

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 839 204**

51 Int. Cl.:

G06F 21/62 (2013.01)

H04L 29/06 (2006.01)

H04L 29/08 (2006.01)

H04L 12/40 (2006.01)

G06F 21/60 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **06.08.2015** **PCT/JP2015/003964**

87 Fecha y número de publicación internacional: **03.03.2016** **WO16031149**

96 Fecha de presentación y número de la solicitud europea: **06.08.2015** **E 15835224 (5)**

97 Fecha y número de publicación de la concesión europea: **21.10.2020** **EP 3188068**

54 Título: **Dispositivo de conversión de datos de un vehículo y método de salida de datos de un vehículo**

30 Prioridad:

26.08.2014 JP 2014171546

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
05.07.2021

73 Titular/es:

DENSO CORPORATION (100.0%)
1-1, Showa-cho,
Kariya-shi, Aichi 448-8661, JP

72 Inventor/es:

KODAMA, TOMOKO y
OKADA, MINORU

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 839 204 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Dispositivo de conversión de datos de un vehículo y método de salida de datos de un vehículo

Referencia cruzada a Solicitudes relacionadas

La presente Solicitud se basa en la Solicitud de Patente Japonesa No. 2014-171546, presentada el 26 de agosto de 2014.

Campo técnico

La presente invención se refiere a un aparato de conversión de datos de un vehículo y a un método de salida de datos que envía datos desde el interior de un vehículo al exterior del vehículo.

Técnica anterior

Por ejemplo, se ha desarrollado una tecnología en la que los usuarios se clasifican de acuerdo con atributos como publicaciones o afiliación, y un usuario de un aparato está limitado de acuerdo con esta clasificación (en referencia al documento de Literatura Patente 1, por ejemplo), como medios para limitar un aparato utilizable por cada usuario. De acuerdo con la tecnología descrita en el documento de Literatura Patente 1, una tabla de gestión de usuarios almacena información de identificación, información de autenticación e información de función utilizable de los usuarios. Cuando se registra información de autenticación de usuario mediante un medio de registro/eliminación de usuario, y cuando unos medios de autenticación de usuario determinan que el usuario es un usuario autenticado de un aparato, el aparato solo se puede utilizar para la función que el usuario debe utilizar.

Los inventores de la presente Solicitud han encontrado lo siguiente.

Recientemente, se ha empezado a solicitar información de un vehículo que se utiliza en el vehículo, desde fuera del vehículo, de manera que los datos del vehículo se utilizan fuera del vehículo. Sin embargo, cuando se puede acceder directamente a los datos del vehículo que tienen una alta confidencialidad desde el exterior del vehículo, datos del vehículo que tienen una gran importancia pueden ser manipulados directamente desde el exterior del vehículo, o bien se pueden utilizar incorrectamente los datos leídos del vehículo. La aplicación de la tecnología de autenticación descrita en el documento de Literatura Patente 1 es insuficiente para mejorar el comportamiento respecto a la seguridad de los datos del vehículo.

El documento de Literatura no Patente 1 divulga una arquitectura de preservación de la privacidad que se basa en la perturbación de los datos del lado en el cliente para garantizar la privacidad de las personas y utiliza técnicas de reconstrucción de toda la comunidad para computar información agregada de interés. En un estudio de caso de un "anализador de tráfico", tales perturbaciones se aplican a dispositivos de GPS que proporcionan información de ubicación y de velocidad de los vehículos en los que se despliegan.

El documento de Literatura Patente 2 describe un dispositivo de captación de información de un vehículo y un método de captación de información de un vehículo para captar una pluralidad de tipos de información del vehículo a través de un conector de diagnóstico del vehículo, capaces de reducir el tiempo de actualización de la información del vehículo que necesita ser actualizada, hasta un corto tiempo con el fin de mejorar la comodidad.

Documentos de literatura de la técnica anterior

Literatura Patente

Documento de Literatura Patente 1: JP 2006-344128 A

Documento de Literatura Patente 2: US2013/0304308 A1

Documento de Literatura no Patente 1: RAGHU K GANTI ET AL: "PoolView", "SENSYS '08 PROCEEDINGS OF THE 6TH ACM CONFERENCE ON EMBEDDED NETWORK SENSOR SYSTEMS" (PROCEDIMIENTOS SENSYS '08 DE LA VI CONFERENCIA DE ACM SOBRE SISTEMAS DE SENSORES DE RED INTEGRADOS, ACM, NUEVA YORK, NY, EE. UU., 5 de noviembre de 2008 (05-11-2008), páginas 281-294, XP058289558

Compendio de la invención

Es un propósito de la presente invención proporcionar un aparato de conversión de datos de un vehículo y un método de salida de datos de un vehículo que permitan la mejora del comportamiento respecto a la seguridad de los datos de vehículo almacenados en un vehículo.

Un aparato de conversión de datos de vehículo de acuerdo con un aspecto de la presente invención incluye: una parte de captación, que capta datos de vehículo pertenecientes un vehículo; una primera parte de almacenamiento, que almacena un método de tratamiento de datos para suministrar como salida los datos del vehículo al exterior del vehículo de acuerdo con un nivel de clasificación correspondiente a los datos del vehículo captados por la parte de

captación; y una parte de salida, que suministra como salida los datos del vehículo que han sido convertidos de acuerdo con el método de tratamiento de datos almacenado en la primera parte de almacenamiento. Además, de acuerdo con un aspecto de la presente invención, se proporciona un método de salida de datos de un vehículo.

De acuerdo con el aparato de conversión de datos de vehículo y el método de salida de datos de vehículo, los datos del vehículo son captados desde el interior del vehículo, y se suministran como salida los datos del vehículo convertidos de acuerdo con el método de tratamiento de datos almacenado en la primera parte de almacenamiento, en asociación con los datos del vehículo, por lo que se puede mejorar la seguridad de los datos del vehículo almacenados en el vehículo.

Breve descripción de los dibujos

Los anteriores y otros propósitos, características y ventajas de la presente invención resultarán más evidentes a partir de la siguiente descripción detallada, con referencia a los dibujos adjuntos; en los dibujos:

La Figura 1 es un diagrama de bloques que ilustra esquemáticamente una configuración eléctrica de un sistema de transmisión/recepción de datos de un vehículo de acuerdo con una primera realización;

La Figura 2 es un diagrama de bloques que ilustra esquemáticamente la configuración eléctrica de un aparato de tratamiento de datos de un vehículo;

La Figura 3 es una vista que ilustra el contenido de una lista de control de acceso que ilustra un ejemplo de clasificación de datos de vehículo y métodos de tratamiento de datos;

La Figura 4 es un diagrama de secuencia que ilustra esquemáticamente un flujo global;

La Figura 5 es un diagrama de flujo que ilustra esquemáticamente el contenido de los procesos ejecutados por el aparato de tratamiento de datos;

La Figura 6 es un diagrama de flujo que ilustra esquemáticamente el contenido de un proceso de tratamiento y actualización de datos;

La Figura 7 es un diagrama que ilustra un ejemplo de datos de máscara para un proceso de cálculo de resolución;

La Figura 8 es un diagrama de flujo que ilustra esquemáticamente el contenido de un proceso de control de actualización de datos;

La Figura 9 es un diagrama de bloques que ilustra esquemáticamente la configuración eléctrica de un sistema de transmisión/recepción de datos de vehículo de acuerdo con una segunda realización;

La Figura 10 es un diagrama de flujo que ilustra esquemáticamente el contenido de los procesos ejecutados por el aparato de tratamiento de datos;

La Figura 11 es un diagrama de flujo que ilustra esquemáticamente el contenido de un tratamiento de datos de acuerdo con una tercera realización;

La Figura 12A es un diagrama que ilustra el contenido de una lista de control de acceso que ilustra un ejemplo de clasificación de personas o aplicaciones y métodos de tratamiento de datos; y

La Figura 12B es un diagrama que ilustra el contenido de una lista de control de acceso que ilustra un ejemplo de clasificación de personas o aplicaciones y métodos de tratamiento de datos.

Descripción de realizaciones

Se describirán a continuación, con referencia a los dibujos, algunas realizaciones de un aparato de conversión de datos de un vehículo y de un método de salida de datos de un vehículo. En cada realización, los componentes que llevan a cabo operaciones iguales o similares se identifican con los mismos números de referencia, y la descripción de los mismos se omitirá cuando sea necesario. La materia objeto referida como realizaciones en la descripción se ha proporcionado a modo de ejemplo. La invención está definida por la reivindicación independiente de aparato 1 y la reivindicación independiente de método 11.

(Primera realización)

En primer lugar, se describirá la configuración esquemática de un sistema 1 de transmisión/recepción de un vehículo con referencia a la Figura 1. Como se ilustra en la Figura 1, muchas ECU 3 y 4 están instaladas en un vehículo 2, y las ECU 3 y 4 están conectadas entre sí a través de una LAN (red de área local –“Local Area Network”–) 5 instalada en el vehículo. Las ECU 3 y 4 captan información de sensor procedente de sensores (no ilustrados) dispuestos en el vehículo 2, y gobiernan dispositivos de accionamiento (no ilustrados) tales como un motor basándose en la información de los sensores. En este caso, las ECU 3 y 4 pueden implementar tecnología de alto rendimiento debido al desarrollo del comportamiento frente al entorno, seguridad, comodidad, tecnología ecológica y similares aspectos del vehículo,

en comparación con la técnica convencional. Son de varios miles a decenas de miles los datos de vehículo que se manejan en un solo vehículo, y el contenido de estos datos de vehículos se actualiza, cuando es necesario, de acuerdo con la evolución tecnológica diaria (por ejemplo, PHV (vehículo híbrido enchufable –“Plug-in Hybrid Vehicle”–)) en relación con el control de un vehículo.

Recientemente, tal como se ilustra en la Figura 1, se ha desarrollado un sistema en el que un dispositivo central 6 situado fuera del vehículo accede a las ECU 3 y 4 dispuestas en el vehículo a través de una red de comunicación externa 7 (que puede incluir una red de comunicación por cable, tal como una red de telefonía móvil, por ejemplo) que se ha desarrollado fuera del vehículo, a fin de solicitar datos del vehículo utilizados en el vehículo, y el dispositivo central 6 utiliza estos datos del vehículo. Por otra parte, de acuerdo con el reciente desarrollo de la tecnología de comunicación inalámbrica de corta distancia, de la tecnología de LAN inalámbrica de otras similares, un terminal móvil 8, tal como un terminal de tableta instalado dentro o fuera del vehículo, puede acceder a los datos del vehículo utilizando una comunicación externa 9. El sistema de la comunicación externa 9 emplea LAN inalámbrica, comunicación inalámbrica de corta distancia (por ejemplo, Bluetooth (marca registrada)) u otras similares. Sin embargo, cuando el dispositivo central 6 o el terminal móvil 8 es capaz acceder directamente a datos del vehículo altamente confidenciales retenidos en el vehículo, el aparato 6 o el terminal móvil 8 puede manipular directamente datos del vehículo que tienen gran importancia, y los datos leídos del vehículo pueden ser mal utilizados. En vista de esto, en la presente realización, la ECU para seguridad 4 está conectada a la LAN 5 instalada en el vehículo como se ilustra en la Figura 1. Para distinguir la ECU para seguridad 4 de las demás ECU 3, la ECU 4 se denomina en lo que sigue aparato 4 de tratamiento de datos.

