en los Estados Unidos de América.

BREVE DESCRIPCIÓN

A continuación se presenta una breve descripción simplificada con el fin de proporcionar un entendimiento de algunos de los aspectos de la materia divulgada. Esta breve descripción no es una vista general extensa de la materia divulgada, y no tiene la intención de identificar elementos clave/críticos o para delinear el alcance de dicha materia. Un propósito de la breve descripción es presentar algunos conceptos en una forma simplificada como un preludio a la divulgación más detallada que se presente en este documento. La divulgación actual proporciona sistemas, aparatos, métodos, etc. para la detección de posible robo de combustible y más particularmente para la detección de

eventos relacionados con el robo de combustible asociados con vehículos tales como aviones, barcos, automóviles y camiones entre otros vehículos.

Algunas modalidades proporcionan sistemas antirrobo de combustible para vehículos que poseen sistemas de combustible que definen una pluralidad de puntos de entrada del fluido. Los sistemas de la modalidad actual nominalmente incluyen un número pre-seleccionado de sensores que se colocan en los puntos de entrada. Cada sensor define un estado nominal/seguro y un estado potencialmente alterado. El estado potencialmente alterado es indicativo de que el sensor está ausente. Los estados reales de los sensores que se combinan para crear un estado combinado real de los sensores. En contraste, los estados nominales del número preseleccionado de sensores se combinan para crear un estado combinado nominal del número preseleccionado de sensores. Además, un controlador del sistema detecta el estado combinado actual de los sensores y determina si el estado combinado actual de los sensores es el estado combinado nominal del número preseleccionado de sensores. En respuesta a ello, el controlador genera una señal que indica si todos del número preseleccionado de sensores están presentes y sin manipulación.

De acuerdo con diversas modalidades, la divulgación actual también proporciona métodos antirrobo de

combustible. Algunos de dichos métodos comprenden una variedad de actividades que incluyen el detectar una señal combinada a partir de una pluralidad de sensores colocados en los puntos de entrada de un sistema de combustible de
5 vehículo. Cada sensor define un estado seguro y un estado de sospecha (indicativo de que el sensor está ausente) de acuerdo con la modalidad actual. Por otra parte, los estados del sensor seguro de un número de sensores nominalmente en el sistema se combinan para crear un estado
10 de sistema seguro. Dichos métodos también comprenden determinar si la señal combinada es casi igual al estado del sistema seguro (para el número de sensores en el sistema) y la salida de una señal correspondiente.

Si lo desea, la detección de la señal combinada puede
15 ser a través de una tierra de chasis de vehículo y/o los sensores pueden ser nominalmente cableados en paralelo. En algunas situaciones una resistencia contribuye a la señal combinada. Además, o en alternativa, tales métodos pueden comprender además mostrar la ubicación del vehículo cuando
20 la señal falla en indicar que la señal combinada es indicativo del estado del sistema de seguridad para el número de sensores.

Diferentes modalidades proporcionan controladores antirrobo de combustible incluyendo un circuito y/o
25 sensores que definen estados nominal (seguro) y manipulado.

Los estados manipulados son indicativos de que los sensores están ausentes. Los controladores de la modalidad actual, además, detectan un estado combinado de (todos de un número preseleccionado de) los sensores y determinan a partir de los mismos si todos del número preseleccionado de sensores están presente y seguros. En algunas modalidades, el controlador detecta los sensores (que pueden ser cableados en paralelo) por medio de una tierra de chasis del vehículo. Si lo desea, se puede conectar una resistencia (que es más o menos eléctricamente equivalente a uno o más de los sensores) y/o una unidad de geoposicionamiento al controlador. Los sensores pueden incluir interruptores normalmente abiertos y abrazaderas que cierran los interruptores cuando se instalan correctamente. Los sensores se pueden asegurar por otros medios tales como sujetadores, proteger por otros medios como los sujetadores, bridas de cable, bridas plásticas, adhesivos, etc. Algunos sensores incluyen tiras de puesta a tierra mientras que otros incluyen conductores de retorno de tierra. En algunas modalidades, los sensores se colocan en el filtro de combustible y/o tapón de combustible del vehículo.

Diferentes modalidades proporcionan controladores antirrobo que comprenden entrada, salida y circuitos de interruptores de carga en comunicación con los mismos. Las

entradas de la modalidad actual están configuradas para detectar las bases de los vehículos de carga en los que están instalados a través de un interruptor de carga. Los Interruptores de carga de la modalidad actual sirven al menos para dos propósitos. Más específicamente, proporcionan una interfaz para las solicitudes de acceso y detectan si la puerta está cerrada o abierta. Los sistemas de las modalidades incluyen otra característica de seguridad tal como sensores infrarrojos, sensores de proximidad, sensores de efecto Hall, sensores RFID (Identificación por radiofrecuencia), sensores ópticos, etc. para proporcionar una percepción adicional como para el estado del interruptor de carga y/o sus alrededores. Además, algunos controladores se configuran de manera que si un alambre es un circuito de entrada se rompe (o si alguien lo rompe), estos controladores interpretan esa condición como indicativo de manipulación y así activan una alarma.

Mientras tanto, las salidas están configuradas para estar en comunicación con cerraduras operadas electrónicamente. Los circuitos están en comunicación con las entradas y las salidas y están configurados para detectar las aberturas de los interruptores de carga por medio de voltajes preseleccionados en las entradas del interruptor de carga. En respuesta a ello, además, los

circuitos están configurados para activar las cerraduras por medio de las salidas. En la modalidad actual los interruptores de carga están acoplados mecánicamente a puntos de acceso de la carga en los vehículos de carga de manera que no se puedan abrir los puntos de acceso sin abrir los interruptores de carga.

En algunas modalidades los circuitos comprenden además salidas de geoposicionamiento y los circuitos están configurados además para sacar una señal indicativa de la abertura del interruptor de carga por medio de la salida de geoposicionamiento. Además, o en la alternativa a ello, los controladores pueden comprender además entradas de geozonas y están configurados además para sacar señales para desbloquear la cerradura sólo en geozonas preseleccionadas. En algunas situaciones el voltaje preseleccionado difiere de una forma de 12 V CC y se puede seleccionar por el usuario.

Además, el controlador además puede estar configurado para detectar un PIN (número de identificación personal) asociado con aberturas y cierres del interruptor de carga, teclado, secuencia de golpeo de audio, teléfono celular (llevado por el usuario), etc. En algunos de estos casos, el controlador puede configurarse también para cambiar el PIN (Número de identificación personal). En el lado mecánico de las cosas, el controlador puede incluir o

acoplarse a un acoplador que se acopla de manera segura al vehículo de carga. También (o en su lugar) puede comprender una entrada en la posición de la cerradura y estar configurada para detectar una posición de la cerradura por medio de la misma. Dichos controladores, además, se pueden configurar para sacar una señal que indique que la cerradura debería cerrarse en respuesta a la posición de la cerradura. Algunos controladores, cerraduras, y/u otros componentes del sistema comprenden además una batería para energizarse.

Para la realización de los fines anteriores y relacionados, ciertos aspectos ilustrativos se describen en el presente con relación en las figuras anexas. Estos aspectos son indicativos de varias maneras no limitantes en que puede practicarse la materia divulgada, todos los cuales se pretenden estén dentro del alcance de la materia divulgada. Otras características novedosas y/o no obvias serán evidentes de la siguiente divulgación detallada cuando se consideran en conjunto con las figuras y están también dentro del alcance de la divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La descripción detallada se describe con referencia a las figuras adjuntas. En las figuras, los dígitos más a la

izquierda de un número de referencia usualmente corresponden a la figura en la que el número de referencia aparece por primera vez. El uso de los mismos números de referencia en diferentes figuras generalmente indican
5 elementos similares o idénticos.

La Fig. 1 ilustra los vehículos sujetos a robo de combustible.

La Fig. 2 ilustra un sistema antirrobo de combustible instalado en un vehículo.

10 La Fig. 3 ilustra esquemáticamente un sistema antirrobo de combustible.

La Fig. 4 ilustra un controlador antirrobo de combustible.

15 La Fig. 5 ilustra un sensor de abrazadera antirrobo de combustible.

La Fig. 6 ilustra un sensor antirrobo de combustible estacionario.

La Fig. 7 ilustra un sensor antirrobo de combustible instalado en una tapa de combustible.

20 La Fig. 8 ilustra un sensor antirrobo de combustible instalado en un filtro de combustible.

La Fig. 9 ilustra un sensor antirrobo de combustible instalado en una línea de succión de combustible.

25 La Fig. 10 ilustra un sensor antirrobo de combustible instalado en una línea de retorno de combustible.

La Fig. 11 ilustra una interfaz gráfica de usuario (GUI) de un sistema antirrobo de combustible.

La Fig. 12 ilustra un diagrama de flujo de un método para detectar el robo de combustible.

5 La Fig. 13 ilustra una computadora para uso en sistemas antirrobo de combustible.

La Fig. 14 ilustra esquemáticamente un sistema antirrobo de combustible.

La Fig. 15 ilustra una unidad de control antirrobo de
10 combustible.

Las Figs. 16 y 17 ilustran un sensor de línea de combustible.

La Fig. 18 ilustra un sensor de tapa de combustible.

La Fig. 19 ilustra un sistema antirrobo de carga.

15 La Fig. 20 ilustra otro sistema antirrobo de carga.

La Fig. 21 ilustra un controlador antirrobo instalado.

La Fig. 22 ilustra esquemáticamente un sistema antirrobo de carga.

20 La Fig. 23 ilustra esquemáticamente otro sistema antirrobo de carga.

La Fig. 24 ilustra un interruptor de carga y un par de conectores de cabina a remolque.

Este documento divulga sistemas, aparatos, métodos, etc. para la detección de posible robo de combustible y más particularmente para la detección de eventos relacionados con el robo de combustible asociados con vehículos tales como aviones, barcos, automóviles y camiones entre otros vehículos.

La Fig. 1 ilustra los vehículos sujetos a robo de combustible. Más en particular, la Fig.1 ilustra un camión de concreto (102), un camión repartidor (104), una excavadora (106), un remolque generador (108), un buque (110), un tanque de combustible (120), un punto de entrada (122), un controlador antirrobo (130) y una antena (132). Estos vehículos, (102), (104), (106), (108) y (110) (entre otros) tienen un número de rasgos comunes. Por un lado, todos contienen combustibles de diversos tipos que son todos al menos algo valiosos. Por otra parte, los propietarios, operadores y otros usuarios asociados con ellos los toman y/o dejan en ubicaciones que a menudo están lejos de otros usuarios y en los que los testigos de un robo potencial de combustible pueden estar lejos o pocos entre los mismos. En la alternativa, o además, muchos testigos potenciales podrían no importarles lo suficiente como para informar de actividades sospechosas o podría incluso estar coludidos con los que van a llevar a cabo

dichas acciones. Así, estos vehículos y/o el combustible en los mismos están susceptibles a robo de combustible de vez en cuando.

Por ejemplo, considere el camión repartidor (104). Un conductor a menudo toma el camión repartidor (104) en rutas de entrega y/o recogiendo diversos productos y/o entregando diversos servicios. Estas rutas podrían meter al conductor en áreas lejos de un depósito, estación u otro lugar en el que el camión normalmente está guardado en un garaje, estacionado, etc. Esos garajes normalmente están dotados por personal por el mismo dueño del camión repartidos (104) y/o empleados u otros agentes del propietario. Así, si un conductor desea tomar combustible del camión repartidor (104) de forma no autorizada por el propietario, es probable que el conductor espere a hacerlo hasta que se encuentren en una ruta o supuestamente en una ruta.

Cuando se sienten listos para tomar el combustible, el conductor normalmente detendrá el camión en un lugar "adecuado" para hacerlo y salir de su cabina. A menudo encontrarán un punto de entrada (122) en el sistema de combustible del camión repartidor (104) a través del cual accede al combustible. Por ejemplo, ellos sacarán la tapa de combustible del tanque de combustible (120), insertarán una manguera en el tanque de combustible (120) y succionarán el combustible del tanque de combustible (120).

Posteriormente, dichos conductores dispondrán también el combustible para uso personal, lo venderán, o harán algún otro uso no autorizado del combustible. Dichos ladrones de combustible (solos y/o en conjunto) pueden representar una importante pérdida para el propietario del camión repartidor (104). Por supuesto, cualquier vehículo que contiene combustible se encuentra en riesgo de dichos ladrones. De hecho, se estimó en 2013 que los robos de combustible costaron a la economía de México sólo de 2 a 4 mil millones de dólares al año. Ver *The Aftermath Of Mexico's Fuel Theft Epidemic: Examining The Texas Black Market And The Conspiracy To Trade In Stolen Condensate* por Luke B. Reinhart, el 9 de mayo de 2014.

Algunas modalidades proporcionan sistemas para detectar posibles robos de combustible y para alertar al propietario y/u otros usuarios de dichas actividades. Como la Fig. 1 muestra además que el controlador antirrobo de combustible (130) puede montarse en, o sobre, el camión repartidor (104) para detectar actividad que podría indicar que alguien podría haber robado combustible, está robando combustible y/o está a punto de robar combustible. El controlador antirrobo de combustible (130) normalmente está conectado a una pluralidad de sensores situados en los puntos de entrada al sistema de combustible del vehículo y los supervisa para posibles manipulaciones.

Los sensores provocan que el controlador antirrobo de combustible (130) generen una señal si alguna actividad, condición, etc. provocan que uno o más de los sensores cambien de estado de un estado seguro a un estado manipulado o si un sensor parece estar faltando en el sistema (ya sea de repente o no). Además, el controlador antirrobo de combustible (130) de las modalidades se comunica y/o coopera con una unidad de geoposicionamiento, computadora, etc. abordo del camión para marcar la hora o marcar la ubicación de dichas ocurrencias. Más aún, el controlador antirrobo de combustible (130), el sistema de geoposicionamiento (132), y/o algún otro dispositivo en el camión repartidor (104) puede transmitir información respecto a dichas ocurrencias al propietario/operadores, consolas de alarma centrales, etc. lejanos.

La Fig. 2 ilustra un sistema antirrobo de combustible instalado en un vehículo. Más en particular, la Fig. 2 ilustra un sistema de combustible (200), el sistema antirrobo (201), un tanque de combustible (202), una bomba de combustible (204), un filtro de combustible (206), un motor (208), una tapa de combustible (210), una entrada de combustible (tubo, tubería, etc.) (211), una bomba de combustible secundaria (212), un regulador de presión de combustible (218), una línea de retorno de combustible (220), un acoplamiento (222), los sensores (223), (225) y

(227) , cables, (224), (226) y (228), un controlador (230), una unidad de geoposicionamiento (232) y un conducto (240). En este momento, una breve discusión del sistema de combustible (200) de un vehículo típico podría ser
5 beneficiosa.

Como aquellos expertos en la materia apreciarán, la mayoría de los vehículos incluyen un sistema de combustible (200) para suministrar el combustible almacenado en un tanque de combustible (202) al motor (208). Aquellos
10 sistemas de combustible (200) están repletos con puntos de entrada que hacen al combustible en el mismo susceptible al robo. Más en particular, en vehículos comerciales en particular, el tanque de combustible (202) puede contener cientos de galones de combustible, cada galón de que se
15 valora en varios dólares estadounidenses a partir de esta escrito.

La tapa del combustible (210) presenta uno de los muchos puntos de entrada asociados a un sistema típico de combustible vehicular. Por otra parte, la tapa del
20 combustible (210) normalmente se encuentra en una ubicación de fácil acceso lo que es particularmente atractivo para los ladrones como un punto de entrada. Por otra parte, a menudo la entrada del combustible (211) y el tanque de combustible (202) se forman integralmente uno con el otro
25 (o se sueldan entre sí o de otra manera se acoplan de forma

permanente). Todavía, en los vehículos en lo que son componentes separados, el acoplamiento entre estos dos componentes representa otro punto de entrada en que el acoplamiento se puede desconectar permitiendo que el combustible se drene fuera del (o sea bombeado fuera del) sistema de combustible (200). Muchos tanques de combustible (202), contienen además, una bomba de combustible secundaria (212) o la tienen montada en proximidad cercana al mismo. Así, la bomba de combustible secundaria (212) de algunos vehículos presenta otro acoplamiento de sistema (o incluso un par de los mismos), y por lo tanto, un punto de entrada.

Desde el tanque de combustible (202), una línea de combustible se dirige a otro componente del sistema de combustible (como se ilustra en Fig. 2) tal como la bomba de combustible primaria (204). Una vez más, este componente presenta otro par de puntos de entrada haciendo el combustible vulnerable al robo. El filtro de combustible (206), el regulador de presión de combustible (218), el motor (208) y la línea de retorno de combustible (220), todos incluyen acoplamientos que también hacen el combustible vulnerable. Por otra parte, los fabricantes de vehículos a veces encuentran deseable usar dos o más piezas de tubos, tuberías, manguera, etc. para conducir el combustible de un componente a otro. Como resultado, un

acoplamiento (222) puede aparecer en muchos lugares aparte de los componentes discretos, ilustrados por la Fig. 2. Como se señaló, por lo tanto, los sistemas de combustible normales (200) están llenos de puntos de entrada que hace
5 que el combustible contenido en los sistemas sea vulnerable al robo.

Continuando con la referencia a la Fig. 2, las modalidades proporcionan sistemas antirrobo (201) sobre los vehículos tal como un camión repartidor (104). El sistema
10 antirrobo (201) de la modalidad actual incluye el controlador (230), la unidad de geoposicionamiento (232), los sensores, (223), (225) y (227) y los cables, (224), (226) y (228) entre otras cosas. El controlador (230) de la modalidad actual reside en el personal de cabina del
15 vehículo y, más particularmente, se puede montar en el tablero o en algún lugar relativamente inaccesible para los usuarios del vehículo. La unidad de geoposicionamiento (232) también puede residir en la cabina aunque, si se desea, se puede ubicar en un área accesible de la cabina.
20 En la alternativa, o además, la unidad de geoposicionamiento (232) puede ser un componente del controlador (230). Los sensores (223), (225) y (227) se sujetan a los acoplamientos (222) y/u otros componentes del sistema de combustible (200) que representan puntos de
25 entrada. Los cables, (224), (226) y (228) se dirigen desde

los sensores (223), (225) y (227) al controlador (230) y también (en la modalidad actual) se dirigen a través de conductos (240).

Los cables, (224), (226) y (228) proporcionan
5 conductividad eléctrica entre los sensores (223), (225) y (227) y el controlador (230), por lo tanto, el controlador (230) permite detectar el estado de los sensores (como un grupo en la modalidad actual). Además, los conductos (240) proporcionan protección a los cables (224), (226) y (228)
10 del daño mecánico que se genera por abuso, negligencia, manipulación directa, etc. Los conductos (240) (y, para ese hecho, los cables, (224), (226) y (228)) pueden ser disimulados para que parezcan ser OEM (fabricantes de equipos originales), después de la venta, etc. equipo que
15 ha estado en el vehículo durante algún tiempo. Los conductos (240) pueden ser (entre otras cosas) una pieza de revestimiento de cable, manguera trenzada, conducto corrugado (del tipo SM-1216-BK y disponible de *Sealcon LLC* ubicado en 7374 S. Eagle St, Centennial CO 80112 etc. y/o
20 puede ser manchada con suciedad, grasa, mugre, etc. normalmente disponibles en el vehículo o creado para tales fines.

Como se divulga además con referencia a las Figs. 3 y 5-10, los sensores, (223), (225) y (227) incluyen
25 abrazaderas e interruptores normalmente abiertos. Las

abrazaderas están configuradas para mantener los sensores contra los diversos acoplamientos/componentes y (haciendo eso) para instar a los interruptores hacia sus posiciones cerradas. Son estas posiciones cerradas (colectivamente, en la modalidad actual) que indican que el sistema de combustible (200) está seguro y/o sin manipulación. De hecho, incluso si uno de los interruptores abiertos (o un sensor desaparece del sistema antirrobo (201)), el controlador (230) de la modalidad actual interpretará ese evento como una indicación de que algún usuario podría estar manipulando el sistema de combustible (200) y/o intentar obtener acceso al combustible a través de un componente/acoplamiento/punto de entrada supervisado.

La Fig. 3 ilustra esquemáticamente un sistema antirrobo de combustible. Más en particular, la Fig. 3 ilustra un sistema antirrobo (300), un subsistema exterior (304), un centro de alerta remoto (306), la "nube" de Internet, un satélite (308), una red de sensores (308), un conjunto de resistencias (312), los sensores (318), interruptores de sensor (320), resistencias de sensor (322), resistencias (324), un controlador (330), una unidad de geoposicionamiento (332), un comparador (334), una antena (338) y un indicador local (340). Si se desea se puede utilizar un procesador en lugar de, o además del comparador (334). En tales casos, el procesador puede

configurarse con una entrada análoga para detectar las resistencias y/o para determinar si el sistema es seguro o potencialmente ha sido manipulado.

Así, el sistema antirrobo (300) permite al
5 controlador (330) comunicarse con el centro de alerta remoto (306) por medio de la Nube (309) y/o por medio del sistema de geoposicionamiento que incluye sus satélites (308) y/u otras infraestructuras). Si el controlador (330) debe emitir una alerta, por lo tanto, el centro de alerta
10 remoto (306) puede recibir la alerta a través de ya sea la nube, el sistema de geoposicionamiento, y/o algún otro sistema de telecomunicaciones (tal como un sistema de teléfono celular). Los usuarios y/o servidores, computadoras, etc. en comunicación con el centro de alerta
15 remoto (306) pueden supervisar, reaccionar a, extraer datos, etc. estas alertas y/o tomar medidas correctivas. Por ejemplo, un propietario del vehículo podría investigar las alertas, poner el vehículo/conductor bajo vigilancia, etc.

20 Continuando con la referencia a la Fig. 3, el controlador (330) reside en un vehículo como lo hace gran parte del resto del sistema antirrobo (300) de la modalidad actual. Por ejemplo, cada uno de los sensores (318) reside en el vehículo y comprende un interruptor normalmente
25 abierto (320) y a menudo cierta resistencia interior

(inherente) (322). Por supuesto, esas resistencias internas (322) podrían asociarse con interconexiones internas de los sensores (318), su cableado externo, las conexiones entre las mismas, etc. Sin embargo, en algunas modalidades, 5 diversos sensores (318) comprenden resistencias de alrededor de 10 k-ohm, 5.1 k-ohm o 3.3 k-ohm con una tolerancia del 1%. Como resultado, cada sensor (318) de la modalidad actual tendrá nominalmente dos estados: un estado seguro y un estado potencialmente manipulado. En el estado 10 seguro, los sensores (318) tienen sus interruptores normalmente abiertos (320) sujetado cerrado por una abrazadera que asegura los sensores en sus respectivos componentes. Así, el sensor (318) (cableado en paralelo con los otros sensores (318)) contribuye su 15 resistencia/conductancia (322) a la red de sensores general (310). Pero, en estado potencialmente manipulado, los interruptores normalmente abiertos (320) están abiertos de manera que los sensores (318) parecen ser caminos "abiertos" eléctricamente contribuyendo así a la no 20 conductancia y/o una resistencia infinita a la red de sensores (308).

Así, cuando un sistema antirrobo (300) está instalado y funcionando nominalmente en un vehículo, todos los interruptores (320) de los sensores (318) se mantiene 25 cerrados por las abrazaderas y son detectados en

consecuencia por el controlador (330). Pero, si uno o más sensores (318) son manipulados, un número correspondiente de interruptores (320) es probable que se abran cambiando así la resistencia/conductancia general de la red de sensores (310). Además, el controlador (330) (y/o su comparador (334)) puede configurarse para detectar si la conductancia/resistencia nominal de la red de sensores (308) está presente o si ha sido alterada. Más específicamente, el comparador (334) puede configurarse para producir una señal basada en sí o no un número preseleccionado/conocido de sensores (318) están presentes con sus interruptores normalmente abiertos (320) en la posición cerrada.

Así, la conductancia/resistencia combinada, general, esperada de la red de sensores sería:

$$R_{\text{seguro}} = 1/n * R_{\text{sensor}}$$

Donde:

R_{seguro} es la resistencia general esperada de la red de sensores, n es el número preseleccionado de sensores (318) (resistencias (322)), y

R_{sensor} es la resistencia (322) de un sensor (318).

Un suministro de energía (335) (interno al controlador (330) de la modalidad actual) puede suministrar

una corriente lenta a la red de sensores (310). Además, el comparador (334) puede configurarse para supervisar la red de sensores (310) para los cambios en el voltaje a través de la red de sensores (310) que corresponden al número
 5 preseleccionado de sensores (318) estando en su estado seguro y presente en la red de sensores (310). Por supuesto, cualquier resistencia (315) asociada con la trayectoria de tierra del chasis puede explicarse en esta determinación por referencia a las siguientes ecuaciones:

$$10 \quad R_{\text{esperado}} = R_{\text{seguro}} + R_{\text{chasis}}$$

Donde:

R_{esperado} es la resistencia esperada y

R_{chasis} es la resistencia (315) de la trayectoria de
 15 tierra del chasis.

Y

$$V_{\text{esperado}} = I_{\text{controlador}} * R_{\text{esperado}}$$

Donde:

V_{esperado} es el voltaje esperado e

$I_{\text{controlador}}$ es la corriente suministrada por el
 20 controlador.

Por lo tanto, el voltaje detectado por el comparador (334) aumenta en alrededor de la cantidad asociada con una abertura de los interruptores (320) (o un sensor (318) que
 25 se retira de la red de sensores (310)), el controlador

(330) puede generar una señal indicativa de manipulación potencial con el sistema de combustible (200). Por supuesto, el punto fijo del comparador (334) puede ajustarse para tener en cuenta las tolerancias asociadas con los parámetros anteriores. Tenga en cuenta que si la resistencia del chasis (315) es baja, ese cambio de voltaje correspondería a un aumento de la resistencia de la red de sensores de:

$$\begin{aligned} \Delta R_{\text{manipulación}} &= R_{\text{esperado}} - t / R_{\text{seguro}}; \\ \Delta V_{\text{manipulación}} &\geq I_{\text{controlador}} * \Delta R_{\text{manipulación}}; \text{ o} \\ V_{\text{manipulación}} &= V_{\text{esperado}} + \Delta V_{\text{manipulación}} \end{aligned}$$

Donde t es el número de sensores abiertos/faltantes

Ya que puede haber situaciones en las que los usuarios puedan querer instalar más sensores (318) del número para el cual un controlador particular (330) está configurado, el punto fijo del comparador (334) puede ajustarse hacia abajo por una cantidad correspondiente a la adición de sensores adicionales (318) (y sus conductancias adicionales en toda la red de sensores paralelos (310)). Por supuesto, un controlador adicional (330) podría añadirse al sistema antirrobo (300) para proporcionar capacidad para los sensores adicionales (318). Si los usuarios desean usar menos que el número de sensores

preseleccionado (318), entonces los usuarios pueden colocar un número correspondiente (y valor) de resistencias (324) a través de las entradas al controlador (330) para emular los sensores desinstalados (318). Esas resistencias (324), por otra parte, podrían estar en la misma (u otra) ubicación segura como el mismo controlador (330). En otras modalidades, las resistencias (324) podrían suministrarse por medio de interruptores DIP (en línea dual) o dispositivos similares en o asociados con el controlador (330). En la alternativa, o además, los sensores no utilizados (318) podrían conectarse al controlador (330) y sujetarse de manera que los interruptores normalmente abiertos (320) permanezcan cerrados.

En algunas modalidades, el controlador (330) está configurado para trabajar en conjunto con 10 (diez) sensores (318). Por otra parte, en la modalidad actual, cada sensor (318) tiene una resistencia de aproximadamente 10 k-ohm. Así, la red de sensores (310) tiene una resistencia eléctricamente equivalente de 1 k-ohm. La Tabla 1, a continuación, enlista las resistencias eléctricamente equivalentes para las redes de sensores (310) teniendo varios números preseleccionados de sensores (318) y enlista las resistencias eléctricamente equivalentes para las redes de sensores (310) (de la modalidad actual) con diferentes números de interruptores abiertos (320).

TABLA 1

	No. de sensores	No. de sensores abiertos	Resistencia (k-ohm)
	1	9	10
	2	8	5
5	3	7	3.33
	4	6	2.5
	5	5	2
	6	4	1.67
	7	3	1.43
10	8	2	1.25
	9	1	1.11
	10	0	1

Por lo tanto, si un usuario intenta manipular el sistema de combustible (200), el controlador (330) lo

15 detectaría. Por ejemplo, el retirar uno de los sensores (318) (ya sea físicamente o electrónicamente) de la red de sensores/sistema antirrobo (201) provocaría que la trayectoria eléctrica correspondiente se abriera incrementando así el voltaje más allá del punto fijo del

20 comparador (334). El desajustar un sensor (318) abriría el interruptor (320) llevando al mismo resultado. Intentar primero (antes de manipular de otra manera con un sistema de combustible) colocar una resistencia de la misma resistencia que la resistencia del sensor (322) daría lugar

25 a una disminución en el voltaje que podría causar que el

comparador (334) (si está configurado para detectar voltajes fuera de una banda) para detectar un intento de manipulación con el sistema de combustible (200) también (aunque sea temporalmente). Y los comparadores (334) de algunas modalidades podrían configurarse para enganchar la señal de salida en dichos casos.

Con una referencia constante a la Fig. 3, la señal de salida por el comparador (334) puede servir para varios propósitos. Para un efecto tal, podría causar que un indicador local (340) señale una manipulación potencial. Por supuesto, algunas modalidades no proporcionan un indicador local (340) o lo proporcionan en una ubicación no accesible para los usuarios normales del vehículo (por ejemplo, el conductor). El indicador local (340) podría estar escondido en un compartimiento cerrado o podría proporcionarse dentro del alojamiento del controlador (330) y, así, estar disponible sólo para los técnicos de servicio y/u otros con las autoridad/herramientas adecuadas para abrir el controlador (330). La señal del comparador también podría comunicarse a la unidad de geoposicionamiento (332).

La unidad de geoposicionamiento (332) podría configurarse para realizar una variedad de actividades. Por ejemplo, podría (en respuesta a la señal del comparador (334)) marcar el tiempo y/o ubicación de las ocurrencias de la señal. Además, la unidad de geoposicionamiento (332)

podría transmitir dicha información al centro de alerta remoto (306) mediante algún sistema de telecomunicaciones. Adicionalmente, o en la alternativa, la unidad de geoposicionamiento (332) podría rastrear la ubicación, 5 velocidad, movimiento, falta de movimiento, etc. del vehículo y transmitir dicha información al centro de alerta remoto (306). Así, el sistema antirrobo (300) de las modalidades puede alertar a los usuarios (tales como propietarios) de manipulación potencial con los sistemas de 10 combustible (200) de diferentes vehículos.

La Fig. 4 ilustra un controlador antirrobo de combustible. El controlador (400) de la modalidad actual incluye un alojamiento resistente a manipulaciones (402) y un número de conectores (404) cableados al controlador 15 (400). El alojamiento resiste a manipulaciones (402) puede ser cualquier tipo de alojamiento suficiente para prevenir que el usuario entre físicamente al alojamiento o al menos suficientemente fuerte que la mayoría de los intentos significativos para hacerlo dejaría marcas de palanca, 20 abolladuras, raspaduras, etc. en el alojamiento. Así, los intentos para entrar al controlador (400) (y/o alterar sus componentes internos tales como el comparador (334)) podrían ser fácilmente evidentes en la inspección del alojamiento. Los conectores (404) también pueden contribuir 25 a la seguridad del sistema antirrobo (300). Por ejemplo,

interno al alojamiento resistente a manipulaciones (402), pueden terminar en conexiones soldadas, soldadas con soldadura fuerte, etc. a un PCB (tablero de circuito impreso) o de lo contrario ser asegurado contra un retiro no detectable del controlador (400).

Por otra parte, en algunas modalidades, los conectores (404) corresponden en número a la cantidad preseleccionada de sensores (318). Por ejemplo, en las modalidades en las que cada sensor (318) se comunica con el controlador (400) mediante un conector positivo y conector de retorno (tierra), el controlador (400) tendrá conectores $2n$ (donde "n" es el número preseleccionado de sensores (318)). Sin embargo, podría ser el caso que uno o más sensores (318) utilizarán la tierra del chasis como una trayectoria de retorno. En dichas situaciones, por consiguiente el número de conductores (404) será reducido y el conjunto asociado de sensores (318) será seleccionado con un número de conectores de retorno apropiados para los controladores configurados de esa manera.

Adicionalmente, o en alternativa, el controlador (400) incluye el indicador local (408). Ese indicador local (408) puede ser cualquier indicador que puede indicar que se ha detectado un evento de manipulación (y/o está en curso ya sea que esté enganchado o no). Por ejemplo, el indicador local (408) puede ser una luz, LED (diodo emisor

de luz), contador, vínculo/fusión soplable, etc. si el controlador (400) está en un lugar seguro (por ejemplo, "enterrado" en un tablero) y luego el indicador local (408) será correspondientemente inaccesible para la mayoría de los usuarios tal como el conductor del vehículo. Por supuesto, el indicador local (408) puede ser reemplazado/aumentados con una chaqueta, conector, etc. lo que permite una conexión del controlador (400) al indicador de un evento externo.

La Fig. 5 ilustra un sensor de abrazadera antirrobo de combustible. El sensor de abrazadera (500) de la modalidad actual comprende un abrazadera de tubería (332), una abrazadera de banda (502), brida plástica de cierre, etc. capaz de asegurar el sensor (500) a un componente del sistema de combustible tal como los que se ilustra en la Fig. 2. La abrazadera (502) puede también, cuando se sujeta, ejercer suficiente fuerza en el interruptor (504) para cerrarla (particularmente si el interruptor (504) es un interruptor normalmente abierto). El interruptor (504) puede ser un interruptor normalmente abierto y puede colocarse en relación con la abrazadera (502) de manera que la abrazadera (502) puede sujetarlo entre la abrazadera y el componente al que está sujeto el sensor (500). En la alternativa, o además, la mayor parte del interruptor (504) puede ubicarse en el exterior de la abrazadera (502) con el

interruptor eléctrico/mecánico real y/o un actuador acoplado operativamente al mismo colocado dentro de la abrazadera (y ser afianzado con abrazadera en la posición eléctricamente "cerrada"). Observe también que el sensor

5 también podría alojar una resistencia para ajustar la resistencia (322) del sensor (500) a un valor deseado si lo desea. Por supuesto, el interruptor (504) (y la resistencia en el mismo) puede cablearse al conector (506) que puede incluir los conductores de ambas trayectorias positivos y

10 retorno a tierra asociados con el sensor (500). Por ejemplo, el conector (506) de las modalidades puede ser un conector tipo modelo no. 45-4610 de *LKG industries, Inc* ubicada en 3860 Publishers Dr, Rockford, IL 61109. Ya que el sensor (500) de la modalidad actual tiene un conector

15 (506), puede utilizarse para supervisar puntos de entrada que están sujetos a relativamente aberturas frecuentes y legítimas. Por ejemplo, podrían utilizarse sensores (500) con conectores en las tapas de combustible (210). Tenga en cuenta que en escenarios que involucran dichos puntos de

20 entrada, el sistema antirrobo (300) todavía puede configurarse para hacer sonar una alarma cuando se desconecta el conector (506) (y se abre la correspondiente ruta conductora). Sin embargo, el centro de alerta remoto (306) puede configurarse para, sobre una alerta, la unidad

25 de geoposicionamiento (332) para la consulta de la

ubicación del vehículo. Si sucede que el vehículo está ubicado en un depósito de combustible, gas, estación, etc. esa ubicación se puede señalar y considerar en cómo se maneja la alerta.

5 La Fig. 6 ilustra un sensor antirrobo de combustible estacionario. El sensor (600) de la modalidad actual incluye una abrazadera (602), un paquete de sensores (604) y un conector (606) (o conectores). Los conectores (606) están configurados para ser permanentemente, acoplados de
10 forma mecánica (y en permanente comunicación eléctrica) con una red de sensores (308). En algunos casos, ese acoplamiento puede ser mediante soldadura, soldadura fuerte, etc. Así, el sensor (600) de la modalidad actual puede utilizarse para supervisar los puntos de entrada que,
15 ordinariamente, experimentaría sólo aperturas ocasionales. En otras palabras, son estacionarios. Por ejemplo, la mayoría de acoplamientos (222) y/u otros componentes (exceptuando la tapa del combustible (210) para la mayoría de los vehículos) se abriría sólo si el vehículo es
20 sometido a mantenimiento. Otra vez, consultando la unidad de geoposicionamiento (334), checando las órdenes/registros de mantenimiento, etc. el centro de alerta remoto (306) puede determinar si el vehículo se encuentra en un depósito de mantenimiento adecuado. La información así obtenida

puede utilizarse en la evaluación de alertas provenientes del sensor (600) de la modalidad actual.

La Fig. 7 ilustra un sensor antirrobo de combustible instalado en una tapa de combustible. El sensor (700) de la
5 modalidad actual comprende un abrazadera (702), un paquete de sensores (704), un conector (706) y una conexión a tierra (708). La conexión a tierra (708) puede utilizarse para conectar a tierra el sensor (700) al chasis del vehículo. Haciendo eso aseguras que el sensor (700) tenga
10 una trayectoria de retorno de tierra a la red de sensores (308) a pesar de la posibilidad de que el material no conductor podría interponerse entre el sensor (700) y la tierra del chasis. Por ejemplo, los OEMs (y fabricantes de repuestos) a menudo hacen tapas de combustible (210) de
15 plástico y/u otros materiales no conductores. Por otra parte, incluso dichos componentes del sistema de combustible (200) deberían de hacerse de materiales conductores, grasa, suciedad, mugre, etc. puede que exista uno o más componentes que los hace no conductores. Por otra
20 parte, algunos componentes pueden ser recubiertos en pintura, cera, imprimante, etc. haciendo dichos componentes no conductores. Por supuesto, los componentes subyacentes podrían ser afianzado con abrazadera, despojado, etc. para aumentar su conductancia en circunstancias apropiadas.
25 Tenga en cuenta que la conexión a tierra (708) podría

comprender un alambre de cobre, trozo de papel de aluminio, etc., sin apartarse de la divulgación actual.

La Fig. 8 ilustra un sensor antirrobo de combustible instalado en un filtro de combustible. Mientras tanto, la
5 Fig. 9 ilustra un sensor antirrobo de combustible instalado en una línea de succión de combustible y la Fig. 10 ilustra un sensor antirrobo de combustible instalado en una línea de retorno de combustible. Así, las Figs. 8-10 ilustran que los sensores (800), (900) y (1000) de las modalidades se
10 pueden instalar en muchas ubicaciones a través de los sistemas de combustible (200) para muchos diferentes tipos de vehículos.

La Fig. 11 ilustra una interfaz gráfica de usuario (GUI) de un sistema antirrobo de combustible. Más
15 particularmente, la Fig. 11 muestra el GUI (1100), y un mapa (1102), una ruta (1104), un destino (1105), un desvío (1106), controles de calendarios (1108), controles de mapa (1110), marcadores de ruta (1112), precauciones de ruta (1114), advertencias de ruta (1116), una pestaña de inicio
20 (1118), una pestaña de mapas (1120), una pestaña de informes (1122) y una pestaña administrativa (1124). El GUI (1100) y la aplicación de *software* subyacente, programa, etc. se puede alojar por centros de alerta remotos (306), servidores, computadoras, dispositivos móviles (por
25 ejemplo, teléfonos celulares, computadoras portátiles,

tabletas, pequeña computadora portátil, etc.) entre otros. El GUI (1100) de la modalidad actual permite al usuario supervisar, explorar, investigar, etc. las actividades que podrían estar relacionadas al robo de combustible vehicular.

Más específicamente, el GUI (1100) ilustrado en la Fig. 11 muestra un mapa (1102) en el que aparece la ruta (1104) del vehículo seleccionado por el usuario. Esa ruta (1104) incluye uno o más destinos (1105) tales como una tienda local, negocio, fábrica, etc. y, como se muestra, un desvío (1106). Por otra parte, la ruta real (1104) (incluyendo el desvío (1106)) puede hacerse en base a los datos de geoposicionamiento por el circuito de geoposicionamiento (334) y/o preguntado a partir del mismo. También tenga en cuenta que las rutas de entrega programadas podrían mostrarse en el GUI (1100). Por supuesto, el desvío (1106) podría ser legítimo como que el conductor actuó para evitar la congestión, construcción, inundaciones, etc. Por otra parte, ese desvío (1106) podría indicar una ubicación en la que el conductor manipuló, está manipulando, y/o está por manipular el sistema de combustible (200).

La Fig. 11 también muestra que el GUI (1100) puede mostrar diferentes marcadores de la ruta (1112), precauciones de la ruta (1114) y/o advertencias de la ruta

(1116). Los marcadores de la ruta (1112) se pueden mostrar correspondientes a las ubicaciones en las que el vehículo procede a (o por encima) de la velocidad seleccionada por el usuario tal como el límite de la velocidad local. Por el contrario, las precauciones de la ruta (1114) pueden mostrarse para ubicaciones en las que el vehículo ha disminuido por debajo de la velocidad seleccionada por el usuario. Dicho comportamiento puede ser indicativo de tráfico/dificultades relacionadas con el camino y/o manipulación inminente del sistema de combustible. La GUI (1100) también muestra varias advertencias de la ruta (1116) que corresponden a lugares en que el vehículo ha disminuido por debajo de cierta velocidad seleccionada por el usuario y/o parado. Tal comportamiento puede ser indicativo de alteración de sistema de combustible inminente o en curso y/o el robo de combustible. Tenga en cuenta que las velocidades del vehículo, ubicación, etc. se pueden obtener remotamente consultando el sistema antirrobo de combustible (300) de las modalidades y/u otros sistemas a bordo. Así, los usuarios tales como propietarios pueden examinar el mapa (1102) para determinar dónde/cuándo puede estar ocurriendo el robo de combustible y/o patrones relacionados con lo mismo.

Por supuesto, la GUI (1100) tiene otras características también. Por ejemplo, los controles de

calendarios (1108) permiten que un usuario vea la fecha/hora actual. En algunas modalidades, los controles de calendario (1108) permiten a los usuarios seleccionar fechas/horas para que la GUI (1100) pueda mostrar los mapas (1102) correspondientes, rutas (1104), marcadores de la ruta (1112), precauciones de la ruta (1114), advertencias de la ruta (1116), etc. Por otra parte, la GUI (1100) puede incluir controles del mapa (1110) para acercar en/fuera de los mapas (1102), navegar en los mapas (1102), guardar los mapas (1102), imprimir los mapas (1102), etc.

Las GUIs (1100) de las modalidades también incluyen controles tales como la pestaña de inicio (1118), la pestaña de los mapas (1120), la pestaña de informes (1122), la pestaña administrativa (1124), etc. Estas pestañas (1118), (1120), (1122) y/o (1124) permiten a los usuarios navegar entre las diferentes y correspondientes porciones de la GUI (1100). Por ejemplo, la pestaña de los mapas (1120) puede permitir a los usuarios navegar entre diferentes mapas (1102) considerando que la pestaña de informes (1122) puede proporcionar una funcionalidad correspondiente para varios informes. La pestaña administrativa (1124) puede permitir a los usuarios manejar ciertas actividades administrativas tales como el mantenimiento del perfil de usuario, mantenimiento del perfil del vehículo, mantenimiento del perfil de conductor,

etc. La ficha de inicio (1118) puede proporcionar controles de navegación de la GUI general tales como los relacionados con inicio de sesión, cierre de sesión, cambio de usuarios, etc.

5 La Fig. 12 ilustra un diagrama de flujo de un método para detectar el robo de combustible. El método (1200) comprende diferentes actividades tales como seleccionar uno o más vehículos en los cuales instalar sistemas antirrobo (300). Estos vehículos podrían ser los implicados en robo
10 de combustible y/u otras actividades sospechosas, un grupo de vehículos que por alguna razón podrían ser particularmente susceptibles a tales actividades, los vehículos impulsados por algunos usuarios, etc. Ver referencia (1202).

15 El método (1200) también puede comprender instalar los diferentes sensores en uno o más de los vehículos seleccionados. Así, los sensores se pueden fijar en la tapa de combustible (210), el consumo de combustible (211), el tanque de combustible (202), la bomba de combustible (204)
20 y/o (212), el filtro de combustible (206), el regulador de presión de combustible (218), varias líneas de combustible tal como combustible de línea de retorno (220) y/o varios acoplamientos (222) en los sistemas de combustible (200) de esos vehículos. Si el número de sensores instalados (318)
25 no es igual a la cantidad de sensores (318)

preseleccionados para un determinado controlador (330), entonces el sistema antirrobo (300) puede configurarse en consecuencia. Por ejemplo, si el sistema antirrobo (300) tiene demasiados sensores (318) para el controlador
5 seleccionado (330), entonces un número adecuado de controladores (330) puede añadirse al sistema antirrobo (300). Si, además, o sin embargo se han instalado muy pocos sensores (318) para el número preseleccionado de sensores asociados con el número de controladores (330) en el
10 sistema antirrobo (300), luego varias resistencias (324) se pueden conectar a través de una o más de las entradas del controlador (330). Así, los controladores (330) pueden conectarse a redes de sensores (310) que tienen resistencias/conductancias generales correspondientes al
15 número preseleccionado de sensores (318). Ver referencia (1204).

Por supuesto, si no se han instalado los controladores (330), entonces pueden ser instalados en el vehículo. Por ejemplo, el controlador (330) puede montarse
20 en el tablero o de otra manera instalarse en algunas ubicaciones relativamente inaccesibles en el vehículo como se indica en la referencia (1206). Si una unidad de geoposicionamiento separada se va a incluir en el sistema antirrobo (300), entonces se puede instalar en/sobre el
25 vehículo y/o conectado al controlador. Ver referencia

(1208). Por otra parte, los diversos conductos (240) se pueden ejecutar a través del vehículo desde la ubicación del sensor (318) al controlador (330). Los alambres, cables, (224), (226) y (228), conexiones a tierra, etc. asociados con los sensores entonces pueden ejecutarse a través de los conductos (240) y/o ejecutarlos por separado. Si lo desea, los conductos, cables, sensores, etc. puede ser disfrazados para parecer como si se han ubicado en el vehículo para todos o una parte de la vida del vehículo. Por ejemplo, suciedad, grasa, mugre, etc. pueden aplicarse a ellos. Ver referencia (1209).

La referencia (1210) de la Fig. 12 ilustra que el vehículo puede ser conducido en algún momento. Por ejemplo, un conductor determinado se podría alertar de la presencia del sistema antirrobo (300) considerando que algunos otros conductores pueden permanecer inconscientes de su presencia. Una manera u otra, mientras se conducen los vehículos, los datos generados por el sistema antirrobo (300) (y/u otros sistemas a bordo) pueden ser reunidos y/o supervisados como se indica en las referencias (1212) y (1214). Si los datos indican que un evento de manipulación podría estar en marcha entonces se pueden enviar/transmitir al centro de alerta remota las advertencias/precauciones de ruta apropiadas. Si los datos sugieren que la manipulación

podría no ocurrir entonces puede continuar la supervisión de los datos. Ver referencia (1216) y (1218).

Continuando con la referencia a las Fig. 12, en escenarios que conllevan una potencial manipulación (y/o de lo contrario), los usuarios tales como los propietarios de vehículos pueden investigar las actividades relacionadas con el vehículo. Ver referencia (1220). Por supuesto, pueden tomar las acciones apropiadas tales como colocar varios conductores, vehículos, etc. bajo vigilancia. El método (1200) se puede repetir en su totalidad o en parte como se indica en la referencia (1222).

La Fig. 13 ilustra una computadora para uso en sistemas antirrobo de combustible. De hecho, la computadora (1306) puede albergar una aplicación (1330) para presentar la GUI (1100) (y el procesamiento de los datos asociados) en el centro de alerta remoto. En algunos casos, el controlador (330) podría incluir algunos o todos los componentes de la computadora (1306) aunque el controlador (330) podría ser implementado en un *hardware* analógico, *firmware*, ASICs (circuitos integrados para aplicaciones específicas), RISC (conjunto de circuitos integrados de instrucciones reducidas), etc.

En este momento unas palabras podrían estar en orden sobre las computadoras (1306) y/u otros sistemas, aparatos, etc., utilizados para diseñar, almacenar, albergar,

recordar, mostrar, transmitir, recibir, etc. programas, aplicaciones, controladores, algoritmos, rutinas, códigos, GUIs, etc. de los sistemas antirrobo de combustible de las modalidades. El tipo de computadora (1306) utilizada para
5 tales propósitos no limita el alcance de la divulgación pero ciertamente incluye los ya conocidos así como de los que surgirán en el futuro. Pero generalmente, estas computadoras (1306) incluirán algún tipo de pantalla (1308), teclado (1310), interfaz (1312), procesador (1314),
10 memoria (1316) y la vía de transmisión (1318).

De hecho, cualquier tipo de interfaz máquina-humano (como se ilustra por la pantalla (1308) y el teclado (1310)) lo hará siempre y cuando permita que algunas o todas de las interacciones humanas con la computadora
15 (1306) como se divulgó en otras partes en el presente. Del mismo modo, la interfaz (1312) puede ser una tarjeta de interfaz de red (NIC), un transmisor WiFi, una interfaz de Eternet, etc. permitiendo que diversos componentes de la computadora (1306) se comuniquen entre sí y/o los otros
20 dispositivos. La computadora (1306), sin embargo, puede ser un dispositivo autónomo sin apartarse del alcance divulgación actual.

Por otra parte, mientras que la Fig. 13 ilustra que la computadora (1306) incluye un procesador (1314), la
25 computadora (1306) podría incluir algún otro tipo de

dispositivo para realizar los métodos divulgados en el presente. Por ejemplo, la computadora (1306) podría incluir un microprocesador, un ASIC (circuito integrado de aplicación específica), un RISC (conjunto de circuitos integrados de instrucciones reducidas), una red neuronal, etc. en vez de, o además, del procesador (1314). Así, el dispositivo utilizado para realizar los métodos divulgados en el presente no está limitando.

De nuevo con referencia a la Fig. 13, la memoria (1316) puede ser cualquier tipo de memoria actualmente disponible o que podría surgir en el futuro. Por ejemplo, la memoria (1316) podría ser un disco duro, una ROM (memoria de sólo lectura), un RAM (memoria de acceso aleatorio), memoria flash, un disco compacto (CD), etc. o una combinación de los mismos. No importa su forma, en la modalidad actual, la memoria (1316) almacena instrucciones que permite al procesador (1314) (u otro dispositivo) realizar por lo menos algunos de los métodos divulgados en el presente así como (quizás) de otros. La memoria (1316) de la modalidad actual también almacena datos relativos a tales métodos, entradas de usuario a los mismos, salidas de los mismos, etc. Al menos algunos de los distintos componentes de la computadora (1306) puede comunicarse sobre cualquier tipo de vía de transmisión (1318) permitiendo sus operaciones en algunos o todos los métodos

divulgados en el presente. Dichas vías de transmisión incluyen, sin limitación, SCSI (interfaz de sistema de computadora pequeña), ISA (arquitectura estándar industrial), EISA (Arquitectura estándar industrial extendida), etc., vías de transmisión o una combinación de los mismos. Con eso dicho, podría ser útil examinar ahora algunos aspectos de la materia divulgada.

La Fig. 14 ilustra esquemáticamente un sistema antirrobo de combustible. Más específicamente, la Fig. 14 ilustra un sistema antirrobo de combustible (1400), una unidad de control (1402), sensores de línea (1418), un sensor de identificación (1420), un sensor de identificación (1422), un microcontrolador (1430), chaquetas (1432), una resistencia de actuación (1434), un rastreador GPS (1436) y una aplicación GPS (1438). El sistema antirrobo de combustible (1400) de la modalidad actual puede utilizarse donde pueden aparecer ciertas actividades rutinarias para ser eventos de robo de tal modo desencadenar falsas alarmas. Por ejemplo, las tapas de combustible y filtros de combustible son más habitualmente abierto/reemplazado que otros componentes en los sistemas de combustible normales.

Las activaciones de los sensores de identificación de la tapa de combustible y el filtro de combustible (1420) y (1422) son típicamente más rutinario que la activación de

otros sensores como los sensores de línea (1418). Así, los usuarios podrían querer responder a la activación de los sensores de identificación (1420) y/o (1422) de manera diferente a la activación de los sensores de línea (1402) (y/o incluso entre sí).

El sistema antirrobo de combustible (1400) que se muestra en la Fig. 14 produce cambios de resistencia diferentes, identificables como detectada en la entrada a la unidad de control (1802). Los valores de resistencia utilizados para el sensor de identificación de la tapa de combustible (1420) (5.1 kohm) y el sensor de identificación del filtro de combustible (1422) (3.3 kohm) son diferentes entre sí y los sensores de línea (1402) (10 kohm) en el sistema antirrobo de combustible (1400). La unidad de control (1402) de la modalidad actual detecta un cambio de valor de resistencia único para cada tipo de sensor y tomar una acción apropiada para notificar a los usuarios de la activación.

Tenga en cuenta que estos cambios de resistencia diferentes pueden ser determinados con referencia a las siguientes ecuaciones y/o Tabla 2. Tengase en cuenta también que mientras los valores anteriores de resistencia fueron seleccionados para ser lo suficientemente diferentes como para producir cambios de resistencia de red fácilmente

discernible, podrían utilizarse otros valores de resistencia.

$$1/R_{\text{seguro}} = 1/R_{\text{tapadecombustible}} + 1/R_{\text{filtrodecombustible}} + n \cdot 1/R_{\text{sensordelíneadecombustible}}$$

Donde:

5 R_{seguro} es la resistencia esperada, general de la red de sensores,

$R_{\text{filtrodecombustible}}$ es la resistencia del sensor de filtro de combustible (3.3 Kohm)

10 $R_{\text{tapadecombustible}}$ es la resistencia del sensor de la tapa de combustible (5.1 Kohm)

$R_{\text{sensordelíneadecombustible}}$ es la resistencia de sensor de línea (10 Kohm)

n es el número preseleccionado (generalmente 8 sensores)

15

20

25

TABLA 1

	<u>Sensores desconectados</u>	<u>Resistencia de la red (k-ohm)</u>
	Ninguno	0.77
	Tapa de combustible	0.9
5	Filtro de combustible	1.004
	1 Línea de combustible	0.83
	2 Líneas de combustible	0.91
	3 Líneas de combustible	1
	4 Líneas de combustible	1.11
10	5 Líneas de combustible	1.25
	6 Líneas de combustible	1.43
	7 Líneas de combustible	1.67
	8 Líneas de combustible	2

15 La Fig. 14 también ilustra que el microcontrolador (1430) (y/o unidad de control

 (1802)) podría incluir chaquetas (1432) para la conveniente conexión/desconexión de los distintos alambres, cables, etc. en el sistema para estos dispositivos. En la
20 alternativa, o además, uno o más de estos cables podrían ser cableados a la unidad de control (1402) y/o microcontrolador (1430).

 Más aún, la Fig. 14 ilustra también que la unidad de control (1402) puede pasar una señal al rastreador GPS
25 (1436)/aplicación GPS (1438) indicativo de si el sistema de

combustible parece ser seguro, potencialmente manipulado, o en alguna condición de rutina. La aplicación GPS (1438) puede configurarse para registrar la ubicación del sistema de combustible (o vehículo) cuando es señal cambia y/o

5 manda un mensaje correspondiente a diferentes usuarios sobre dichos cambios. Si lo desea, la aplicación GPS (1438) puede configurarse para enviar una señal más o menos continua de manera que el estado detectado del sistema sea conocido en todo momento. Además, la aplicación GPS se

10 puede configurar con una interfaz de usuario (por ejemplo, una interfaz gráfica de usuario) que permite a los usuarios crear sus propias reglas para responder a las alertas. Por ejemplo, un usuario puede configurar la aplicación GPS para desactivar automáticamente el circuito de encendido del

15 vehículo si una alerta indica que puede ocurrir un robo de combustible (o ha ocurrido).

La Fig. 15 ilustra una unidad de control antirrobo de combustible. La unidad de control antirrobo de combustible (1502) de la modalidad actual incluye una serie de

20 chaquetas (1532) para conectar los sensores de la red a la misma. También incluye varios indicadores (1518), (1520) y (1522) correspondientes a los sensores en línea (1518) y sensores de identificación (1520) y (1522). La unidad de control (1502) también puede incluir un indicador (1524)

25 configurado para activarse si más de un sensor se activa.

Las Figs. 16 y 17 ilustran un sensor de línea de combustible. El sensor de línea de combustible (1600) de la modalidad actual puede instalarse alrededor accesorios de compresión (u otros componentes) en líneas de combustible de vehículo. En caso de que el sensor de línea de combustible (1600) es desinstalado para permitir el acceso al accesorio (o de otra manera la manipulación), la conexión eléctrica interna a la tierra del vehículo se romperá (o destruirá), y el microcontrolador de la modalidad actual detectará el cambio de estado y enviará una alerta.

Además, la Fig. 16 ilustra que el sensor de línea de combustible (1600) puede asegurarse a varios componentes a través de una brida para cable de doble correa (1602) (o bridas, bridas plásticas, cierres plásticos, etc.). La Fig. 16 muestra que el sensor de línea de combustible (1600) también incluye un contenedor de circuito (1604) y un conector de cable de señal (1606) y define un orificio de alambre de señal (1608).

Mientras la Fig. 16 ilustra el sensor de línea de combustible (1600) en una condición desinstalada, la Fig. 17 ilustra cómo se instala una tuerca de ajuste de compresión (1710) y con un alambre de señal (1712) conectado al mismo por medio de un orificio de alambre de señal (1608)/ conector de alambre de señal (1606). Tenga en

cuenta que la brida de cable de doble correa (1602) ha sido apretado jalando contra la tuerca de ajuste de compresión. (1710).

La Fig. 18 ilustra un sensor de la tapa de combustible. El sensor (de identificación) de la tapa de combustible (1800) de la modalidad actual se puede instalar en diferentes tapas de combustible. El sensor de la tapa de combustible (1800) puede asegurarse a la tapa de combustible (1802) mediante un adhesivo mientras que el contenedor del circuito (1804) puede asegurarse al tanque de combustible (1806) por un adhesivo también. En caso de que el sensor de la tapa de combustible esté desconectado (1800) para permitir el acceso al tanque de combustible (1806), el circuito para ese sensor está roto y se envía una alerta. Cuando el sensor de la tapa de combustible (1800) está desinstalado (o quitado por la fuerza o de otra manera manipulado) destruye su conexión eléctrica con el suelo del vehículo. El microcontrolador de la modalidad actual detecta el cambio de estado y se envía una alerta.

Tenga en cuenta que la Fig. 18 ilustra también una tapa lateral del contenedor de circuitos (1808) y las dos mitades de una rápida desconexión (1810) del sensor de la tapa de combustible (1800). Además, el contenedor lateral del tanque o contenedor de circuito base (1804) define o incluye un punto de unión del alambre de señal (1812).

En algunas modalidades los sistemas antirrobo de carga/combustible incluyen sensores digitales que transmiten sus únicos código o identificaciones inalámbricamente para configurar de manera adecuada los controladores. Si el sensor detecta que se ha sido manipulado, retirado del sistema, etc., deja de transmitir su identificación. Por supuesto, el controlador de la modalidad actual revisa periódicamente la presencia de transmisiones recientes/contemporáneas de los identificadores asociados con sus sensores. Si uno o más parecen faltar dichos controladores podrían enviar una alerta (por ejemplo, encender una luz, timbre, altavoz, claxon, etc.), de alarma, enviar un mensaje al centro de control, enviar un correo electrónico a una persona en particular, dispositivo móvil o de informática, teléfono celular, etc. Los controladores podrían también, o como alternativa, registrar la ubicación, tiempo y (si se instrumentan de forma apropiada), las condiciones de registro en/cerca del vehículo incluyendo temperatura, presión atmosférica, humedad, etc.

Además, algunas modalidades proporcionan sistemas antirrobo de combustible/carga que se configuran para consumir poca energía. Estos sistemas, por lo tanto, pueden funcionar en varios vehículos por largos períodos de tiempo. Los sistemas de la modalidad actual pueden

configurarse para funcionar en voltajes bajos y/o con flujo de corriente limitado de manera que cumplen intrínsecamente requisitos de seguridad para varios lugares peligrosos como se define en dichos documentos como el Código Eléctrico Nacional de los Estados Unidos. En algunas modalidades, los sistemas antirrobo se proporcionan en un *software* como un servicio (SaaS) formado en el servidor de red y70 servidor de base de datos. Así, en algunas modalidades, no necesita existir una aplicación en el vehículo y/o en el campo.

10 Los controladores de diferentes modalidades restringen las señales que detectan desde diferentes sensores en comunicación con los mismos. Por ejemplo, puede ser deseable filtrar la señal de manera que el ruido en el circuito no parezca ser un caso potencial de manipulación.

15 Por ejemplo, se puede aplicar a la señal un filtro de serie de tiempo de 6 segundos antes de que los controladores de la modalidad actual detecten/respondan a la señal. De esta manera, las falsas alarmas puede ser reducidas si no eliminadas. Pero otros acondicionamientos de señal

20 más/menos complejos pueden aplicarse a la señal sin apartarse del alcance de la divulgación actual.

 Las modalidades proporcionan sistemas, sensores, controladores, etc. antirrobo de combustible que permiten supervisar los sistemas de combustible del vehículo para un

25 robo de combustible y/o manipulación potencial. Algunos

dichos sistemas permiten una supervisión del sistema de combustible discreto, invisible y potencialmente insospechado. En algunas modalidades, los sensores, controladores, sistemas, etc. son confiables, resistentes y relativamente baratos para instalar y/u operar. Los sistemas de algunas modalidades permiten a los usuarios investigar posibles eventos de robo de combustible de forma remota y para implementar acciones correctivas. Ahora haciendo referencia a las Figs. 19 a 25, podría ser útil divulgar aspectos de los sistemas de protección antirrobo de carga.

La Fig. 19 ilustra un sistema antirrobo de carga. En general, la Fig.19 muestra el sistema antirrobo de carga instalado en un vehículo de carga. Esto permite que un propietario u otro usuario interesado supervise el estatus de la carga de los vehículos incluso en ubicaciones remotas. Y si ocurre alguna manipulación aparente, el sistema alerta ese usuario del potencial de que alguien está intentando robar carga o de otra manera la esté manipulando. Más específicamente, la Fig. 19 ilustra un sistema (1900) un vehículo (1902), un compartimiento de carga (1904), una cabina (1906), un punto de acceso (1908), un controlador (1910), un circuito de geoposicionamiento (1912), por lo menos una cerradura (1914), un interruptor

de carga (1916) y sus mitades de interruptor (1918) y (1920).

Como al vehículo (1902), el vehículo particular (1902) ilustrado por la Fig. 19 es un camión de combustible. Sin embargo, podría ser un remolque, un semirremolque, un camión de "cubo", una furgoneta repartidora, un barco, un bote, un avión, etc. Sin embargo, incluyen o define un compartimiento de carga (1904) que a menudo tiene carga y frecuentemente limita la carga en el mismo. De hecho, el compartimiento de carga (1904) (o las estructuras que lo definen) a menudo protege la carga de los elementos, daños durante el envío, manipulación, robo y similares. Por ejemplo, en muchos camiones, furgonetas, etc. el compartimiento de carga (1904) se encuentra dentro de una serie de paredes/paneles del vehículo (1902) tales como pisos, cubiertas/techos, cascos, fuselajes, mamparos, etc.

Por otra parte, el vehículo (1902) a menudo comprende dos o más partes distintas tales como un tráiler (que podría definir el compartimiento de carga) y una cabina, tractor, puente, cabina del piloto, etc. En muchos escenarios, la cabina alberga un usuario que conduce, opera, navega, controla, etc. el vehículo (1902). Ese usuario tiene también con frecuencia tareas relativas al cargo de la carga sobre el vehículo (1902) (y/o la

descarga). Así, mientras que no sea siempre el caso, el usuario tiene acceso a todo el vehículo (1902) incluyendo el compartimiento de carga (1904), la cabina (1906) y/o la misma carga. Por supuesto, los terceros podrían también
5 intentar acceder al compartimiento de carga (1904), la carga en el mismo, y/o la cabina (1906) para quizás propósitos nefastos y/o maliciosos. Y, en parte, el compartimiento de carga (1904) está protegido a menudo con cerraduras en sus varios puntos de acceso (1908) para prevenir o al menos
10 obstaculizar tal acceso no autorizado.

Como se divulga además en otras partes en el presente, la cabina (1906) generalmente contiene controles y/o instrumentos para ayudar al usuario en la operación del vehículo. Y puede contener varios componentes del sistema
15 (1900) tal como el controlador (1910) y/o circuito de geoposicionamiento (1912). Por supuesto, uno o más de estos componentes pueden montarse en el techo de la cabina (1906) y/o el compartimiento de carga (1904) para, por ejemplo, proporcionar a su antena (si tiene una) acceso a señales
20 electromagnéticas que de lo contrario podría estar protegida por la estructura del vehículo (1902). Por supuesto la cabina (1906) se puede proteger del acceso no autorizado por cerraduras y similares así como para proteger estos componentes y otros objetos en la cabina
25 (1906). Tenga en cuenta que los componentes montados fuera

del compartimiento de carga, (1904) y la cabina (1906) pueden ser un poco escondidos siendo camuflados o colocados en lugares poco visibles. Por ejemplo, muchos vehículos (1902) son lo suficientemente altos para que un componente montado sobre el vehículo (1902) no pueda ser notado por el usuario y/o terceras personas que podrían ser conscientes de la presencia del sistema (1900).

El punto de acceso (1908) asume varias configuraciones y el que se muestra en la Fig. 19 es una caja de válvula para un camión de combustible. Esta caja de válvula contiene las válvulas que están en comunicación con el combustible en el camión (es decir, la carga) y los puertos de carga/descarga, acoplamientos, etc. En otros casos, el punto de acceso (1908) podría ser una puerta, escotilla, toberas, etc. Y, por supuesto, el punto de acceso (1908) generalmente refleja la naturaleza de la carga y/o el vehículo (1902) si la carga es sólida, líquida, gaseosa, paquetes, dinero, material granular, a granel, etc.

Continuando con la referencia a la Fig. 19, el controlador (1910) realiza ciertas funciones y/o se comunica con varios otros componentes del sistema (1900) para hacerlo. Por ejemplo, el controlador (1910) puede detectar la posición, estado y/o condición del interruptor de carga (1916) y de aquella información inferir o no un

intento de acceder al compartimento de carga (1904) podría estar en marcha. También puede enviar una señal indicativa de la posición del interruptor de carga (1916) al circuito de geoposicionamiento (1912). Además, puede almacenar un

5 PIN (número de identificación Personal) asociado con las aperturas y/o cierres del interruptor de carga (1904) y determinar si el interruptor de carga (1916) ha sido abierto/cerrado en un patrón correspondiente a ese PIN. Si

10 tiene, entonces el controlador (1910) puede enviar una señal al circuito de geoposicionamiento (1912) que una entrada autorizada (o acceso) en el compartimiento de carga (1904) está en marcha. Si el patrón falla en coincidir con el PIN, luego el controlador (1910) puede en consecuencia señalar el circuito de geoposicionamiento (1912). Por

15 ejemplo, si el PIN debe ser 3124, un usuario abriría y cerraría el interruptor de carga 3 veces tomando una cantidad preseleccionada de tiempo entre la apertura/cierre del interruptor, pausar durante otro tiempo preseleccionado (y quizás más), abrir/cerrar el interruptor una vez,

20 esperar, abrir/cerrar el interruptor dos veces, esperar, y abrir/cerrar el interruptor 4 veces más para ingresar ese PIN. En algunas modalidades, el controlador (1910) almacena (o recupera desde un centro de control remoto sobre la Internet u otro sistema de telecomunicación) una lista de

25 PINs y, cada vez que se utiliza uno, éste elimina el PIN

utilizado. Después carga otro PIN de la lista para que el siguiente PIN esté activo/correcto. De esta manera, los usuarios pueden señalar el sistema (1900) que tienen autoridad para acceder al compartimiento de carga (1904) una vez (o un número predeterminado de veces) sin que se dispare una alarma (pero tal vez haciendo la transmisión de una señal de acceso autorizado).

En la alternativa, o además, los PINs pueden ser basados en el tiempo. En otras palabras, cada dígito del pin puede indicar que tanto el usuario debe mantener el interruptor de carga (1916) en las posiciones abierto/empalmado y cerrado/desempalmado. Por ejemplo, supongamos que el PIN es 315. Para indicar al controlador que un acceso a la carga autorizada es inminente, el usuario abriría el interruptor, después lo cierra durante 3 segundos. El usuario después cerraría el interruptor durante un (1) segundo y lo cerraría durante 5 segundos. Después del final del período de 5 segundos el usuario abriría el interruptor y accedería a la carga sin establecer una alarma. Aunque el controlador (1910) pudo registrar el evento y enviar una señal indicativa lo mismo.

El controlador (1910) también puede controlar las cerraduras (1914) por medio de comunicaciones codificadas si se desea. De hecho, si aparece una entrada autorizada en marcha (detectado por medio de un PIN por ejemplo) el

controlador (1910) puede enviar una señal para abrir la cerradura (1914). La cerradura se instala normalmente por dentro de la bahía de carga haciéndola inaccesible desde el exterior y por lo tanto haciendo difícil la manipulación.

5 Por supuesto, el controlador también puede bloquear la cerradura (1914) en otros escenarios. Por ejemplo, el defecto, pérdida de energía, y/o estado seguro en falla de la señal y/o bloqueo podría ser en el estado bloqueado. En algunas modalidades, el controlador (1910) también podría

10 recibir una señal anulada para desbloquear la cerradura de un centro de control remoto (y quizá sobre un sistema de telecomunicaciones). Además, el controlador (1910) de las modalidades puede recibir del circuito de geoposicionamiento (1912) una señal que indica si el

15 sistema (1900) está en una geozona en donde la entrada puede considerarse ya sea autorizado o no autorizado. Así, el sistema (1900) puede establecer, mantener, detectar, etc. si el vehículo (1902) está en una ubicación donde se autoriza el acceso al compartimento de carga (1904). Esas

20 ubicaciones pueden corresponder a destinos esperados/programados para el vehículo y/o carga. Otra vez, si se intentó un acceso en una ubicación que no sea una geoubicación autorizada después el controlador (1910) puede enviar una alarma. En esta forma, y/o en otros, el sistema

(1900) puede crear "Geocercas" alrededor de las áreas de acceso legítimo.

Por supuesto, podría suceder que se pudiera realizar un intento de acceder de manera legítima pero no autorizada al compartimento de carga (1904). Por ejemplo, el vehículo (1902) podría detenerse por la policía tal como la patrulla de caminos, policía, un servicio de inmigración, una agencia de control de bebidas alcohólicas, una agencia de armas de fuego, un funcionario de aduanas, etc. En cuyo caso, se le podría pedir al operador que abra el compartimento de carga (1904) para inspección y/o búsqueda. En tales casos el operador puede obtener un PIN del centro de control (o tener uno memorizado o de lo contrario disponible) y obtener la autorización de esa o en una manera similar. Asimismo, el mantenimiento no programado puede provocar que el operador legítimamente necesite tener acceso al compartimento de carga y el PIN puede permitir eso. Y, por supuesto, muchas otras situaciones pueden surgir donde dicho acceso es necesario de forma legítimo. En tales casos el controlador (1910) puede todavía informar que ese acceso se produjo para seguimiento posterior por los usuarios interesados.

Además, el controlador (1910) puede estar en comunicación con una batería para recibir y/o distribuir energía al sistema (1900). Por otra parte, esa batería

podría ser una batería interna. Por supuesto, el controlador (1910) podría recibir energía del vehículo (1902), un panel solar (1930) (ya sea en el controlador o externo), una batería u otra fuente de energía. Sin embargo, ese no siempre podría ser el caso. Por ejemplo, cuando el controlador está ubicado en el compartimiento de carga (1904), la energía del vehículo podría no estar disponible porque la cabina (1906) ya no está presente. O la energía del vehículo podría fallar. Por lo tanto, podría ser el caso que el controlador (1910) pierde energía y por lo tanto está sin energía. En tales casos, el circuito de geoposicionamiento (1912) puede detectar la pérdida del controlador (1910) mediante la falta de señales provenientes del controlador e informa que el controlador no está energizado y/o presente. También puede informar la ubicación en la que reside actualmente al centro de control. Así, al seguir las actividades se puede determinar si ocurrió un simple apagón, si el controlador fue manipulado, destruido, deshabilitado, retirado, etc. Por otra parte, en estos casos, será conocido donde estaba el circuito de geoposicionamiento (1912) (y presumiblemente el vehículo (1902)) en el momento de los hechos y tal vez después también.

Tenga en cuenta también que el controlador (1910) puede comunicarse con el centro de control directamente

sobre su propio vínculo de telecomunicaciones (por ejemplo, un vínculo de telefonía celular). También, o en lugar, puede configurarse para comunicarse entre ellos vía el circuito de geoposicionamiento (1912). Y, en algunas
5 modalidades, puede configurarse para hacer ambas cosas. Por otra parte, aunque algunas modalidades proporcionan comunicaciones/conexiones cableadas con los distintos otros componentes del sistema (1900), no necesita ser el caso. Por ejemplo, el sistema entero (1900) o componentes
10 seleccionados del mismo podrían comunicarse entre sí por medio de tecnología WiFi, infrarrojo, RFID, *Bluetooth*, *Zigbee*®, etc.

Con referencia constante a la Fig. 19, el sistema (1900) se muestra instalado como componentes individuales.
15 Sin embargo, algunos son todos ellos que se pueden combinar en una caja integrada o componente. Por ejemplo el controlador (1910) (con o sin batería) y el circuito de geoposicionamiento (1912) pueden montarse dentro de un contenedor electrónico resistente para
20 prevenir/obstaculizar que los usuarios manipulen con los mismos. Ese recinto puede ser montado y mecánicamente acoplado al vehículo (1902) dentro de un volumen de control de acceso como el compartimiento de carga (1904) o cabina (1906) para protección adicional o alternativa de
25 manipulación, daño y/o similares. De hecho, puede

instalarse en el volumen que es para supervisar. El montaje también puede ser por medio de sujetadores especiales, soldadura, remachado, etc. de manera que los intentos de abrir el contenedor sería fácilmente evidente después de la
5 inspección o de otra manera.

La Fig. 20 ilustra otro sistema antirrobo de carga. Este sistema (2000) se instala en un tráiler. La Fig. 20 ilustra diversos componentes del sistema (2000) incluyendo un compartimiento de carga (2004), un punto de acceso
10 (2008), un controlador (2010), un circuito de geoposicionamiento (2012), una cerradura (2014), una mitad de interruptor (2018) y una cámara (2022). Otros sensores tales como sensores de temperatura, humedad, presión, luz, vibración, precipitación, etc. podrían incluirse en el
15 sistema para proporcionar información sobre la carga y/o su entorno. El compartimiento de carga (2004) está situado en la bahía del tráiler y el punto de acceso (2008) es el par de puertas en un extremo de ese tráiler. Estas puertas generalmente se configuran de manera que una se superponga
20 con la otra lo que es necesario para abrir esa puerta primero y luego la otra puerta. Una puerta normalmente incluye una manija bloqueable de forma manual y/o *hardware* para montar una cerradura independiente de tal manera que asegure las puertas. Sin embargo, otros tipos de puertas

y/o puntos de acceso están dentro del alcance de la divulgación actual.

Por otra parte, el controlador (2010) de la modalidad actual se muestra como componente separado. Pero otra vez, 5 podrían integrarse con otros componentes notablemente el circuito de geoposicionamiento (1912) y/o la cerradura. También se muestra montado en una pared lateral del tráiler aunque se podría montar en el piso, en un "ático de madre" (para furgonetas móviles), en el techo, debajo de, etc. si 10 se desea. En la modalidad actual, el circuito de geoposicionamiento (2012) está montado en el techo del tráiler y también asegurado al tráiler en una manera en que se podrían hacer intentos de manipularlo y/o retirarlo detectable como se divulgo en otras partes en el presente. 15 Su ubicación también se proporciona con un punto de vista relativamente bueno en el que se puede enviar/recibir señales a/desde un sistema de telecomunicaciones y/o un sistema de geoposicionamiento. Su ubicación también lo protege de una observación casual por los que podrían estar 20 atentos de la presencia del sistema (2000).

La cerradura (2014) de la modalidad actual es una cerradura operada por un perno solenoide aunque otros tipos de cerraduras están dentro del alcance de la divulgación. Por ejemplo, un motor de CC, motor paso a paso u otro 25 dispositivo de actuación podría conducir la cerradura. Y,

por supuesto, podría ser cargado por un resorte o de otra manera inclinado en una posición predeterminada tal como la posición bloqueada. La cerradura (2014) de la modalidad actual podría proporcionarse con el sistema (2000) aunque
5 las cerraduras preexistentes podrían estar cableadas en el sistema si lo desea. Por otra parte, se muestra como montado en la segunda puerta de apertura del tráiler y dentro del mismo aunque esa necesidad no sea el caso. Esta posición, sin embargo, casi obligaría a un usuario no
10 autorizado de alguna manera a abrir la primera puerta de apertura y luego a entrar al menos en parte al compartimiento de carga (2004) antes de que pudieran manipular la cerradura (2014). Sin embargo, la cerradura (2014) podría incluir o ser equipada con un interruptor o
15 indicador de posición de manera que controlador (2010) pudiera detectar un movimiento inesperado (o no) de la cerradura (2014) y/o su perno. Si ese evento ocurre (por ejemplo, el interruptor u otro sensor de estado de perno indica movimiento no ordenado), el controlador (2010) puede
20 configurarse para enviar un comando a la cerradura (2014) para intentar bloquearse a sí mismo y podría enviar una señal al circuito de geoposicionamiento (2012) (y/o centro de control) indicativa del evento.