La configuración esquemática del aparato 4 de tratamiento de datos que sirve como aparato de conversión de datos de un vehículo, se describirá con referencia a la Figura 2. La Figura 2 ilustra esquemáticamente la configuración eléctrica del aparato de tratamiento de datos en forma de diagrama de bloques. El aparato 4 de tratamiento de datos incluye una ECU que realiza un tratamiento según sea necesario cuando se solicitan datos del vehículo desde el exterior del vehículo, y determina si es procedente suministrar como salida los datos del vehículo, que se han procesado o no, al exterior del vehículo. El tratamiento indica un procedimiento para limitar la resolución de la precisión de los datos, un procedimiento para modificar un ciclo de actualización de datos, un procedimiento para modificar un sistema de cifrado de datos de acuerdo con el nivel de confidencialidad, o procedimientos similares. Sólo los datos que son aprobados por el aparato 4 de tratamiento de datos para ser suministrados como salida al exterior del vehículo pueden ser suministrados como salida al exterior del vehículo a través de un aparato de comunicación. En consecuencia, se evita que la información altamente confidencial existente en el vehículo, tal como un contenido de control, sea captada desde el exterior del vehículo.

El aparato 4 de tratamiento de datos incluye un controlador de CAN (red de área de controlador –“Controller Area Network”–) (transceptor) 11, un controlador de comunicación de conexión externa (transceptor) 12 y una microcomputadora 13. El controlador de CAN 11 establece una conexión de comunicación con la red 5 existente en el vehículo a través de una CAN, por ejemplo. La microcomputadora 13 está conectada al controlador de CAN 11 mediante un dispositivo de accionamiento 14 de CAN, a fin de establecer comunicación con las demás ECU 3 conectadas a la red 5 instalada en el vehículo. La CAN es un ejemplo de una especificación de red y un dispositivo relacionado que se pueden utilizar para un dispositivo instalado en un vehículo.

La microcomputadora 13 incluye principalmente un módulo de comunicación (Com) 15, una parte de almacenamiento de datos 16, que contiene diversos datos, una parte de control de información 17, que sirve como parte de conversión, una parte de almacenamiento de lista de control de acceso (correspondiente a una primera parte de almacenamiento) 18, que almacena una lista de control de acceso L (haciendo referencia a la Figura 3), y una pila de conexión externa (correspondiente a una parte de salida) 19, y una aplicación 100 puede usar los datos tratados por la parte de control de información 17.

La parte de almacenamiento 18 de lista de control de acceso está configurada por una memoria volátil o una memoria no volátil, por ejemplo, y almacena la lista de control de acceso L. La parte de almacenamiento 18 de la lista de control de acceso está configurada de manera que su contenido de almacenamiento es reinscribible por la parte de control de información 17. En la presente realización, la parte de almacenamiento de datos 16 está configurada por un registro, por ejemplo, y está dividida en un registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo (correspondiente a una parte de captación), y un registro de almacenamiento intermedio de comunicación externa (correspondiente a una segunda parte de almacenamiento) 16b. Con respecto al registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo, en la parte de almacenamiento de datos 16, la parte correspondiente a una trama 16c de datos de CAN es de uno a ocho bytes, y los datos de la trama 16c se dividen en datos individuales y se actualizan periódicamente mediante una señal de recepción procedente de la red 5 instalada en el vehículo.

Aquí, la presente realización describe el sistema de tal manera que utiliza CAN como comunicación dentro del vehículo. Sin embargo, se puede utilizar LIN para que la comunicación dentro del vehículo establezca una conexión de comunicación. Cabe señalar que la configuración ilustrada en la Figura 2 puede usarse comúnmente para la trama 16c y el formato de datos del registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo y manejado en una capa inferior desde el módulo de comunicación 15, en CAN y LIN.

Los datos del vehículo captados de la red 5 instalada en el vehículo se almacenan periódicamente en el registro de almacenamiento intermedio de comunicación 16a del vehículo, y la parte de control de información 17 trata los datos del vehículo almacenados basándose en la lista de control de acceso L (véase la Figura 3) almacenada en la parte de almacenamiento 18 de la lista de control de acceso, y permite que el registro de almacenamiento intermedio de comunicación externa 16b retenga los datos resultantes según sea necesario. En cuanto a los datos más adelante descritos para los que se define el ciclo de actualización, el registro de almacenamiento intermedio de comunicación externa 16b puede haberse preparado en el número correspondiente al número de clasificaciones definidas en la lista de control de acceso L para los datos individuales almacenados en el registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo.

La pila de conexión externa 19 almacena colectivamente los datos retenidos en el registro de almacenamiento intermedio de comunicación externa 16b. La microcomputadora 13 está conectada al controlador de comunicación de conexión externa 12 mediante un dispositivo de accionamiento de comunicación de conexión externa 20, y el controlador de comunicación de conexión externa 12 está conectado a una red de comunicación 7 situada fuera del vehículo a través de un módulo de comunicación inalámbrica 21, por ejemplo. Con esto, la microcomputadora 13 del aparato 4 de tratamiento de datos puede conectarse comunicativamente a la red de comunicación 7, por lo que es capaz de comunicarse con un dispositivo externo al vehículo, tal como el dispositivo central 6 o el terminal móvil 8.

Se describirá aquí la clasificación de los datos del vehículo. Como se ha descrito anteriormente, son de varios miles a decenas de miles los datos de vehículo que se manejan dentro de un solo vehículo. Los datos del vehículo se clasifican de antemano en varios tipos, y se determina un nivel de clasificación correspondiente a un nivel de seguridad de acuerdo con las clasificaciones. La presente realización describe el caso en el que los datos del vehículo se clasifican en niveles de clasificación I a IV en orden ascendente de confidencialidad y grado de importancia (nivel de seguridad).

Los datos del vehículo situados en el nivel de clasificación I se especifican como información que puede ser confirmada directamente por el usuario del vehículo, por ejemplo. Es, por ejemplo, información de un medidor que se presenta visualmente (por ejemplo, información del medidor de velocidad) y que es captada por el usuario al observar el cuadro de instrumentos del vehículo. Aquí, la información de la presentación visual de medidores son los datos tratados para el dispositivo de presentación visual de medidores por la ECU 3 montada en el vehículo 2. Por lo tanto, la información de presentación visual de los medidores, en sí, tiene la más baja confidencialidad e importancia, y se establece como el nivel de clasificación I. Los datos del vehículo contenidos en el nivel de clasificación I se agrupan según este tipo.

Los datos del vehículo contenidos en el nivel de clasificación II se definen como información de sensores tales como un sensor añadido por el usuario del vehículo 2, por ejemplo. En el caso de que el usuario del vehículo 2 monte externamente un sistema de navegación (no ilustrado) en el interior del vehículo 2 una vez adquirido el cuerpo del vehículo, el sistema de navegación montado externamente puede suministrar como salida información, tal como información diversa de la carretera (información de latitud/longitud, valor de pendiente de un nivel del suelo), a varias ECU 3 a través de la red 5 instalada en el vehículo. La diversa información anteriormente descrita que se suministra como salida por dispositivo montado externamente es de confidencialidad e importancia relativamente bajas, y se establece como el nivel de clasificación II. Los datos del vehículo contenidos en el nivel de clasificación II también se agrupan de acuerdo con este tipo.

Los datos del vehículo contenidos en el nivel de clasificación III se definen como información de un módulo ensamblado montado en el vehículo 2 de antemano, por ejemplo. Un sistema de navegación ensamblado en el vehículo (no ilustrado) suministra como salida información, tal como información diversa de la carretera (información de latitud/longitud, valor de pendiente de un nivel del suelo), a varias ECU 3 a través de la red 5 instalada en el vehículo, de forma casi similar a el sistema de navegación montado externamente descrito en lo anterior. Por otra parte, los datos sin tratar de diversos sensores (no ilustrados) tales como un sensor de velocidad del vehículo, un sensor de precipitación y diversos sensores de presión, tienen una confidencialidad e importancia relativamente altas y se clasifican en el nivel de clasificación III. Los datos del vehículo contenidos en el nivel de clasificación III también se agrupan de acuerdo con este tipo.

Los datos del vehículo contenidos en el nivel de clasificación IV se definen como información sin tratar de un valor estimado que depende de una lógica de estimación, por ejemplo. Ejemplos de tales datos de vehículo incluyen datos en bruto del par estimado de un eje y datos en bruto de un valor de pendiente estimado de un nivel de suelo. Dicha información depende de los conocimientos técnicos de un proveedor del módulo ensamblado para el vehículo 2. Cuando dicha información se suministra como salida al exterior, los conocimientos técnicos de la lógica de estimación podrían quedar expuestos de acuerdo con la información en bruto del valor estimado. En vista de esto, dichos datos se establecen como el nivel de clasificación IV, que tiene la mayor confidencialidad e importancia. Los datos del vehículo contenidos en el nivel de clasificación IV también se agrupan de acuerdo con este tipo.

A continuación, se describirá el detalle de la lista de control de acceso L almacenada en la parte de almacenamiento 18 de la lista de control de acceso. La lista de control de acceso L indica una lista en la que métodos de tratamiento de datos para enviar los datos del vehículo al exterior del vehículo, se almacenan en asociación con datos del vehículo captados desde el interior del vehículo de acuerdo con el nivel de importancia y el nivel de confidencialidad de los datos. La Figura 3 ilustra esquemáticamente el detalle de la lista de control de acceso L en la transferencia de datos entre el exterior y el interior del vehículo.

La lista de control de acceso L describe métodos de tratamiento de datos concernientes a la resolución de datos, la regulación temporal de la actualización, y el sistema de cifrado de acuerdo con los niveles de clasificación I a IV descritos anteriormente, por ejemplo. Es de destacar que el método de tratamiento de datos no se limita a estos tres tipos, y que pueden utilizarse uno o dos de los tipos de métodos de tratamiento antes mencionados u otros diversos métodos de tratamiento de datos distintos del método de tratamiento mencionado anteriormente.

Como se ilustra en la Figura 3, la parte de almacenamiento 18 de la lista de control de acceso almacena el método de tratamiento de datos de tal manera que el nivel de seguridad de los datos del vehículo se eleva al incrementarse los niveles de clasificación mencionados anteriormente (I → II → III → IV). Es decir, el nivel de clasificación I corresponde al nivel más bajo y el nivel de clasificación IV corresponde al nivel más alto. En cuanto a la resolución de datos, la parte de almacenamiento 18 de la lista de control de acceso almacena los datos en bruto, como tales, que se pueden suministrar como salida en el nivel de clasificación I, mientras que en el nivel de clasificación II se realiza con los datos en bruto un tratamiento de redondeo con el fin de ignorar los dígitos situados después del punto decimal.