Los sistemas de algunas modalidades recaen en la
25 cerradura manual que normalmente se suministran en las

puertas de la mayoría de los vehículos. El sistema incluye un pasador de bloqueo suficientemente fuerte que los intentos de forzar la cerradura no la dañan lo suficiente que no sería probable que se suelte o se rompa. En dichas

5 modalidades, el controlador operaría el pasador de bloqueo con el usuario suministrando la fuerza para abrir la cerradura manual. Así, en lugar de desarrollar suficiente energía para superar la fricción, inercia, etc. asociados con la cerradura manual, el controlador produciría

10 suficiente energía para operar el pasador de bloqueo relativamente más pequeño.

La Fig. 20 también muestra una mitad de un interruptor de carga o una mitad del interruptor (2018). Otra mitad del interruptor de la modalidad actual se

15 encuentra al otro lado del camión y/o puerta aunque no es visible en la Fig. 20. Las mitades del interruptor (2018) pueden ser diseñadas y/o acopladas de manera mecánica a un cable resistente tal como un hecho de un metal trenzado o algún otro material resistente al corte, quemadura,

20 romperse, y/u otras formas de actividad destructiva que de alguna manera podría cortarla. Por supuesto el cable podría reemplazarse con o aumentado con una barra resistente, varilla, etc. en varias modalidades. Por otra parte, los cables pueden ser de una longitud suficiente para alcanzar

25 a través del punto de acceso (2008) con holgura mínima. La

mitad del interruptor (2018) también puede incluir (o conectarse a) un alambre (o un transmisor inalámbrico) de manera que el controlador (2010) pueda detectar el estado del interruptor (las dos mitades en combinación). El

5 mecanismo de detección del interruptor puede incluir: sensores RFID, sensores infrarrojos, sensores de proximidad, sensores de efecto Hall, sensores ópticos, etc. Tenga en cuenta que una mitad del interruptor (1218) sería un componente macho y el otro sería un componente hembra en

10 modalidades de manera que las dos mitades se pueden sacar y acoplar entre sí. Ya que las mitades del interruptor están acopladas mecánicamente a los lados opuestos del punto de acceso (2008), haciendo eso necesariamente implicaría cerrar las puertas y cualquier abertura de las puertas (un

15 daño estructural significativo del mismo ausente) necesariamente implicaría desconectar, desacoplar, o de lo contrario, separar las dos mitades del interruptor (1218). Esa acción podría ser detectada por el controlador (2010) enviando así una alarma o al menos enviar una señal

20 apropiada al circuito de geoposicionamiento (2012) y/o centro de control.

El sistema (2000) de la modalidad actual también incluye la cámara (2022) y podría incluir cámaras adicionales. La cámara puede colocarse para ver el punto de

25 acceso (2008) y/u otras ubicaciones en las los usuarios

(incluyendo los autorizados y no autorizados) y/o terceros podrían intentar acceder/entrar en el compartimiento de carga (2004). Por otra parte, una cámara (2022) podría colocarse en el exterior del tráiler con una vista del entorno circundante. Más todavía, puede colocarse una cámara (2022) en la cabina y/o con una vista de la carga. Estas cámaras pueden montarse firmemente de manera que la manipulación con ellos sería evidente, como con otros componentes del sistema (2000). Estas cámaras (2022) también pueden configurarse para comunicarse con el controlador (2010) y/o circuito de geoposicionamiento (2012) por diversos medios como se divulga en otras partes en el presente. También puede configurarse para comunicarse con el centro de control a través de una red de telecomunicaciones tal como un sistema de telefonía celular.

En algunas modalidades, el controlador (2010) podría ser configurado para generar una señal tras la detección de un evento inusual que causaría que las cámaras (2022) capturen una imagen de la escena que vieron en el momento del evento. Las cámaras también pueden configurarse para transmitir esas imágenes al controlador (2010), el circuito de geoposicionamiento (2012), el centro de control etc. Y, si lo desea, esas imágenes pueden ser registradas con tiempo, fecha y/o ubicación y pueden estar asociadas con

algún tipo de identificador de eventos. En algunos sistemas las cámaras son activadas por medio de luz de manera que una abertura del punto de acceso se detectaría a través de la luz ambiente que puede iluminar la zona de carga. En la

5 modalidad actual, por lo tanto, cuando ocurre un evento y/o incidente, las imágenes actuales de las áreas cerca del punto de acceso, el tráiler, la cabina, la carga, etc., se pueden obtener, conservar, almacenar, etc. para una revisión inmediata o posterior. En algunos casos, las

10 cámaras se activan después de una señal solicitada del circuito de geoposicionamiento y/o centro de control. Por otra parte, cuando el controlador de la modalidad actual detecta un cambio de estado del interruptor, éste envía una señal para activar las cámaras.

15 Por lo tanto, es probable que se pudiera obtener una imagen del usuario, terceros, perpetrador, y/u otros que pudieran estar presentes. Las imágenes del estado de la carga en el momento del evento también se pueden obtener de esta manera. Tenga en cuenta que las cámaras (2022) podrían

20 incluso, o en cambio ser activadas en alguna programación periódica y sobre las entradas autorizadas. En los sistemas de dichas modalidades, se conocería el estado de la carga mejor que con los sistemas hasta ahora disponibles. De hecho, las fotos de la carga se pueden obtener al inicio de

25 cada evento de carga o descarga y comparadas para

determinar si la cantidad apropiada de carga fue cargada o descargada. Por otra parte, el aspecto de la carga, pasajeros, etc. no autorizado podría identificarse y reportarse.

5 La Fig. 21 ilustra un controlador antirrobo instalado. El controlador (2110) de la modalidad actual es un integrado con las capacidades tanto de control y geoposicionamiento residente en el mismo y pasa a ser montado firmemente en un panel fuerte del vehículo (212)

10 que es suficientemente resistente para soportar probables intentos de penetrar, dañar o destruir. Además, el controlador (o su contenedor) tiene un reborde semejantemente fuerte (2114) que define un número de orificios del sujetador. La Fig. 21 muestra varios

15 sujetadores (2116) y (2118) tales como pernos y tuercas fijando el controlador (2110) al panel del vehículo (2112) a modo de brida (2114). Estos sujetadores (2116) y (2118) pueden ser de un tipo que requieren herramientas especializadas, raras o modificadas para asegurar o

20 desasegurarlos. En ese diseño (y/u otros diseños) terceros no autorizados sin esas herramientas resultaría difícil de quitar el controlador (2110) del panel del vehículo (2112). Por otra parte, estos sujetadores (2116) y (2118) podrían estar cableados, cubiertos, pintados, etc. de forma segura

25 una vez instalados para permitir una detección lista de

intentos para desajustarlos del controlador (2110) y/o panel del vehículo (2112). Esa detección sería a modo de determinar si el cable de seguridad estaba intacto y/o la cubierta, pintura, etc. está rayada. Así, la modalidad actual proporciona un controlador (2110) que si es manipulado sería evidencia de la misma.

La Fig. 22 ilustra esquemáticamente un sistema antirrobo de carga. El sistema de la modalidad actual incluye un controlador (2210), un circuito de geoposicionamiento (2212), una cerradura (2214), un interruptor de carga (2216), una batería (2220), una entrada de geozona (2222), una salida de carga (2224), y una entrada de interruptor de carga (2226). La Fig. 22 muestra que el controlador (2210) de la modalidad actual se comunica con el interruptor de carga (2216) y un par de cerraduras (2214). Es energizado por una batería separada (2220) como es el circuito de geoposicionamiento (2212). También se comunica con el circuito de geoposicionamiento (2212) por medio de tres señales: la entrada de geozona (2222), salida de carga (2224), la entrada del interruptor de carga (2226). El circuito de geoposicionamiento genera la salida de geozona para indicar al controlador (2210) que el sistema (2200) está (o no) en una geozona autorizada. El controlador (2210) detecta el estado del interruptor de carga (2216) por medio de la entrada del interruptor de

carga (2226) igual que el circuito de geoposicionamiento. Aunque uno u otro de estos dos dispositivos podría detectar en las modalidades. Por otra parte, la Fig. 22 ilustra que el controlador (2210) genera la salida de carga (2224) la señal que indica que el acceso se está produciendo (o se ha producido) y que es detectada por el circuito de geoposicionamiento (2212). Adicionalmente, en la modalidad actual, el controlador genera una señal de control de bloqueo común (2228) que se utiliza para controlar las cerraduras (2214) aunque las cerraduras se activan por separado podrían proporcionarse en las modalidades.

Con otra referencia a la Fig. 22, tenga en cuenta que muchos circuitos de geoposicionamiento incluyen baterías a bordo. Estas baterías pueden seleccionarse de manera que suministran un período de funcionamiento más largo que la batería (2220) (si el controlador (2210) es interno o externo). De esta manera, el circuito de geoposicionamiento puede seguir funcionando incluso después de que la batería (2220) se descarga y deja al controlador (2210) inoperable. Cuando ocurren tales eventos, el circuito de geoposicionamiento (2212) puede continuar reportando la geoubicación del sistema (2200) y cualquier dato que se puede obtener, por ejemplo, la entrada del interruptor de carga (2226) y/o varias cámaras.

La Fig. 23 ilustra esquemáticamente otro sistema antirrobo de carga. En la modalidad actual, la unidad de control (2300) incluye circuitos relacionados a la protección de carga y combustible. Más específicamente, la

5 unidad de control (2300) incluye y/o se comunica con un interruptor de carga (2304), una resistencia (2306), un solenoide de cerradura (2308), un interruptor de la cerradura (2312) y una batería (2316). El interruptor de carga se ilustra como un par de contactos normalmente

10 abiertos, aunque puede estar hechos de dos mitades del interruptor como se divulgó en otras partes en el presente. Tenga en cuenta que la unidad de control (2300) detecta el interruptor de carga (2304) a través de la resistencia variable que divide el voltaje (2306) de manera que el

15 voltaje detectado en la unidad de control (2300) se puede configurar por el usuario. En la modalidad actual, el valor de la resistencia (2306) puede programarse vía la unidad de control (2300) sobre un sistema de telecomunicaciones (por ejemplo, por un usuario en el centro de control). Por

20 consiguiente, la unidad de control (2300) se puede configurar para generar una señal relacionada con el interruptor de carga si el voltaje lo detecta como que una entrada está incorrecta (y/o apagada por más de alguna cantidad predeterminada). Así, si un tercero intenta imitar

25 la presencia de un interruptor de carga cerrado en esa

entrada de la unidad de control (2300) con un suministro de voltaje, la unidad de control (2300) es probable detectar un evento anómalo y levantar una señal correspondiente.

5 Tenga en cuenta también que la unidad de control (2300) detecta la posición de la cerradura mediante el interruptor de la cerradura (2312). Mientras que el interruptor de la cerradura (2312) se indica como un interruptor, podría utilizarse cualquier tipo de sensor de posición de dicho componente. Por ejemplo, podría
10 utilizarse un indicador de posición de resistencia lineal. La unidad de control (2300) de la modalidad actual también acciona el solenoide de cerradura (2308). Así, puede controlar la posición (ordenada) de una o más cerraduras. La unidad de control (2300) también incluye una batería a
15 bordo (2316). Por lo tanto, puede operar independientemente de un suministro de energía del vehículo por lo menos durante algún tiempo. Y para los componentes montados en el exterior, se puede proporcionar un panel solar para energizar dichos componentes y/o el sistema.

20 La Fig. 24 ilustra un interruptor de carga y un par de conectores de cabina a remolque. Las mitades del interruptor (2402) y (2404) (del interruptor de cable (2400)) se muestran mecánicamente acopladas a un par de cables (2406) y alambres (2408) correspondientes. Una mitad
25 de interruptor (2402) es macho mientras que la otra es

hembra en la modalidad actual. La Fig. 24 ilustra también un par de cabinas a las mitades de interruptor de tráiler (2410) y (2412) una de las cuales es macho y la otra hembra. Estas mitades de interruptor (2410) y (2412) se
5 pueden utilizar para conectar componentes ubicados en el tráiler de varias modalidades a los componentes ubicados en la cabina.

Haciendo referencia otra vez a la Fig. 12, tenga en cuenta que ese método (1200) puede incluir la supervisión
10 de los controladores antirrobo de carga, circuitos de geoposicionamiento, interruptores de carga, interruptores de la cerradura, cámaras, sistemas, etc. divulgados en el presente. Así, las modalidades proporcionan sistemas, sensores, controladores, etc. antirrobo de carga que
15 permiten supervisar el compartimiento de carga del vehículo para un robo de carga y/o manipulación potencial. Algunos dichos sistemas permiten una supervisión de la carga discreto, invisible y potencialmente insospechado. En algunas modalidades, los sensores, controladores, sistemas,
20 etc. son confiables, resistentes y relativamente baratos para instalar y/u operar. Los sistemas de algunas modalidades permiten a los usuarios investigar posibles eventos de robo de carga de forma remota e implementar acciones correctivas.

CONCLUSIÓN

Aunque la materia de referencia se ha divulgado en lenguaje específico de características estructurales y/o acciones metodológicas, debe entenderse que la materia de referencia definida en las reivindicaciones adjuntas no está necesariamente limitada a las características descritas o acciones divulgadas anteriormente. Por el contrario, las características y las acciones específicas descritas en el presente documento se divulgan como formas ejemplares para implementar las reivindicaciones.

REIVINDICACIONES

1. Un controlador de protección antirrobo de carga que comprende:

5 una entrada de interruptor de carga configurada para detectar una tierra de un vehículo de carga a través de un interruptor de carga;

 una salida configurada para estar en comunicación con una cerradura electrónicamente operada; y

10 un circuito en comunicación con la entrada y la salida y está configurado para detectar una apertura del interruptor de carga por medio de un voltaje preseleccionado en la entrada del interruptor de carga y, en respuesta a los mismos, para activar la cerradura a
15 través de la salida;

 en donde el interruptor de carga se acopla mecánicamente a un punto de acceso de la carga en el vehículo de carga de manera que el punto de acceso de la carga no se puede abrir con la apertura del interruptor de
20 carga.

2. El controlador de conformidad con la reivindicación 1, que comprende además una salida de geoposicionamiento en comunicación con el circuito, el circuito que está configurado además para sacar una señal

indicativa de la abertura del interruptor de carga por medio de la salida de geoposicionamiento.

3. El controlador de conformidad con la reivindicación 1, que comprende además una entrada a la geozona y que está configurada además para sacar una señal por medio de la salida para desbloquear la cerradura sólo en las geozonas preseleccionadas.

4. El controlador de conformidad con la reivindicación 1, en donde el voltaje preseleccionado difiere de 12 V CC.

5. El controlador de conformidad con la reivindicación 1, que comprende además una entrada de usuario configurada para aceptar un voltaje seleccionado por el usuario, el controlador está configurado además para cambiar el voltaje preseleccionado al voltaje seleccionado por el usuario.

6. El controlador de conformidad con la reivindicación 1, en donde el controlador se configura además para detectar un PIN (número de identificación personal) asociado con aperturas y cierres del interruptor de carga.

7. El controlador de conformidad con la reivindicación 1, que comprende además un acoplador mecánico configurado para acoplar de forma segura el controlador al vehículo de carga.

8. El controlador de conformidad con la reivindicación 1, que comprende además una entrada de posición de bloqueo y en donde el controlador está configurado además para detectar una posición de la cerradura por medio de la entrada de posición de bloqueo y para detectar si la entrada de posición de bloqueo se abre electrónicamente.

9. El controlador de conformidad con la reivindicación 8, en donde además el controlador se configura además para sacar una señal indicativa de que la cerradura debería bloquearse en respuesta a la posición de la cerradura.

10. El controlador de conformidad con la reivindicación 1, que comprende además una batería configurada para energizar el controlador.

11. El controlador de conformidad con la reivindicación 1, en donde el controlador se configura además para cambiar un PIN (número de identificación personal) asociado con aperturas y cierres del interruptor de carga.

12. Un sistema de protección antirrobo que comprende:
Un controlador que comprende además:
una entrada de interruptor de carga configurada para detectar una tierra de un vehículo de carga a través de un interruptor de carga;

una salida configurada para estar en comunicación con una cerradura electrónicamente operada; y

un circuito en comunicación con la entrada y la salida y está configurado para detectar una apertura del interruptor de carga por medio de un voltaje preseleccionado en la entrada del interruptor de carga y, en respuesta a los mismos, para activar la cerradura a través de la salida;

un interruptor de carga en comunicación eléctrica con la entrada del interruptor de carga;

un bloqueo operado electrónicamente en comunicación con la salida; y

un acoplamiento mecánico en donde el interruptor de carga se acopla mecánicamente a un punto de acceso de la carga en el vehículo de carga de manera que el punto de acceso de la carga no se puede abrir sin la apertura del interruptor de carga.

13. El sistema de conformidad con la reivindicación 1, que comprende además una salida de geoposicionamiento en comunicación con el circuito, el circuito que está configurado además para sacar una señal indicativa de la apertura del interruptor de carga por medio de la salida de geoposicionamiento.

14. El sistema de conformidad con la reivindicación 1, que comprende además una entrada a la geozona y que está

configurada además para sacar una señal por medio de la salida para desbloquear la cerradura sólo en las geozonas preseleccionadas.

15 15. El sistema de conformidad con la reivindicación 1, en donde el voltaje preseleccionado difiere de 12 V CC.

10 16. El sistema de conformidad con la reivindicación 1, que comprende además una entrada de usuario configurada para aceptar un voltaje seleccionado por el usuario, el controlador está configurado además para cambiar el voltaje preseleccionado al voltaje seleccionado por el usuario.

17. El sistema de conformidad con la reivindicación 1, en donde el controlador se configura además para detectar un PIN (número de identificación personal) asociado con aperturas y cierres del interruptor de carga.

15 18. El sistema de conformidad con la reivindicación 1, que comprende además un acoplador mecánico configurado para acoplar de forma segura el controlador al vehículo de carga.

20 19. El sistema de conformidad con la reivindicación 1, que comprende además una entrada de posición de bloqueo y en donde el controlador está configurado además para detectar una posición de la cerradura por medio de la entrada de posición de bloqueo.

20. Un método para proteger una carga que comprende:

Original (for SUBMISSION)

VIII-3-1	Declaration: Entitlement to claim priority Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application specified below, where the applicant is not the applicant who filed the earlier application or where the applicant's name has changed since the filing of the earlier application (Rules 4.17(iii) and 51bis.1(a)(iii)) Name	In relation to this international application NUVE, INC. is entitled to claim priority of earlier application No. 61/980,470 by virtue of the following:
VIII-3-1(i v)		an assignment from TSOGBE, Elom to NUVE, INC., dated 14 April 2015 (14.04.2015)
VIII-3-1(i v)		an assignment from AROCHA, Antonio to NUVE, INC., dated 15 April 2015 (15.04.2015)
VIII-3-1(i v)		an assignment from GREIG, Michael to NUVE, INC., dated 14 April 2015 (14.04.2015)

Original (for SUBMISSION)

VIII-2-1	Declaration: Entitlement to apply for and be granted a patent Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent (Rules 4.17(ii) and 51bis.1(a)(ii)), in a case where the declaration under Rule 4.17(iv) is not appropriate: Name (LAST, First)	In relation to this international application NUVE, INC. is entitled to apply for and be granted a patent by virtue of the following:
VIII-2-1(i v)		an assignment from TSOGBE, Elom to NUVE, INC., dated 14 April 2015 (14.04.2015)
VIII-2-1(i v)		an assignment from AROCHA, Antonio to NUVE, INC., dated 15 April 2015 (15.04.2015)
VIII-2-1(i v)		an assignment from GREIG, Michael to NUVE, INC., dated 14 April 2015 (14.04.2015)

LISTA DE INVENTORES

PCT/US2015/026169

Elom TSOGBE

Suite 100 7320 North Mopac Expressway
Austin,
Texas 78731
Estados Unidos

Antonio AROCHA

Suite 100 7320 North Mopac Expressway
Austin,
Texas 78731
Estados Unidos

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference NUVE-1002WO	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2015/026169	International filing date (day/month/year) 16 April 2015	(Earliest) Priority Date (day/month/year) 16 April 2014
Applicant NUVE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (see Box No. II).

3. ☐ Unity of invention is lacking (see Box No. III).

4. With regard to the title,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

a. the figure of the drawings to be published with the abstract is Figure No. 19

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2015/026169

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - B60R 25/01 (2015.01)

CPC - B60 R 25/01 (2015.04)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - B60R 25/00, B60R 25/01, B60R 25/10, B60R 25/23 (2015.01)

USPC - 180/287; 303/89; 340/6.1, 425.5, 426.28, 431, 542

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

CPC - B60R 25/00, B60R 25/01, B60R 25/1001, B60R 25/1004, B60R 25/23, Y10T 70/00, Y10T 70/5889 (2015.04) (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Orbit, Google Patents, Google.

Search terms used: anti-theft, controller, switch, cargo vehicle, lock, voltage, ground, personal identification number

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1,584,526 B1 (BERGSTEN) 06 July 2011 (06.07.2011) entire document	1, 4-5, 7-10, 12, 15-16 & 18-19
Y		2-3, 6, 11, 13-14, 17 & 20
Y	US 2002/0089434 A1 (GHAZARIAN) 11 July 2002 (11.07.2002) entire document	2-3, 13-14 & 20
Y	US 2007/0085680 A1 (COHEN) 19 April 2007 (19.04.2007) entire document	6, 11, 17 & 20
A	US 2004/0178880 A1 (MEYER et al) 16 September 2004 (16.09.2004) entire document	1-20
A	US 2010/0089108 A1 (DUTT et al) 15 April 2010 (15.04.2010) entire document	1-20
A	US 2009/0072956 A1 (KALOUS) 19 March 2009 (19.04.2009) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

15 June 2015

Date of mailing of the international search report

23 JUL 2015

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Blaine Copenheaver

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774



- (51) **International Patent Classification:**
B60R 25/01 (2013.01)
- (21) **International Application Number:**
PCT/US2015/026169
- (22) **International Filing Date:**
16 April 2015 (16.04.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/980,470 16 April 2014 (16.04.2014) US
PCT/US2014/054796
9 September 2014 (09.09.2014) US
- (71) **Applicant:** NUVE, INC. [US/US]; 7320 North Mopac Expressway, Suite 100, Austin, Texas 78731 (US).
- (72) **Inventors:** **TSOGBE, Elom**; 7320 North Mopac Expressway, Suite 100, Austin, Texas 78731 (US). **AROCHA, Antonio**; 7320 North Mopac Expressway, Suite 100, Austin, Texas 78731 (US). **GREIG, Michael**; 7320 North Mopac Expressway, Suite 100, Austin, Texas 78731 (US).
- (74) **Agent:** **VILLHARD, Robert L.**; The Villhard Patent Group, Suite 120-275, 13492 Research Blvd., Austin, Texas 78750 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

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

- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

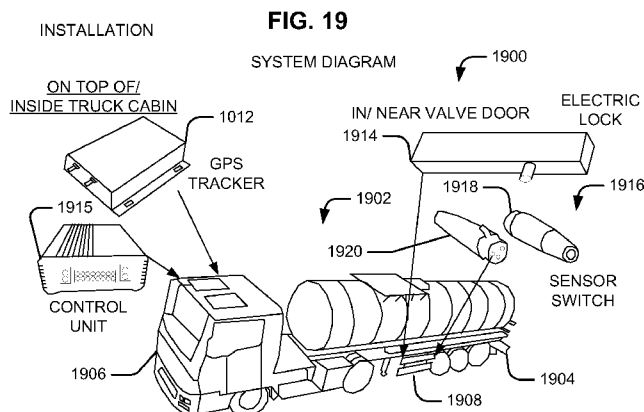
Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report (Art. 21(3))*

(54) **Title:** CARGO ANTI-THEFT SYSTEMS, APPARATUS, AND METHODS



(57) **Abstract:** Cargo anti-theft systems, apparatus, and related methods. Anti-theft controllers of embodiments are configured to sense the openings of cargo switches and to electronically operate locks responsive thereto. Moreover, the switches are mechanically coupled to the access points in manners such that the access points cannot be opened without opening the switches. Some controllers are configured to output signals indicative of openings of the switches while some are configured to unlock the locks only in pre-selected geo-zones. The pre-selected voltages, moreover, can differ from 12 VDC and can be user-selected. Furthermore, controllers can be configured to sense (modifiable) PINs associated with openings of the cargo switches. The controllers can include a coupler which securely couples it to the vehicle. It can also be configured to sense a position of the lock. Such controllers, furthermore, can be configured to lock the lock responsive to the lock position and/or can comprise a battery.



CARGO ANTI-THEFT SYSTEMS, APPARATUS, AND METHODS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to Patent Cooperation Treaty patent application No. PCT/US14/54796, titled FUEL ANTI-THEFT SYSTEMS, APPARTUS, AND METHODS, filed by Elom Tsogbe on September 9, 2014 which claims priority to U.S. provisional patent application No. 61/883,431 titled FUEL ANTI-THEFT SYSTEMS, APPARTUS, AND METHODS, filed by Elom Tsogbe on September 27, 2013, the entirety of both of which is incorporated herein as if set forth in full. This application also claims priority to and is a non-provisional application of U.S. provisional patent application No. 61/980,470 titled CARGO PROTECTION SYSTEMS, APPARTUS, AND METHODS, filed by Elom Tsogbe on April 16, 2015 the entirety of which is incorporated herein as if set forth in full.

BACKGROUND

[0002] Theft of gasoline, diesel fuel, and/or other vehicular fuels represents a substantial loss to cargo carriers in many parts of the world. Notably, in many developing countries, fuel represents an easily sold commodity that cannot be traced and which garners a high return in the black market. Thus, parked vehicles stand as undefended targets for fuel thieves. Even attended vehicles, though, can be at risk particularly if the driver is “on the make.”

[0003] Of course, the fuel contained in these vehicles can be accessed via the fuel fill cap (or simply “fuel cap”). A thief can remove the fuel cap, route a tube or hose through the adjoining fill tube, and siphon fuel from the tank. Moreover, vehicular fuel systems typically present a number of less conventional “entry points” through which a thief can access the fuel contained therein. More specifically, typical vehicular fuel systems include a fuel tank (sometimes with a drain fixture/feature), a

fuel pump (often submerged, but sometimes external to the tank), a fuel filter, various valves, a recirculation line, test ports, flow rate sensors, and/or a connection to a carburetor (in older vehicles), or the fuel injectors (in most late model vehicles), and/or a fuel “rail” which feeds the fuel injectors. That list, by the way, is not exclusive but serves to illustrate that each system component has at least one mechanical/fluid coupling that can be tampered with to access the fuel. Additionally, there might be some such fluid couplings between otherwise separate tubes, pipes, hoses, etc. which convey fuel through the vehicle. All of these couplings, components, etc. represent fuel system “entry points” and render the fuel therein subject to theft.

[0004] Such risks, moreover, do not exist with land-based vehicles alone. Rather the cars, trucks, lorries, vans, etc. which exist on the roads represent just one category of susceptible vehicle. Aircraft (for instance, helicopters, prop-driven planes, jet planes, etc.), marine vehicles (for instance, boats, hovercraft, tugboats, crane boats, etc.) and other categories of vehicles also stand at risk of fuel-theft. Aviation fuel (av-gas, jet A, mogas) which sells at a premium compared to even automobile gasoline, not to mention diesel represents a particularly “rich” target at unguarded airports, airfields, and the like. Of course, elevated prices and/or scarcity (whether local, regional, or otherwise) aggravate the threat.

[0005] Similar considerations apply to cargo which the trucks and/or other vehicles might be carrying. For instance, in poor areas, food, water, beverages, etc. might be highly prized and deemed worthy of attempted theft and/or other types of misappropriation. More valuable cargo such as consumer electronic devices might be sought after with less than ethical characters willing to steal these products from their employers, others, etc. And, of course, rarer merchandise such as gold, jewelry, money itself (conveyed in armored vehicles) could become targeted for theft.

Furthermore, whole shipments need not be stolen for a shipper to suffer significant losses particularly if viewed over time. For instance, even legitimate customers of the shipper might be tempted to take advantage of the lack of security typically present when a truck arrives at their facility. In such situations, some persons might remove their legitimately ordered cargo and then proceed to take more cargo than they ordered or are otherwise entitled to take. In the alternative, or in addition, such persons might fraudulently claim that cargo was missing from a shipment when in fact it was present. And, of course, other scenarios too numerous to list here can give rise to discrepancies associated with cargo shipments. Such issues extend beyond emerging countries. According to the FBI, cargo theft has reached an epidemic portion averaging up to 30\$ billion lost annually in just the United States of America.

SUMMARY

[0006] The following presents a simplified summary in order to provide an understanding of some aspects of the disclosed subject matter. This summary is not an extensive overview of the disclosed subject matter, and is not intended to identify key/critical elements or to delineate the scope of such subject matter. A purpose of the summary is to present some concepts in a simplified form as a prelude to the more detailed disclosure that is presented herein. The current disclosure provides systems, apparatus, methods, etc. for detecting potential fuel theft and more particularly for detecting fuel theft related events associated with vehicles such as planes, boats, automobiles, and trucks among other vehicles.

[0007] Some embodiments provide fuel anti-theft systems for vehicles which possess fuel systems defining a plurality of fluid entry points. Systems of the current embodiment nominally include a pre-selected number of sensors which are positioned at the entry points. Each sensor defines a nominal/secure state and a potentially tampered-with state. The potentially tampered-with state is indicative of the sensor

being absent. The actual states of the sensors combining to create an actual combined state of the sensors. In contrast, the nominal states of the pre-selected number of sensors combine to create a nominal combined state of the pre-selected number of sensors. Furthermore, a controller of the system senses the actual combined state of the sensors and determines whether the actual combined state of the sensors is the nominal combined state of the pre-selected number of sensors. Responsive thereto, the controller generates a signal which indicates whether all of the pre-selected number of sensors are present and un-tampered-with.

[0008] In accordance with various embodiments, the current disclosure also provides fuel anti-theft methods. Some such methods comprise a variety of activities including sensing a combined signal from a plurality of sensors positioned at entry points of a vehicle fuel system. Each sensor defines a secure state and a suspect state (indicative of the sensor being absent) in accordance with the current embodiment. Moreover, the secure sensor states of a number of the sensors nominally in the system combine to create a secure system state. Such methods also comprise determining whether the combined signal about equals the secure system state (for the number of sensors in the system) and outputting a corresponding signal.

[0009] If desired, the sensing of the combined signal can be via a vehicle chassis ground and/or the sensors can be nominally wired in parallel. In some situations a resistor contributes to the combined signal. In addition, or in the alternative, such methods can further comprise noting the location of the vehicle when the signal fails to indicate that the combined signal is indicative of the secure system state for the number of sensors.

[0010] Various embodiments provide fuel anti-theft controllers including a circuit and/or sensors which define nominal (secure) and tampered-with states. The tampered-with states are indicative of the sensor(s) being absent. The controllers of

the current embodiment, moreover, sense a combined state of (all of a pre-selected number of) the sensors and determine therefrom whether all of the pre-selected number of sensors are present and secure. In some embodiments, the controller senses the sensors (which can be wired in parallel) via a vehicle chassis ground. If desired, a resistor (which is about electrically equivalent to one or more of the sensors) and/or a geo-positioning unit can be connected to the controller. The sensors can include normally open switches and clamps which close the switches when installed properly. The sensors can be secured by other means such as fasteners, cable ties, zip ties, adhesives, etc. Some sensors include grounding straps while others include ground return leads. In some embodiments, sensors are positioned at the vehicle fuel cap and/or fuel filter.

[0011] Various embodiments provide anti-theft controllers comprising cargo switch inputs, outputs, and circuits in communication therewith. The inputs of the current embodiment are configured to sense the grounds of the cargo vehicles on which they are installed through a cargo switch. Cargo switches of the current embodiment serve at least two purposes. More specifically, they provide an interface for access requests and they detect whether the door is shut or open. Systems of embodiments include other security feature such as infrared sensors, proximity sensors Hall effect sensors, RFID (Radio Frequency Identification) sensors, optical sensors, etc. to provide additional insight as to the state of the cargo switch and/or its environs. Further, some controllers are configured such that if a wire in an input circuit breaks (or is broken by someone), these controllers interpret that condition as indicative of tampering and thus raise an alarm.

[0012] Meanwhile, the outputs are configured to be in communication with electronically operated locks. The circuits are in communication with the inputs and the outputs and are configured to detect openings of the cargo switches via pre-

selected voltages at the cargo switch inputs. Responsive thereto, moreover, the circuits are configured to activate the locks via the outputs. In the current embodiment the cargo switches are mechanically coupled to cargo access points on the cargo vehicles so that the cargo access points cannot be opened without opening the cargo switches.

[0013] In some embodiments the circuits further comprise geo-positioning outputs and the circuits are further configured to output a signal indicative of the opening of the cargo switch via the geo-positioning output. In addition, or in the alternative thereto, controllers can further comprise geo-zone inputs and are further configured to output signals to unlock the lock only in pre-selected geo-zones. In some situations the pre-selected voltage differs from 12 VDC and can be user-selected.

[0014] Furthermore, the controller can be further configured to sense a PIN (personal identification number) associated with openings and closings of the cargo switch, keypad, audio knock sequence, cellular phone (carried by the user), etc.. In some of these cases, the controller can also be configured to change the PIN (Personal Identification Number). On the mechanical side of things, the controller can include or be coupled to a coupler which securely couples it to the cargo vehicle. It can also (or instead) comprise a lock position input and be configured to sense a position of the lock via it. Such controllers, furthermore, can be configured to output a signal indicating that the lock should lock responsive to the position of the lock. Some controllers, locks, and/or other system components moreover comprise a battery to power themselves.

[0015] To the accomplishment of the foregoing and related ends, certain illustrative aspects are described herein in connection with the annexed figures. These aspects are indicative of various non-limiting ways in which the disclosed subject

matter may be practiced, all of which are intended to be within the scope of the disclosed subject matter. Other novel and/or nonobvious features will become apparent from the following detailed disclosure when considered in conjunction with the figures and are also within the scope of the disclosure.

BRIEF DESCRIPTION OF THE FIGURES

[0016] The detailed description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number usually corresponds to the figure in which the reference number first appears. The use of the same reference numbers in different figures usually indicates similar or identical items.

[0017] Fig. 1 illustrates vehicles subject to fuel theft.

[0018] Fig. 2 illustrates a fuel anti-theft system installed on a vehicle.

[0019] Fig. 3 schematically illustrates a fuel anti-theft system.

[0020] Fig. 4 illustrates a fuel anti-theft controller.

[0021] Fig. 5 illustrates a fuel anti-theft clamp sensor.

[0022] Fig. 6 illustrates a stationary fuel anti-theft sensor.

[0023] Fig. 7 illustrates a fuel anti-theft sensor installed on a fuel cap.

[0024] Fig. 8 illustrates a fuel anti-theft sensor installed on a fuel filter.

[0025] Fig. 9 illustrates a fuel anti-theft sensor installed on a fuel suction line.

[0026] Fig. 10 illustrates a fuel anti-theft sensor installed on a fuel return line.

[0027] Fig. 11 illustrates a graphical user interface (GUI) of a fuel anti-theft system.

[0028] Fig. 12 illustrates a flowchart of a method of sensing fuel theft.

[0029] Fig. 13 illustrates a computer for use in fuel anti-theft systems.

[0030] Fig. 14 schematically illustrates a fuel anti-theft system.

[0031] Fig. 15 illustrates a fuel anti-theft control unit.

- [0032] Figs. 16 and 17 illustrate a fuel line sensor.
- [0033] Fig. 18 illustrates a fuel cap sensor.
- [0034] Fig. 19 illustrates a cargo anti-theft system.
- [0035] Fig. 20 illustrates another cargo anti-theft system.
- [0036] Fig. 21 illustrates an installed anti-theft controller.
- [0037] Fig. 22 schematically illustrates a cargo anti-theft system.
- [0038] Fig. 23 schematically illustrates another cargo anti-theft system.
- [0039] Fig. 24 illustrates a cargo switch and a pair of cab to trailer connectors.

DETAILED DESCRIPTION

[0040] This document discloses systems, apparatus, methods, etc. for detecting potential fuel theft and more particularly for detecting fuel theft related events associated with vehicles such as planes, boats, automobiles, and trucks among other vehicles.

[0041] Fig. 1 illustrates vehicles subject to fuel theft. More particularly, Fig. 1 illustrates a concrete truck 102, a delivery truck 104, a bulldozer 106, a generator trailer 108, a ship 110, a fuel tank 120, an entry point 122, an anti-theft controller 130, and an antenna 132. These vehicles 102, 104, 106, 108, and 110 (among others) have a number of common traits. For one thing, they all contain fuels of various types which are all at least somewhat valuable. Moreover, the owners, operators, and other users associated with them take and/or leave them at locations which are often remote from other users and at which witnesses of a potential fuel theft might be far and few between. In the alternative, or in addition, many potential witnesses might not care enough to report suspicious activities or might even be sympathetic to those who would undertake such actions. Thus, these vehicles and/or the fuel in them are susceptible to fuel-theft from time to time.

[0042] For instance, consider the delivery truck 104. A driver often takes the delivery truck 104 on routes delivering and/or picking up various goods and/or delivering various services. Those routes might take the driver into areas far from a depot, station, or other location at which the truck is normally garaged, parked, etc. Those garages are typically staffed by the owner of the delivery truck 104 and/or employees or other agents of the owner. Thus, if a driver desires to take fuel from the delivery truck 104 in a manner not authorized by the owner, it is likely that the driver will wait to do so until they are on a route or supposedly on a route.

[0043] When they feel ready to take the fuel, the driver will typically stop the truck in a spot “suitable” for doing so and exit its cab. They will then often find an entry point 122 in the fuel system of the delivery truck 104 through which to access the fuel. For instance, they will take the fuel cap off of the fuel tank 120, insert a hose into the fuel tank 120, and siphon fuel from the fuel tank 120. Subsequently, such drivers will either put the fuel to their personal use, sell it, or make some other unauthorized use of the fuel. Such fuel thefts (alone and/or cumulatively) can represent a significant loss for the owner of the delivery truck 104. Of course, any vehicle which contains fuel stands at risk of such thefts. Indeed, it was estimated in 2013 that fuel thefts cost the economy of Mexico alone 2-4 Billion \$US annually. See *The Aftermath Of Mexico’s Fuel Theft Epidemic: Examining The Texas Black Market And The Conspiracy To Trade In Stolen Condensate* by Luke B. Reinhart, May 9, 2014.