La parte de almacenamiento 18 de la lista de control de acceso también almacena que el procedimiento para establecer la resolución de manera que sea A1 veces la resolución de los datos en bruto, se lleva a cabo para los datos situados en el nivel de clasificación III. Por otra parte, en cuanto a la regulación temporal de actualización, la parte de almacenamiento 18 de la lista de control de acceso almacena que no hay limitación para los datos de los niveles de clasificación I y II, mientras que un procedimiento de salida se realiza solo con un ciclo de actualización A2 (> ciclo básico) para datos situados en el nivel de clasificación III. En cuanto al método de cifrado, la parte de almacenamiento 18 de la lista de control de acceso almacena que no se lleva a cabo ningún cifrado para los datos situados en el nivel de clasificación I, mientras que se utiliza un sistema de cifrado con alta seguridad tal como el RSA (marca registrada) o el AES para los datos de los niveles de clasificación II y III. Además, la parte de almacenamiento 18 de la lista de control de acceso almacena los datos del nivel de clasificación IV, que nunca se emiten. Como se ha descrito anteriormente, los métodos de tratamiento de datos de acuerdo con los respectivos niveles de clasificación I a IV se almacenan en la parte de almacenamiento 18 de la lista de control de acceso.

A continuación, se describirá con referencia a la Figura 4 un procedimiento de funcionamiento en el caso en el que el dispositivo central 6 o el terminal móvil 8, que es el dispositivo situado fuera del vehículo, acceda a los datos del vehículo que fluyen a través de la red 5 instalada en el vehículo, a través de la red externa con el fin de solicitar los datos del vehículo. La Figura 4 ilustra una secuencia de funcionamiento esquemática completa. Nótese que el procedimiento efectuado por el aparato 4 de tratamiento de datos en la Figura 4 indica principalmente el procedimiento llevado a cabo por la microcomputadora 13.

En primer lugar, cuando el dispositivo central 6 o el terminal móvil 8 pretenden captar datos del vehículo contenidos en el vehículo 2, se realiza un registro de autenticación del dispositivo de antemano. En caso de registro de autenticación del terminal móvil 8 frente al aparato 4 de tratamiento de datos situado en el vehículo por parte del usuario del terminal móvil 8, el terminal móvil 8 emite, en primer lugar, una petición de conexión al aparato 4 de tratamiento de datos (S1). En ese momento, el terminal móvil 8 solicita autenticación transmitiendo una ID de dispositivo y un código de seguridad (código de seguridad de ID del dispositivo) del terminal móvil 8 al aparato 4 de tratamiento de datos, y el aparato 4 de tratamiento de datos devuelve datos de autenticación de acuerdo con la ID del dispositivo y el código de seguridad al terminal móvil 8, y, de esta forma, se completa el registro del dispositivo (S2). Es de destacar que el procedimiento de autenticación del terminal móvil 8 no se limita al método descrito anteriormente.

Cuando el terminal móvil 8 solicita la transmisión de datos del vehículo (S3), el tipo de datos (ID de datos) de los datos solicitados se transmite al aparato 4 de tratamiento de datos junto con la ID del dispositivo. Una vez confirmada la ID del dispositivo del terminal móvil 8 (S4) y la ID de datos (S5), el aparato 4 de tratamiento de datos permite que se suministren como salida los datos del vehículo (S6b) con la condición de que los datos puedan suministrarse como salida en el nivel de clasificación descrito en la lista de control de acceso L (S6a: SÍ). Por el contrario, cuando no se satisface esta condición (S6a: NO), el aparato 4 de tratamiento de datos no permite la salida de los datos del vehículo (S6c).

Cuando se permite la salida de los datos del vehículo, el aparato 4 de tratamiento de datos trata los datos según sea necesario y, a continuación, suministra como salida los datos tratados al terminal móvil al tiempo que controla la regulación de la secuencia temporal de comunicación (S7). Con esto, el terminal móvil 8 puede realizar un tratamiento de datos utilizando estos datos (S8). Un procedimiento similar se realiza también en el caso de que el dispositivo central 6 solicite datos a través de la conexión al aparato 4 de tratamiento de datos (S11 a S18).

A continuación, se describirá el proceso interno del aparato 4 de tratamiento de datos con referencia a las Figuras 5 a 7. La microcomputadora 13 situada en el aparato 4 de tratamiento de datos extrae datos de la red 5 instalada en el vehículo siguiendo un criterio basado en tramas (T1) y copia los datos en el registro de almacenamiento intermedio de comunicación 16a (T2) instalado en el vehículo. La parte 17 de control de información realiza el tratamiento de datos (T3) y copia los datos resultantes en el registro de almacenamiento intermedio de comunicación externa 16b (T4). El detalle del tratamiento de los datos se ilustra esquemáticamente en la Figura 6. Como se ilustra en la Figura 6, la parte de control de información 17 lee el método de tratamiento de datos de la lista de control de acceso L situada en la parte de almacenamiento 18 de la lista de control de acceso (U1), calcula la resolución (U2), almacena que se

ha de llevar a cabo el procedimiento de cifrado almacenado en la lista de control de acceso L (U3), y escribe los datos (U4). Cabe señalar que, en el intervalo del tratamiento de los datos, se puede realizar un procedimiento de detección de falsificación de datos de acuerdo con los niveles de clasificación I a IV. El procedimiento de detección de falsificación de datos puede realizarse de manera que se confirme la confianza mediante la emisión de un certificado. Alternativamente, cuando el valor de almacenamiento del registro de almacenamiento intermedio de comunicación instalado en el vehículo 16a es diferente entre los datos previos y los datos de ese momento, puede detectarse la falsificación de datos independientemente de que la magnitud de intercambio exceda o no un nivel de umbral. Alternativamente, la falsificación de datos puede detectarse utilizando un código de detección de errores tal como una suma de comprobación. De acuerdo con esto, la fiabilidad de los datos acumulados en el registro de almacenamiento intermedio de comunicación 16a del vehículo o en el registro de almacenamiento intermedio de comunicación externo 16b se puede mejorar.

La Figura 7 ilustra datos de máscara para el procedimiento de cálculo de resolución de acuerdo con el nivel de clasificación de datos. Se realiza el procedimiento para validar los datos en el dígito en el que los datos de la máscara son "1", y se realiza el procedimiento para invalidar los datos en el dígito en el que los datos de la máscara son "0". Específicamente, los datos se pueden tratar validando solo los dígitos de orden superior e invalidando los dígitos de orden inferior. La Figura 7 ilustra los datos de máscara que enmascaran datos en dígitos binarios. Sin embargo, los datos de la máscara no están limitados por estos. Los datos se pueden enmascarar en dígitos decimales (por ejemplo, según se indica por "sin tener en cuenta los dígitos después del punto decimal" en el nivel de clasificación II de la Figura 3). De esta manera, en la presente realización, el aparato de tratamiento de datos 4 trata los datos por adelantado, antes de que se emita una solicitud de datos desde el exterior.

La parte de control de información 17 realiza el tratamiento de datos en la etapa T3 de la Figura 5, y copia los datos en el registro de almacenamiento intermedio de comunicación externa 16b en la etapa T4. La parte de control de información 17 determina si se realiza o no el procedimiento de actualización en los datos copiados en cada ciclo básico predeterminado (por ejemplo, 1 milisegundo), y realiza el procedimiento de actualización según sea necesario. El proceso de control de actualización de datos llevado a cabo por la parte de control de información 17 se ilustra esquemáticamente en la Figura 8.

Como se ilustra en la Figura 8, la parte de control de información 17 determina si los datos que se actualizan según sea necesario están o no presentes en el registro de almacenamiento intermedio de comunicación 16a dispuesto en el vehículo, haciendo referencia al registro de almacenamiento intermedio de comunicación 16a dispuesto en el vehículo (V1). Cuando se determina que los datos que se han de actualizar están presentes (V1: Sí), la parte de control de información 17 incrementa los contadores de tiempo de actualización (no ilustrados) correspondientes a todos los datos que se han de actualizar, que son el objetivo de la actualización (V2), y determina si se ha establecido o no un control de actualización para el nivel de acceso de objetivo o pretendido (nivel de clasificación) (V3). En particular, los contadores de tiempo de actualización se preparan de forma preliminar en la microcomputadora 13 de manera que se correspondan con los datos individuales que se han de actualizar, por ejemplo.

Cuando se determina que se ha establecido el control de actualización para el nivel de acceso de objetivo (nivel de clasificación), la parte de control de información 17 determina si el tiempo indicado por el contador de tiempo de actualización para los datos que se han de actualizar excede o no un ciclo de actualización (V4). Cuando se determina que el tiempo excede el ciclo de actualización, la parte de control de información 17 actualiza los datos del registro de almacenamiento intermedio de comunicación externa 16b (V5) y pone el contador de tiempo de actualización a cero (V6). Los procedimientos de V3 a V6 se realizan para todos los datos que se han de actualizar (V7: Sí).

Con esto, los datos que se han de actualizar se actualizan hacia el registro de almacenamiento intermedio de comunicación externa 16b, según sea necesario, de acuerdo con la regulación temporal de actualización correspondiente a los niveles de clasificación I a IV contenidos en la lista de control de acceso L. Se describirá el ejemplo ilustrado en la lista de control de acceso L de la Figura 3. En cuanto a los datos clasificados en los niveles de clasificación I y II, todos los datos por actualizar se actualizan de inmediato en sincronización con el ciclo de actualización de los datos de CAN, mediante la ejecución de la rutina ilustrada en la Figura 8, independientemente del contenido de los contadores de actualización. Los datos clasificados en el nivel de clasificación III se actualizan de acuerdo con el ciclo de actualización A2 (> ciclo básico: ciclo fijo de 100 milisegundos, por ejemplo) del contador de actualización. Por tanto, la regulación temporal de actualización de los datos se puede modificar de acuerdo con el nivel de seguridad.

Por ejemplo, el momento en el que el dispositivo central 6 o el terminal móvil 8, que está fuera del vehículo, emite una petición de transmisión de datos hacia el interior del vehículo 2, no coincide con el momento deseable para la configuración (ECU 3 y 4) dentro del vehículo 2. Por lo tanto, el aparato 4 de tratamiento de datos hace que el registro de almacenamiento intermedio de comunicación externa 16b actualice previamente los datos tratados de acuerdo con el ciclo de actualización del contador de actualización, de conformidad con el nivel de seguridad. De esta forma, incluso cuando el dispositivo central 6 o el terminal móvil 8 emite una petición de transmisión de datos en un momento cualquiera, los datos del vehículo pueden ser inmediatamente suministrados como salida en respuesta a la petición de transmisión, de acuerdo con el nivel de seguridad de cada dato.

Como se ilustra en la Figura 5, la parte de control de información 17 existente en la microcomputadora 13 existente en el aparato 4 de tratamiento de datos trata los datos, copia los datos resultantes en el registro de almacenamiento intermedio de comunicación externa 16b, y realiza el control de actualización de datos como se ilustra en la Figura 8, en la Etapa T4. En ese momento, la microcomputadora 13 determina si se emite la petición de transmisión de los datos (T5). Cuando se emite la petición de transmisión de los datos (T5: Sí), la microcomputadora 13 capta los datos del registro de almacenamiento intermedio de comunicación externa 16b y almacena los datos en la pila de conexión externa 19 (T6). A continuación, la microcomputadora 13 lleva a cabo el procedimiento de cifrado almacenado en la etapa U3, e inscribe los datos en el controlador de comunicación de conexión externa 12 desde la pila de conexión externa 19 (T7), y el controlador de comunicación de conexión externa 12 suministra como salida los datos al dispositivo que emite la petición de transmisión, tal como el terminal móvil 8 o el dispositivo central 6 situado fuera del vehículo, a través del módulo de comunicación inalámbrica 21 (T8). De esta manera, la microcomputadora 13 puede suministrar como salida los datos al dispositivo externo que emite la petición de transmisión, cuando se emite la petición de datos.

(Ejemplo específico 1)

A continuación, se describirá un ejemplo específico. Por ejemplo, se describirá el caso en el que el dispositivo central 6 situado fuera del vehículo requiere la presentación periódica de información de velocidad de las ruedas, comunicada a través de un bus múltiple de la red 5 instalada en el vehículo. La información de velocidad de las ruedas se comunica a través de la red 5 instalada en el vehículo y se almacena periódicamente en el registro de almacenamiento intermedio de comunicación 16a del vehículo. La parte de control de información 17 lee el método de tratamiento de datos almacenado en la lista de control de acceso L, en la parte de almacenamiento 18 de la lista de control de acceso. La parte de control de información 17 determina que la información de velocidad de las ruedas captada a través de la red 5 instalada en el vehículo son los datos clasificados en el nivel de clasificación III, y lee el método de tratamiento de datos almacenado en la lista de control de acceso L, en la parte de almacenamiento 18 de la lista de control de acceso. Se supone que dicha información indica que se establece una resolución de diez veces como la "resolución de datos" de la información de velocidad del vehículo, e indica como el "tiempo de actualización" que los datos son presentados una vez después de que los datos hayan sido recibidos diez (= A2) veces a través de la red instalada en el vehículo.

A propósito de esto, la resolución de diez veces significa lo siguiente. Concretamente, cuando los datos son "50.23", "50.35", "51.23", "51.20", "51.25", "50.10", "50.33", "50.40", "50.45", "51.10", "51.21" y "51.00", en notación decimal, las cifras por debajo la primera posición decimal no se tienen en cuenta y, por lo tanto, se suministran como salida los datos de "50.2", "50.3", "51.2", "51.2", "51.2", "50.1", "50.3", "50.4", "50.4", "51.1", "51.2" y "51.0". Cabe señalar que puede emplearse un procedimiento de redondeo. Además, en el caso de que los datos se presenten una vez después de que los datos se hayan recibido diez veces, se suministran como salida "50.2", que es el primer dato, y "51.2", que es el undécimo dato, al registro de almacenamiento intermedio de comunicación externa 16b. El dispositivo central 6 emite la petición de transmisión de datos al aparato 4 de tratamiento de datos una vez que ha recibido la autenticación. Después de recibir la petición de transmisión, el aparato 4 de tratamiento de datos capta los datos del registro de almacenamiento intermedio de comunicación externa 16b, y transmite los datos al dispositivo central 6 a través del módulo de comunicación inalámbrica 21. Con esto, el dispositivo central 6 puede recibir los datos de "50.2" y "51.2" procedentes del aparato 4 de tratamiento de datos.

(Ejemplo específico 2)

El caso en el que el terminal móvil 8 solicita los datos de temperatura del agua del motor comunicados a través de la red 5 instalada en el vehículo, se describirá en el ejemplo específico 2. Los datos de la temperatura del agua del motor son comunicados a través de la red 5 instalada en el vehículo y se almacenan periódicamente en el registro de almacenamiento intermedio de comunicación 16a del vehículo. La parte de control de información 17 lee el método de tratamiento de datos almacenado en la parte de almacenamiento 18 de la lista de control de acceso, en la lista de control de acceso L. Se supone aquí que, en cuanto a la información de la temperatura del agua del motor, se establece como la "resolución de datos" el hecho de ignorar los dígitos situados por debajo del punto decimal, se establece como ausencia de limitación el "tiempo de actualización", y se emplea RSA como cifrado, por ejemplo. La parte de control de información 17 almacena los datos de temperatura del agua del motor en el registro de almacenamiento intermedio de comunicación externa 16b una vez ignorados los dígitos situados después del punto decimal.

Después de recibir la autenticación desde el aparato 4 de tratamiento de datos situado en el vehículo, el terminal móvil 8 emite la petición de transmisión de datos. Al recibir la petición de transmisión, el aparato 4 de tratamiento de datos cifra con RSA los datos de temperatura del agua del motor almacenados en el registro de almacenamiento intermedio de comunicación externa 16b, y transmite los datos resultantes al terminal móvil 8 a través del módulo de comunicación inalámbrica 21. De esta forma, el terminal móvil 8 puede recibir los datos de la temperatura del agua del motor desde el aparato 4 de tratamiento de datos.

Como se ha descrito anteriormente, de acuerdo con la presente realización, la parte de almacenamiento 18 de la lista de control de acceso almacena los métodos de tratamiento de datos con el fin de suministrar como salida los datos al exterior del vehículo de acuerdo con los niveles de clasificación I a IV, y el aparato de tratamiento de datos 4 suministra como salida datos convertidos, los cuales se han convertido basándose en el método de tratamiento de datos

correspondiente a cada uno de los niveles de clasificación I a IV de la pila de conexión externa 19. Por tanto, se puede mejorar la seguridad de los datos del vehículo almacenados en el vehículo.

Por ejemplo, a la hora de establecer medidas de seguridad para cada uno de los vehículos o para cada uno de los datos de los vehículos, se necesita mucho tiempo de trabajo humano no solo para establecer estas medidas, sino también para garantizar la calidad. Por otra parte, la presente realización gestiona los datos del vehículo presentes en cada uno de los grupos de datos clasificados según el tipo de datos del vehículo, y estos grupos de datos se clasifican dentro de los niveles de clasificación I a IV y se gestionan.

Por lo tanto, incluso cuando se desarrolla una nueva política de seguridad, no es necesario cambiar ni establecer un nivel de seguridad para cada uno de los datos del vehículo. Además, incluso cuando se añaden datos del vehículo, solo es necesario configurarlos de manera que los nuevos datos del vehículo se añadan a un grupo de datos de los niveles de clasificación I a IV clasificados preliminarmente.

Una empresa de desarrollo de un dispositivo para vehículos puede definir nuevamente los datos del vehículo como un parámetro durante el desarrollo del dispositivo de vehículo y avanzar en el desarrollo utilizando los datos del vehículo. Durante el desarrollo, los datos del vehículo son clasificados en los niveles de clasificación I a IV como en la presente realización, por lo que se puede garantizar un cierto nivel de seguridad. Sin embargo, cuando muchas empresas de desarrollo se unen al desarrollo, las políticas de seguridad pueden diferir entre estas empresas de desarrollo.

En vista de esto, de acuerdo con la presente realización, los datos del vehículo se agrupan en los niveles de clasificación I a IV, y la parte de control de información 17 puede modificar y establecer los datos del vehículo en cualquiera de los niveles de clasificación I a IV contenidos en la lista de control de acceso L almacenada en la parte de almacenamiento 18 de la lista de control de acceso. Con esto, incluso cuando las políticas de seguridad difieren entre las empresas de desarrollo, el nivel de seguridad se puede cambiar al nivel que satisfaga la demanda de estas empresas de desarrollo. Por tanto, la presente realización puede responder de manera flexible a las políticas de las empresas de desarrollo.

El registro de almacenamiento intermedio de comunicación externa 16b almacena datos convertidos que han sido previamente tratados, y, cuando se solicitan datos del vehículo desde el exterior, el registro de almacenamiento intermedio de comunicación externa 16b suministra como salida los datos convertidos. Por lo tanto, el registro de almacenamiento intermedio de comunicación externa 16b puede responder inmediatamente a la petición de transmisión de datos emitida desde el exterior.

Por otra parte, el registro de almacenamiento intermedio de comunicación externa 16b almacena los datos convertidos que han sido previamente tratados para cada uno de los niveles de clasificación I a IV de los datos del vehículo en el momento de actualización almacenado en la lista de control de acceso L situada en la parte de almacenamiento 18 de lista de control de acceso. Por lo tanto, ya sea que el ciclo de actualización esté sincronizado con el ciclo de actualización de datos con CAN, ya sea que el ciclo de actualización sea el ciclo de actualización A2 más largo que el ciclo básico, los datos convertidos pueden ser previamente preparados en el registro de almacenamiento intermedio de comunicación externa 16b, por lo que el registro de almacenamiento intermedio de comunicación externa 16b puede responder inmediatamente a la petición de transmisión de datos emitida desde el exterior.

Además, la microcomputadora 13 establece el ciclo de actualización como el ciclo de actualización A2, por ejemplo, cambiando la regulación temporal de actualización de datos de acuerdo con el ciclo de actualización de datos, y suministra como salida los datos de tal manera que el tiempo de actualización interno de los datos del vehículo y el tiempo de salida de los datos del vehículo se desincronizan. Esta configuración hace que sea difícil estimar el ciclo del control del vehículo, la regulación temporal del control del dispositivo de accionamiento por parte de la ECU 3 y similares desde el exterior.

Además, los datos son tratados de acuerdo con el atributo de datos del vehículo, y esto puede dificultar la captación de información que tiene un alto nivel de confidencialidad y seguridad, tal como el contenido del control del vehículo, desde el exterior del vehículo.

(Segunda realización)

Las Figuras 9 y 10 ilustran la segunda realización. La segunda realización indica la configuración en la que no se ha proporcionado el registro de almacenamiento intermedio de comunicación externa 16b. La primera realización indica que el aparato 4 de tratamiento de datos trata previamente los datos antes de recibir una petición de transmisión desde un dispositivo como el terminal móvil 8 o el dispositivo central 6, y almacena los datos tratados en el dispositivo de almacenamiento intermedio de comunicación externa 16b. La segunda realización indica que un aparato 104 de tratamiento de datos trata los datos en el momento de recibir una petición de transmisión desde el dispositivo 8 o 6.

El aparato 104 de tratamiento de datos de la Figura 9, que es una alternativa al aparato 4 de tratamiento de datos de la Figura 1, incluye un registro de almacenamiento intermedio de comunicación externa 16a como parte 116 de almacenamiento de datos que es una alternativa a la parte 16 de almacenamiento de datos, pero no incluye el registro de almacenamiento intermedio de comunicación externa 16b. Como se ilustra en el diagrama de flujo de la Figura 10, en lugar de como en la Figura 5, la microcomputadora 13 del aparato 104 de tratamiento de datos extrae datos a

través de la red 5 instalada en el vehículo, según un criterio por tramas (W1), y copia los datos en el registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo (W2). Estos procedimientos son los mismos que los de las etapas T1 y T2 ilustradas en la Figura 5. Sin embargo, la microcomputadora 13 espera entonces sin tratar los datos de antemano.