[0044] Some embodiments provide systems for detecting potential fuel thefts and for alerting owner and/or other users of such activities. As Fig. 1 further shows the fuel anti-theft controller 130 can be mounted in, or on, the delivery truck 104 to detect activity which might indicate that someone might have stolen fuel, is stealing fuel, and/or is about to steal fuel. The fuel anti-theft controller 130 is typically

connected to a plurality of sensors located at entry points to the vehicle's fuel system and monitors the same for potential tampering.

[0045] The sensors cause the fuel anti-theft controller 130 to generate a signal should some activity, condition, etc. cause one or more of the sensors to change state from a secure state to a tampered-with state or should a sensor appear to be missing from the system (whether suddenly or not). Moreover, the fuel anti-theft controller 130 of embodiments communicates and/or cooperates with an onboard geo-positioning unit, computer, etc. to time stamp and/or location stamp such occurrences. Further still, the fuel anti-theft controller 130, the geo-positioning system 132, and/or some other device on the delivery truck 104 can transmit information regarding such occurrences to remote owner/operators, central alarm consoles, etc.

[0046] Fig. 2 illustrates a fuel anti-theft system installed on a vehicle. More particularly, Fig. 2 illustrates a fuel system 200, the anti-theft system 201, a fuel tank 202, a fuel pump 204, a fuel filter 206, an engine 208, a fuel cap 210, a fuel inlet (tube, pipe, etc.) 211, a secondary fuel pump 212, a fuel pressure regulator 218, a fuel return line 220, a coupling 222, sensors 223, 225, and 227, cables 224, 226, and 228, a controller 230, a geo-positioning unit 232, and a conduit 240. At this juncture, a brief discussion of the fuel system 200 of a typical vehicle might be beneficial.

[0047] As those skilled in the art will appreciate, most vehicles include a fuel system 200 to deliver fuel stored in a fuel tank 202 to the engine 208. Those fuel systems 200 are replete with entry points making the fuel therein susceptible to theft. More particularly, in commercial vehicles in particular, the fuel tank 202 can contain hundreds of gallons of fuel, each gallon of which being valued at several US dollars as of this writing.

[0048] The fuel cap 210 presents one of the many entry points associated with a typical vehicular fuel system. Moreover, the fuel cap 210 is usually located in an

easily accessible location making it particularly attractive to thieves as an entry point. Moreover, often the fuel inlet 211 and fuel tank 202 are formed integrally with one another (or are welded together or otherwise permanently coupled). Yet, in vehicles in which they are separate components, the coupling between these two components represents another entry point in that the coupling can be disconnected allowing fuel to drain out of (or be pumped out of) the fuel system 200. Many fuel tanks 202, furthermore, contain a secondary fuel pump 212 or have it mounted in close proximity thereto. Thus, the secondary fuel pump 212 of some vehicles presents another system coupling (or even a pair thereof), and therefore, an entry point.

[0049] From the fuel tank 202, a fuel line runs to another fuel system component (as illustrated by Fig 2) such as the primary fuel pump 204. Again, this component presents another pair of entry points rendering the fuel vulnerable to theft. The fuel filter 206, fuel pressure regulator 218, engine 208, and fuel return line 220, all include couplings that also render the fuel vulnerable. Moreover, vehicle manufacturers sometimes find it desirable to use two or more pieces of tubing, piping, hose, etc. to route fuel from one component to another. As a result, a coupling 222 can appear in many places apart from the discrete components illustrated by Fig. 2. As noted, therefore, typical fuel systems 200 are replete with entry points which render the fuel contained in the systems vulnerable to theft.

[0050] With continuing reference to Fig. 2, embodiments provide anti-theft systems 201 on vehicles such as delivery truck 104. The anti-theft system 201 of the current embodiment includes the controller 230, the geo-positioning unit 232, the sensors 223, 225, and 227, and the cables 224, 226, and 228 among other things. The controller 230 of the current embodiment resides in the crew cabin of the vehicle and, more particularly, can be mounted in the dashboard or at some location relatively inaccessible to users of the vehicle. The geo-positioning unit 232 can also reside in

the cabin although, if desired, it can be located in an accessible area of the cabin. In the alternative, or in addition, the geo-positioning unit 232 can be a component of the controller 230. The sensors 223, 225, and 227 are clamped to the couplings 222 and/or other components of the fuel system 200 which represent entry points. The cables 224, 226 and 228 run from the sensors 223, 225, and 227 to the controller 230 and also (in the current embodiment) run through conduits 240.

[0051] The cables 224, 226, and 228 provide electrical conductivity between the sensors 223, 225, and 227 and the controller 230 and, therefore, allow the controller 230 to sense the state of the sensors (as a group in the current embodiment). Furthermore, the conduits 240 provide protection to the cables 224, 226, and 228 from mechanical damage arising from abuse, neglect, outright tampering, etc. The conduits 240 (and, for that matter, the cables 224, 226, and 228) can be disguised to appear to be OEM (original equipment manufacturer), after-market, etc. equipment that has been on the vehicle for some time. The conduits 240 can be (among other things) a piece of cable sheathing, braided hose, corrugated conduit (of type SM-1216-BK and available from Sealcon LLC located on 7374 S. Eagle St, Centennial CO 80112 etc. and/or can be smeared with dirt, grease, grime, etc. normally available on the vehicle or created for such purposes.

[0052] As is further disclosed with reference to Figs. 3 and 5-10, the sensors 223, 225, and 227 include normally open switches and clamps. The clamps are configured to hold the sensors against the various couplings/components and (by doing so) to urge the switches toward their closed positions. It is these closed positions (collectively, in the current embodiment) which indicate that the fuel system 200 is secure and/or un-tampered-with. Indeed, should even one of the switches open (or a sensor disappear from the anti-theft system 201), the controller 230 of the current embodiment will interpret that event as an indication that some user might be

tampering with the fuel system 200 and/or attempting to gain access to the fuel via a monitored entry point/coupling/component.

[0053] Fig. 3 schematically illustrates a fuel anti-theft system. More particularly, Fig. 3 illustrates an anti-theft system 300, an exterior subsystem 304, a remote alert center 306, the Internet “Cloud,” a satellite 308, a sensor network 310, a set of resistors 312, sensors 318, sensor switches 320, sensor resistances 322, resistors 324, a controller 330, geo-positioning unit 332, a comparator 334, an antenna 338, and a local indicator 340. If desired a processor could be used instead of, or in addition to the comparator 334. In such cases, the processor could be configured with an analog input to sense the resistors and/or to determine whether the system is secure or has potentially been tampered with.

[0054] Thus, the anti-theft system 300 allows the controller 330 to communicate with the remote alert center 306 via the Cloud 309 and/or via a geo-positioning system including its satellites 308 and/or other infrastructure). If the controller 330 should issue an alert, therefore, the remote alert center 306 can receive the alert via either the cloud, the geo-positioning system, and/or some other telecommunications system (such as a cellular telephone system). Users and/or servers, computers, etc. in communication with the remote alert center 306 can monitor, react to, data mine, etc. these alerts and/or take corrective action. For instance, a vehicle owner could investigate the alerts, place the vehicle/driver under surveillance, etc.

[0055] With continuing reference to Fig. 3, the controller 330 resides on a vehicle as does much of the rest of the anti-theft system 300 of the current embodiment. For instance, each of the sensors 318 resides on the vehicle and comprises a normally open switch 320 and often some (inherent) internal resistance 322. Of course, that internal resistances 322 might be associated with internal

interconnects of the sensors 318, its external wiring, connections there between, etc. However, in some embodiments, various sensors 318 comprise resistors of about 10 k-ohm, 5.1 k-ohm or 3.3k-ohm with a 1% tolerance. As a result, each sensor 318 of the current embodiment will nominally have two states: a secure state and a potentially tampered-with state. In the secure state, the sensors 318 have their normally open switches 320 clamped closed by a clamp which secures the sensors on their respective components. Thus, the sensor 318 (wired in parallel with the other sensors 318) contributes its conductance/resistance 322 to the overall sensor network 310. But, in the potentially tampered-with state, the normally open switches 320 are open so that the sensors 318 appear to be electrical “open” paths thereby contributing no conductance and/or an infinite resistance to the sensor network 310.

[0056] Thus, when an anti-theft system 300 is installed and operating nominally on a vehicle, all of the switches 320 of the sensors 318 are held closed by the clamps and are sensed accordingly by the controller 330. But, if one or more sensors 318 are tampered-with, a corresponding number of switches 320 are likely to open thereby changing the overall resistance/conductance of the sensor network 310. Furthermore, the controller 330 (and/or its comparator 334) can be configured to sense whether the nominal conductance/resistance of the sensor network 310 is present or whether it has been altered. More specifically, the comparator 334 can be configured to produce a signal based on whether or not a known/pre-selected number of sensors 318 are present with their normally open switches 320 in the closed position.

[0057] Thus, the expected, overall, combined resistance/conductance of the sensor network would be:

$$R_{\text{secure}} = 1/n * R_{\text{sensor}}$$

Where:

R_{secure} is the expected, overall resistance of the sensor network,
 n is the pre-selected number of sensors 318 (resistances 322), and
 R_{sensor} is the resistance 322 of one sensor 318.

[0058] A power supply 335 (internal to the controller 330 of the current embodiment) can supply a trickle current to the sensor network 310. Furthermore, the comparator 334 can be configured to monitor the sensor network 310 for changes in the voltage across the sensor network 310 that correspond to the pre-selected number of sensors 318 being in their secure state and present in the sensor network 310. Of course, any resistance 315 associated with the chassis ground path can be accounted for in this determination by reference to the following equations:

$$R_{\text{expected}} = R_{\text{secure}} + R_{\text{chassis}}$$

Where:

R_{expected} is the expected resistance and

R_{chassis} is the resistance 315 of the chassis ground path.

And

$$V_{\text{expected}} = I_{\text{controller}} * R_{\text{expected}}$$

Where:

V_{expected} is the expected voltage and

$I_{\text{controller}}$ is the current supplied by the controller.

[0059] Thus, should the voltage sensed by the comparator 334 increase by about the amount associated with one of the switches 320 opening (or a sensor 318 being removed from the sensor network 310), the controller 330 can generate a signal indicative of potential tampering with the fuel system 200. Of course, the set point of

the comparator 334 can be adjusted to account for tolerances associated with the foregoing parameters. Note that if the chassis resistance 315 is low, that voltage change would correspond to an increase of the resistance of the sensor network of:

$$\Delta R_{\text{tamper}} = R_{\text{expected}} - t/R_{\text{secure}};$$

$$\Delta V_{\text{tamper}} \geq I_{\text{controller}} * \Delta R_{\text{tamper}}; \text{ or}$$

$$V_{\text{tamper}} = V_{\text{expected}} + \Delta V_{\text{tamper}}$$

Where t is the number of open/missing sensors

[0060] Since there might be scenarios in which users might want to install more sensors 318 than the number that a particular controller 330 is configured for, the set point of the comparator 334 can be adjusted downward by an amount corresponding to the addition of additional sensors 318 (and their additional conductances across the parallel sensor network 310). Of course, an additional controller 330 could be added to the anti-theft system 300 to provide capacity for additional sensors 318. Should users wish to use fewer than the pre-selected number of sensors 318, then users can place a corresponding number (and value) of resistors 324 across the inputs to the controller 330 to emulate the un-installed sensors 318. Those resistors 324, moreover, could be in the same (or another) secure location as the controller 330 itself. In other embodiments, the resistors 324 could be supplied via DIP (dual in-line) switches or similar devices in or associated with the controller 330. In the alternative, or in addition, the unused sensors 318 could be connected to the controller 330 and clamped such that the normally open switches 320 remain closed.

[0061] In some embodiments, the controller 330 is configured to work in conjunction with 10 (ten) sensors 318. Moreover, in the current embodiment, each sensor 318 has a resistance of approximately 10 k-ohm. Thus, the sensor network 310

has an electrically equivalent resistance of 1 k-ohm. Table 1, below, lists electrically equivalent resistances for sensor networks 310 having various pre-selected numbers of sensors 318 and lists electrically equivalent resistances for sensor networks 310 (of the current embodiment) with various numbers of open switches 320.

TABLE 1

<u>No. of Sensors</u>	<u>No. of Open Sensors</u>	<u>Resistance (k-ohm)</u>
1	9	10
2	8	5
3	7	3.33
4	6	2.5
5	5	2
6	4	1.67
7	3	1.43
8	2	1.25
9	1	1.11
10	0	1

[0062] Thus, should a user attempt to tamper with the fuel system 200, the controller 330 would sense it. For instance, removing one of the sensors 318 (either physically or electronically) from the sensor network/anti-theft system 201 would cause the corresponding electrical path to open thereby increasing the voltage to beyond the comparator 334 set point. Unclamping a sensor 318 would open the switch 320 leading to the same result. Attempting to first (before otherwise tampering with a fuel system) place a resistor of the same resistance as the sensor resistance 322 would result in a decrease in voltage which could cause the comparator 334 (if configured to sense voltages outside of a band) to sense an attempt to tamper with the

fuel system 200 also (even if temporarily). And comparators 334 of some embodiments could be configured to latch the output signal in such situations.

[0063] With ongoing reference to Fig. 3, the signal output by the comparator 334 could serve several purposes. For one such purpose, it could cause a local indicator 340 to signal potential tampering. Of course, some embodiments either do not provide a local indicator 340 or provide it at a location not accessible to the normal users of the vehicle (for instance, the driver). The local indicator 340 could be hidden in a locked compartment or it could be provided within the housing of the controller 330 and, thus, available only to service technicians and/or others with the proper authority/tools to open the controller 330. The comparator signal could also be communicated to the geo-positioning unit 332.

[0064] The geo-positioning unit 332 could be configured to perform a variety of activities. For instance, it could (responsive to the comparator 334 signal) time and/or location stamp the occurrence(s) of the signal. Furthermore, the geo-positioning unit 332 could transmit such information to the remote alert center 306 via some telecommunications system. Additionally, or in the alternative, the geo-positioning unit 332 could track the location, speed, movement, lack of movement, etc. of the vehicle and transmit such information to the remote alert center 306. Thus, the anti-theft system 300 of embodiments can alert users (such as owners) to potential tampering with the fuel systems 200 of various vehicles.

[0065] Fig. 4 illustrates a fuel anti-theft controller. The controller 400 of the current embodiment includes a tamper-resistant housing 402 and a number of leads 404 hardwired to the controller 400. The tamper-resistant housing 402 can be any sort of housing sufficient to either prevent users from physically entering the housing or at least sufficiently strong that most significant attempts to do so would leave pry marks, dents, scrapes, etc. on the housing. Thus, attempts to enter the controller 400 (and/or

alter its internal components such as the comparator 334) could be readily evident upon inspection of the housing. The leads 404 can also contribute to the security of the anti-theft system 300. For instance, internal to the tamper-resistant housing 402, they can terminate in soldered, brazed, etc. connections to a PCB (printed circuit board) or otherwise be secured against un-detectable removal from the controller 400.

[0066] Moreover, in some embodiments, the leads 404 correspond in number to the pre-selected number of sensors 318. For instance, in embodiments in which every sensor 318 communicates with the controller 400 via a positive and a (ground) return lead, the controller 400 will have $2n$ leads (where “ n ” is the pre-selected number of sensors 318). However, it might be the case that one or more sensors 318 will use the chassis ground as a return path. In such situations, the number of leads 404 will be reduced accordingly and the associated set of sensors 318 will be selected with a number of return leads appropriate for controllers configured in that manner.

[0067] Additionally, or in the alternative, the controller 400 includes the local indicator 408. That local indicator 408 could be any indicator which can indicate that a tampering event has been detected (and/or is ongoing whether latched or not). For instance, the local indicator 408 could be a light, LED (light emitting diode), counter, blowable fuse/link, etc. If the controller 400 is in a secure location (for instance, “buried” in a dashboard) then the local indicator 408 will be correspondingly inaccessible to most users such as the vehicle driver. Of course, the local indicator 408 could be replaced/augmented with a jack, connector, etc. allowing for a connection of the controller 400 to an external event indicator.

[0068] Fig. 5 illustrates a fuel ant-theft clamp sensor. The clamp sensor 500 of the current embodiment comprises a pipe clamp 332, a band clamp 502, zip lock tie, etc. capable of securing the sensor 500 to a fuel system component such as those illustrated by Fig. 2. The clamp 502 can also, when clamped, exert sufficient force on

the switch 504 so as to close it (particularly if the switch 504 is a normally open switch). The switch 504 can be a normally open switch and can be positioned relative to the clamp 502 such that the clamp 502 can clamp it between the clamp and the component to which the sensor 500 is clamped. In the alternative, or in addition, the bulk of the switch 504 can be located on the outside of the clamp 502 with the actual electrical/mechanical switch and/or an actuator operatively coupled thereto positioned within the clamp (and subject to being clamped in the electrically “closed” position). Note, also that the sensor could also house a resistor to set the resistance 322 of the sensor 500 to a desired value if desired. Of course, the switch 504 (and resistor therein) could be wired to the connector 506 which can include conductors for both the positive and ground return paths associated with the sensor 500. For instance, the connector 506 of embodiments can be a model no. 45-4610 type connector available from LKG industries, Inc located on 3660 Publishers Dr, Rockford, IL 61109. Since the sensor 500 of the current embodiment has a connector 506, it can be used to monitor entry points which are subject to relatively frequent and legitimate openings. For instance, sensors 500 with connectors could be used on fuel caps 210. Note that in scenarios involving such entry points, the anti-theft system 300 could still be configured to raise an alarm when the connector 506 is disconnected (and the corresponding conductive path opens). But, the remote alert center 306 could be configured to, upon an alert, query the geo-positioning unit 332 for the location of the vehicle. If the vehicle happens to be located at a fueling depot, gas, station, etc. that location can be noted and considered in how the alert is handled.

[0069] Fig. 6 illustrates a stationary fuel anti-theft sensor. The sensor 600 of the current embodiment includes a clamp 602, a sensor package 604, and a lead 606 (or leads). The leads 606 are configured to be permanently, mechanically coupled (and in permanent electrical communication) with a sensor network 310. In some

cases, that coupling can be via soldering, brazing, etc. Thus, the sensor 600 of the current embodiment can be used to monitor entry points which, ordinarily, would experience only occasional openings. In other words, they are stationary. For instance, most couplings 222 and/or other components (exempting the fuel cap 210 for most vehicles) would be opened only if the vehicle is undergoing maintenance. Again, by querying the geo-positioning unit 334, checking maintenance orders/records, etc. the remote alert center 306 can determine whether the vehicle is located at an appropriate maintenance depot. The information so gained can be used in evaluating alerts arising from the sensor 600 of the current embodiment.

[0070] Fig. 7 illustrates a fuel anti-theft sensor installed on a fuel cap. The sensor 700 of the current embodiment comprises a clamp 702, a sensor package 704, a lead 706, and a grounding strap 708. The grounding strap 708 can be used to ground the sensor 700 to the vehicle chassis. Doing so ensures that the sensor 700 has a ground return path to the sensor network 310 despite the possibility that non-conductive material might interpose themselves between the sensor 700 and the chassis ground. For instance, OEMs (and after market manufacturers) often make fuel caps 210 from plastic and/or other non-conductive materials. Moreover, even should such fuel system 200 components be made of conductive materials, grease, dirt, grime, etc. might exist on one or more components rendering them non conductive. Moreover, some components might be coated in paint, wax, primer, etc. rendering such components non conductive. Of course, the underlying components could be clamped, stripped, etc. to increase their conductance in appropriate circumstances. Note that the grounding strap 708 could comprise a copper wire, piece of aluminum foil, etc. without departing from the current disclosure.

[0071] Fig. 8 illustrates a fuel anti-theft sensor installed on a fuel filter. Meanwhile, Fig. 9 illustrates a fuel anti-theft sensor installed on a fuel suction line and

Fig. 10 illustrates a fuel anti-theft sensor installed on a fuel return line. Thus, Figs. 8-10 illustrate that sensors 800, 900, and 1000 of embodiments can be installed at many locations throughout fuel systems 200 for many different types of vehicles.

[0072] Fig. 11 illustrates a graphical user interface (GUI) of a fuel anti-theft system. More particularly, Fig. 11 shows the GUI 1100, and a map 1102, a route 1104, a destination 1105, a detour 1106, calendaring controls 1108, map controls 1110, route markers 1112, route cautions 1114, route warnings 1116, a home tab 1118, a maps tab 1120, reports tab 1122, and an administrative tab 1124. The GUI 1100 and underlying software application, program, etc. can be hosted by remote alert centers 306, servers, computers, mobile devices (for instance, cellular telephones, laptops, tablets, notebooks, etc.) among others. The GUI 1100 of the current embodiment allows users to monitor, explore, investigate, etc. activities which might be related to vehicular fuel theft.

[0073] More specifically, the GUI 1100 illustrated in Fig. 11 displays a map 1102 on which the route 1104 of a user-selected vehicle is displayed. That route 1104 includes one or more intended destinations 1105 such as a local shop, business, factory, etc. and, as displayed, a detour 1106. Moreover, the actual route 1104 (including the detour 1106) can be rendered based on geo-positioning data provided by the geo-positioning circuit 334 and/or queried therefrom. Note also that scheduled delivery routes could be displayed on the GUI 1100. Of course, the detour 1106 might be legitimate such as where the driver acted to avoid congestion, construction, flooding, etc. On the other hand, that detour 1106 could indicate a location at which the driver has tampered-with, is tampering with, and/or is about to tamper with the fuel system 200.

[0074] Fig. 11 also shows that the GUI 1100 can display various route markers 1112, route cautions 1114, and/or route warnings 1116. The route markers 1112 can

be displayed corresponding to the locations at which the vehicle is proceeding at (or above) a user selected speed such as the local speed limit. In contrast, the route cautions 1114 can be displayed for locations at which the vehicle has slowed to below a user selected speed. Such behavior might be indicative of traffic/road related difficulties and/or imminent fuel system tampering. The GUI 1100 also shows several route warnings 1116 which correspond to locations at which the vehicle has slowed below some user-selected speed and/or stopped. Such behavior could be indicative of imminent or ongoing fuel system tampering and/or fuel theft. Note that the vehicle speeds, location, etc. can be obtained remotely by querying the fuel anti-theft system 300 of embodiments and/or other onboard systems. Thus, users such as owners can examine the map 1102 to determine where/when fuel theft might be occurring and/or patterns related thereto.

[0075] Of course, the GUI 1100 has other features as well. For instance, the calendaring controls 1108 allow a user to see the current date/time. In some embodiments, the calendaring controls 1108 allow users to select dates/times for which the GUI 1100 can display corresponding maps 1102, routes 1104, route markers 1112, route cautions 1114, route warnings 1116, etc. Moreover, the GUI 1100 can include map controls 1110 for zooming into/out of maps 1102, navigating on maps 1102, saving maps 1102, printing maps 1102, etc.

[0076] GUIs 1100 of embodiments also include controls such as the home tab 1118, the maps tab 1120, the reports tab 1122, the administrative tab 1124, etc. These tabs 1118, 1120, 1122, and/or 1124 allow users to navigate between various and corresponding portions of the GUI 1100. For instance, the maps tab 1120 can allow users to navigate between various maps 1102 whereas the reports tab 1122 can provide corresponding functionality for various reports. The administrative tab 1124 can allow users to handle certain administrative activities such as user profile

maintenance, vehicle profile maintenance, driver profile maintenance, etc. The home tab 1118 can provide overall GUI navigation controls such as those related to logging in, logging in, logging out, switching users, etc.

[0077] Fig. 12 illustrates a flowchart of a method of sensing fuel theft. The method 1200 comprises various activities such as selecting one or more vehicles on which to install anti-theft systems 300. These vehicles might be those involved in fuel theft and/or other suspicious activities, a group of vehicles which for some reason might be particularly susceptible to such activities, the vehicles driven by certain users, etc. See reference 1202.

[0078] Method 1200 can also comprise installing the various sensors on one or more of the selected vehicles. Thus, sensors can be clamped on to the fuel cap 210, the fuel intake 211, the fuel tank 202, the fuel pump(s) 204 and/or 212, the fuel filter 206, the fuel pressure regulator 218, various fuel lines such as the fuel return line 220, and/or various couplings 222 in the fuel systems 200 of those vehicles. If the number of installed sensors 318 does not equal the pre-selected number of sensors 318 for a given controller 330, then the anti-theft system 300 can be configured accordingly. For instance, if the anti-theft system 300 has too many sensors 318 for the selected controller 330, then an appropriate number of controllers 330 can be added to the anti-theft system 300. If, though or in addition, too few sensors 318 have been installed for the pre-selected number(s) of sensors associated with the number of controllers 330 in the anti-theft system 300, then various resistors 324 can be connected across one or more of the controller 330 inputs. Thus, the controllers 330 can be connected to sensor networks 310 having overall resistances/conductances corresponding to the pre-selected number(s) of sensors 318. See reference 1204.

[0079] Of course, if the controller(s) 330 have not already been installed, then they can be installed on the vehicle. For instance, the controller 330 can be mounted

into the dashboard or otherwise installed at some relatively inaccessible location on the vehicle as indicated at reference 1206. If a separate geo-positioning unit is to be included in the anti-theft system 300, then it can be installed in/on the vehicle and/or connected to the controller. See reference 1208. Moreover, the various conduits 240 can be run through the vehicle from the location(s) of the sensor(s) 318 to the controller 330. The wires, cables 224, 226, and 228, grounding straps, etc. associated with the sensors can then be run through the conduits 240 and/or run separately therefrom. If desired, the conduits, cables, sensors, etc. can be disguised to appear as if they have been located on the vehicle for all or a portion of the life of the vehicle. For instance, dirt, grease, grime, etc. can be applied to them. See reference 1209.

[0080] Reference 1210 of Fig. 12 illustrates that the vehicle may be driven at some point. For instance, a particular driver(s) might be alerted to the presence of the anti-theft system 300 whereas some other drivers might be allowed to remain unaware of its presence. One way or another, as the vehicles are driven, the data generated by the anti-theft system 300 (and/or other onboard systems) can be gathered and/or monitored as indicated at references 1212 and 1214. If the data indicates that a tampering event might be underway then the appropriate route cautions/warnings can be raised/transmitted to the remote alert center. If the data suggests that tampering might not be occurring then the data monitoring can continue. See reference 1216 and 1218.

[0081] With continuing reference to Fig 12, in scenarios involving potential tampering (and/or otherwise), users such as vehicle owners can investigate activities associated with the vehicle. See reference 1220. Of course, they can take appropriate actions such as placing various drivers, vehicles, etc. under surveillance. Method 1200 can repeat in whole or in part as indicated at reference 1222.

[0082] Fig. 13 illustrates a computer for use in fuel anti-theft systems. Indeed, the computer 1306 could host an application 1330 for presenting the GUI 1100 (and processing the associated data) at the remote alert center. In some cases, the controller 330 could include some or all of the components of the computer 1306 although the controller 330 could be implemented in analog hardware, firmware, ASICs (application specific integrated circuits), RISC (reduced instruction set integrated circuits), etc.

[0083] At this juncture a few words might be in order about the computer(s) 1306 and/or other systems, apparatus, etc. used to design, store, host, recall, display, transmit, receive, etc. programs, applications, controllers, algorithms, routines, codes, GUIs, etc. of fuel anti-theft systems of embodiments. The type of computer 1306 used for such purposes does not limit the scope of the disclosure but certainly includes those now known as well as those which will arise in the future. But usually, these computers 1306 will include some type of display 1308, keyboard 1310, interface 1312, processor 1314, memory 1316, and bus 1318.

[0084] Indeed, any type of human-machine interface (as illustrated by display 1308 and keyboard 1310) will do so long as it allows some or all of the human interactions with the computer 1306 as disclosed elsewhere herein. Similarly, the interface 1312 can be a network interface card (NIC), a WiFi transceiver, an Ethernet interface, etc. allowing various components of computer 1306 to communicate with each other and/or other devices. The computer 1306, though, could be a stand-alone device without departing from the scope of the current disclosure.

[0085] Moreover, while Fig. 13 illustrates that the computer 1306 includes a processor 1314, the computer 1306 might include some other type of device for performing methods disclosed herein. For instance, the computer 1306 could include a microprocessor, an ASIC (Application Specific Integrated Circuit), a RISC

(Reduced Instruction Set IC), a neural network, etc. instead of, or in addition, to the processor 1314. Thus, the device used to perform the methods disclosed herein is not limiting.

[0086] Again with reference to Fig. 13, the memory 1316 can be any type of memory currently available or that might arise in the future. For instance, the memory 1316 could be a hard drive, a ROM (Read Only Memory), a RAM (Random Access Memory), flash memory, a CD (Compact Disc), etc. or a combination thereof. No matter its form, in the current embodiment, the memory 1316 stores instructions which enable the processor 1314 (or other device) to perform at least some of the methods disclosed herein as well as (perhaps) others. The memory 1316 of the current embodiment also stores data pertaining to such methods, user inputs thereto, outputs thereof, etc. At least some of the various components of the computer 1306 can communicate over any type of bus 1318 enabling their operations in some or all of the methods disclosed herein. Such buses include, without limitation, SCSI (Small Computer System Interface), ISA (Industry Standard Architecture), EISA (Extended Industry Standard Architecture), etc., buses or a combination thereof. With that having been said, it might be useful to now consider some aspects of the disclosed subject matter.

[0087] Fig. 14 schematically illustrates a fuel anti-theft system. More specifically, Fig. 14 illustrates a fuel anti-theft system 1400, a control unit 1402, line sensors 1418, an identifiable sensor 1420, an identifiable sensor 1422, a microcontroller 1430, jacks 1432, a pull-up resistor 1434, a GPS Tracker 1436, and a GPS application 1438. The fuel anti-theft system 1400 of the current embodiment can be used where certain routine activities might appear to be theft-events thereby triggering false alarms. For instance, fuel caps and fuel filters are more routinely opened/replaced than other components in typical fuel systems.

[0088] Activations of the fuel cap and fuel filter identifiable sensors 1420 and 1422 are typically more routine than activation of other sensors such as the line sensors 1418. Thus, users might want to respond to activation of the identifiable sensors 1420 and/or 1422 differently than activation of the line sensors 1418 (and/or even each other).

[0089] The fuel anti-theft system 1400 shown in Fig. 14 produces different, identifiable resistance changes as sensed at the input to the control unit 1802. The resistor values used for the fuel cap identifiable sensor 1420 (5.1 kohm) and the fuel filter identifiable sensor 1422 (3.3 kohm) are different from each other and the line sensors 1418 (10 kohm) in the fuel anti-theft system 1400. The control unit 1402 of the current embodiment will detect a unique resistance change value for each sensor type and take appropriate action to notify users of the activation.

[0090] Note that these differing resistance changes can be determined with reference to the following equations and/or Table 2. Note also that while the foregoing resistance values were selected to be different enough to produce readily discernible network resistance changes, other resistance values could be used.

$$1/R_{\text{secure}} = 1/R_{\text{fuelcap}} + 1/R_{\text{fuelfilter}} + n \cdot 1/R_{\text{fuellinesensor}}$$

Where:

R_{secure} is the expected, overall resistance of the sensor network,

$R_{\text{fuelfilter}}$ is fuel filter sensor resistance (3.3 Kohm)

R_{fuelcap} is fuel cap sensor resistance (5.1 Kohm)

$R_{\text{fuellinesensor}}$ is fuel line sensor resistance (10 Kohm)

n is the pre-selected number (usually 8 sensors)

TABLE 1

<u>Disconnected Sensors(s)</u>	<u>Network resistance (k-ohm)</u>
None	0.77
Fuel Cap	0.9
Fuel Filter	1.004
1 Fuel Line	0.83
2 Fuel Line	0.91
3 Fuel Line	1
4 Fuel Line	1.11
5 Fuel Line	1.25
6 Fuel Line	1.43
7 Fuel Line	1.67
8 Fuel Line	2

[0091] Fig. 14 also illustrates that the microcontroller 1430 (and/or control unit 1802) could include jacks 1432 for convenient connection/disconnection of the various wires, cables, etc. in the system to these devices. In the alternative, or in addition, one or more of these cables could be hardwire to the control unit 1402 and/or microcontroller 1430.

[0092] Further still, Fig. 14 also illustrates that the control unit 1402 can pass a signal to the GPS tracker 1436/GPS application 1438 indicative of whether the fuel system appears to be secure, potentially tampered with, or in some routine condition. The GPS application 1438 can be configured to record the location of the fuel system (or vehicle) when that signal changes and/or can send a corresponding message to various users upon such changes. If desired, the GPS application 1438 can be configured to send a more or less continuous signal so that the sensed state of the

system is known at all times. Furthermore, the GPS application can be configured with a user interface (such as, a graphical user interface) which allows users to create their own rules for responding to alerts. For instance, a user could configure the GPS application to automatically disable the ignition circuit of the vehicle if an alert indicates that fuel theft might be occurring (or has occurred).

[0093] Fig. 15 illustrates a fuel anti-theft control unit. The fuel anti-theft control unit 1502 of the current embodiment includes a series of jacks 1532 for connecting the sensors of the network to it. It also includes several indicators 1518, 1520, and 1522 corresponding to the line sensors 1518 and identifiable sensors 1520 and 1522. The control unit 1502 can also include an indicator 1524 configured to be activated should more than one sensor be activated.

[0094] Figs. 16 and 17 illustrate a fuel line sensor. The fuel line sensor 1600 of the current embodiment can be installed around compression fittings (or other components) on vehicle fuel lines. In the event that the fuel line sensor 1600 is uninstalled to allow access to the fitting (or otherwise tampered with), the internal electrical connection to the vehicle ground will be broken (or destroyed), and the microcontroller of the current embodiment will detect the change of state and will send an alert.

[0095] Furthermore, Fig. 16 illustrates that the fuel line sensor 1600 can be secured to various components via a dual strap cable tie 1602 (or cable ties, zip ties, zip locks, etc.). Fig. 16 also shows that the fuel line sensor 1600 also includes a circuit enclosure 1604 and a signal wire connector 1606 and defines a signal wire hole 1608.

[0096] While Fig. 16 illustrates the fuel line sensor 1600 in an uninstalled condition, Fig. 17 illustrates it as being installed on a compression fitting nut 1710 and with a signal wire 1712 connected thereto via the signal wire hole 1608/signal wire

connector 1606. Note that the dual strap cable tie 1602 has been pulled snug against the compression fitting nut. 1710.

[0097] Fig. 18 illustrates a fuel cap sensor. The fuel cap (identifiable) sensor 1800 of the current embodiment can be installed on various fuel caps. The fuel cap sensor 1800 can be secured to the fuel cap 1802 via an adhesive while the circuit enclosure 1804 can be secured to the fuel tank 1806 by an adhesive too. In the event that the fuel cap sensor 1800 is unplugged to allow access to the fuel tank 1806, the circuit for that sensor is broken and an alert is sent. When the fuel cap sensor 1800 is uninstalled (or removed by force or otherwise tampered with) it destroys its electrical connection to the vehicle ground. The microcontroller of the current embodiment detects the change of state and an alert is sent.

[0098] Note that Fig. 18 also illustrates a cap-side circuit enclosure 1808 and the two halves of a quick disconnect 1810 of the fuel cap sensor 1800. Further, the tank-side or base circuit enclosure 1804 defines or includes a signal wire attachment point 1812.

[0099] In some embodiments fuel/cargo anti-theft systems include digital sensors which transmit their unique IDs or codes wirelessly to appropriately configured controllers. If the sensor detects that it has been tampered with, removed from the system, etc., it stops transmitting its ID. Of course, the controller of the current embodiment periodically checks for the presence of recent/contemporaneous transmissions of the IDs associated with its sensors. Should one or more appear to be missing such controllers could then raise an alarm (for instance, turn on a light, buzzer, speaker, klaxon, etc.), alert, send a text message to the control center, send an email to a particular person, mobile or computing device, cellular phone, etc. The controllers could also, or in the alternative, record the location, time, and (if

instrumented appropriately), record conditions in/near the vehicle including temperature, atmospheric pressure, humidity, etc.

[00100] Furthermore, some embodiments provide fuel/cargo anti-theft systems which are configured to consume little power. These systems, therefore, can operate on various vehicles for extended periods of time. Systems of the current embodiment can be configured to operate on low voltages and/or with limited current flow such that they meet intrinsically safe requirements for various hazardous locations as defined by such documents as the National Electric Code of the United States. In some embodiments, anti-theft systems are provided in a software as a service (SaaS) form on a web server and/or database server. Thus, in some embodiments, no application need exist on the vehicle and/or in the field.

[00101] Controllers of various embodiments condition the signal(s) which they sense from the various sensors in communication therewith. For instance, it might be desirable to filter the signal so that noise on the circuit will not appear to be a potential case of tampering. For instance, a 6 second, time-series filter can be applied to the signal before controllers of the current embodiment sense/respond to the signal. In this manner, false alarms can be reduced if not eliminated. But other more/less complex signal conditioning can be applied to the signal without departing from the scope of the current disclosure.

[00102] Embodiments provide fuel anti-theft systems, sensors, controllers, etc. which allow for the monitoring of vehicle fuel systems for potential tampering and/or fuel theft. Some such systems allow for discreet, unobtrusive, and potentially unsuspected fuel system monitoring. In some embodiments, the sensors, controllers, systems, etc. are reliable, rugged, and relatively inexpensive to install and/or operate. Systems of some embodiments allow users to investigate potential fuel-theft events

remotely and to implement corrective actions. Now with reference to Figs. 19 to 25, it might be helpful to disclose aspects of cargo anti-theft protection systems.

[00103] Fig. 19 illustrates a cargo anti-theft system. Generally, Fig. 19 shows the cargo anti-theft system installed on a cargo vehicle. It allows an owner or other interested user to monitor the status of cargo on vehicles even in remote locations. And should some apparent tampering occur, the system alerts that user of the potential that someone might be attempting to steal cargo or otherwise tamper with it. More specifically, Fig. 19 illustrates a system 1900, a vehicle 1902, a cargo compartment 1904, a cab 1906, an access point 1908, a controller 1910, a geo-positioning circuit 1912, at least one lock 1914, a cargo switch 1916, and its switch halves 1918 and 1920.

[00104] As to the vehicle 1902, the particular vehicle 1902 illustrated by Fig. 19 happens to be a fuel truck. However, it could be a trailer, a semi-trailer, a “cube” truck, a delivery van, a ship, a boat, an airplane, etc. However, it does include or define a cargo compartment 1904 which often holds cargo and frequently confines the cargo therein. Indeed, the cargo compartment 1904 (or the structure(s) defining it) often shield the cargo from the elements, damage during shipment, tampering, theft, and the like. For instance, in many trucks, vans, etc. the cargo compartment 1904 lies within a series of walls/panels of the vehicle 1902 such as floors, roofs/ceilings, hulls, fuselages, bulkheads, etc.