- 5 Cuando se recibe una petición de transmisión de datos (W3: Sí), la parte de control de información 17 del aparato 104 de tratamiento de datos capta datos del registro de almacenamiento intermedio 16a de comunicación instalado en el vehículo (W4), y trata los datos (W5). El detalle del tratamiento es similar al procedimiento de la Figura 6, por lo que se omitirá la descripción. Los datos que se han tratado se almacenan directamente en la pila de conexión externa 19. A continuación, la microcomputadora 13 inscribe los datos en el controlador de comunicación de conexión externa 12 desde la pila de conexión externa 19 (W6), y el controlador de comunicación de conexión externa 12 suministra como salida los datos al dispositivo que emite la petición de transmisión, tal como el terminal móvil 8 o el dispositivo central 6 situados fuera del vehículo, a través del módulo de comunicación inalámbrica 21 (W7). De esta manera, los datos pueden ser suministrados como salida al dispositivo 6 u 8 que emite la petición de transmisión, cuando se emite la petición de transmisión.
- 10
- 15 Como se ha descrito anteriormente, de acuerdo con la presente realización, la microcomputadora 13 convierte los datos del vehículo de acuerdo con el método de tratamiento de datos que se describe en la lista de control de acceso L, cuando se emite una petición de datos desde el exterior del vehículo. También en este caso, el método de tratamiento de datos de los datos del vehículo puede ser modificado de acuerdo con los niveles de clasificación I a IV, por lo que el nivel de seguridad de los datos del vehículo puede modificarse de acuerdo con los niveles de clasificación I a IV. Por tanto, se puede obtener el mismo efecto que en la realización anterior.
- 20

(Tercera realización)

- Las Figuras 11 a 12B ilustran la tercera realización. La tercera realización indica que se establecen medidas de seguridad para cada uno de los dispositivos que emiten una petición de transmisión de datos o cada una de las clasificaciones de aplicación. La primera realización indica la manera en que se cambian las medidas de seguridad para cada uno de los niveles de clasificación I a IV para los datos del vehículo. Por otro lado, en la presente realización, la medida de seguridad es modificable para cada uno de los dispositivos que emiten una petición de transmisión de datos o cada uno de los casos de uso de aplicación, además de la forma anteriormente descrita.
- 25

- Se instala una aplicación en un dispositivo externo como el terminal móvil 8 o el dispositivo central 6, de manera que el dispositivo externo puede acceder al aparato de tratamiento de datos 4 instalado en el vehículo desde el exterior del vehículo a través del funcionamiento de la aplicación. Aunque la fuente de acceso varía según la información, tal como un atributo de ID del terminal móvil 8 o del dispositivo central 6 (información del terminal, información del dispositivo), información personal (información de privacidad) del propietario del dispositivo, una aplicación utilizada y otra información similar, la información de ID del dispositivo que emite la petición es registrada de antemano antes de que se emita la petición de transmisión de datos (véase la Figura 4 y su descripción), como se ha descrito en las realizaciones anteriores.
- 30
- 35

- En este caso, el derecho de acceso (ya sea que el acceso esté permitido o no), pueden establecerse medidas de seguridad (método de tratamiento de datos) para cada dispositivo, cada aplicación, cada usuario de la aplicación o cada desarrollador de la aplicación. Alternativamente, el derecho de acceso puede establecerse para cada grupo tal como el trabajo o el departamento de cada desarrollador que es el usuario, y/o para cada grupo tal como una categoría o género de la aplicación, por ejemplo.
- 40

- Por ejemplo, en el caso de que el dispositivo central 6 emita una petición de datos, esta puede ser de tal manera que el nivel de seguridad (nivel de clasificación) se mantenga bajo para el operador del dispositivo central 6, mientras que el nivel de seguridad (nivel de clasificación) se eleva para un prestatario (por ejemplo, un proveedor de servicios, tal como un mensajero) del terminal móvil 8.
- 45

- Desde otro punto de vista, en el caso de que un dispositivo instalado en el dispositivo central 6 emita una petición de datos y la seguridad (confidencialidad) de la red de comunicación 7 entre el dispositivo central 6 y el vehículo 2 esté suficientemente garantizada, esta puede ser tal, que el nivel de seguridad (nivel de clasificación) se mantiene bajo para el dispositivo central 6, al contrario que en el caso anterior. Por otro lado, en el caso de que el terminal móvil 8 emita una petición de datos y la seguridad de la comunicación 9 instalada en el vehículo no esté suficientemente garantizada, el nivel de seguridad (nivel de clasificación) puede elevarse para el terminal móvil 8.
- 50

- En el caso de que se adopte la medida de seguridad más detallada, la clasificación puede establecerse de forma multidimensional, tal como los niveles de clasificación I a IV descritos en la primera realización y el nivel de clasificación para una persona o aplicación. La Figura 12A ilustra el esquema del nivel de clasificación, y la Figura 12B ilustra que la clasificación se establece de forma multidimensional. Los contenidos ilustrados en las Figuras 12A y 12B se almacenan en la parte de almacenamiento 18 de lista de control de acceso como la lista de control de acceso L.
- 55

El eje vertical indica los niveles de clasificación I a IV descritos en la primera realización, y el eje horizontal indica los niveles de clasificación X a Z para las aplicaciones. Téngase en cuenta que cada uno de los niveles de clasificación I

a IV se clasifica además en dos (el nivel de clasificación marcado con "_1" indica un nivel de seguridad baja y el nivel de clasificación marcado con "_2" indica un nivel de seguridad alta en el eje vertical en la Figura 12B).

Suponiendo que el eje horizontal indique la clasificación de una persona, el nivel de clasificación X en el eje horizontal se asigna a la información de ID de una persona que tiene una autoridad relativamente más alta para manejar datos, tal como el propietario del terminal móvil 8 o un operador de confianza del dispositivo central 6, por ejemplo. El nivel de clasificación Y en el eje horizontal se asigna a la información de ID de una persona que tiene una autoridad no tan alta como la del propietario pero que tiene una fiabilidad relativamente alta, tal como un distribuidor de automóviles (concesionario). El nivel de clasificación Z en el eje horizontal se asigna a la información de ID de un proveedor de servicios específico, como un prestatario del terminal móvil 8 o un mensajero. Por ejemplo, el nivel de clasificación Z del eje horizontal se asigna a la información de identificación de una persona que tiene menor confiabilidad que el propietario.

Suponiendo que el eje horizontal indique la clasificación de una aplicación, el nivel de clasificación X en el eje horizontal se asigna a una aplicación que requiere autenticación personal (por ejemplo, una aplicación que requiere una contraseña de inicio de sesión), y los niveles de clasificación Y y Z son asignados a aplicaciones accesibles al público. Por otra parte, estas clasificaciones pueden establecerse para cada grupo de personas o cada grupo de aplicaciones.

Como se indica en el nivel de seguridad bidimensional ilustrado en la Figura 12B, el nivel de seguridad para el nivel de clasificación X se establece de manera que sea relativamente bajo, y el nivel de seguridad para el nivel de clasificación Z se establece de manera que sea relativamente alto. Esto se basa en el esquema según el cual, cuando se emite una petición de transmisión de datos del vehículo de una persona o aplicación que tiene una alta fiabilidad, la seguridad puede mantenerse baja, y cuando se emite una petición de transmisión de datos del vehículo de una persona o aplicación que tiene una baja fiabilidad, la seguridad debe mantenerse alta.

Como se ilustra en la Figura 11, que indica esquemáticamente el método de tratamiento de datos por parte del aparato 4 de tratamiento de datos, después de captar la fuente desde la cual se ha emitido la petición de datos (ID de dispositivo) y el nombre de datos de destino (ID de datos) (X1), el aparato de tratamiento de datos 4 capta los niveles de clasificación de entre los niveles de clasificación I a IV y X a Z de la lista de control de acceso L ilustrada en las Figuras 12A y 12B (X2), calcula la resolución de acuerdo con el nivel de clasificación descrito en la lista de control de acceso L (X3), y realiza el procedimiento de cifrado (X4). Entonces, la microcomputadora 13 instalada en el aparato 4 de tratamiento de datos transmite los datos del vehículo que se han tratado a la fuente de la petición de datos. En este caso, los datos convertidos que han sido tratados pueden prepararse de antemano en el registro de almacenamiento intermedio de comunicación externa 16b como se describe en la primera realización, o bien, como en la segunda realización, el registro de almacenamiento intermedio de comunicación externa 16b puede no estar disponible, el procedimiento de conversión de datos puede realizarse en el momento de recibir una petición de datos desde el exterior, y los datos resultantes pueden ser transmitidos. De esta manera, se implementa el procedimiento de conformidad con la presente realización.

De acuerdo con la presente realización, en el caso en el que la parte de almacenamiento 18 de la lista de control de acceso almacena el método de tratamiento de datos en la lista de control de acceso L para cada una de las aplicaciones que solicitan datos del vehículo o para cada uno de los grupos de aplicaciones formados clasificando las aplicaciones, la parte de control de información 17 puede convertir o tratar los datos del vehículo de acuerdo con el método de tratamiento de datos, de forma independiente para cada una de las aplicaciones o grupos de aplicaciones. De este modo, se puede mejorar la seguridad.

Además, en el caso de que la parte de almacenamiento 18 de la lista de control de acceso almacene el método de tratamiento de datos para cada uno de los usuarios que utilizan datos del vehículo o para cada uno de los grupos de usuarios, la parte de control de información 17 puede convertir o tratar los datos del vehículo de acuerdo con el método de tratamiento de datos, de forma independiente para cada uno de los usuarios o grupos. Con esto, es posible asegurar la seguridad.

Además, en el caso de que la parte de almacenamiento 18 de la lista de control de acceso almacene multidimensionalmente el método de tratamiento de datos para cada uno de los niveles de clasificación I a IV ilustrados en la primera realización y para cada una de las aplicaciones o cada uno de los grupos de aplicaciones, la seguridad puede verse más mejorada en comparación con el procedimiento en la primera realización, por ejemplo.

Además, en el caso de que la parte de almacenamiento 18 de la lista de control de acceso almacene multidimensionalmente el método de tratamiento de datos para cada uno de los niveles de clasificación I a IV ilustrados en la primera realización y para cada uno de los usuarios o grupos de usuarios, la seguridad puede verse más mejorada en comparación con el procedimiento en la primera realización, por ejemplo.

Cuando el registro de almacenamiento intermedio de comunicación externa 16b almacena datos convertidos que han sido previamente tratados para cada una de las aplicaciones que solicitan datos del vehículo o cada uno de los grupos de aplicaciones formados al clasificar las aplicaciones, el registro de almacenamiento intermedio de comunicación externa 16b puede responder inmediatamente a la petición de transmisión de datos emitida desde el exterior.

Cuando el registro de almacenamiento intermedio de comunicación externa 16b almacena los datos convertidos que han sido previamente tratados para cada uno de los usuarios que solicitan datos del vehículo o para cada grupo de usuarios, el registro de almacenamiento intermedio de comunicación externa 16b puede responder inmediatamente a la petición de transmisión de datos emitida desde el exterior.

5 (Otras realizaciones)

La presente invención no se limita a las realizaciones descritas anteriormente, y son posibles las modificaciones o extensiones que se describen a continuación.

10 Se ha descrito anteriormente la parte de almacenamiento 18 de la lista de control de acceso, que almacena el método de tratamiento de datos en sí mismo, de acuerdo con cada uno de los niveles de clasificación I a IV. Sin embargo, la parte de almacenamiento 18 de la lista de control de acceso puede almacenar información de ID o similar del método de tratamiento de datos de acuerdo con cada uno de los niveles de clasificación I a IV, y el detalle del método de tratamiento de datos puede almacenarse por separado. El "método de tratamiento de datos" de acuerdo con la presente invención incluye esta configuración.

15 Por ejemplo, en caso de robo, puede instalarse un sensor de intrusos (no ilustrado) en el vehículo 2. En tal caso, la información del sensor de intrusos se acumula en el registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo, a través de la red 5 instalada en el vehículo. Las presentes realizaciones pueden aplicarse a la configuración en la que, cuando se produce un suceso interno relacionado con la detección de una intrusión, por ejemplo, por parte del sensor de intrusos (no ilustrado) instalado en el vehículo 2, la microcomputadora 13 suministra como salida voluntariamente datos del vehículo al dispositivo central 6 situado fuera del vehículo. También en tal caso, 20 se puede obtener el efecto descrito en las realizaciones descritas anteriormente. Las configuraciones de las realizaciones anteriormente descritas se pueden aplicar de forma independiente o en combinación.

25 El aparato 4 y 104 de tratamiento de datos corresponde a un aparato de conversión de datos de vehículos en la presente descripción, el registro de almacenamiento intermedio de comunicación 16a instalado en el vehículo corresponde a una parte de captación, el registro de almacenamiento intermedio de comunicación externa 16b corresponde a una segunda parte de almacenamiento, la parte de control de información 17 corresponde a una parte de conversión, la parte de almacenamiento 18 de la lista de control de acceso corresponde a una primera parte de almacenamiento, y la pila de conexión externa 19 corresponde a una parte de salida.

30 Se aprecia que un diagrama de flujo o el tratamiento del diagrama de flujo de la presente Solicitud incluye secciones (también denominadas etapas), cada una de las cuales se ha representado, por ejemplo, como S1, U1, T1, V1, W1 y X1. Por otra parte, cada etapa se puede dividir en varias subetapas, en tanto que varias etapas se pueden combinar en una sola etapa.

35 Aunque se han ejemplificado diversas realizaciones, configuraciones y aspectos del aparato de conversión de datos de un vehículo y el método de salida de datos de un vehículo de acuerdo con la presente invención, las realizaciones, configuraciones y aspectos de la presente invención no están limitados por los descritos anteriormente. Por ejemplo, las realizaciones, configuraciones y aspectos obtenidos de una combinación apropiada de elementos técnicos descritos en realizaciones, configuraciones y aspectos diferentes, también se incluyen dentro del alcance de las realizaciones, configuraciones y aspectos de la presente divulgación.

REIVINDICACIONES

1. Un aparato de conversión de datos de un vehículo, que comprende:

una parte de captación (16a), que capta datos de vehículo de un vehículo;

una primera parte de almacenamiento (18), que almacena un método de tratamiento de datos para suministrar como salida los datos del vehículo al exterior del vehículo de acuerdo con un nivel de clasificación correspondiente a un grupo, siendo clasificados los datos del vehículo de acuerdo con un tipo de datos del vehículo dentro del grupo;

una segunda parte de almacenamiento (16b), que almacena datos convertidos que han sido tratados de antemano por el método de tratamiento de datos almacenado en la primera parte de almacenamiento; y

una parte de salida (19), que suministra como salida los datos del vehículo que han sido convertidos de acuerdo con el método de tratamiento de datos almacenado en la primera parte de almacenamiento,

de tal manera que:

el método de tratamiento de datos no suministra como salida al exterior del vehículo los datos del vehículo incluidos en un grupo que está incluido en un nivel de clasificación que tiene la más alta confidencialidad;

la parte de salida suministra como salida los datos convertidos almacenados en la segunda parte de almacenamiento cuando los datos del vehículo son solicitados desde el exterior del vehículo;

la primera parte de almacenamiento almacena, además, un tiempo de actualización de acuerdo con el nivel de clasificación, como método de tratamiento de datos;

la segunda parte de almacenamiento almacena los datos convertidos tratados de antemano para cada uno de los niveles de clasificación de los datos del vehículo en el momento de actualización, que se almacena en la primera parte de almacenamiento;

los datos del vehículo incluidos en el grupo incluido en el nivel de clasificación que tiene la mayor confidencialidad son información en bruto de un valor estimado que depende de la lógica de estimación; y

se realiza un tratamiento de datos de acuerdo con el método de tratamiento de datos, por adelantado, antes de que se emita una petición de datos desde fuera del aparato de conversión de datos de vehículo.

2. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1, en el que:

la primera parte de almacenamiento es capaz de cambiar y establecer el método de tratamiento de datos correspondiente a los datos del vehículo de acuerdo con un cambio en una política de seguridad.

3. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1, en el que:

la primera parte de almacenamiento almacena el método de tratamiento de datos para cada una de las aplicaciones que solicitan los datos del vehículo o para cada uno de los grupos de aplicaciones configurados clasificando las aplicaciones.

4. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1 o la reivindicación 3, en el que:

la primera parte de almacenamiento almacena el método de tratamiento de datos para cada uno de los usuarios que utilizan los datos del vehículo o para cada uno de los grupos de usuarios.

5. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1, en el que:

la primera parte de almacenamiento almacena el método de tratamiento de datos para cada uno de los niveles de clasificación clasificados de acuerdo con los datos del vehículo, y también para cada una de las aplicaciones que solicitan los datos del vehículo o para cada uno de los grupos de aplicaciones configurados clasificando las aplicaciones.

6. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1 o la reivindicación 5, en el que:

la primera parte de almacenamiento almacena el método de tratamiento de datos para cada uno de los niveles de clasificación clasificados de acuerdo con los datos del vehículo, y también para cada uno de los grupos de usuarios que utilizan los datos del vehículo.

7. El aparato de conversión de datos de un vehículo de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en el que:

la primera parte de almacenamiento almacena, como método de tratamiento de datos, uno o una combinación de dos o más de un método de tratamiento de resolución de los datos del vehículo, un ciclo de actualización de datos, un sistema de cifrado de datos, y un procedimiento de detección de falsificación de datos.

8. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1, en el que:

5 la segunda parte de almacenamiento almacena los datos convertidos tratados de antemano para cada una de las aplicaciones que solicitan los datos del vehículo o para cada uno de los grupos de aplicaciones configurados clasificando las aplicaciones.

9. El aparato de conversión de datos de un vehículo de acuerdo con la reivindicación 1, en el que:

10 la segunda parte de almacenamiento almacena los datos convertidos tratados de antemano para cada uno de los usuarios que utilizan los datos del vehículo o para cada uno de los grupos de usuarios.

10. El aparato de conversión de datos de un vehículo de acuerdo con una cualquiera de las reivindicaciones 1 a 7, que comprende, además:

una parte de conversión (17), que realiza una conversión mediante el método de tratamiento de datos almacenado en la primera parte de almacenamiento, cuando los datos del vehículo se solicitan desde el exterior.

15 11. Un método de salida de datos de un vehículo, que comprende:

captar datos de vehículo de un vehículo;

almacenar un método de tratamiento de datos para enviar los datos del vehículo al exterior del vehículo de acuerdo con un nivel de clasificación correspondiente a un grupo, clasificándose los datos del vehículo de acuerdo con un tipo de datos del vehículo dentro del grupo;

20 almacenar datos convertidos que han sido tratados de antemano por el método de tratamiento de datos; y

suministrar como salida los datos del vehículo que han sido convertido de antemano de acuerdo con el método de tratamiento de datos almacenado previamente en la primera parte de almacenamiento correspondiente a los datos del vehículo,

de tal manera que:

25 el método de tratamiento de datos no envía al exterior del vehículo los datos del vehículo incluidos en un grupo que está incluido en un nivel de clasificación que tiene la más alta confidencialidad;

la parte de salida suministra como salida los datos convertidos almacenados en la segunda parte de almacenamiento, cuando los datos del vehículo son solicitados desde el exterior del vehículo;

30 la primera parte de almacenamiento almacena, además, un tiempo de actualización de acuerdo con el nivel de clasificación como método de tratamiento de datos;

la segunda parte de almacenamiento almacena los datos convertidos tratados de antemano para cada uno de los niveles de clasificación de los datos del vehículo, en el momento de actualización que está almacenado en la primera parte de almacenamiento;

35 los datos del vehículo incluidos en el grupo incluido en el nivel de clasificación que tiene la mayor confidencialidad, son información en bruto de un valor estimado que depende de la lógica de estimación; y

se realiza por adelantado un tratamiento de datos de acuerdo con el método de tratamiento de datos, antes de que se emita una petición de datos desde el exterior del aparato de conversión de datos del vehículo.