[00105] Moreover, the vehicle 1902 often comprises two or more distinct parts such as a trailer (which might define the cargo compartment) and a cab, tractor, bridge, cockpit, etc. In many scenarios, the cab hosts a user who drives, operates, navigates, controls, etc. the vehicle 1902. That user also frequently has duties pertaining to loading cargo onto the vehicle 1902 (and/or unloading it). Thus, while not always the case, the user has access to the entire vehicle 1902 including the cargo

compartment 1904, the cab 1906, and/or the cargo itself. Of course, third parties might also attempt to gain access to the cargo compartment 1904, the cargo therein, and/or the cab 1906 for perhaps nefarious and/or malicious purposes. And, in part, the cargo compartment 1904 is often protected with locks on its various access points 1908 to prevent or at least hinder such unauthorized access.

[00106] As further disclosed elsewhere herein, the cab 1906 usually contains controls and/or instruments to aid the user in operating the vehicle. And it can contain various components of the system 1900 such as the controller 1910 and/or geo-positioning circuit 1912. Of course, one or more of these components can be mounted on the roof of the cab 1906 and/or the cargo compartment 1904 to, for instance, provide its antenna (if it has one) access to electromagnetic signals that might otherwise be shielded by the structure of the vehicle 1902. Of course the cab 1906 can be protected from unauthorized access by locks and the like as well to protect these components and other objects in the cab 1906. Note that components mounted outside of the cargo compartment 1904 and cab 1906 can be somewhat hidden by being camouflaged or placed in inconspicuous locations. For instance, many vehicles 1902 are tall enough that a component mounted on top of the vehicle 1902 might not be noticed by the user and/or third parties who might be unaware of the presence of the system 1900.

[00107] The access point 1908 takes on various configurations and the one shown in Fig. 19 happens to be a valve box for a fuel truck. This valve box contains valves which are in communication with the fuel in the truck (i.e., the cargo) and load/unload ports, couplings, etc. In other instances, the access point 1908 could be a door, hatch, manway, etc. And, of course, the access point 1908 will usually reflect the nature of the cargo and/or the vehicle 1902 whether the cargo is solid, liquid, gaseous, packages, granular, bulk material, money, etc.

[00108] With continuing reference to Fig. 19, the controller 1910 performs certain functions and/or communicates with various other components of the system 1900 to do so. For instance, the controller 1910 can sense the position, state, and/or condition of the cargo switch 1916 and from that information infer whether or not an attempt to access the cargo compartment 1904 might be underway. It can also send a signal indicative of the position of the cargo switch 1916 to the geo-positioning circuit 1912. Moreover, it can store a PIN (Personal Identification Number) associated with the openings and/or closings of the cargo switch 1904 and determine whether the cargo switch 1916 has been opened/closed in a pattern corresponding to that PIN. If it has, then the controller 1910 can send a signal to the geo-positioning circuit 1912 that an authorized entry (or access) to the cargo compartment 1904 is underway. If the pattern fails to match the PIN, then the controller 1910 can signal the geo-positioning circuit 1912 accordingly. For instance, should the PIN be 3124, a user would open and close the cargo switch 3 times taking a pre-selected amount of time between opening/closing the switch, pause for another pre-selected (and perhaps longer) time, open/close the switch once, wait, open/close the switch twice, wait, and open/close the switch 4 more times to enter that PIN. In some embodiments, the controller 1910 stores (or retrieves from a remote control center over the Internet or other telecommunications system) a list of PINs and, each time one is used, it deletes the used PIN. It then loads another PIN from the list to be the next active/correct PIN. In this way, users can signal the system 1900 that they have authority to access the cargo compartment 1904 once (or a pre-determined number of times) without triggering an alarm (but perhaps causing the transmission of an authorized access signal).

[00109] In the alternative, or in addition, PINs can be time-based. In other words, each digit of the pin can indicate how long the user should hold the cargo switch 1916 in the open/mated and closed/de-mated positions. For instance, suppose

the PIN is 315. To signal the controller that an authorized cargo access is imminent, the user would open the switch, then close it for 3 seconds. The user would then close the switch for a (1) second and close it for 5 seconds. Upon the end of the 5 second period the user would open the switch and access the cargo without setting off an alarm. Although the controller 1910 could log the event and send a signal indicative thereof.

[00110] The controller 1910 can also control the lock(s) 1914 via encoded communications if desired. Indeed, if an authorized entry appears to be under way (as sensed via the PIN for instance) the controller 1910 can send a signal to the lock 1914 to open. The lock is typically installed inside the cargo bay making it inaccessible from outside and therefore making tampering with it difficult. Of course, the controller can also lock the lock 1914 in other scenarios. For instance, the default, loss-of-power, and/or fail-safe state of the signal and/or the lock could be in the locked state. In some embodiments, the controller 1910 could also receive an override signal to unlock the lock from a remote control center (and perhaps over a telecommunications system). Furthermore, the controller 1910 of embodiments can receive from the geo-positioning circuit 1912 a signal indicating whether the system 1900 is in a geozone wherein entry can be deemed either authorized or unauthorized. Thus, the system 1900 can establish, maintain, sense, etc. whether the vehicle 1902 is in a location where access to the cargo compartment 1904 is authorized. Those locations can correspond to expected/scheduled destinations for the vehicle and/or cargo. Again, if access is attempted in a location other than an authorized geolocation then the controller 1910 can raise an alarm. In this manner, and/or others, the system 1900 can create “geofences” around legitimate access areas.

[00111] Of course, it might happen that a legitimate but unauthorized attempt might be made to access the cargo compartment 1904. For instance, the vehicle 1902

might be stopped by law enforcement such as the highway patrol, police, an immigration service, an alcoholic beverage control agency, a firearms agency, a customs officer, etc. In which case, the operator might be ordered to open the cargo compartment 1904 for inspection and/or search. In such cases the operator can obtain a PIN from the control center (or have one memorized or otherwise available) and obtain authorization in that or a similar manner. Likewise, unscheduled maintenance might cause the operator to legitimately need access to the cargo compartment and the PIN can allow for that. And, of course, many other situations might arise where such access is legitimately needed. In such cases the controller 1910 can still report that access occurred for subsequent follow up by interested users.

[00112] In addition, the controller 1910 can be in communication with a battery to receive and/or distribute power to the system 1900. That battery, moreover, could be an internal battery. Of course, the controller 1910 could receive power from the vehicle 1902, a solar panel 1930 (whether on the controller or external), a battery, or some other power source. However, that might not always be the case. For instance, when the controller is located in the cargo compartment 1904, vehicle power might not be available because the cab 1906 is no longer present. Or vehicle power could fail. Thus, it might be the case that the controller 1910 loses power and is consequently unpowered. In such instances, the geo-positioning circuit 1912 can detect the loss of the controller 1910 via the lack of signals coming from the controller and report that the controller is no longer powered and/or present. It can also report the location at which it currently resides to the control center. Thus, follow up activities can determine whether a mere power failure occurred, whether the controller was tampered with, destroyed, disabled, removed, etc. Moreover, in such situations, it will be known where the geo-positioning circuit 1912 (and presumably the vehicle 1902) was at the time of the incident and perhaps afterward as well.

[00113] Note also that the controller 1910 can communicate with the control center directly over its own telecommunications link (for instance, a cellular telephony link). It can also, or instead, be configured to communicate therewith via the geo-positioning circuit 1912. And, in some embodiments, it can be configured to do both. Moreover, while some embodiments provide for hard wired communications/connections with the various other components of the system 1900, that need not be the case. For instance, the entire system 1900 or select components thereof could communicate with each other via WiFi, infrared, RFID, Bluetooth, Zigbee®, etc. technology.

[00114] With ongoing reference to Fig. 19, the system 1900 happens to be shown installed as individual components. However, some or all of them can be combined into an integrated box or component. For instance the controller 1910 (with or without battery) and the geo-positioning circuit 1912 can be mounted inside a rugged electronics enclosure to prevent/hinder users from tampering with the same. That enclosure can be mounted and/or mechanically coupled to the vehicle 1902 inside an access-controlled volume such as the cargo compartment 1904 or cab 1906 for further, or alternate protection from tampering, damage, and/or the like. Indeed, it can be installed in the volume it is to monitor. The mounting can also be by way of special fasteners, welding, riveting, etc. so that attempts to open the enclosure would be readily apparent upon inspection or otherwise.

[00115] Fig. 20 illustrates another cargo anti-theft system. This system 2000 happens to be installed on a trailer. Fig. 20 also illustrates various components of the system 2000 including a cargo compartment 2004, an access point 2008, a controller 2010, a geo-positioning circuit 2012, a lock 2014, a switch valve 2018, and a camera 2022. Other sensors such as temperature, humidity, pressure, light, vibration, precipitation, etc. sensors could be included in the system to provide information

regarding the cargo and/or its environment. The cargo compartment 2004 is located in the bay of the trailer and the access point 2008 is the pair of doors at one end of that trailer. These doors are usually configured such that one overlaps the other making it necessary to open that door first and then the other door. One door typically includes a manually lockable handle and/or hardware to mount a separate lock in such a way as to secure the doors. But, other types of doors and/or access points are within the scope of the current disclosure.

[00116] Moreover, the controller 2010 of the current embodiment is shown as a separate component. But again, it could be integrated with other components notably the geo-positioning circuit 1912 and/or the lock. It is also shown mounted on a side wall of the trailer although it could be mounted on the floor, in a “mother’s attic” (for moving vans), on the roof, underneath, etc. if desired. In the current embodiment, the geo-positioning circuit 2012 is mounted on the roof of the trailer and is also secured to the trailer in a manner that would make attempts to tamper with and/or remove it detectable as disclosed elsewhere herein. Its location also provides it with a relatively good vantage point at which it can send/receive signals to/from a telecommunications system and/or a geo-positioning system. Its location also shields it from casual observation by those who might not be aware of the presence of the system 2000.

[00117] The lock 2014 of the current embodiment is a solenoid-bolt-operated lock although other types of locks are within the scope of the disclosure. For instance, a DC motor, stepper motor, or other actuation device could drive the lock. And, of course, it could be spring loaded or otherwise biased into a default position such as the locked position. The lock 2014 of the current embodiment could be provided with the system 2000 although pre-existing locks could be wired into the system if desired. Moreover, it is shown as being mounted on the second-opening door of the trailer and inside thereof although that need not be the case. This position, though, would almost

force an unauthorized user to somehow open the first-opening door and then at least partially enter the cargo compartment 2004 before they could tamper with the lock 2014. Nonetheless the lock 2014 could include or be outfitted with a position indicator or switch so that the controller 2010 could sense an unexpected (or otherwise) movement of the lock 2014 and/or its bolt. Should that event occur (for instance, the switch or other bolt status sensor indicates un-commanded movement), the controller 2010 could be configured to send a command to the lock 2014 to try to lock itself and could send a signal to the geo-positioning circuit 2012 (and/or control center) indicative of the event.

[00118] Systems of some embodiments rely on the manual lock ordinarily supplied on the doors of most vehicles. The system includes a locking pin sufficiently strong that attempts to force the lock do not damage it enough that it would not be likely to release or break. In such embodiments, the controller would operate the locking pin with the user supplying the force to open the manual lock. Thus, instead of developing enough power to overcome the friction, inertia, etc. associated with the manual lock, the controller would produce enough power to operate the relatively smaller locking pin.

[00119] Fig. 20 also shows one half of a cargo switch or a switch halve 2018. Another switch halve of the current embodiment is located on the other side of the truck and/or door although it is not visible in Fig. 20. The switch halves 2018 can be fashioned from and/or mechanically coupled to a sturdy cable such as one made of stranded metal or some other material resistant to cutting, burning, snapping, and/or other forms of destructive activity that might somehow sever it. Of course the cable could be replaced with or augmented with a sturdy bar, rod, etc. in various embodiments. Moreover, the cables can be of a length sufficient to reach across the access point 2008 with minimal slack. The switch halve 2018 can also include (or be

connected to) a wire (or some wireless transmitter) so that the controller 2010 can sense the state of the switch (the two halves in combination). The switch sensing mechanism may include: RFID sensors, infrared sensors, proximity sensors, Hall effect sensors, optical sensors, etc. Note that one switch half 1218 would be a male component and the other would be a female component in embodiments so that the two halves can be drawn together and mated. Since the switch halves are mechanically coupled to opposite sides of the access point 2008, doing so would necessarily involve closing the doors and any opening of the doors (absent significant structural damage thereto) would necessarily involve disconnecting, de-mating, or otherwise separating the two switch halves 1218. That action could be sensed by the controller 2010 thereby raising an alarm or at least sending an appropriate signal to the geo-positioning circuit 2012 and/or control center.

[00120] System 2000 of the current embodiment also includes the camera 2022 and could include additional cameras. The camera can be positioned to view the access point 2008 and/or other locations at which users (including authorized and unauthorized) users and/or third parties might attempt access/entry into the cargo compartment 2004. Moreover, a camera 2022 could be positioned on the outside of the trailer with a view of the surrounding environment. Further still, a camera 2022 could be positioned in the cab and/or with a view of the cargo. These cameras can be mounted securely so that tampering with them would be evident as with other components of system 2000. These cameras 2022 can also be configured to communicate with the controller 2010 and/or geo-positioning circuit 2012 by various means as disclosed elsewhere herein. They can also be configured to communicate with the control center via a telecommunications network such as a cellular telephony system.

[00121] In some embodiments, the controller 2010 could be configured to generate a signal upon detection of an unusual event that would cause the cameras 2022 to capture an image of the scene they view at the time of the event. The cameras could also be configured to transmit those images to the controller 2010, the geo-positioning circuit 2012, the control center etc. And, if desired, those images can be time, date, and/or location stamped and can be associated with some sort of event identifier. In some systems the cameras are light activated so that an opening of the access point would be detected via ambient light that might illuminate the cargo area. In the current embodiment, therefore, when an event and/or incident occurs, contemporaneous images of the areas near the access point, the trailer, the cab, the cargo etc. can be obtained, preserved, stored, etc. for immediate and/or subsequent review. In some instances, the cameras are activated upon signal requested from the Geo positioning circuit and/or control center. Moreover, when the controller of the current embodiment detects a change of state of the switch, it sends a signal to activate the camera(s).

[00122] Therefore, it seems likely that an image of the user, third party, perpetrator, and/or others who might be present would be obtained. Images of the state of the cargo at the time of the event might also be obtained in this way. Note that the cameras 2022 could even, or instead be activated on some (a) periodic schedule and even upon authorized entries. In systems of such embodiments, the state of the cargo would be known better than with heretofore available systems. Indeed, photos of the cargo can be obtained at the beginning of each (un)loading event and compared to determine whether the appropriate amount of cargo was (un)loaded. Moreover, the appearance of unauthorized cargo, passengers, etc. could be identified and reported.

[00123] Fig. 21 illustrates an installed anti-theft controller. The controller 2110 of the current embodiment is an integrated one with both control and geo-positioning

capabilities resident therein and it happens to be mounted securely to a sturdy vehicle panel 212 that is rugged enough to withstand likely attempts to penetrate, damage, or destroy it. Moreover, the controller (or its enclosure) has a similarly sturdy flange 2114 which defines a number of fastener holes. Fig. 21 shows several fasteners 2116 and 2118 such as bolts and nuts securing the controller 2110 to the vehicle panel 2112 by way of the flange 2114. These fasteners 2116 and 2118 can be of a type requiring specialized, rare, and/or customized tools to fasten and/or unfasten them. In that fashion (and/or other fashions) unauthorized parties without those tools would find it difficult to remove the controller 2110 from the vehicle panel 2112. Moreover, these fasteners 2116 and 2118 could be safety wired, coated, painted, etc. once installed to allow for ready detection of attempts to unfasten them from the controller 2110 and/or vehicle panel 2112. That detection would be by way of determining whether the safety wire was intact and/or the coating, paint, etc. is scratched. Thus, the current embodiment provides a controller 2110 that if tampered with would bear evidence of the same.

[00124] Fig. 22 schematically illustrates a cargo anti-theft system. The system of the current embodiment includes a controller 2210, a geo-positioning circuit 2212, a lock 2214, a cargo switch 2216, a battery 2220, a geozone input 2222, a cargo output 2224, and a cargo switch input 2226. Fig. 22 shows that the controller 2210 of the current embodiment communicates with the cargo switch 2216 and a pair of locks 2214. It is powered by a separate battery 2220 as is the geo-positioning circuit 2212. It also communicates with the geo-positioning circuit 2212 by way of three signals: the geozone input 2222, the cargo output 2224, and the cargo switch input 2226. The geo-positioning circuit generates the geozone output to indicate to the controller 2210 that the system 2200 is (or is not) in an authorized geozone. The controller 2210 senses the state of the cargo switch 2216 via the cargo switch input 2226 as does the

geo-positioning circuit. Although, one or the other of these two devices could sense it in embodiments. Moreover, Fig. 22 illustrates that the controller 2210 generates the cargo output 2224 signal which indicates that access is occurring (or has occurred) and which is sensed by the geo-positioning circuit 2212. Additionally, in the current embodiment, the controller generates a common lock control signal 2228 which it uses to control the locks 2214 although separately activated locks could be provided in embodiments.

[00125] With further reference to Fig. 22, note that many geo-positioning circuits include onboard batteries. These batteries can be selected such that they supply a longer operating period than the battery 2220 (whether internal to the controller 2210 or external). In this manner, the geo-positioning circuit can continue to operate even after the battery 2220 discharges and renders the controller 2210 inoperable. When such events occur, the geo-positioning circuit 2212 can continue reporting the geo location of the system 2200 and any data that it might be able to obtain from, for instance, the cargo switch input 2226 and/or various cameras.

[00126] Fig. 23 schematically illustrates another cargo anti-theft system. In the current embodiment, the control unit 2300 includes both fuel and cargo protection-related circuits. More specifically, the control unit 2300 includes and/or communicates with a cargo switch 2304, a resistor 2306, a lock solenoid 2308, a lock switch 2312, and a battery 2316. The cargo switch is illustrated as a pair of normally open contacts although it can be made from two switch halves as disclosed elsewhere herein. Note that the control unit 2300 senses the cargo switch 2304 through the voltage dividing variable resistor 2306 such that the voltage sensed at the control unit 2300 can be set by the user. In the current embodiment, the value of the resistor 2306 can be programmed via the control unit 2300 over a telecommunications system (for instance, by a user in the control center). Accordingly, the control unit 2300 can be

configured to generate a cargo switch-related signal if the voltage it senses at its input is incorrect (and/or off by more than some pre-determined amount). Thus, if a third party attempts to mimic the presence of a closed cargo switch at that input of the control unit 2300 with a voltage supply, the control unit 2300 is likely to detect an anomalous event and raise a corresponding signal.

[00127] Note also that the control unit 2300 senses the position of the lock via lock switch 2312. While lock switch 2312 is indicated as a switch, any type of position sensor could be used for that component. For instance, a linear resistor position indicator could be used. The control unit 2300 of the current embodiment also drives the lock solenoid 2308. Thus, it can control the (commanded) position of one or more locks. The control unit 2300 also includes an onboard battery 2316. Thus, it can operate independently of a vehicle power supply at least for some time. And, for outside mounted components, a solar panel could be provided to power such components and/or the system.

[00128] Fig. 24 illustrates a cargo switch and a pair of cab to trailer connectors. The switch halves 2402 and 2404 (of the cable switch 2400) are shown mechanically coupled to a corresponding pair of cables 2406 and wires 2408. One switch half 2402 is male while the other is female in the current embodiment. Fig. 24 also illustrates a pair of cab to trailer switch halves 2410 and 2412 one of which is male and the other of which is female. These switch halves 2410 and 2412 can be used to connect trailer-located components of various embodiments to cab-located components.

[00129] With reference again to Fig. 12, note that method 1200 can include monitoring the cargo anti-theft controllers, geo-positioning circuits, cargo switches, lock switches, cameras, systems, etc. disclosed herein. Thus, embodiments provide cargo anti-theft systems, sensors, controllers, etc. which allow for the monitoring of vehicle cargo compartment for potential tampering and/or cargo theft. Some such

systems allow for discreet, unobtrusive, and potentially unsuspected cargo monitoring. In some embodiments, the sensors, controllers, systems, etc. are reliable, rugged, and relatively inexpensive to install and/or operate. Systems of some embodiments allow users to investigate potential cargo-theft events remotely and to implement corrective actions.

CONCLUSION

[00130] Although the subject matter has been disclosed in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts disclosed above. Rather, the specific features and acts described herein are disclosed as illustrative implementations of the claims.

CLAIMS

What is claimed is:

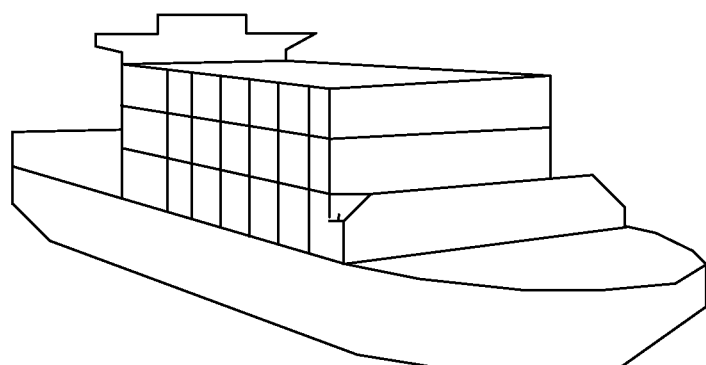
1. A cargo anti-theft protection controller comprising:
 - a cargo switch input configured to sense a ground of a cargo vehicle through a cargo switch;
 - an output configured to be in communication with an electronically operated lock;
 - and
 - a circuit in communication with the input and the output and being configured to detect an opening of the cargo switch via a pre-selected voltage at the cargo switch input and, responsive thereto, to activate the lock via the output;
 - wherein the cargo switch to be mechanically coupled to a cargo access point on the cargo vehicle in such a manner that the cargo access point cannot be opened without opening the cargo switch.
2. The controller of claim 1 further comprising a geo-positioning output in communication with the circuit, the circuit being further configured to output a signal indicative of the opening of the cargo switch via the geo-positioning output.
3. The controller of claim 1 further comprising a geo-zone input and being further configured to output a signal via the output to unlock the lock only in pre-selected geo-zones.
4. The controller of claim 1 wherein the pre-selected voltage differs from 12 VDC.

5. The controller of claim 1 further comprising a user input configured to accept a user-selected voltage, the controller being further configured to change the pre-selected voltage to the user-selected voltage.
6. The controller of claim 1 wherein the controller is further configured to sense a PIN (personal identification number) associated with openings and closings of the cargo switch.
7. The controller of claim 1 further comprising a mechanical coupler configured to securely couple the controller to the cargo vehicle.
8. The controller of claim 1 further comprising a lock position input and wherein the controller is further configured to sense a position of the lock via the lock position input and to sense whether the lock position input is electronically open.
9. The controller of claim 8 further wherein the controller is further configured to output a signal indicative that the lock should lock responsive to the position of the lock.
10. The controller of claim 1 further comprising a battery configured to power the controller.
11. The controller of claim 1 wherein the controller is further configured to change a PIN (Personal Identification Number) associated with openings and closings of the cargo switch.

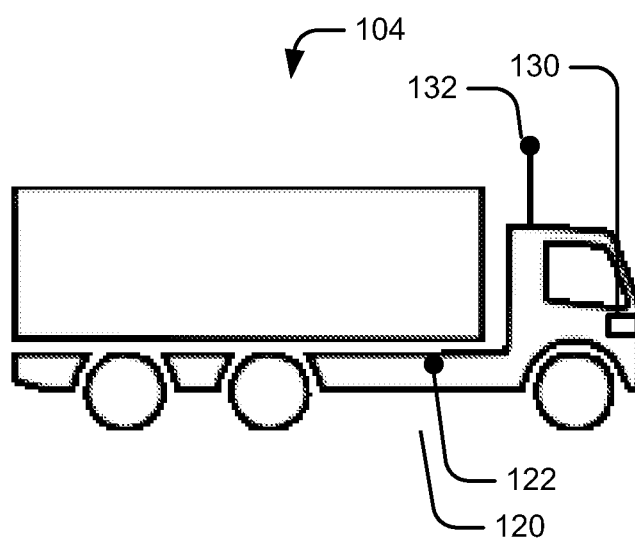
12. An anti-theft protection system comprising:
- a controller further comprising,
 - a cargo switch input configured to sense a ground of a cargo vehicle through a cargo switch;
 - an output configured to be in communication with an electronically operated lock;
 - and
 - a circuit in communication with the input and the output and being configured to detect an opening of the cargo switch via a pre-selected voltage at the cargo switch input and, responsive thereto, to activate the lock via the output;
 - a cargo switch in electrical communication with the cargo switch input;
 - an electronically operated lock in communication with the output; and
 - a mechanical coupling wherein the cargo switch is mechanically coupled to a cargo access point on the cargo vehicle in such a manner that the cargo access point cannot be opened without opening the cargo switch.
13. The system of claim 1 further comprising a geo-positioning output in communication with the circuit, the circuit being further configured to output a signal indicative of the opening of the cargo switch via the geo-positioning output.
14. The system of claim 1 further comprising a geo-zone input and being further configured to output a signal via the output to unlock the lock only in pre-selected geo-zones.
15. The system of claim 1 wherein the pre-selected voltage differs from 12 VDC.

16. The system of claim 1 further comprising a user input configured to accept a user-selected voltage, the controller being further configured to change the pre-selected voltage to the user-selected voltage.
17. The system of claim 1 wherein the controller is further configured to sense a PIN (personal identification number) associated with openings and closings of the cargo switch.
18. The system of claim 1 further comprising a mechanical coupler configured to securely couple the controller to the cargo vehicle.
19. The system of claim 1 further comprising a lock position input and wherein the controller is further configured to sense a position of the lock via the lock position input.
20. A method of protecting cargo comprising:
- sensing a ground of a cargo vehicle through a cargo switch;
 - using a circuit in communication with the cargo switch to detect the opening of the cargo switch via a pre-selected voltage;
 - responsive thereto, and using the circuit, activating a lock positioned at a cargo access point on the cargo vehicle;
 - wherein the cargo switch is mechanically coupled to the cargo access point in such a manner that the cargo access point cannot be opened without opening the cargo switch;
 - outputting a signal indicative of the opening of the cargo switch to a geo-positioning circuit in communication with the circuit;
 - sensing a PIN (personal identification number) associated with openings and closings of the cargo switch.

FIG. 1



110 →



104
132 130
122 120

FIG. 1
(Cont'd)

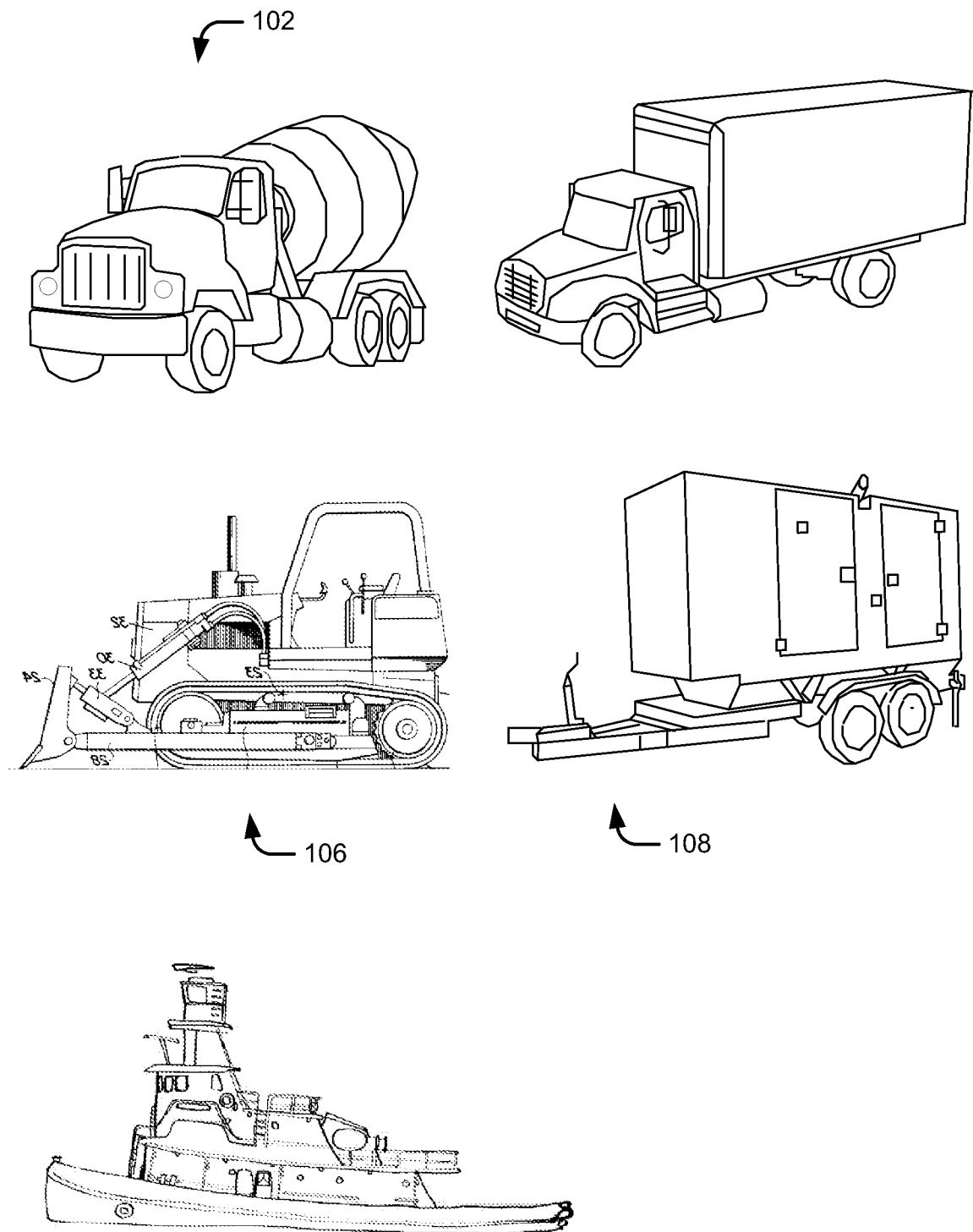
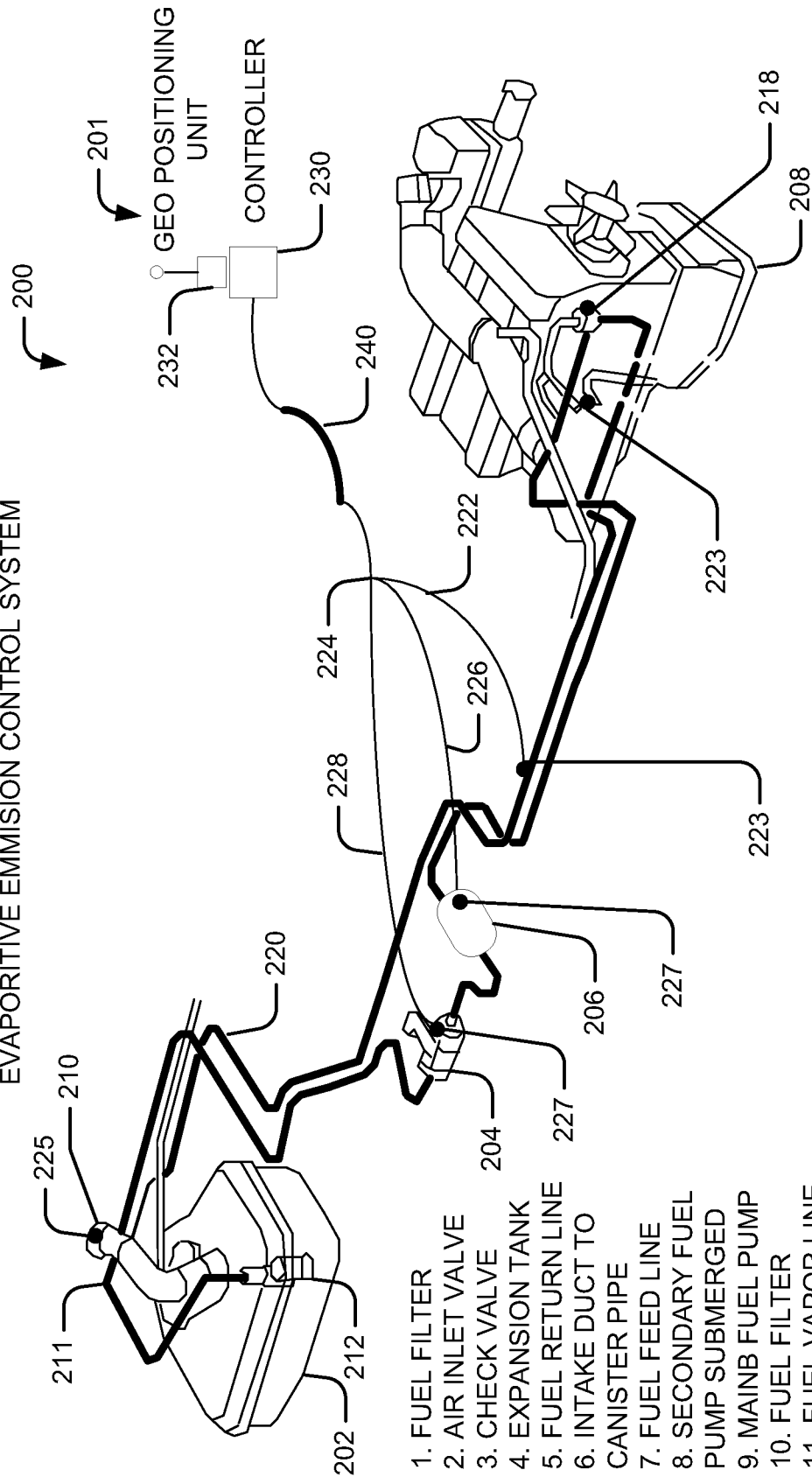


FIG. 2**EVAPORATIVE EMISSION CONTROL SYSTEM**

1. FUEL FILTER
2. AIR INLET VALVE
3. CHECK VALVE
4. EXPANSION TANK
5. FUEL RETURN LINE
6. INTAKE DUCT TO CANISTER PIPE
7. FUEL FEED LINE
8. SECONDARY FUEL PUMP SUBMERGED
9. MAINB FUEL PUMP
10. FUEL FILTER
11. FUEL VAPOR LINE
12. CANISTER
13. CANISTER TO PLENUM CHAMBER PIPE
14. OIL SEPARATOR
15. FUEL PRESSURE REGULATOR

FIG. 3

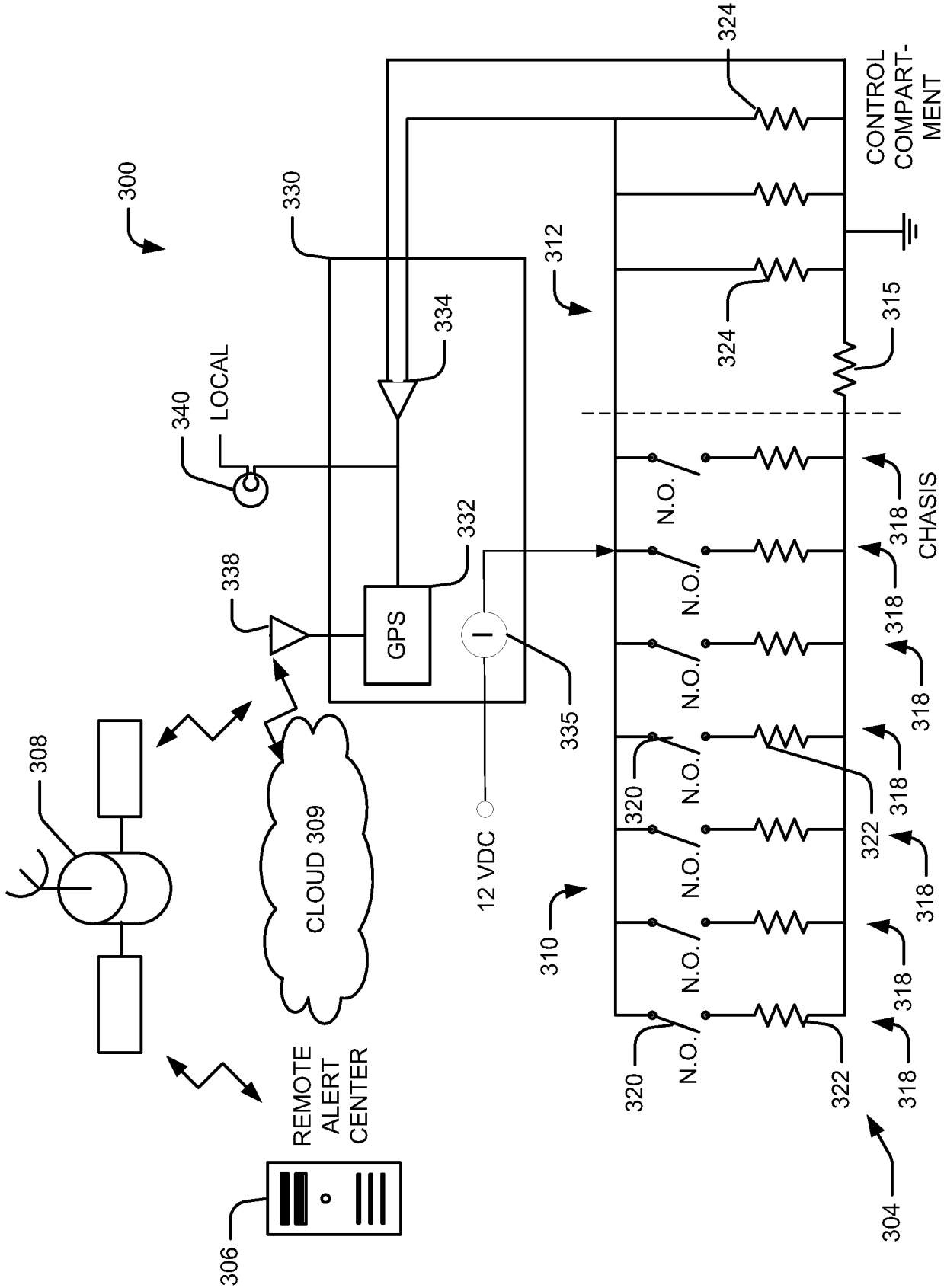


FIG. 4

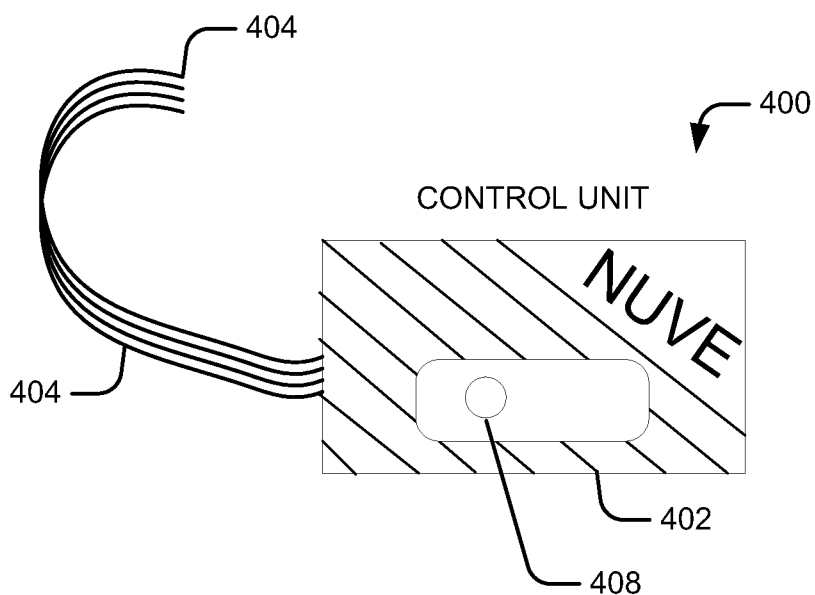


FIG. 5

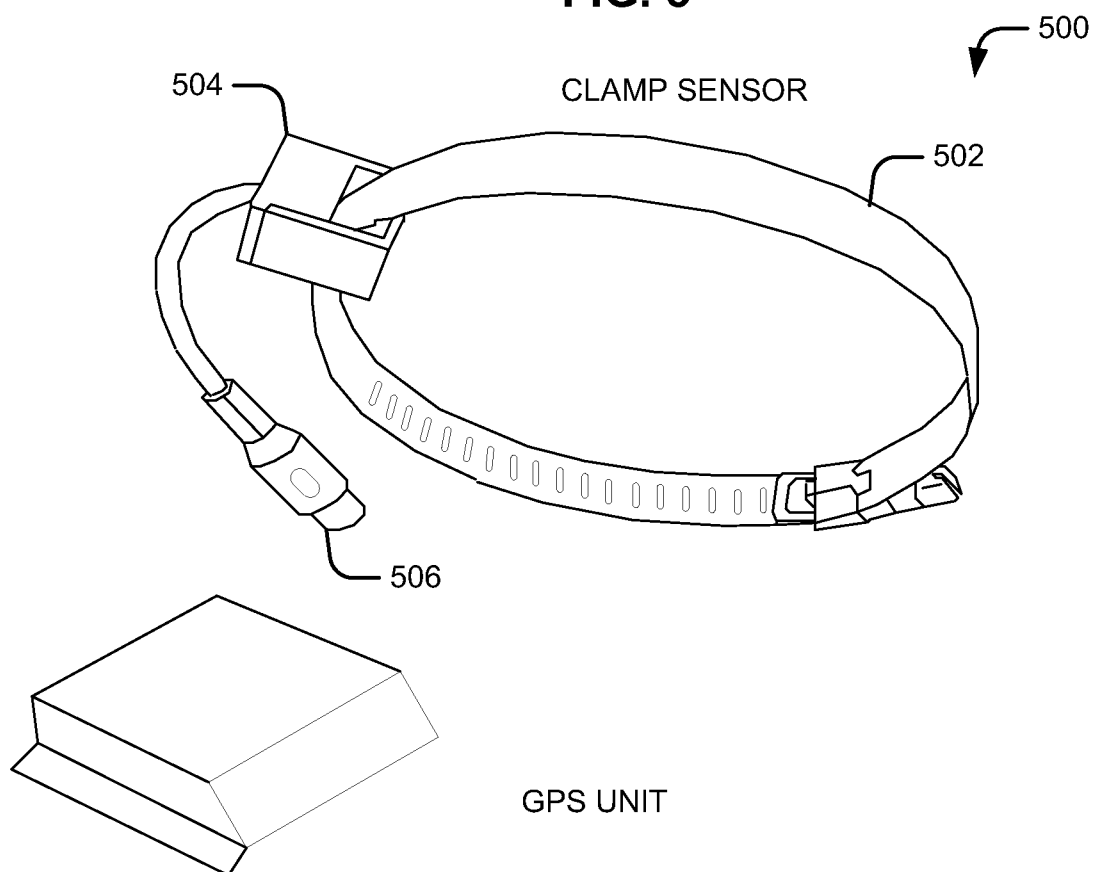


FIG. 6

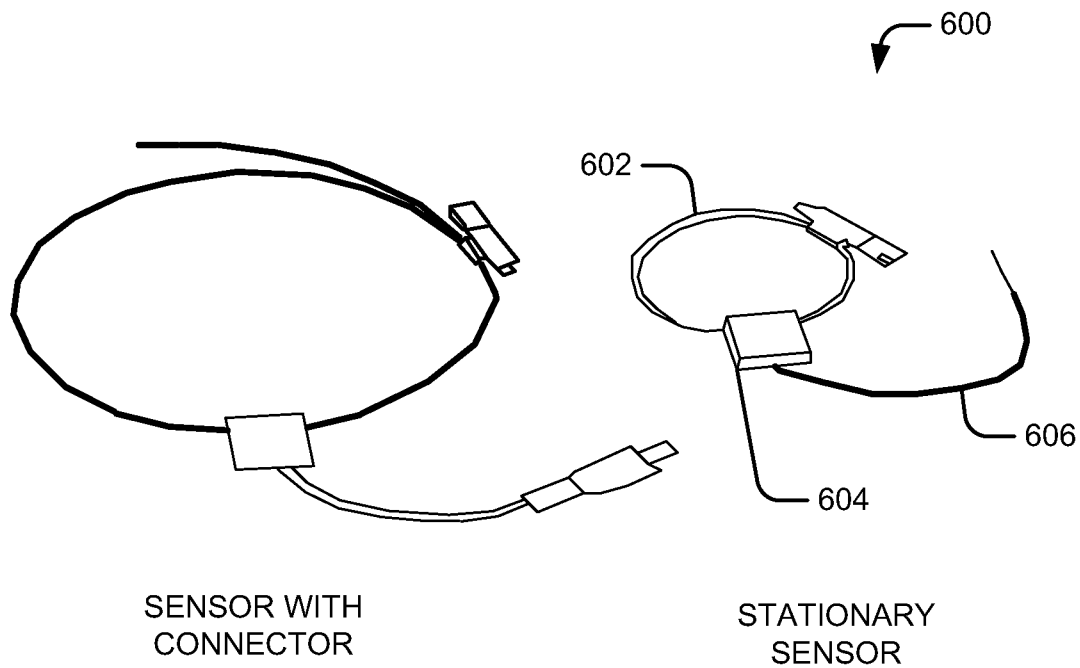
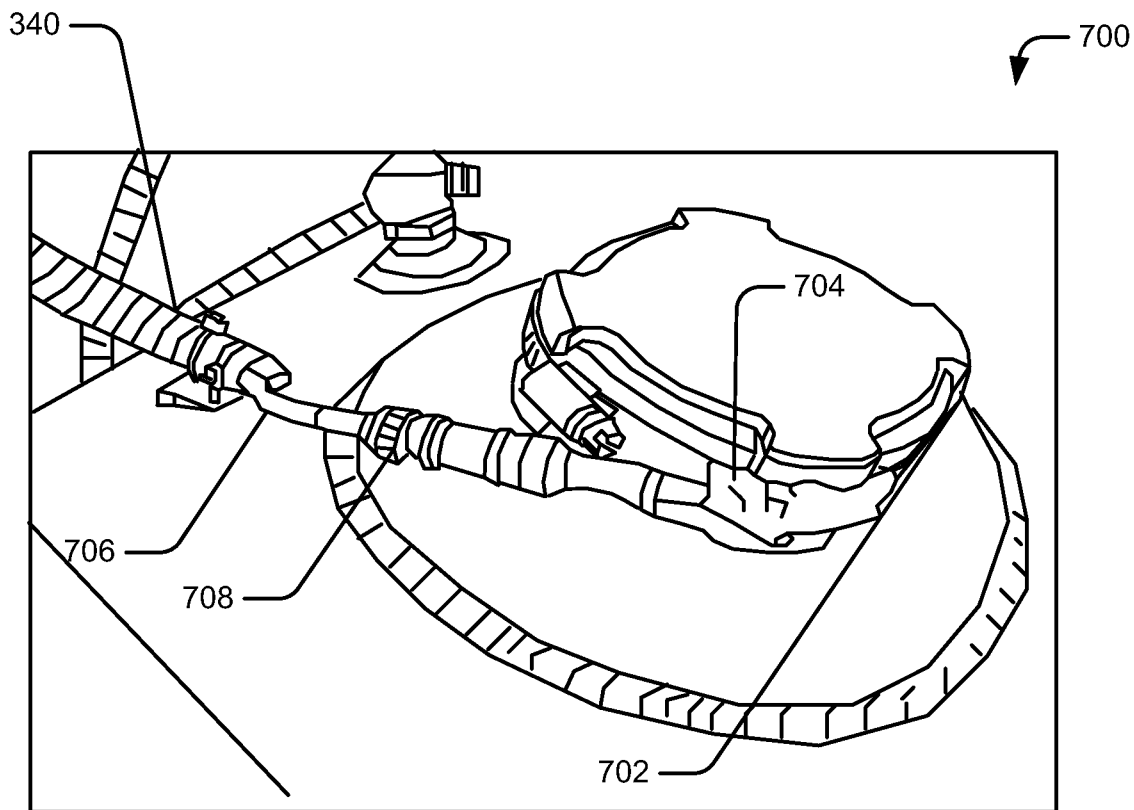
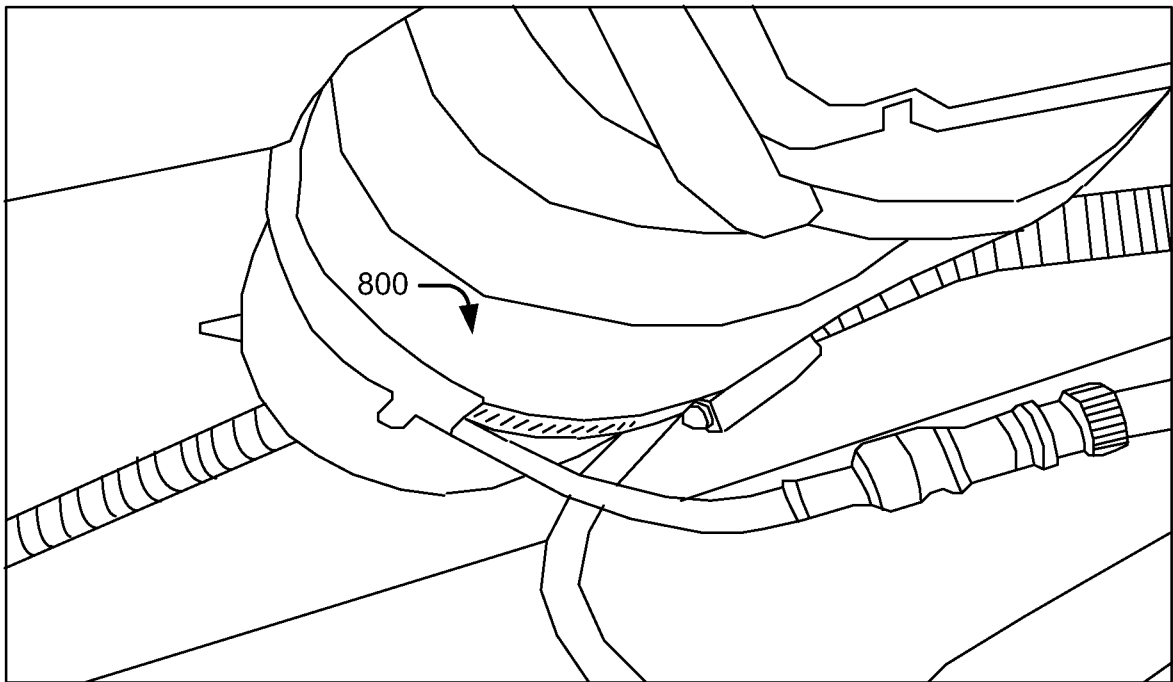


FIG. 7



SENSOR INSTALLED ON FUEL CAP

FIG. 8



SENSOR INSTALLED ON FUEL FILTER

FIG. 9

900

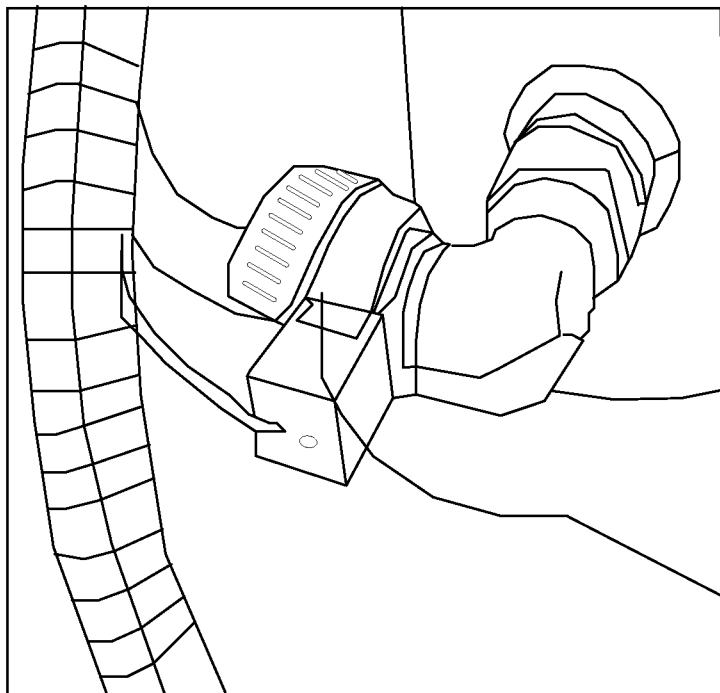


FIG. 10

1000

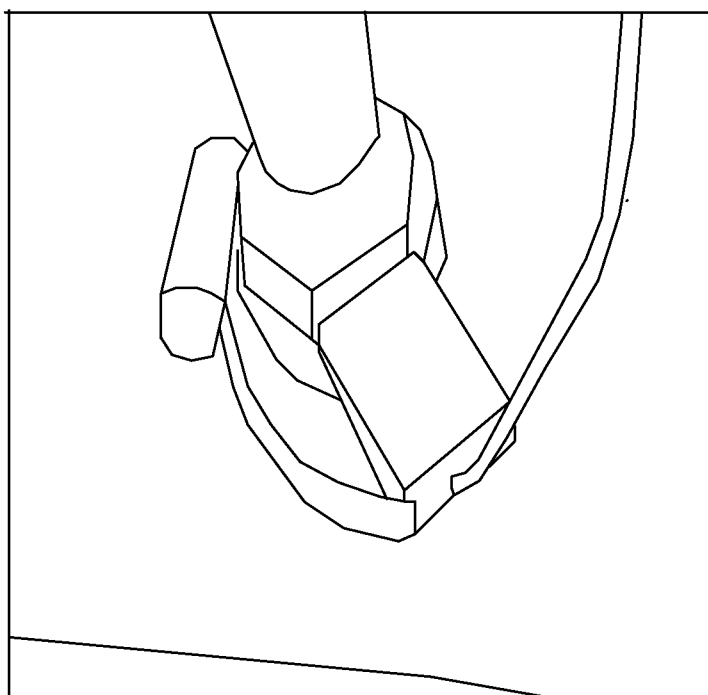


FIG. 11



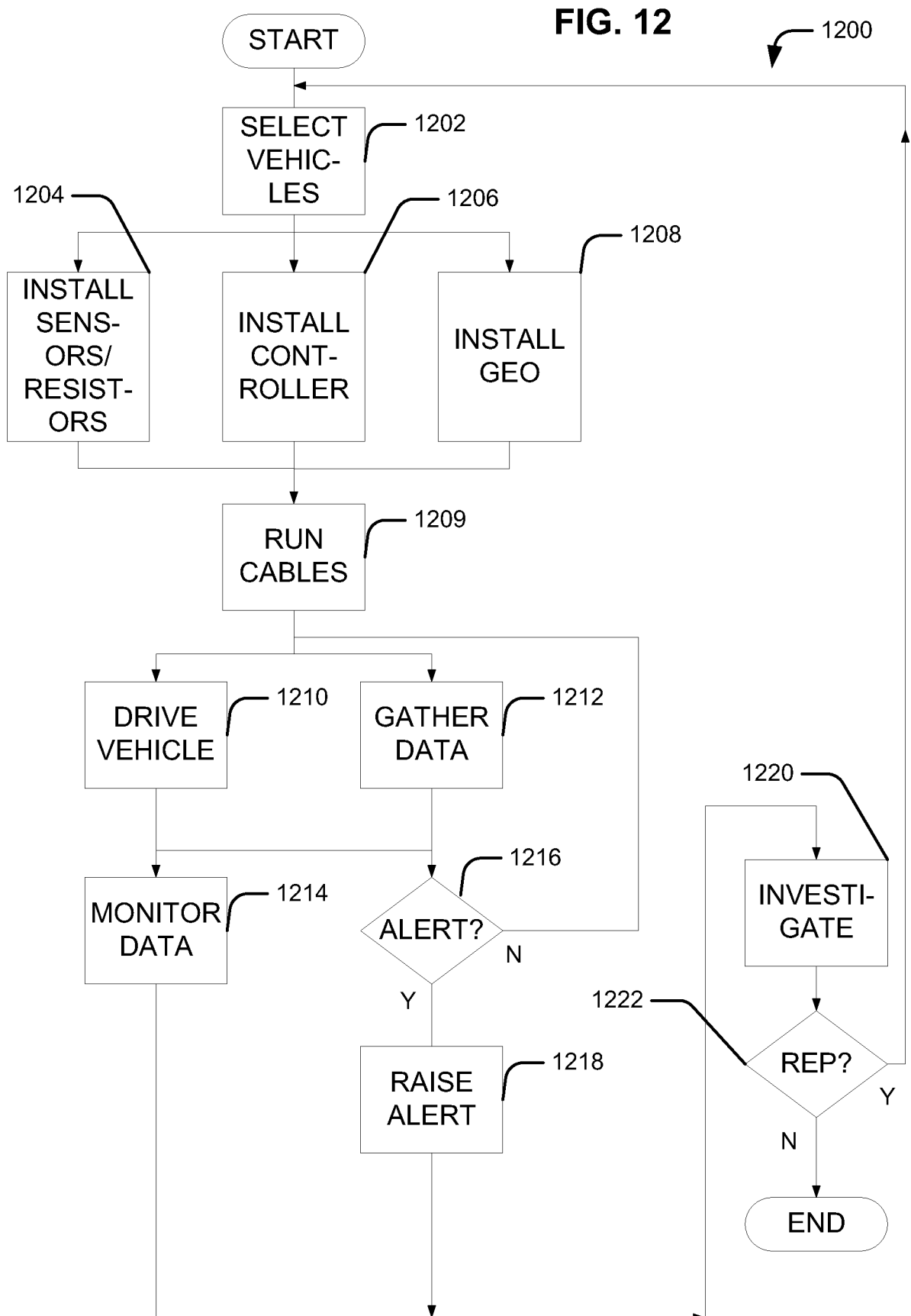


FIG. 13

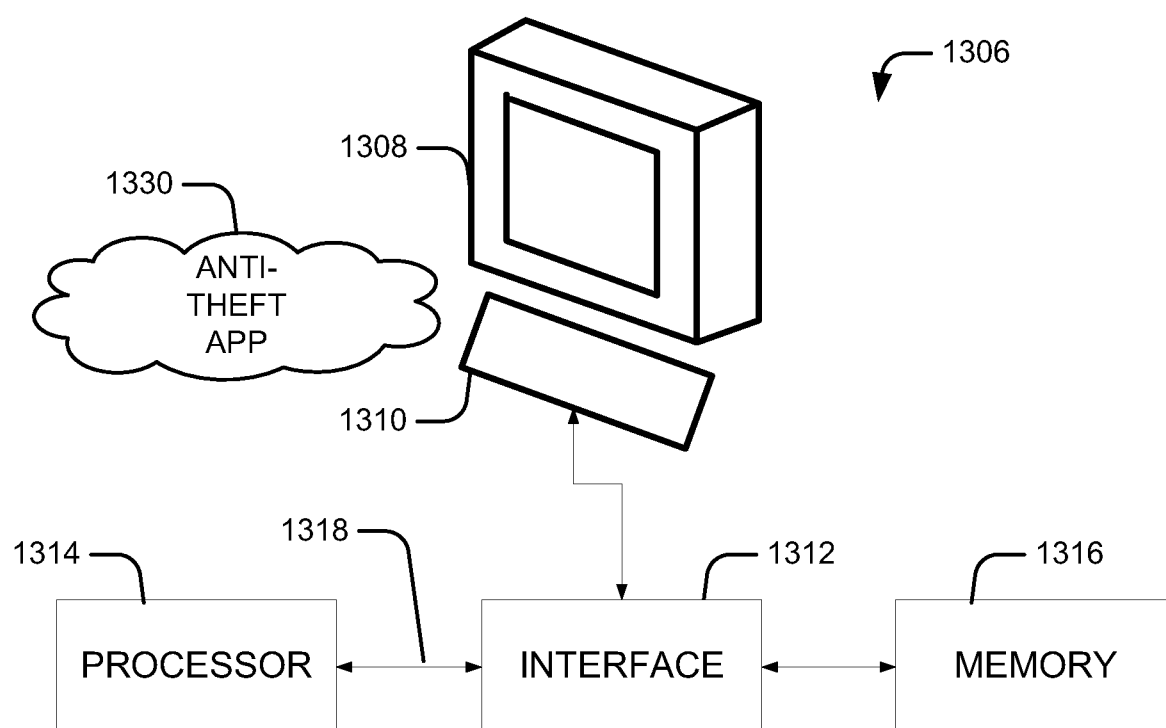


FIG. 14

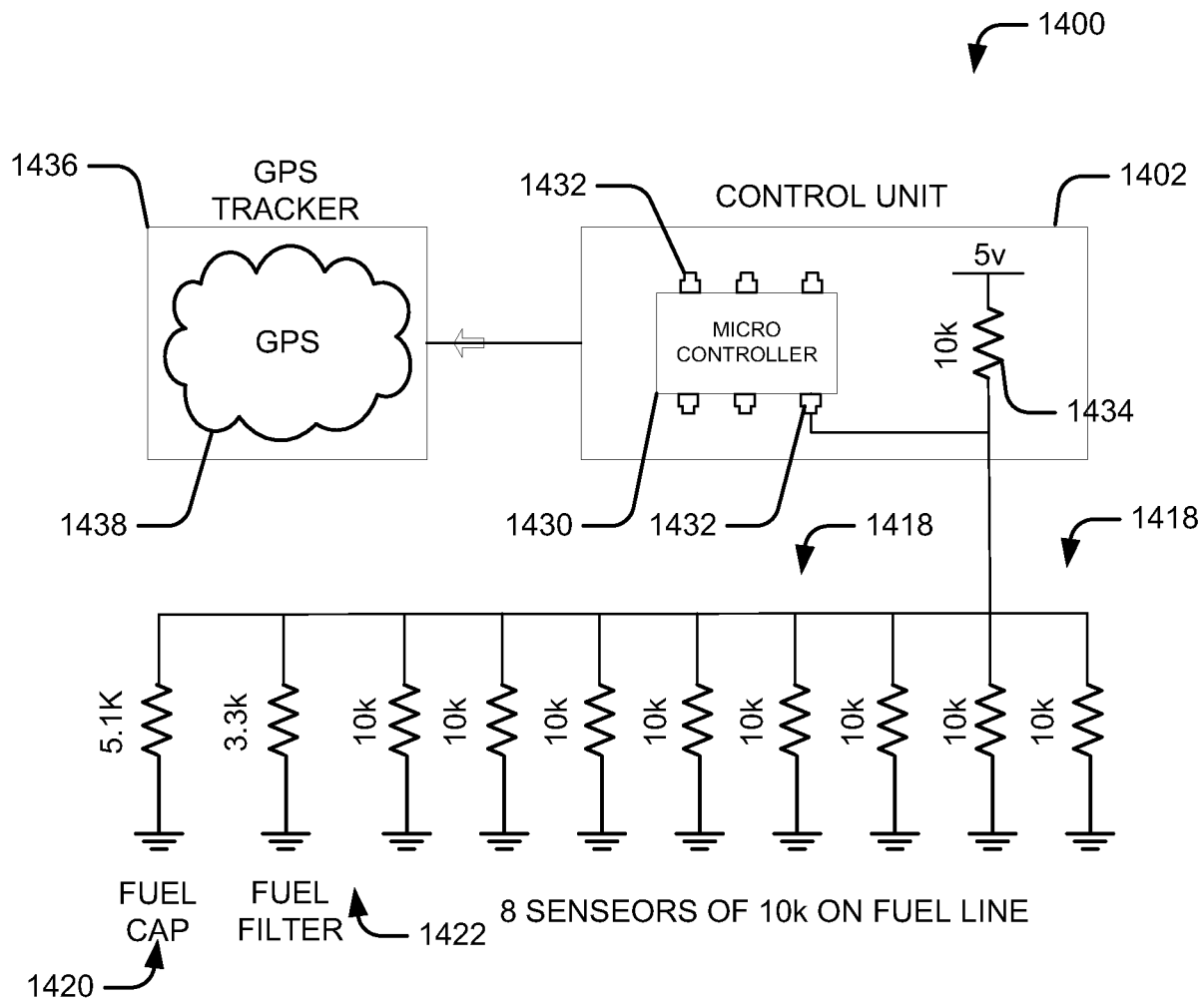
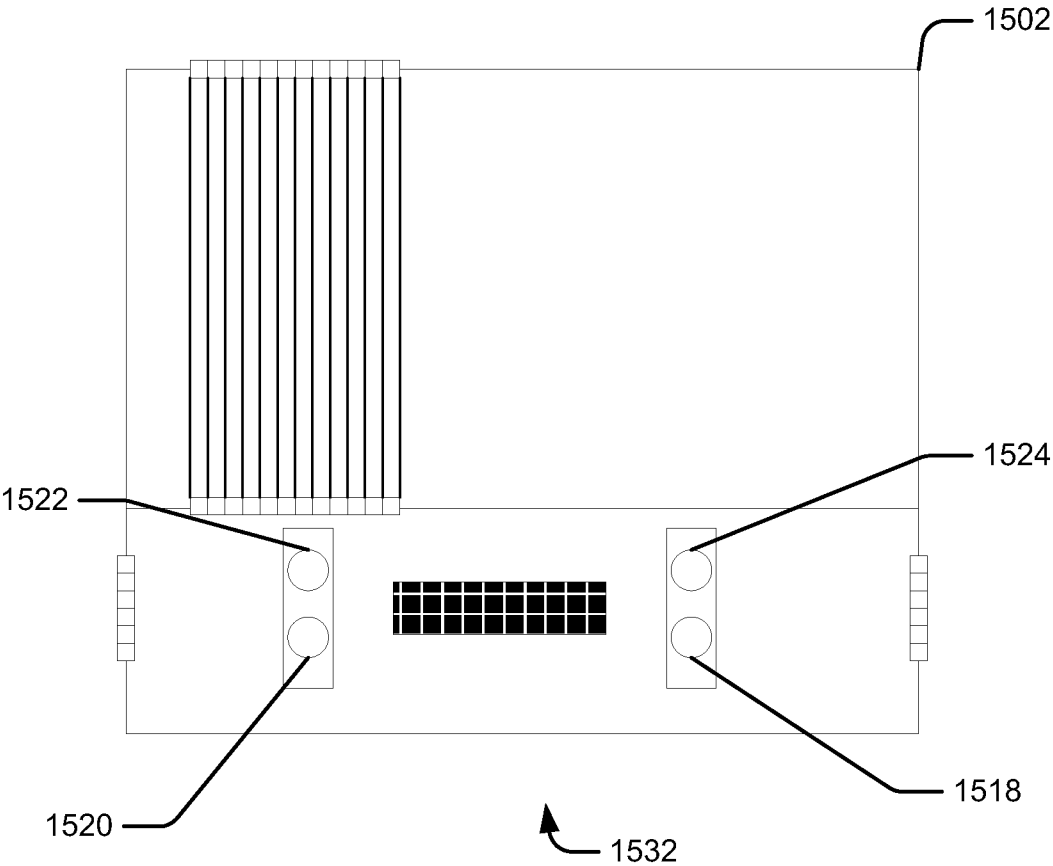


FIG. 15



+

ZIPTIE FUEL LINE SENSOR

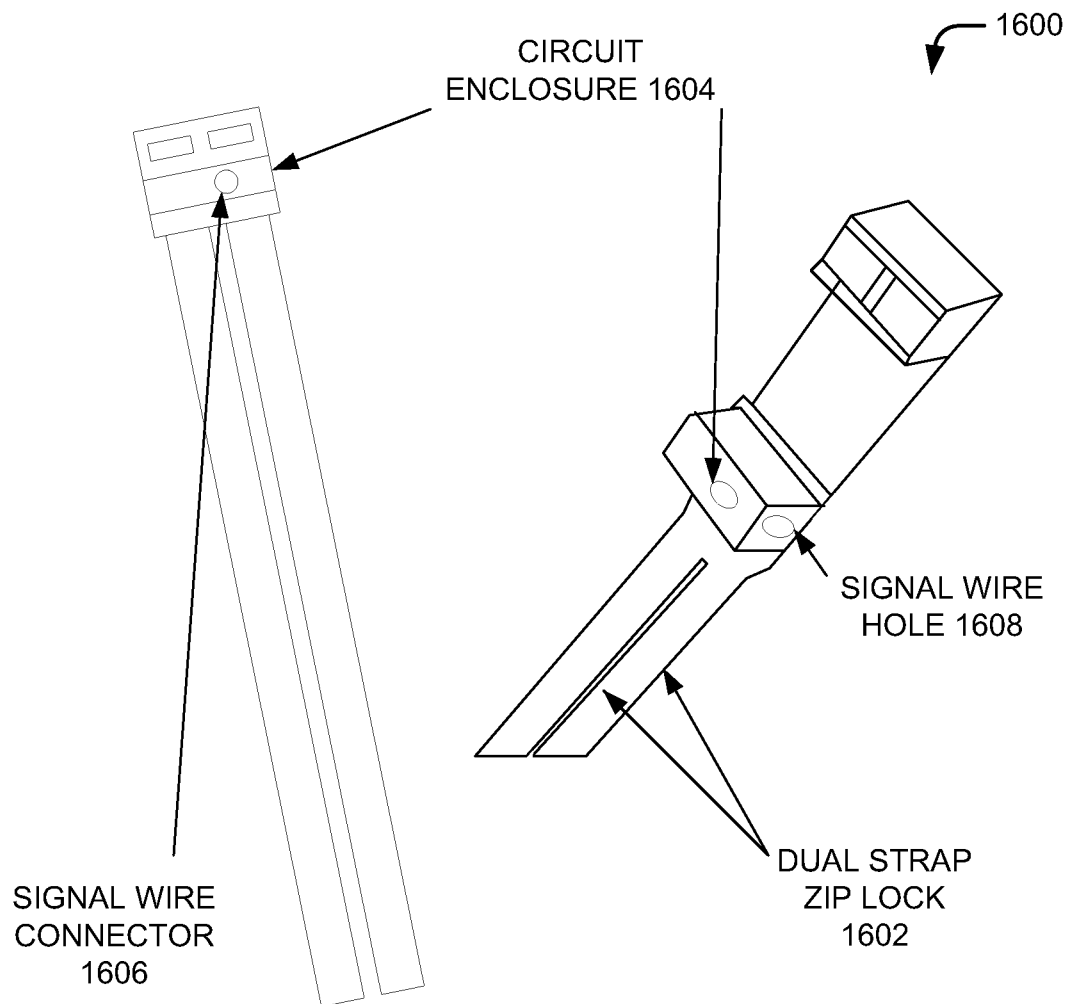


FIG. 16

+

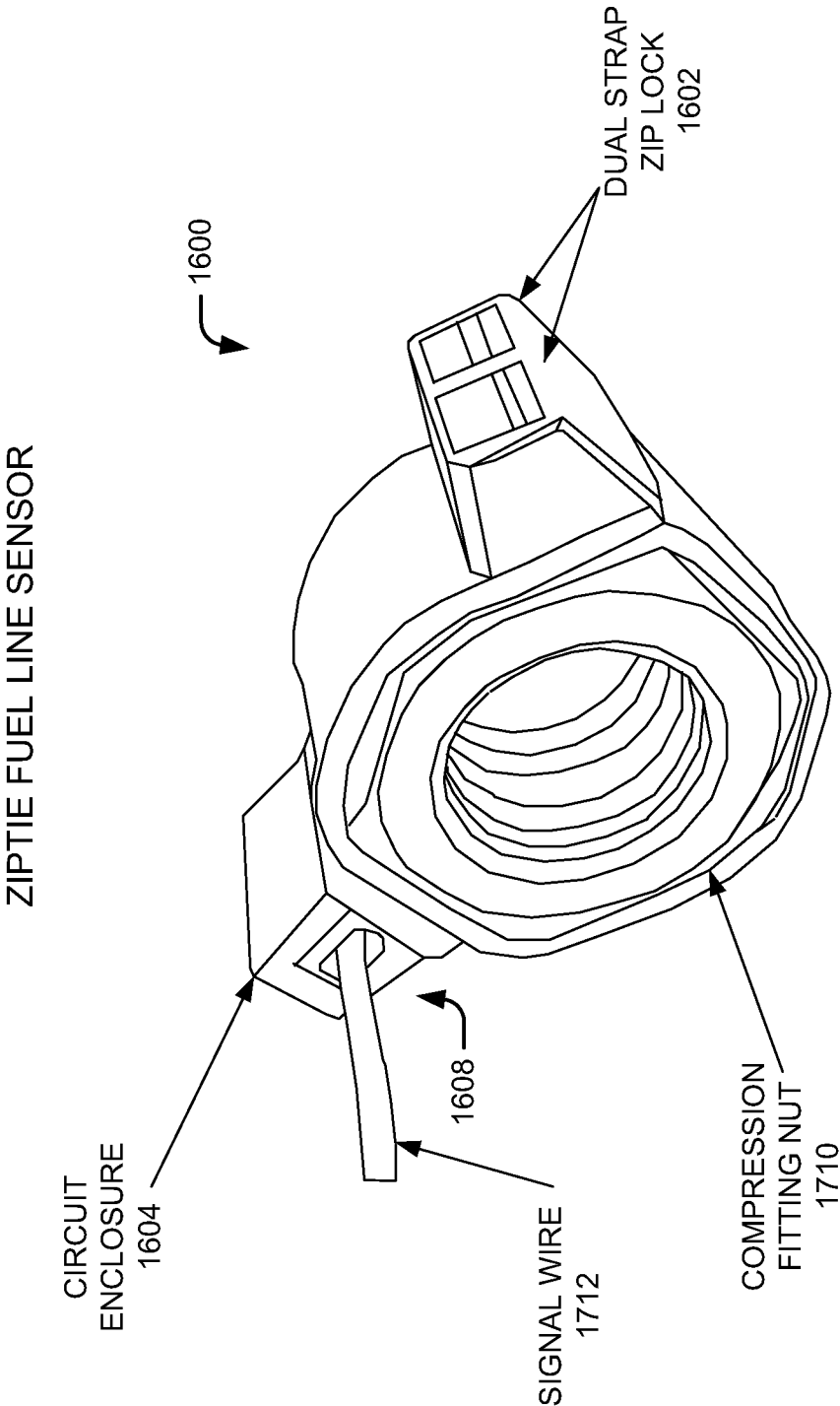
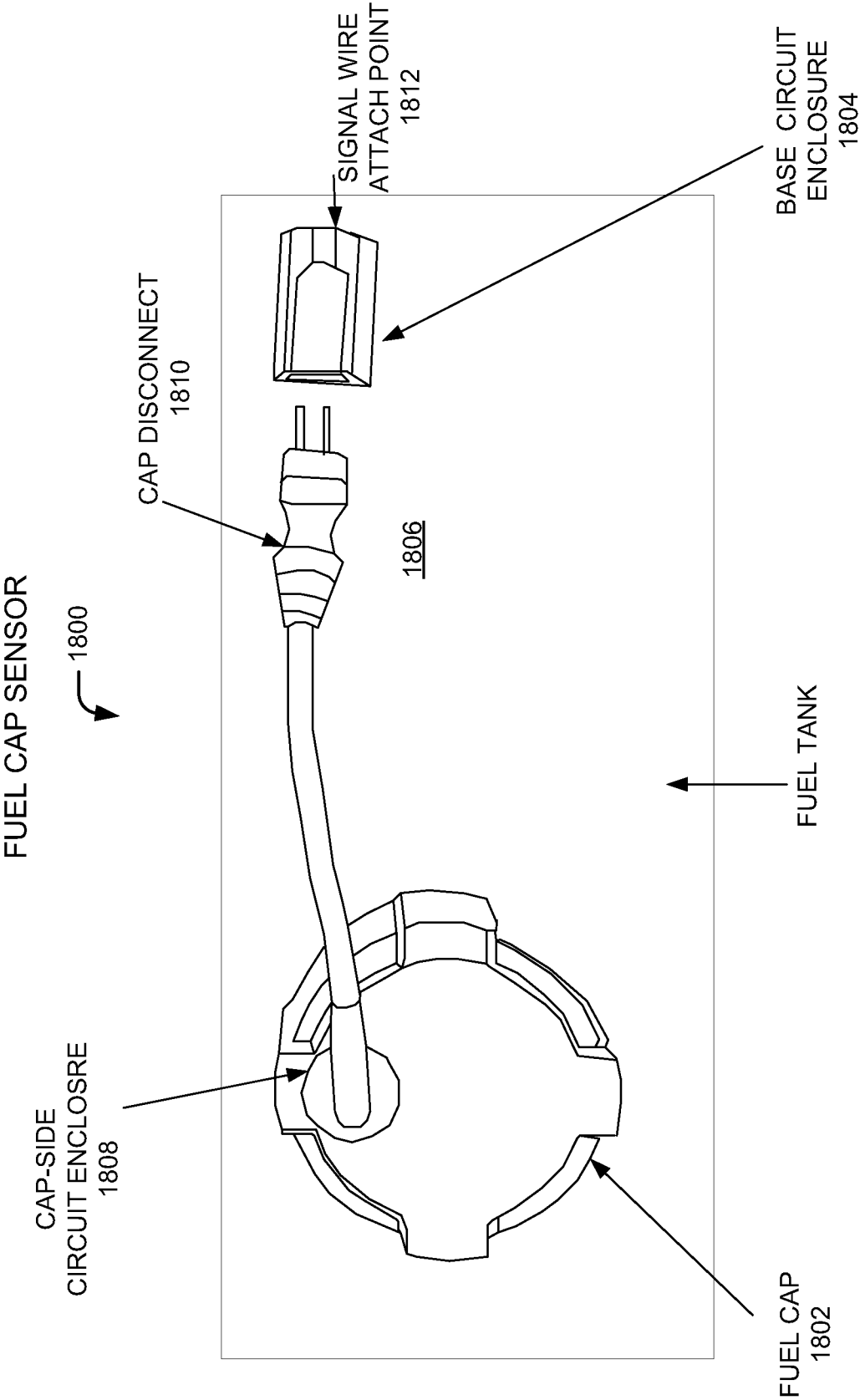