FIG. 1

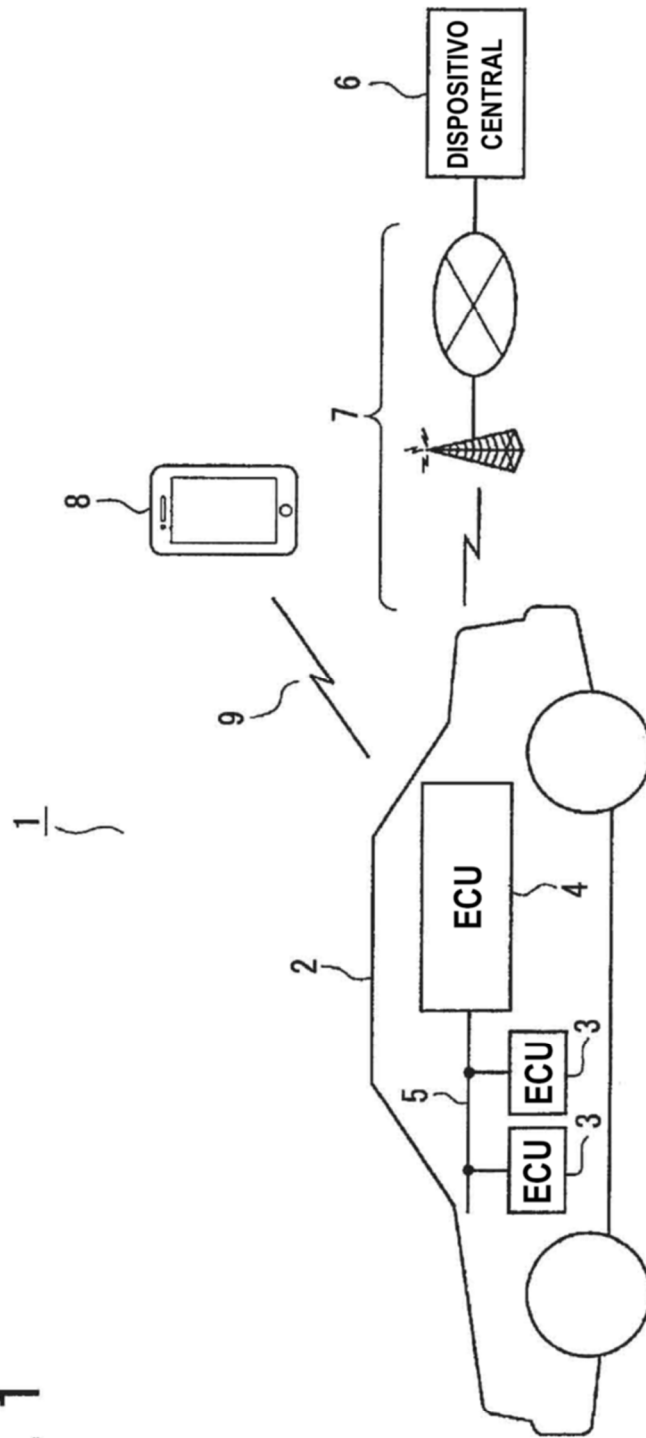


FIG. 2

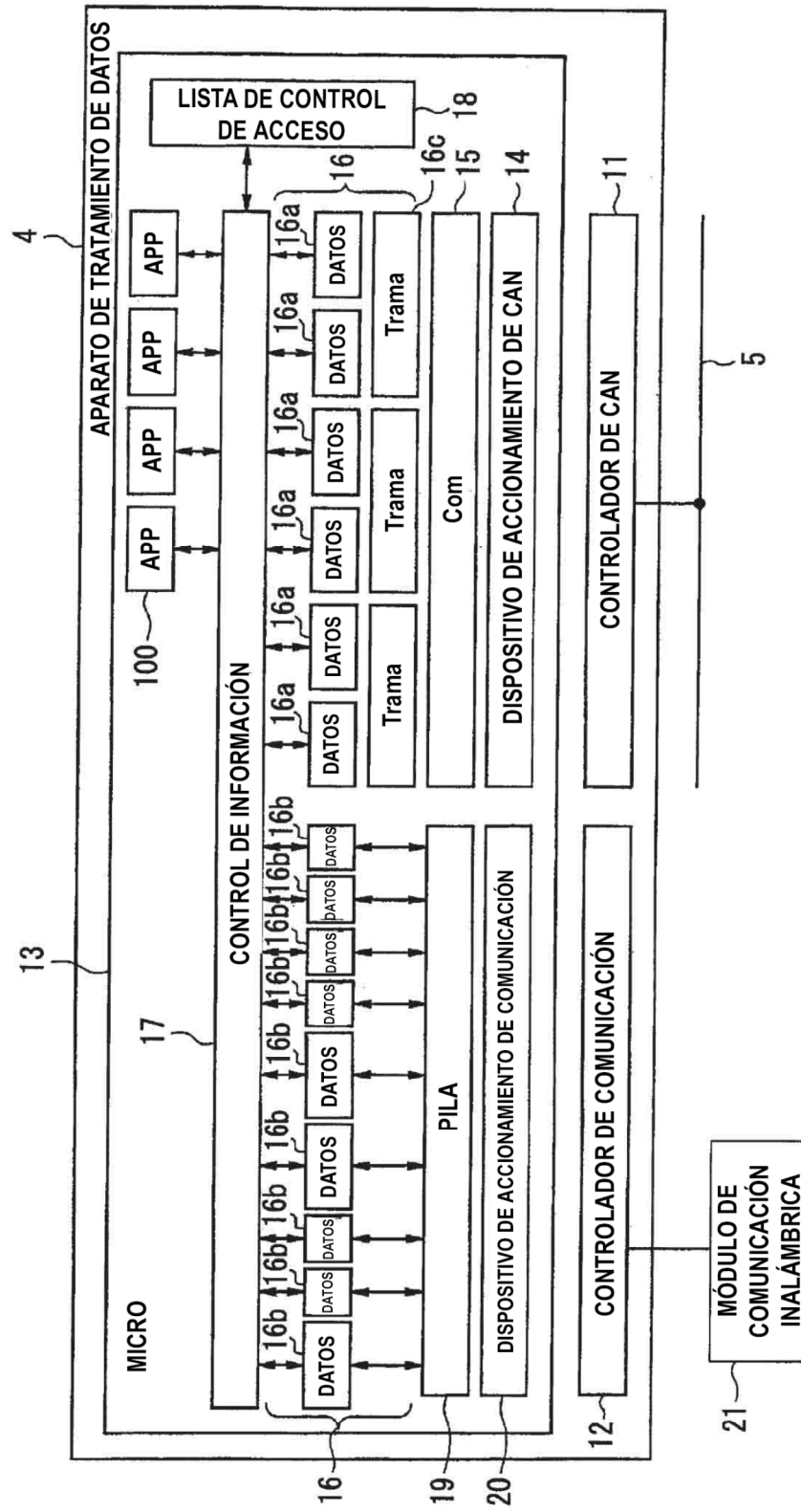


FIG. 3

18
↙

	RESOLUCIÓN DE DATOS	TIEMPO DE ACTUALIZACIÓN	SISTEMA DE CIFRADO	
NIVEL DE CLASIFICACIÓN I	DATOS EN BRUTO	SIN LIMITACIÓN	SIN CIFRADO	L
NIVEL DE CLASIFICACIÓN II	IGNORAR DÍGITOS TRAS EL PUNTO DECIMAL		RSA	...
NIVEL DE CLASIFICACIÓN III	ESTABLECER RESOLUCIÓN DE MANERA QUE SEA A1 VECES	CICLO DE ACTUALIZACIÓN A2	AES	
NIVEL DE CLASIFICACIÓN IV	INHIBIR SALIDA			