FIG. 17

FIG. 18



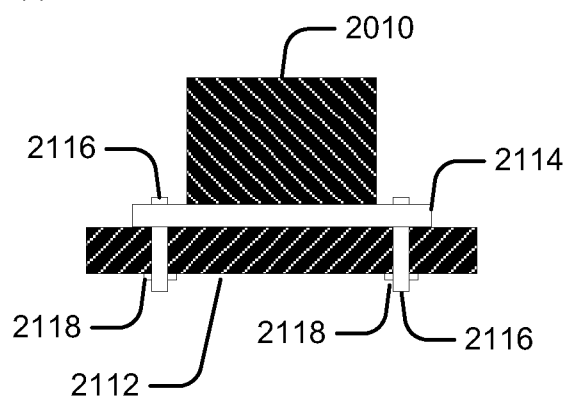
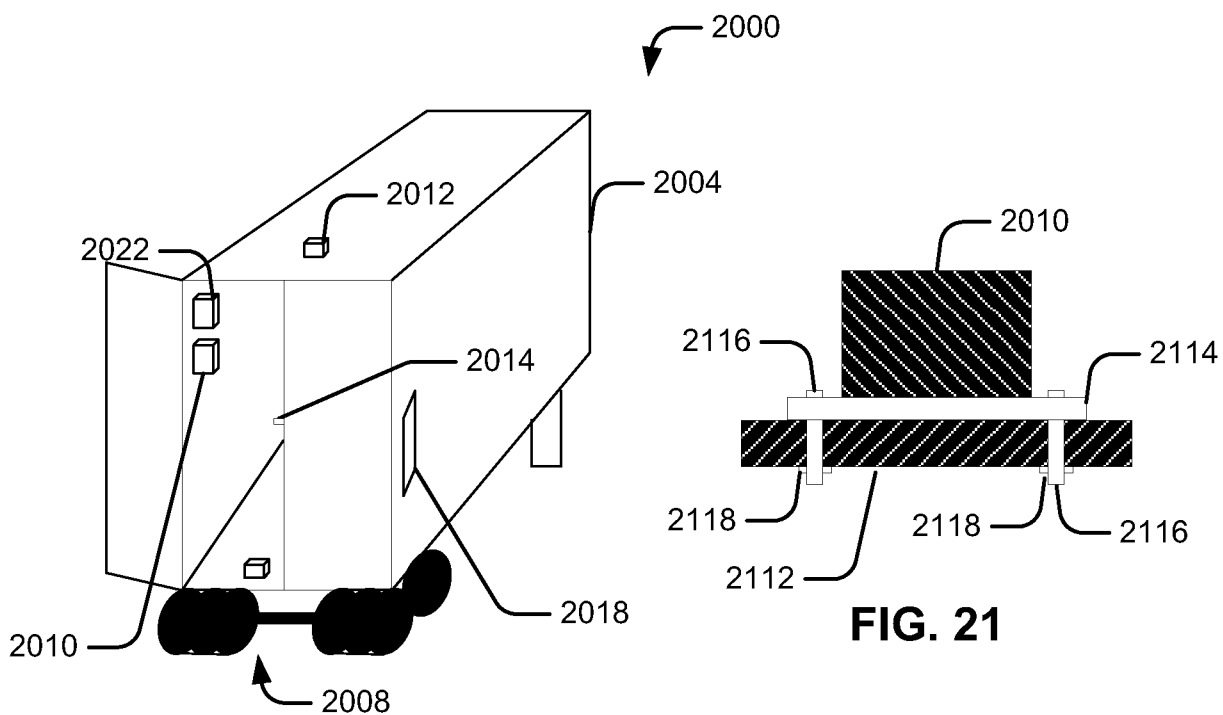
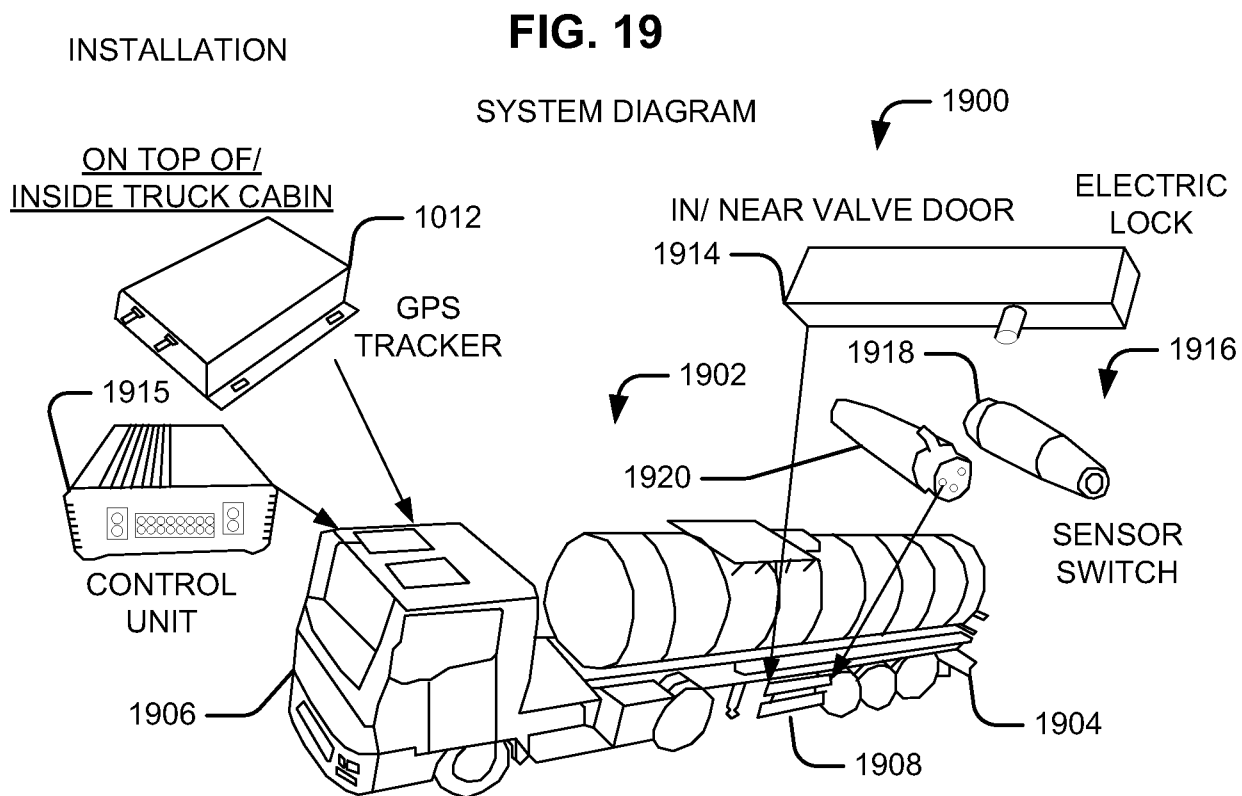
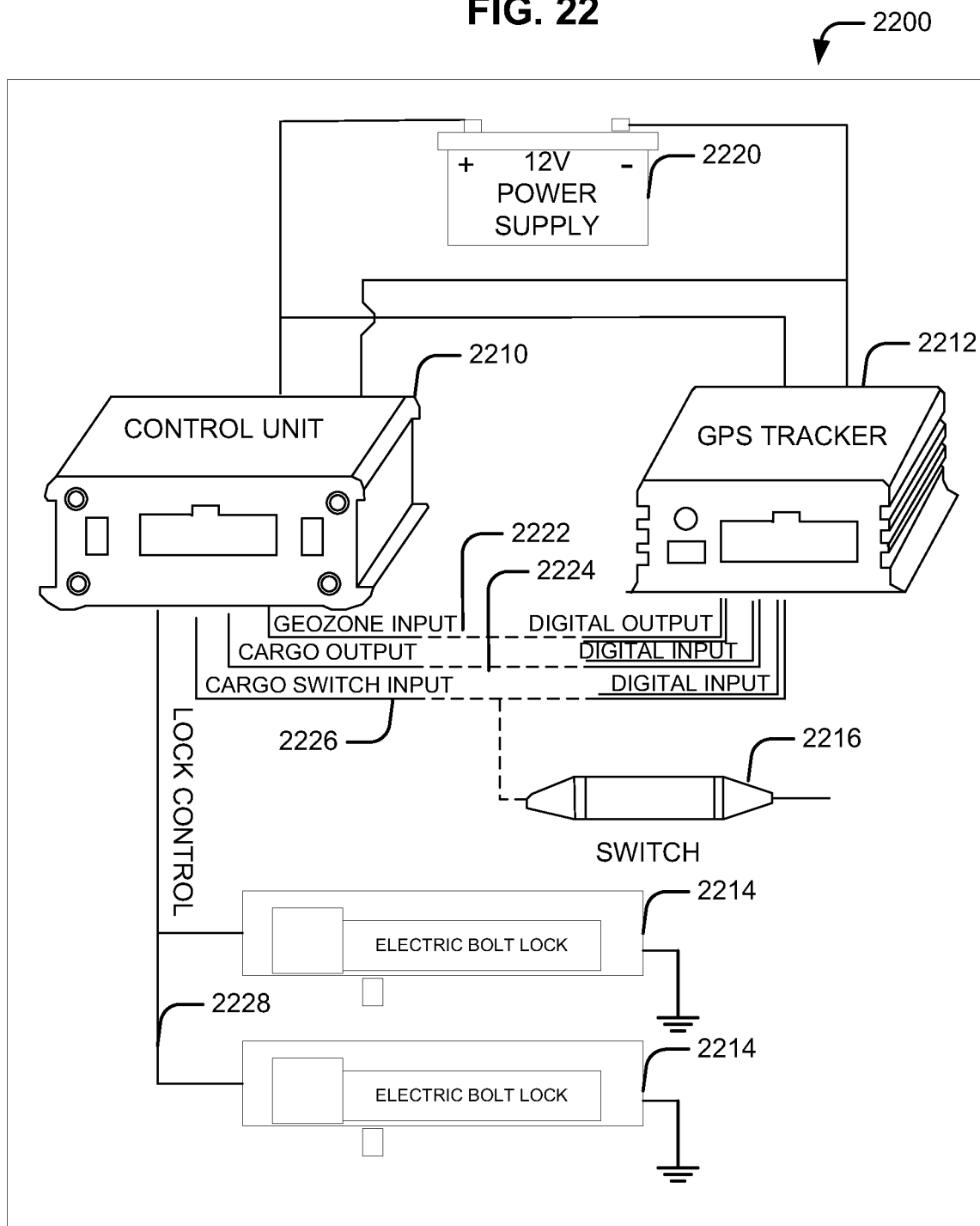
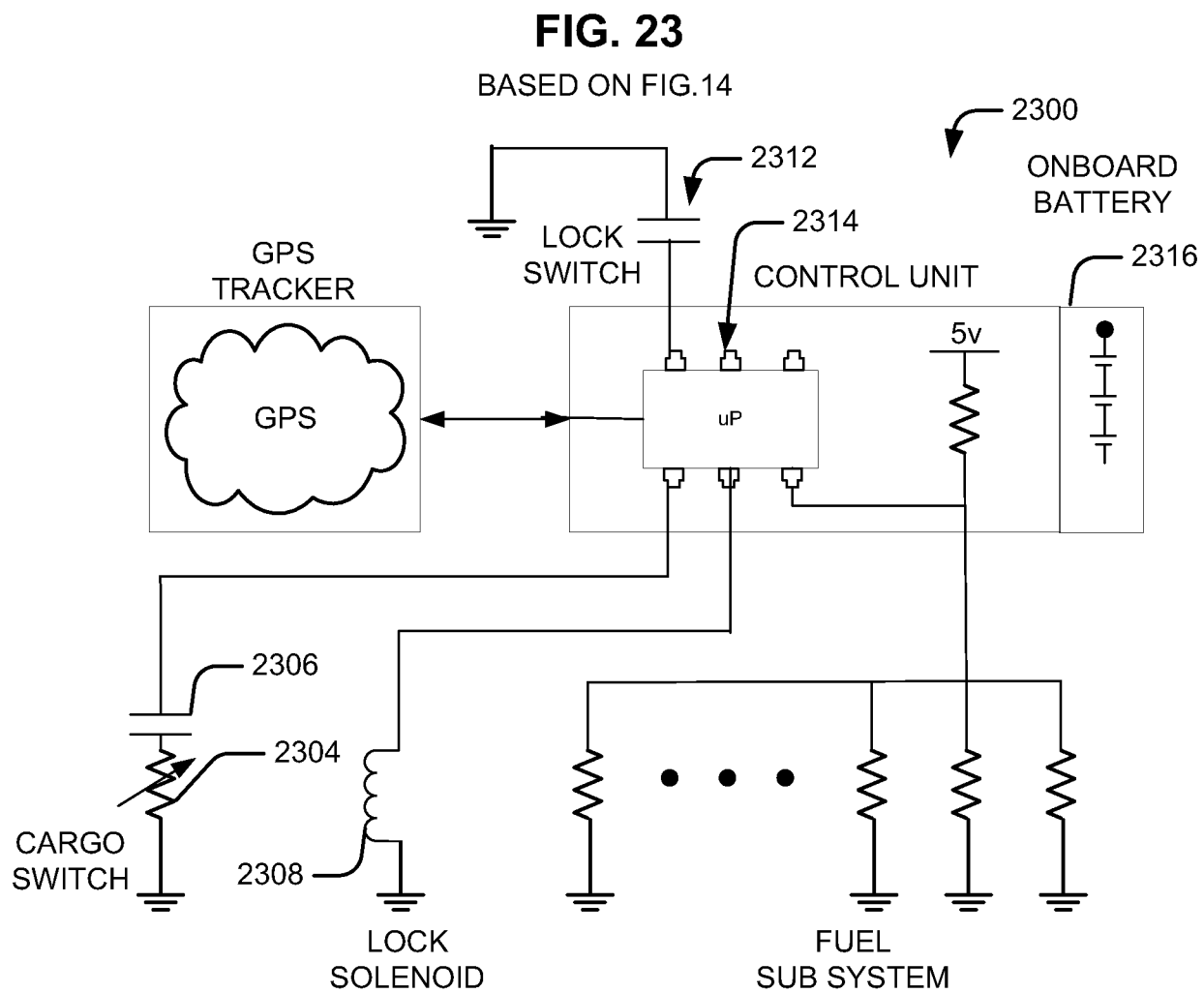
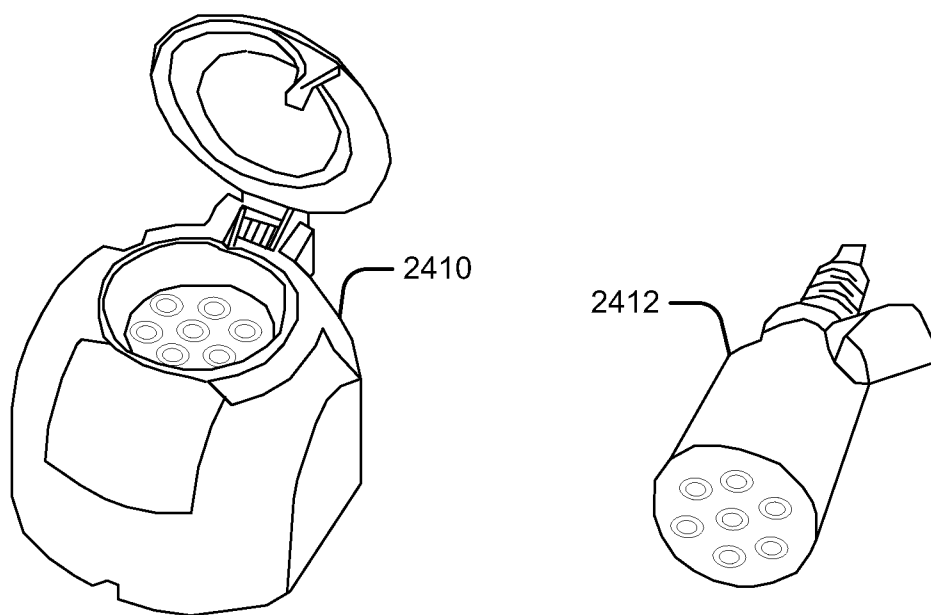
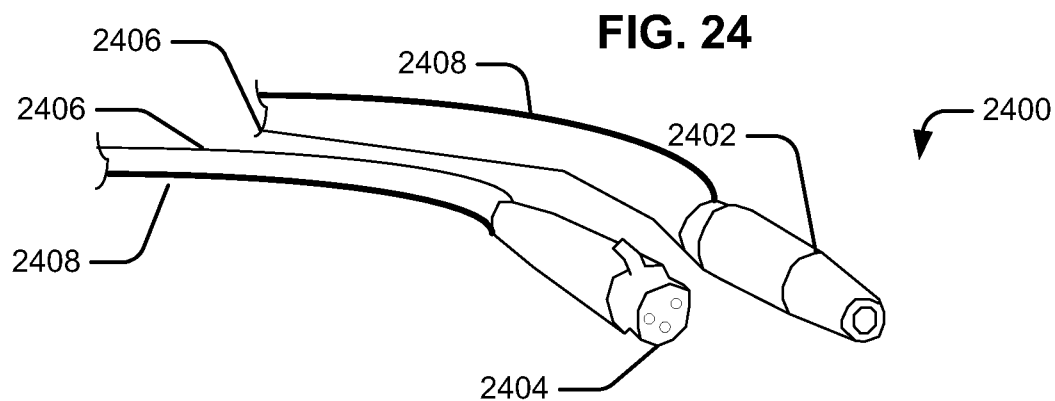


FIG. 22







INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2015/026169

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - B60R 25/01 (2015.01)

CPC - B60 R 25/01 (2015.04)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - B60R 25/00, B60R 25/01, B60R 25/10, B60R 25/23 (2015.01)

USPC - 180/287; 303/89; 340/6.1, 425.5, 426.28, 431, 542

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

CPC - B60R 25/00, B60R 25/01, B60R 25/1001, B60R 25/1004, B60R 25/23, Y10T 70/00, Y10T 70/5889 (2015.04) (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Orbit, Google Patents, Google.

Search terms used: anti-theft, controller, switch, cargo vehicle, lock, voltage, ground, personal identification number

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	EP 1,584,526 B1 (BERGSTEN) 06 July 2011 (06.07.2011) entire document	1, 4-5, 7-10, 12, 15-16 & 18-19 — 2-3, 6, 11, 13-14, 17 & 20
Y	US 2002/0089434 A1 (GHAZARIAN) 11 July 2002 (11.07.2002) entire document	2-3, 13-14 & 20
Y	US 2007/0085680 A1 (COHEN) 19 April 2007 (19.04.2007) entire document	6, 11, 17 & 20
A	US 2004/0178880 A1 (MEYER et al) 16 September 2004 (16.09.2004) entire document	1-20
A	US 2010/0089108 A1 (DUTT et al) 15 April 2010 (15.04.2010) entire document	1-20
A	US 2009/0072956 A1 (KALOUS) 19 March 2009 (19.04.2009) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

15 June 2015

Date of mailing of the international search report

23 JUL 2015

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Blaine Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774

RESUMEN

Sistemas, aparatos y métodos relacionados antirrobo de carga. Los controladores antirrobo de las modalidades
5 están configurados para detectar las aperturas de interruptores de carga y para operar electrónicamente las cerraduras en respuesta a los mismos. Además, los interruptores están acoplados mecánicamente a los puntos de acceso en maneras tales que los puntos de acceso no se
10 pueden abrir sin abrir los interruptores. Algunos controladores están configurados para las señales de salida de las aberturas de los interruptores mientras que algunos están configurados para desbloquear las cerraduras sólo en geozonas previamente seleccionadas. Los voltajes
15 previamente seleccionados, por otra parte, pueden diferir de 12 V CC y pueden ser seleccionados por el usuario. Además, los controladores pueden configurarse para detectar PINs (modificables) asociados a las aperturas de los interruptores de carga. Los controladores pueden incluir un
20 acoplador que se acopla de forma segura al vehículo. También se puede configurar para detectar una posición de la cerradura. Dichos controladores, además, pueden configurarse para bloquear la cerradura en respuesta a la posición de bloqueo y/o pueden comprender una batería.

FIG. 1

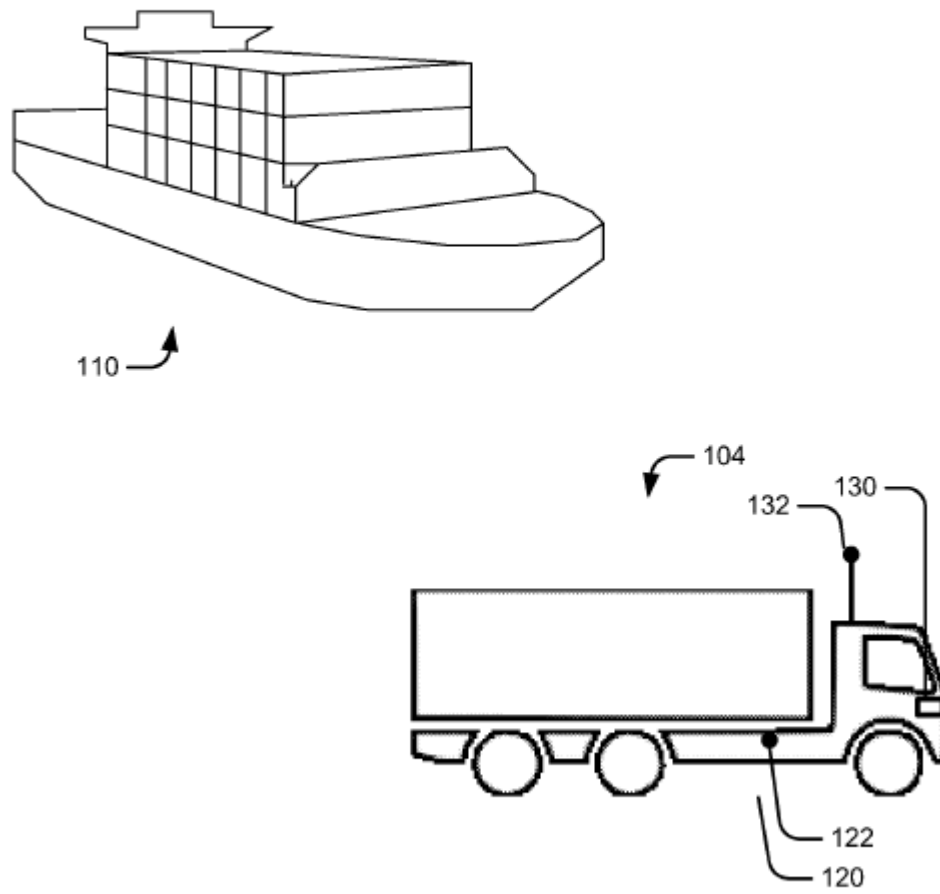
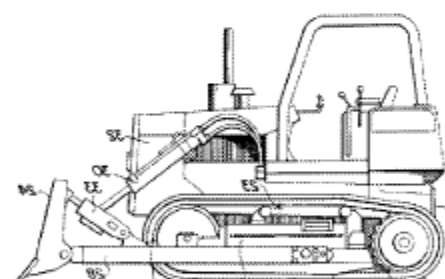
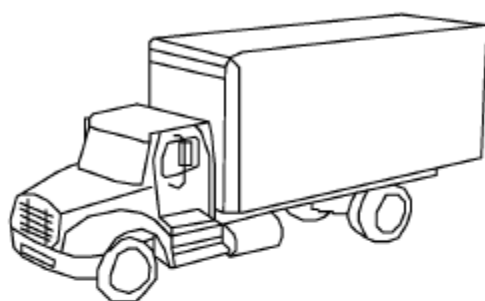
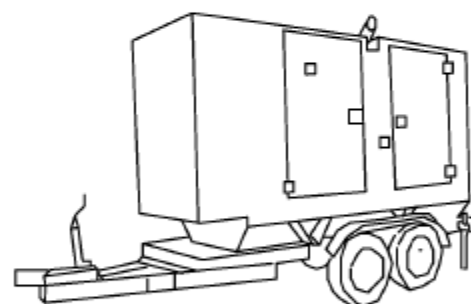


FIG. 1
(Cont'd)

102



106



108

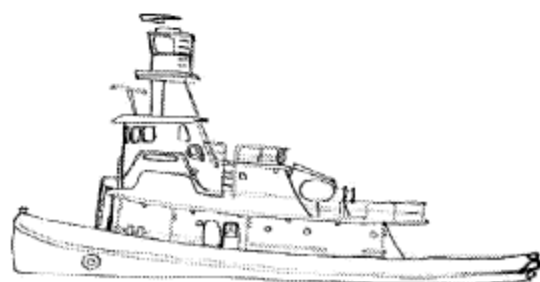


FIG. 2

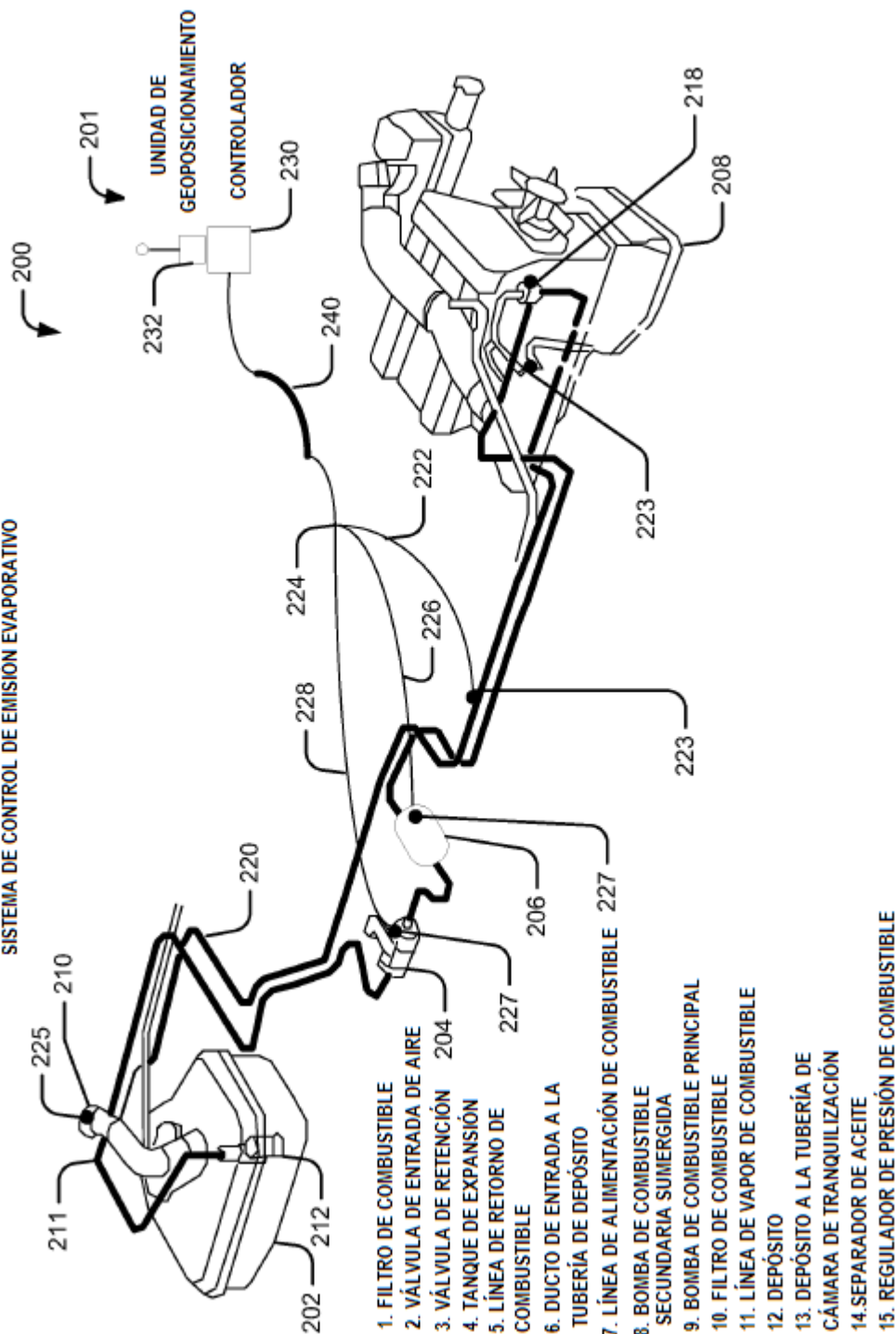


FIG. 3

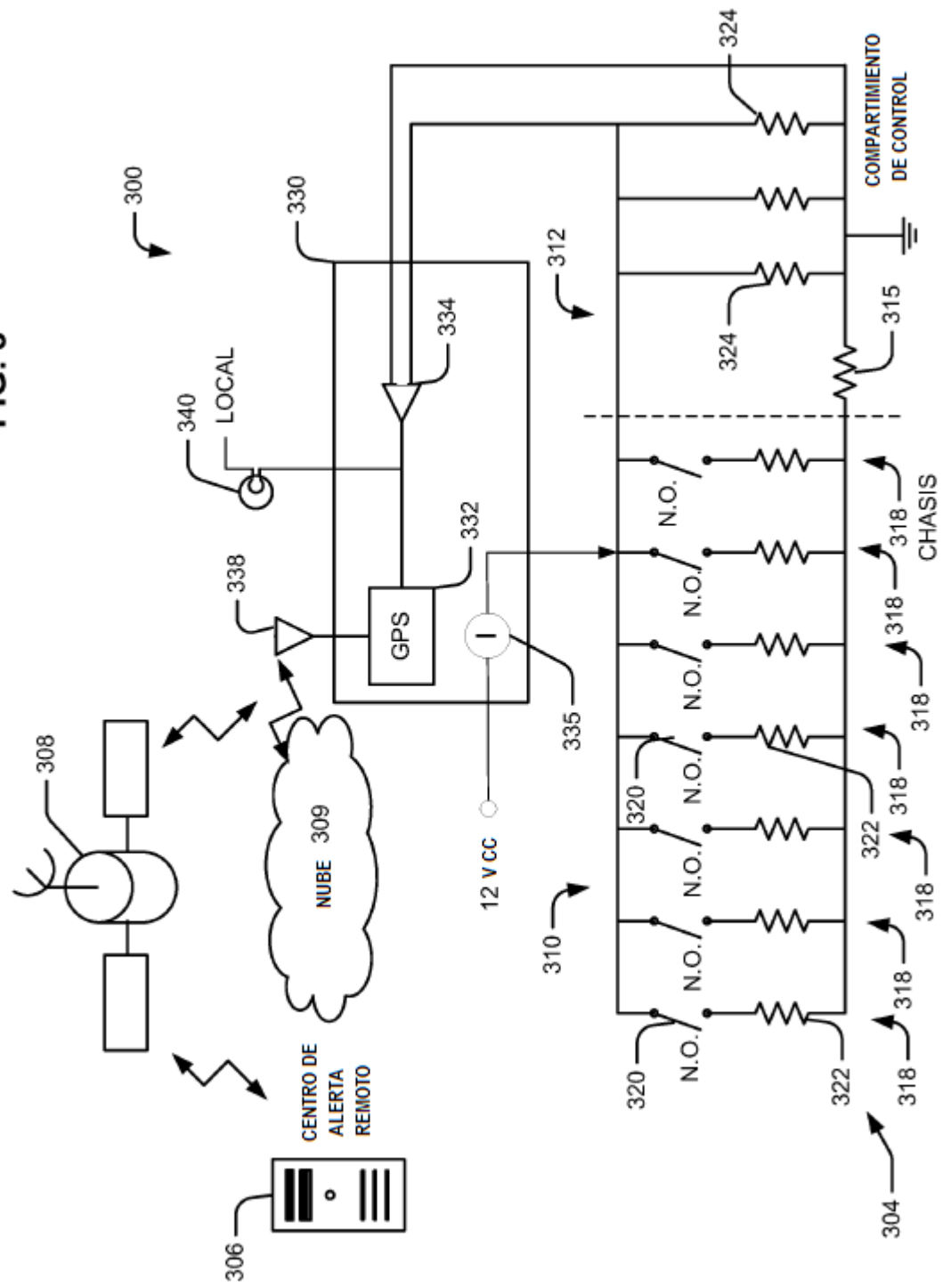


FIG. 4

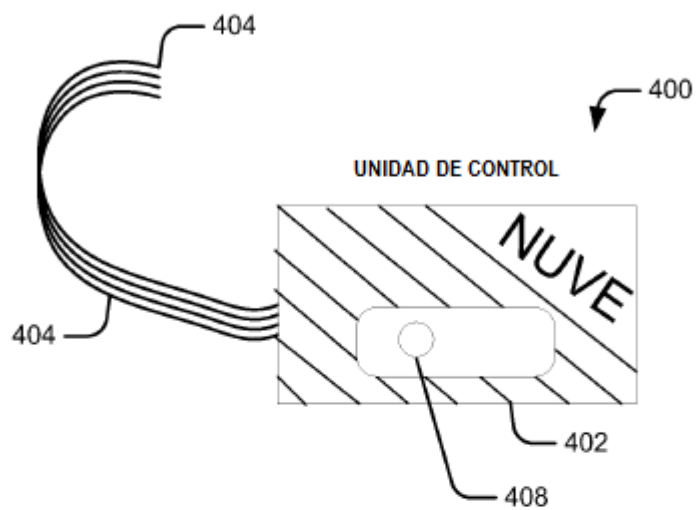


FIG. 5

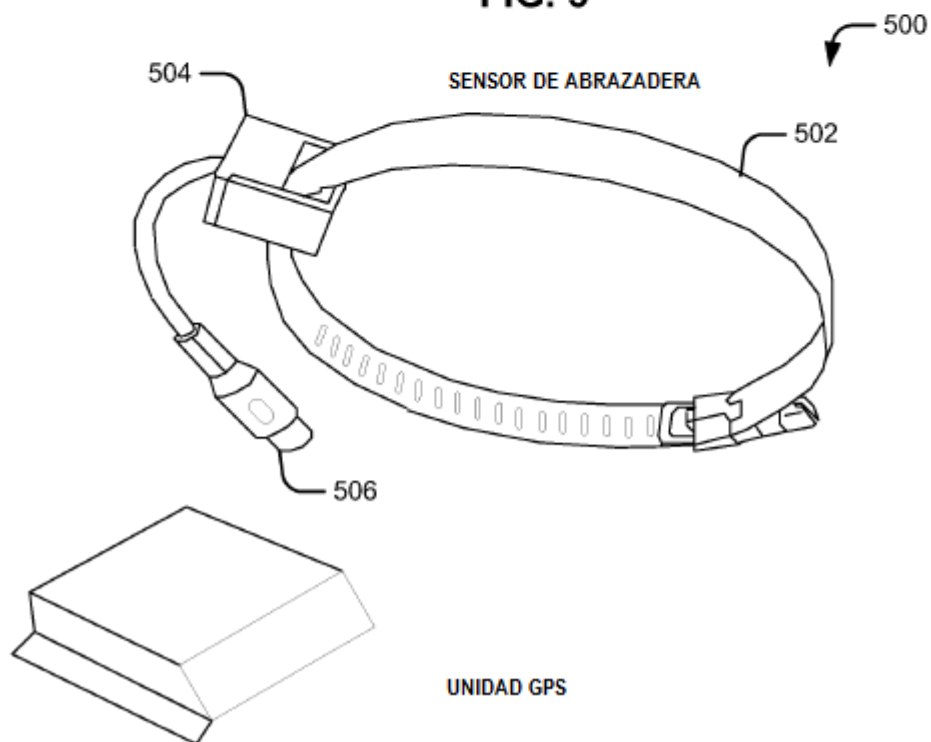


FIG. 6

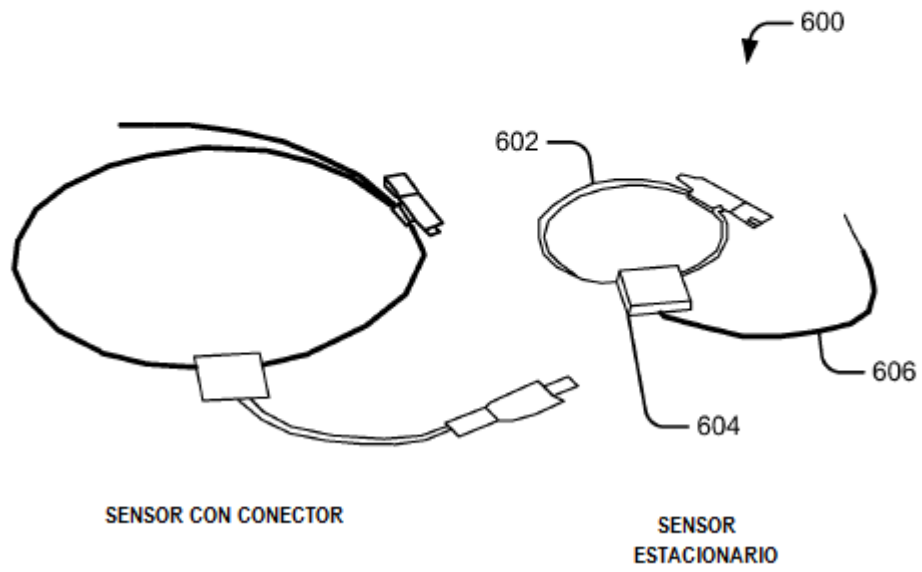
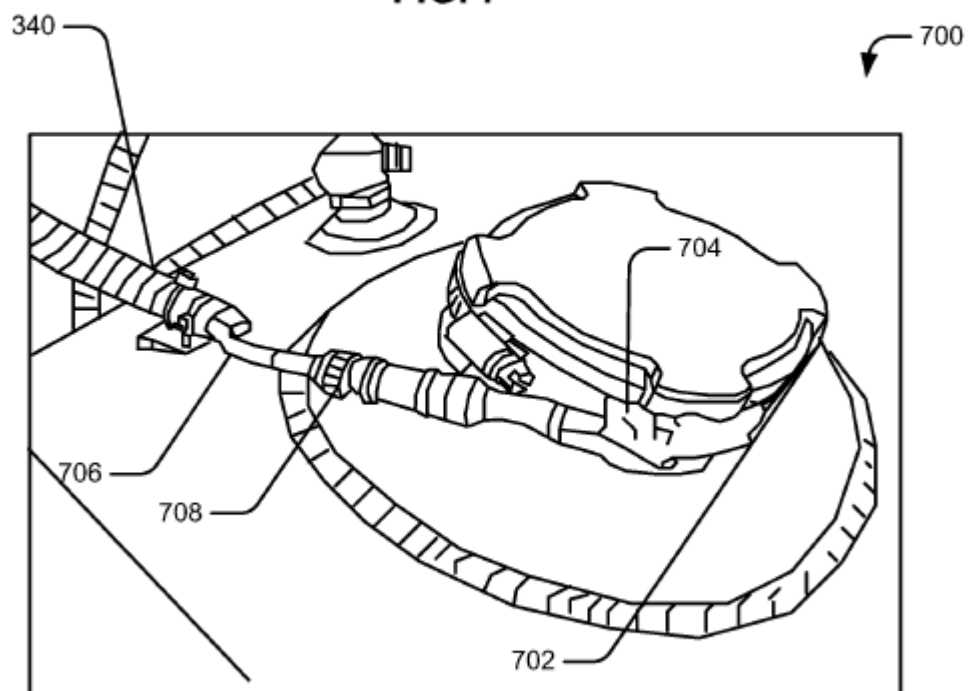
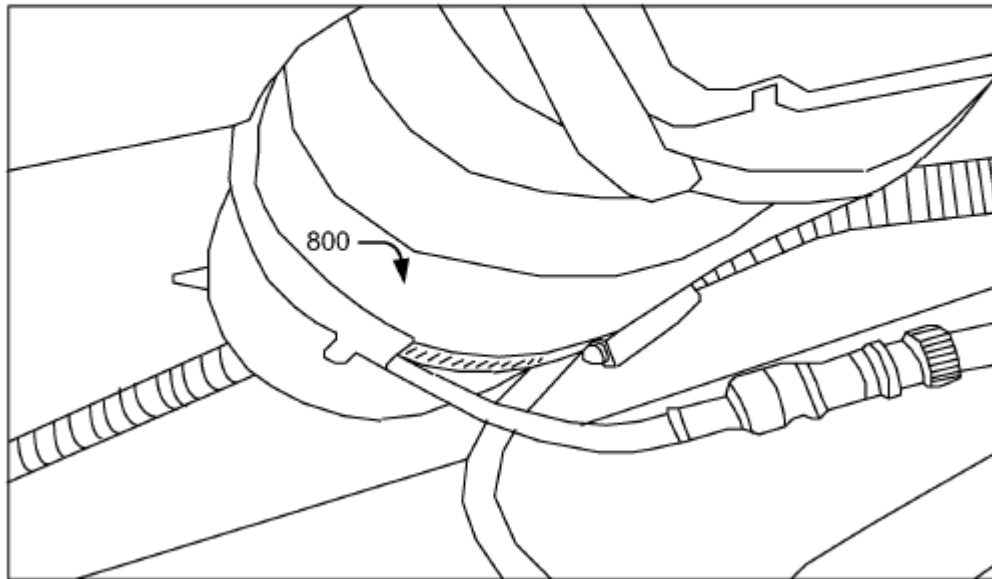


FIG. 7



SENSOR INSTALADO EN LA TAPA DE COMBUSTIBLE

FIG. 8



SENSOR INSTALADO EN EL FILTRO DE COMBUSTIBLE

FIG. 9

900

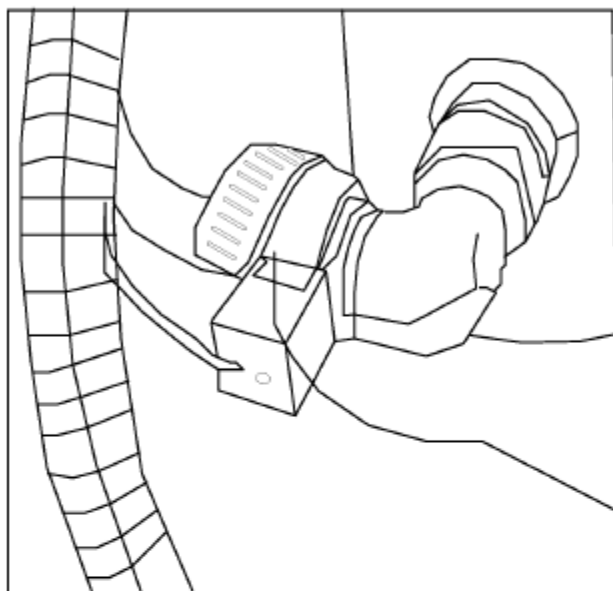


FIG. 10

1000

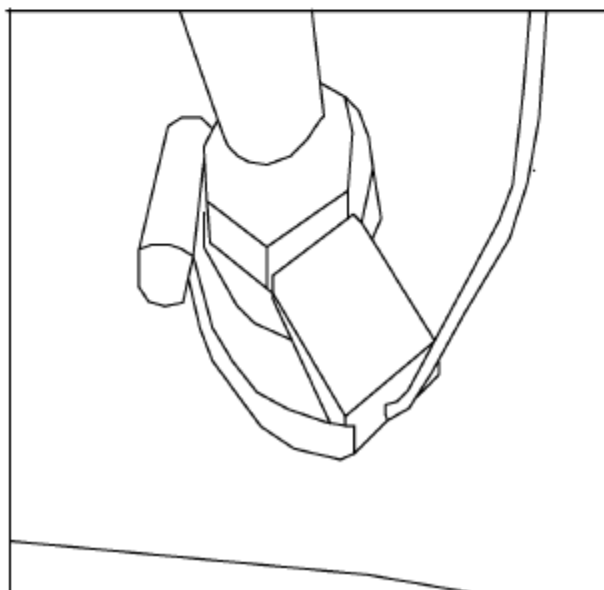


FIG. 11



FIG. 12

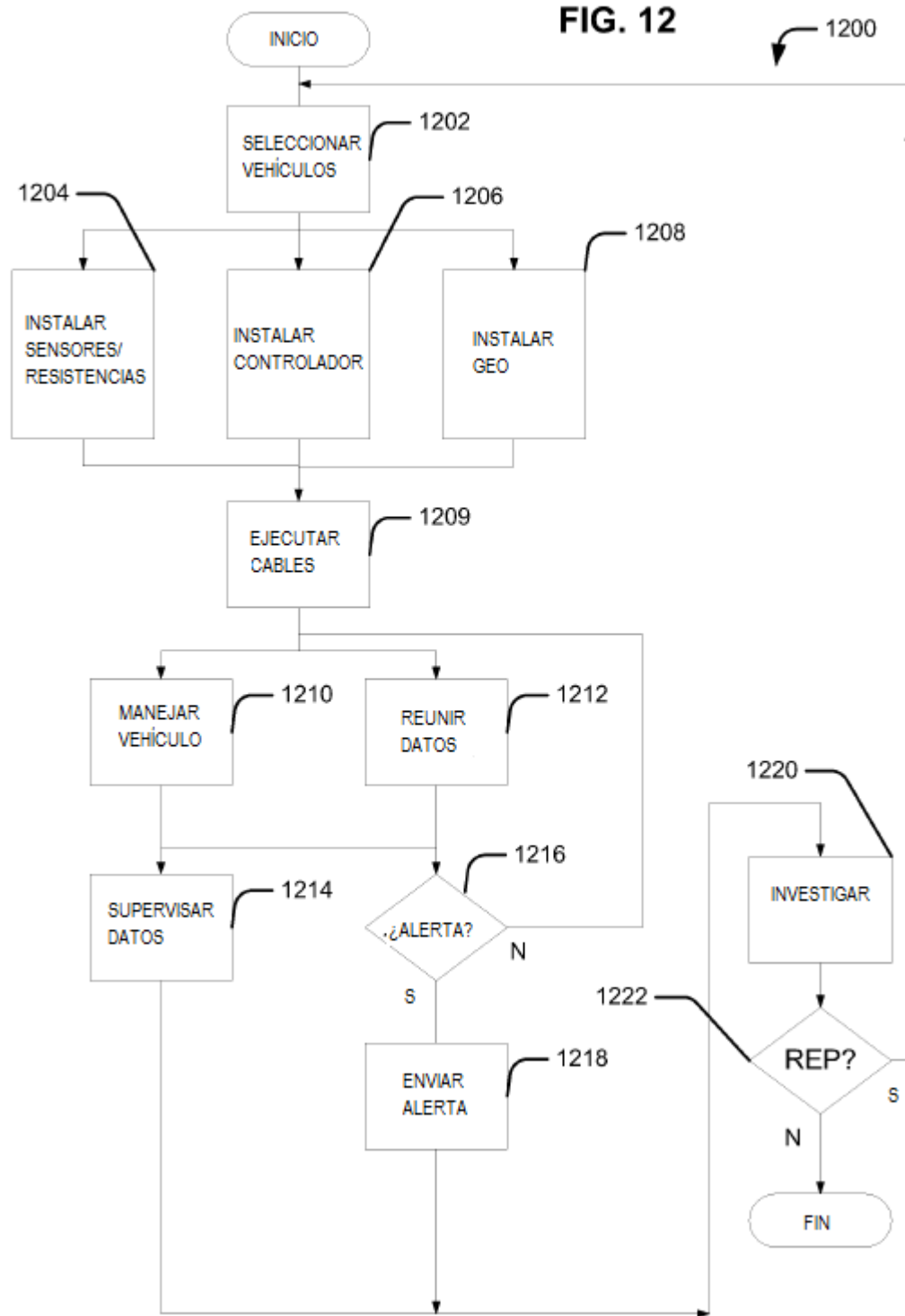


FIG. 13

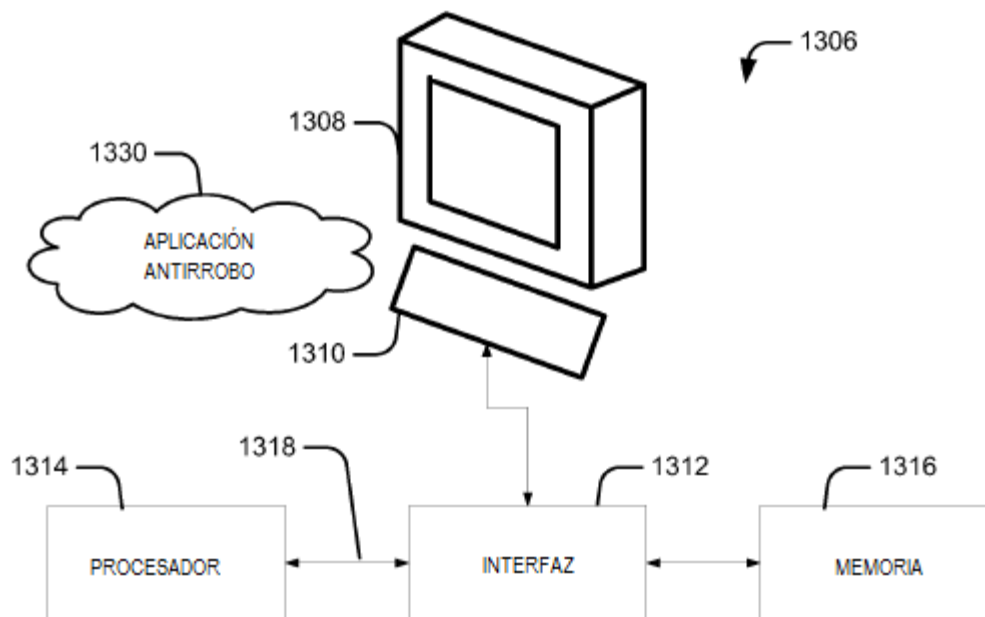


FIG. 14

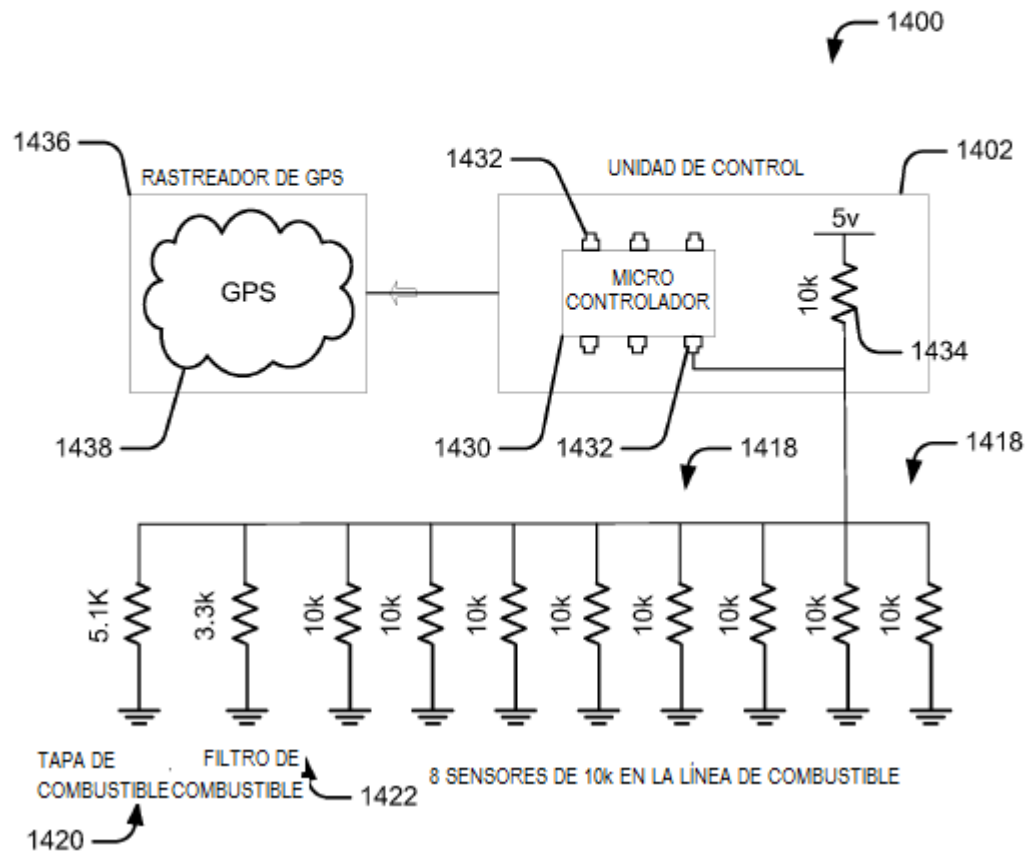
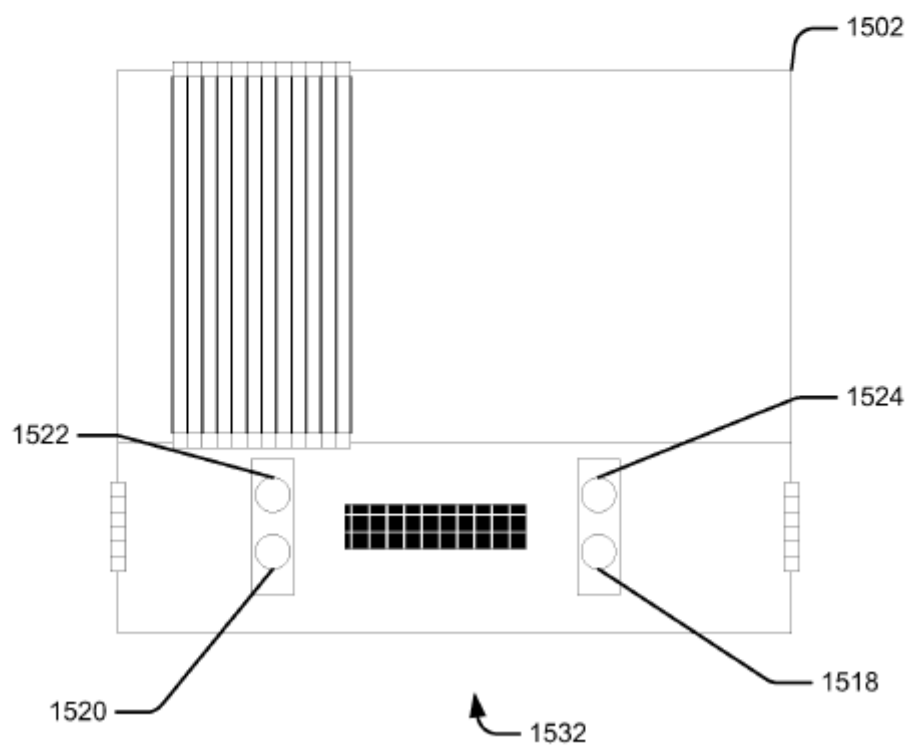


FIG. 15



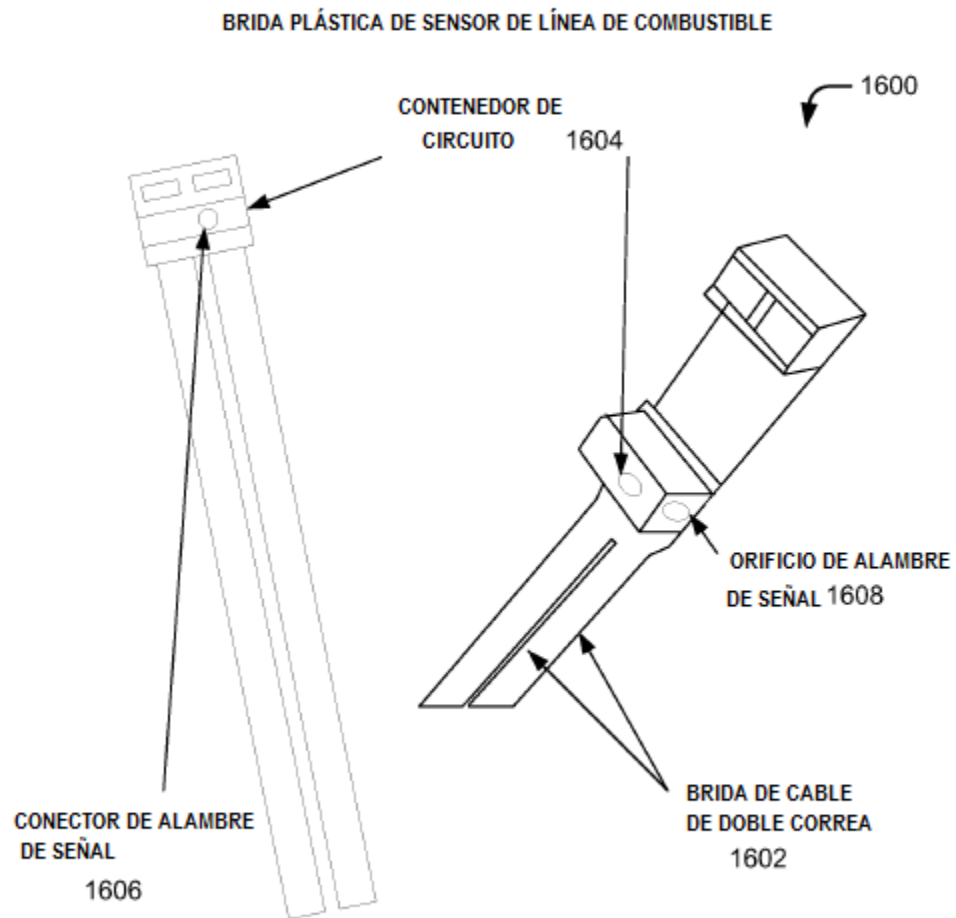


FIG. 16

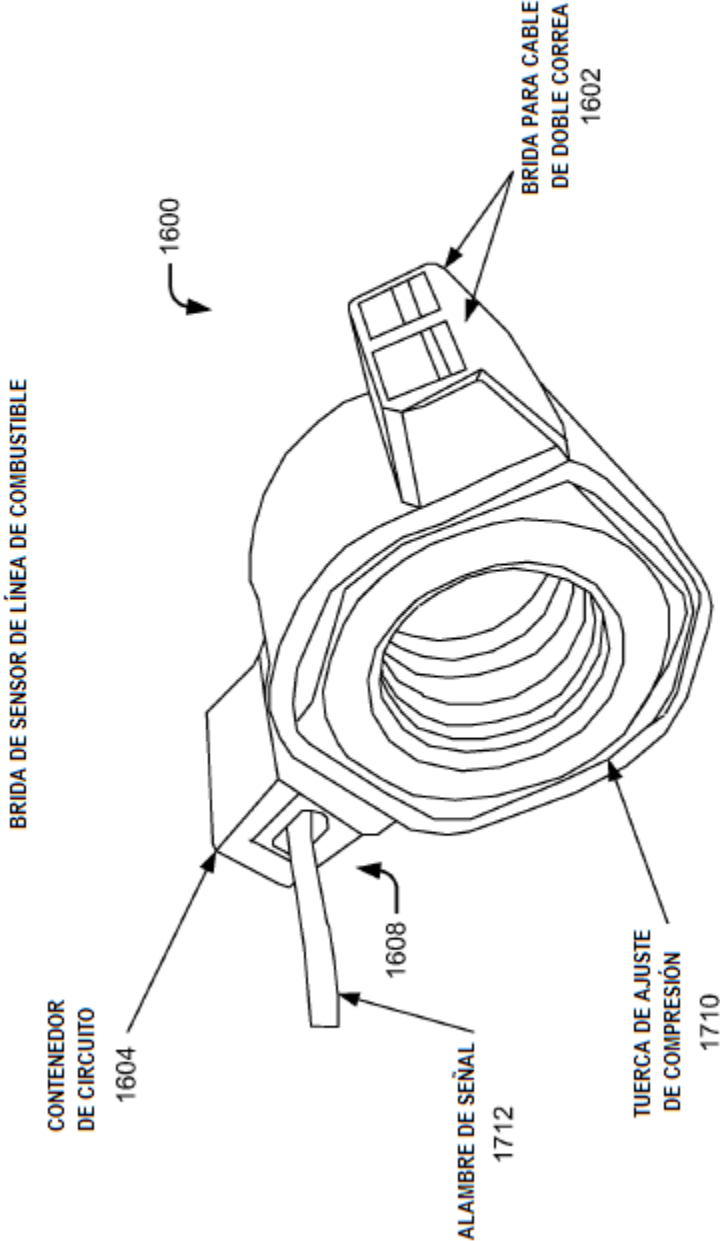


FIG. 17

FIG. 18

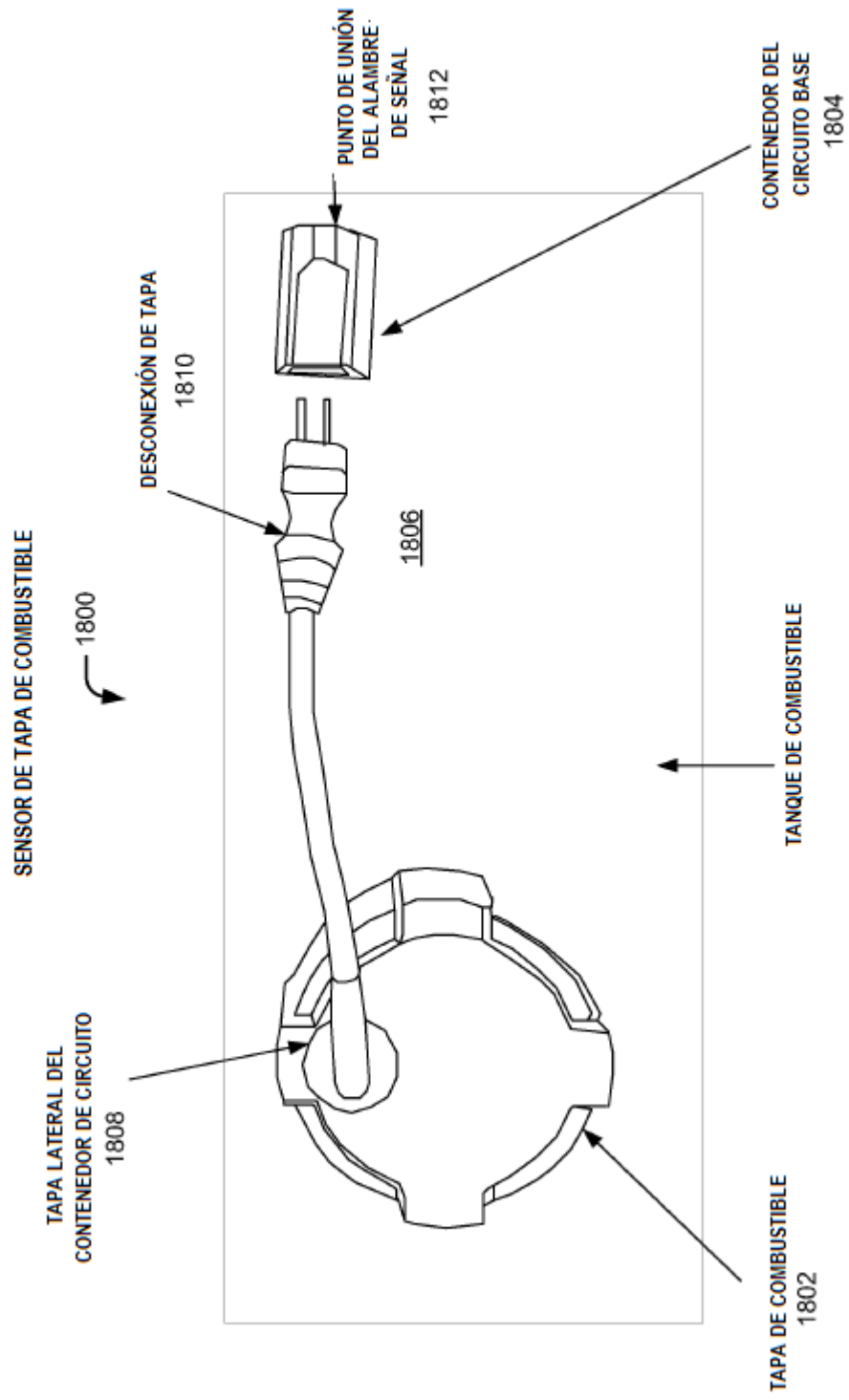


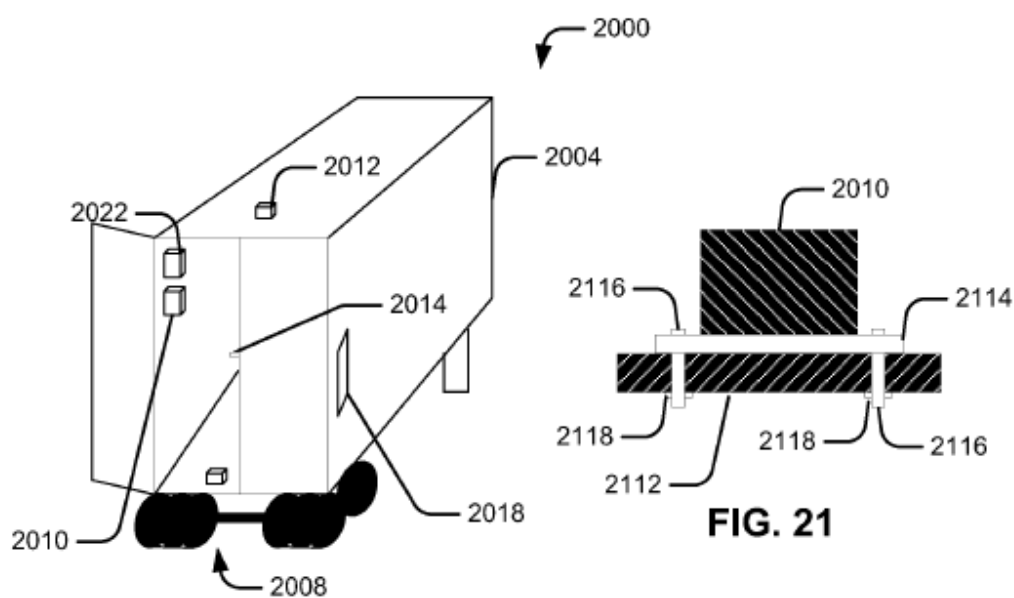
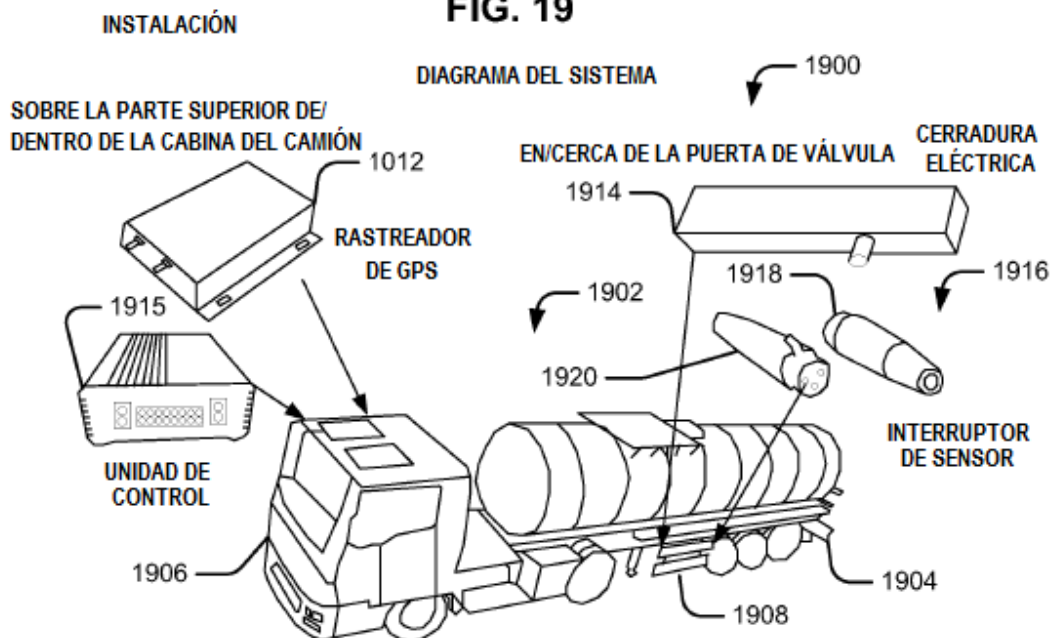
FIG. 19**FIG. 20****FIG. 21**

FIG. 22

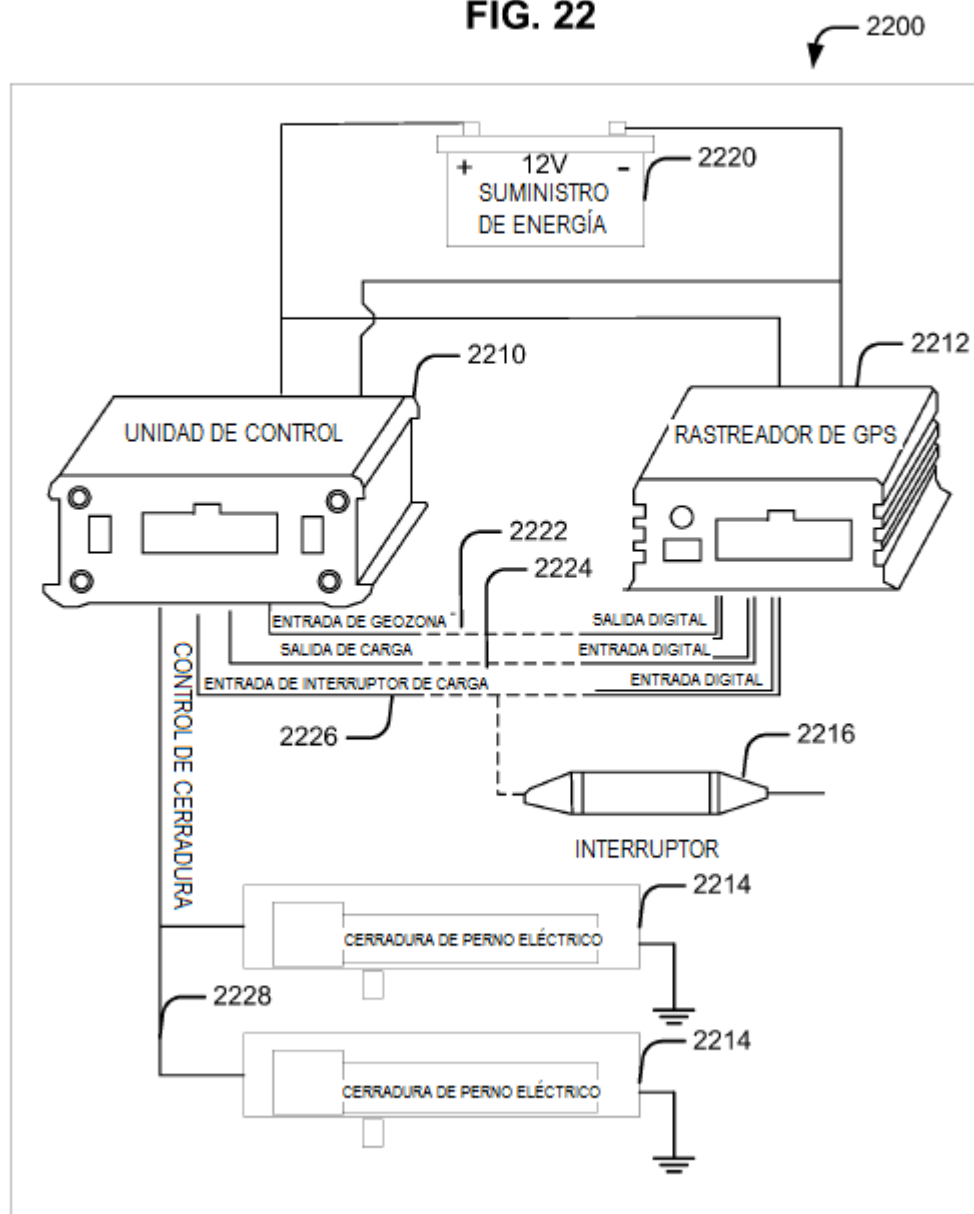


FIG. 23

CON BASE EN LA FIG. 14

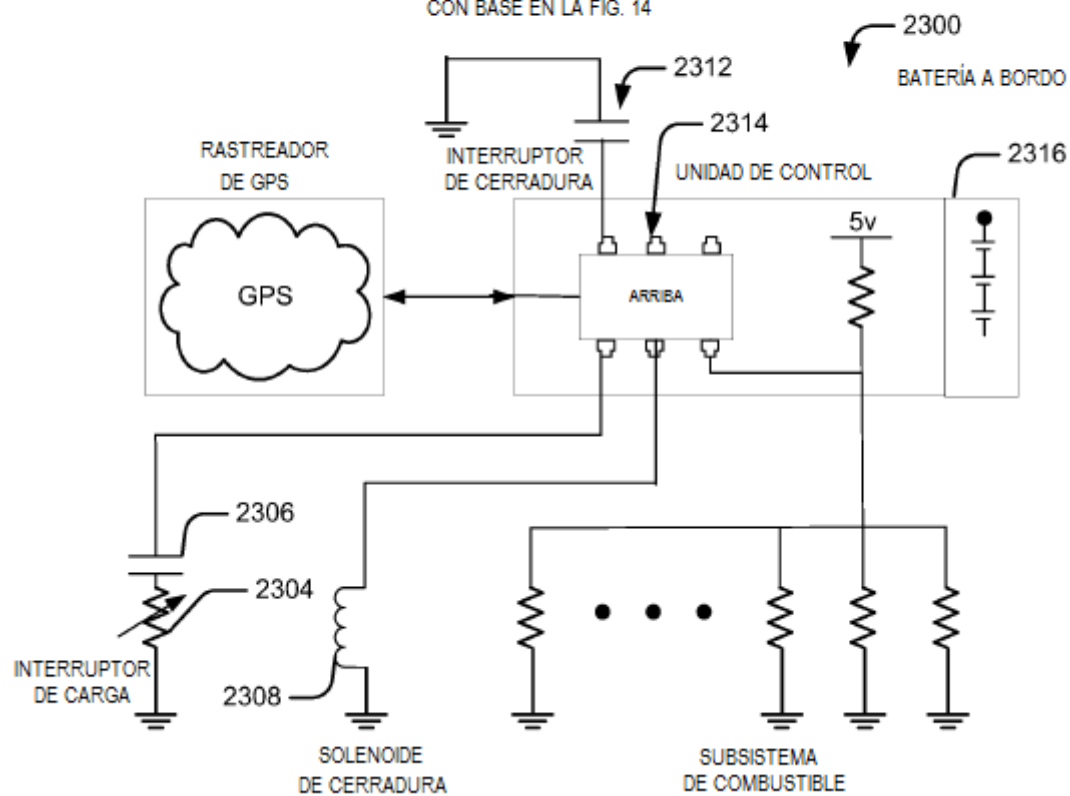
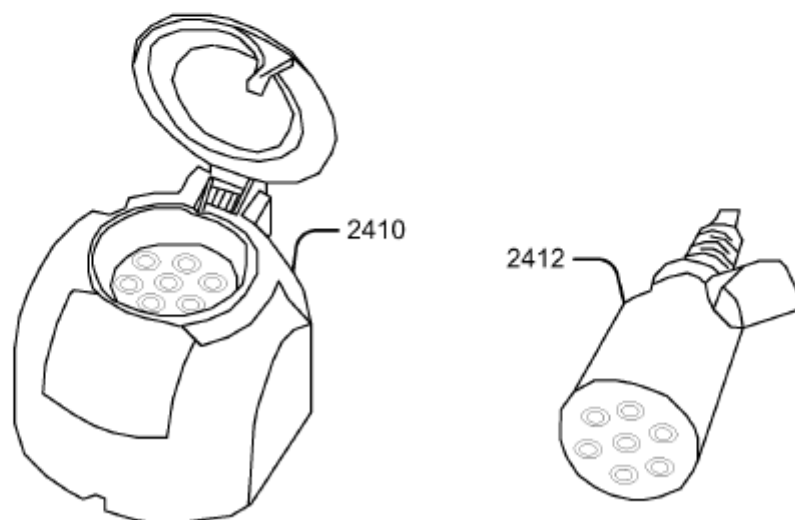
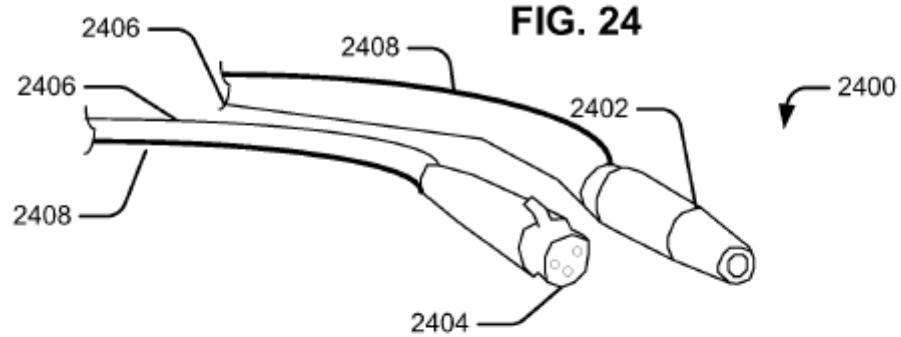


FIG. 24

INSTALACIÓN

FIG. 19

DIAGRAMA DEL SISTEMA

SOBRE LA PARTE SUPERIOR DE/
DENTRO DE LA CABINA DEL CAMIÓN