FIG. 4

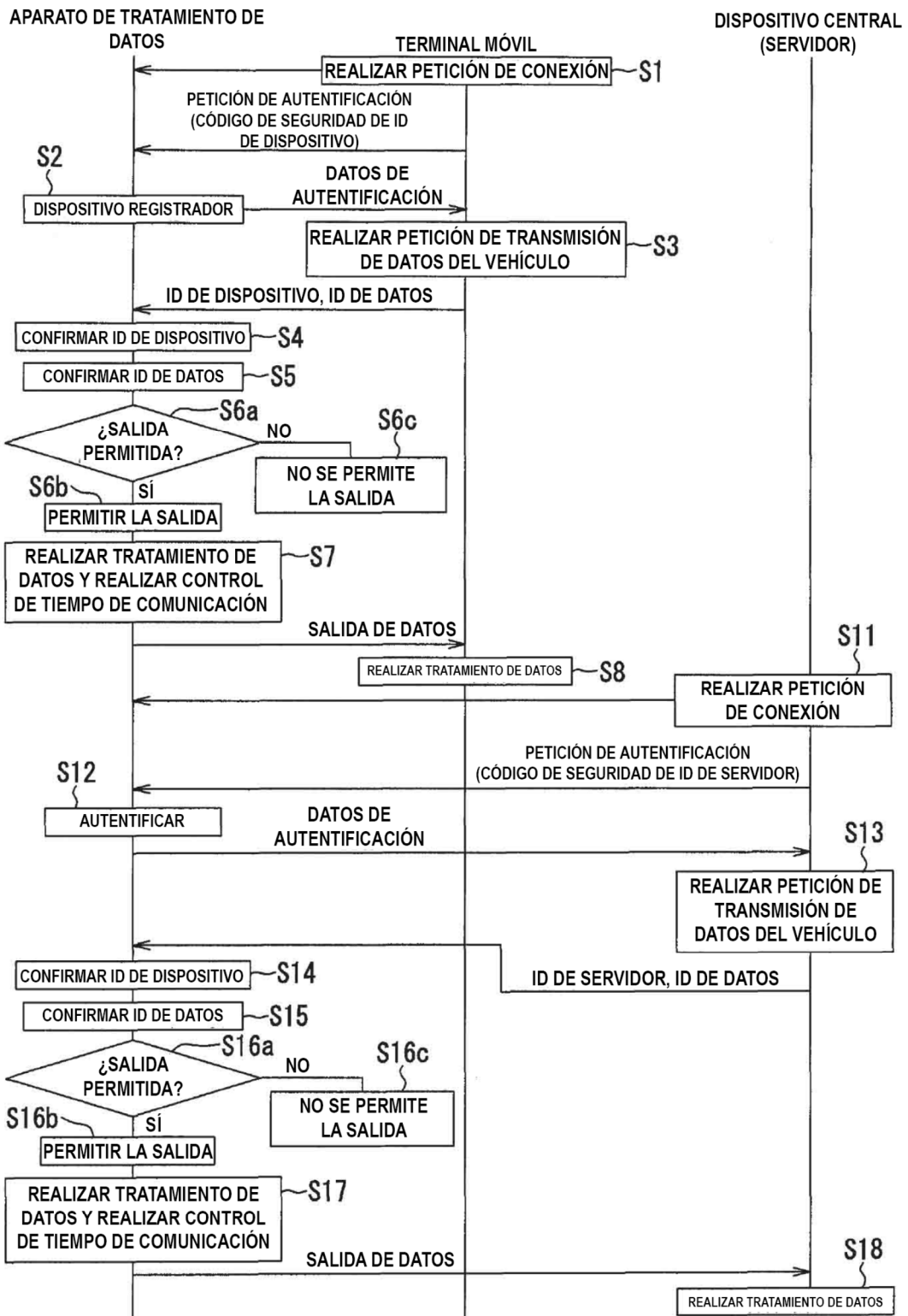


FIG. 5

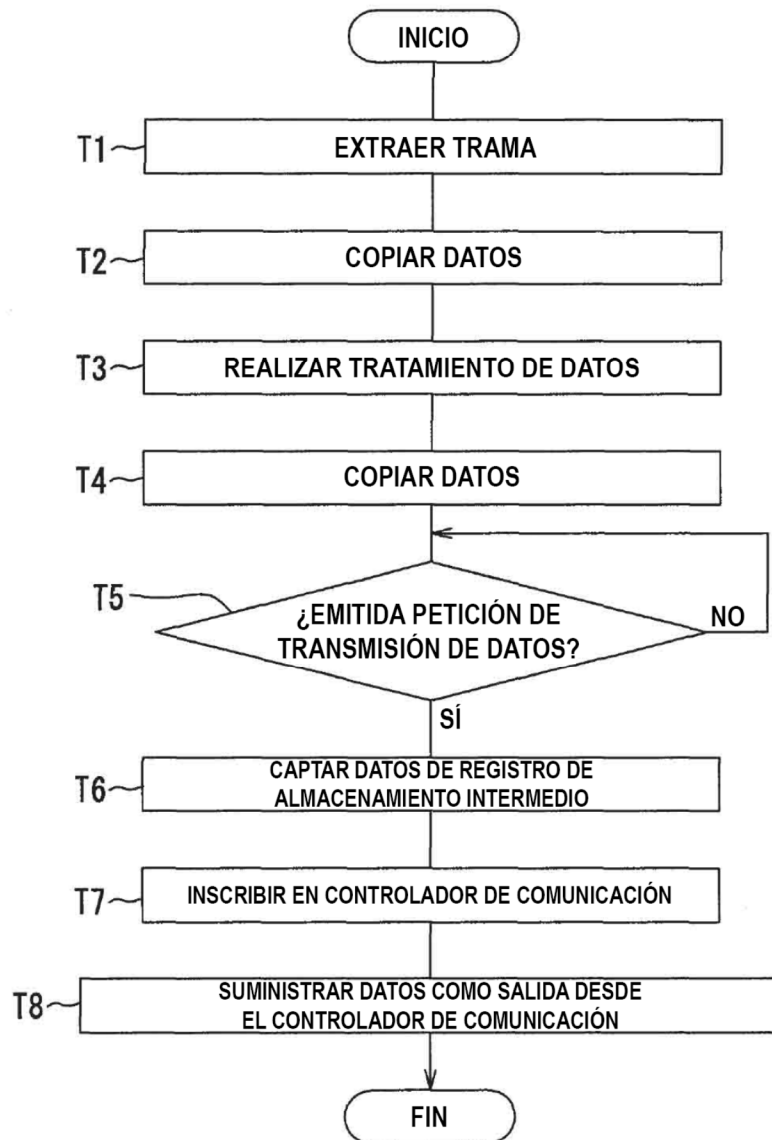


FIG. 6

TRATAMIENTO DE DATOS, PROCEDIMIENTO DE ACTUALIZACIÓN DE DATOS

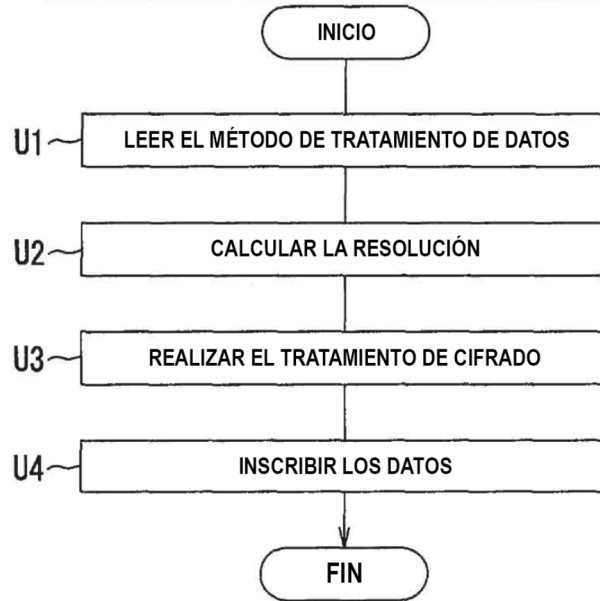


FIG. 7

NIVEL DE CLASIFICACIÓN	MÁSCARA PARA RESOLUCIÓN
I	1111 1111
II	1111 1100
III	1111 0000
IV	—

FIG. 8

PROCEDIMIENTO DE CONTROL DE ACTUALIZACIÓN DE DATOS

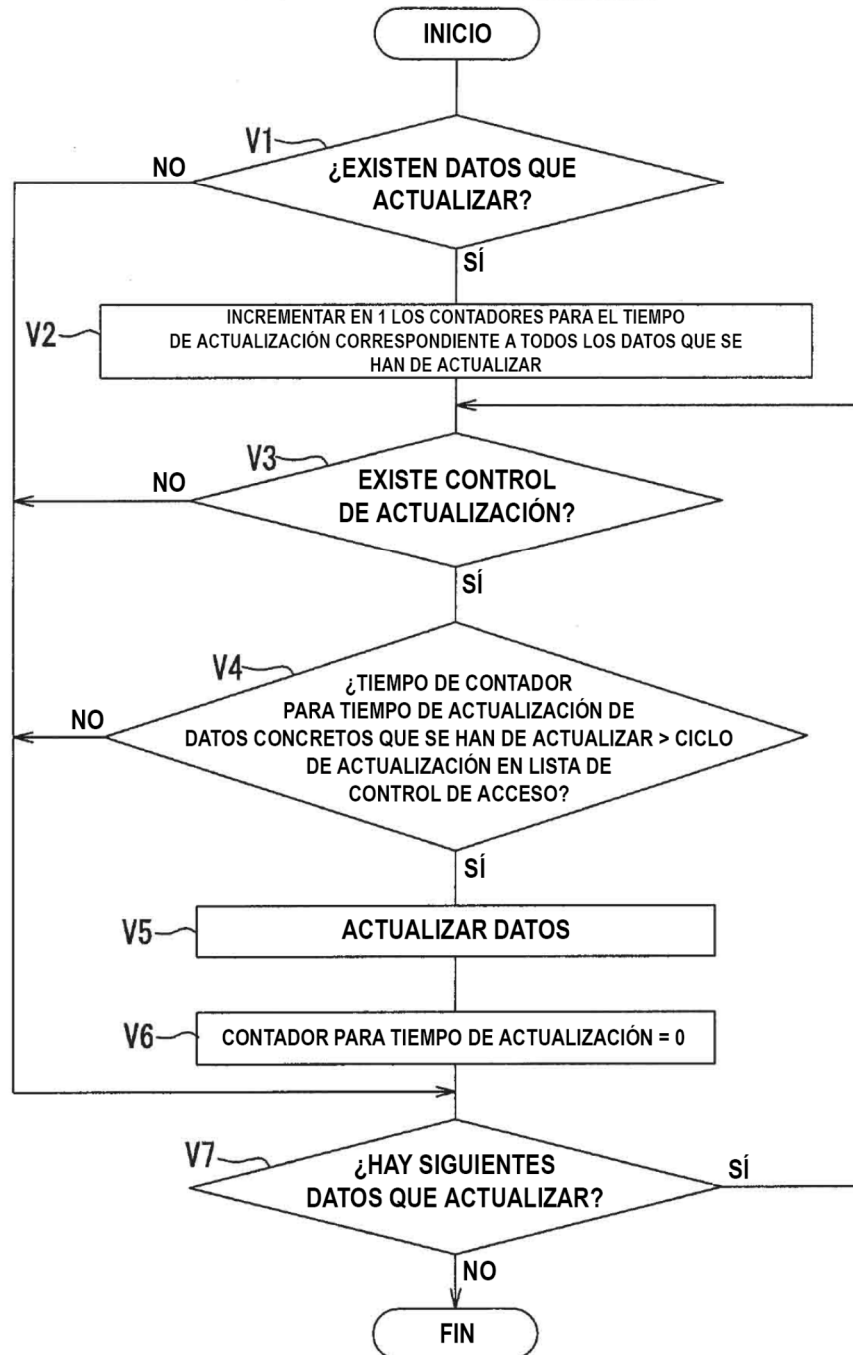


FIG. 9

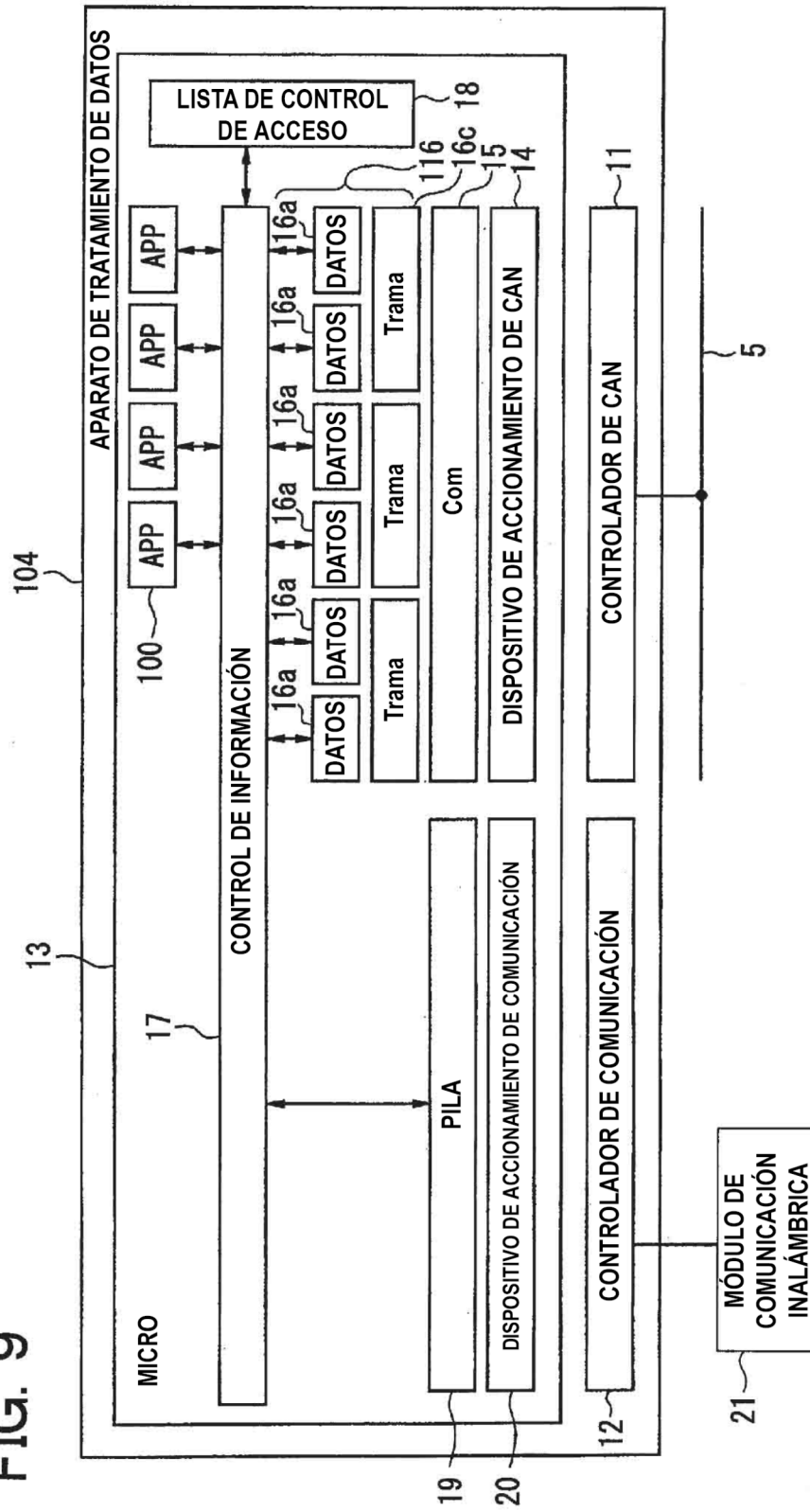


FIG. 10

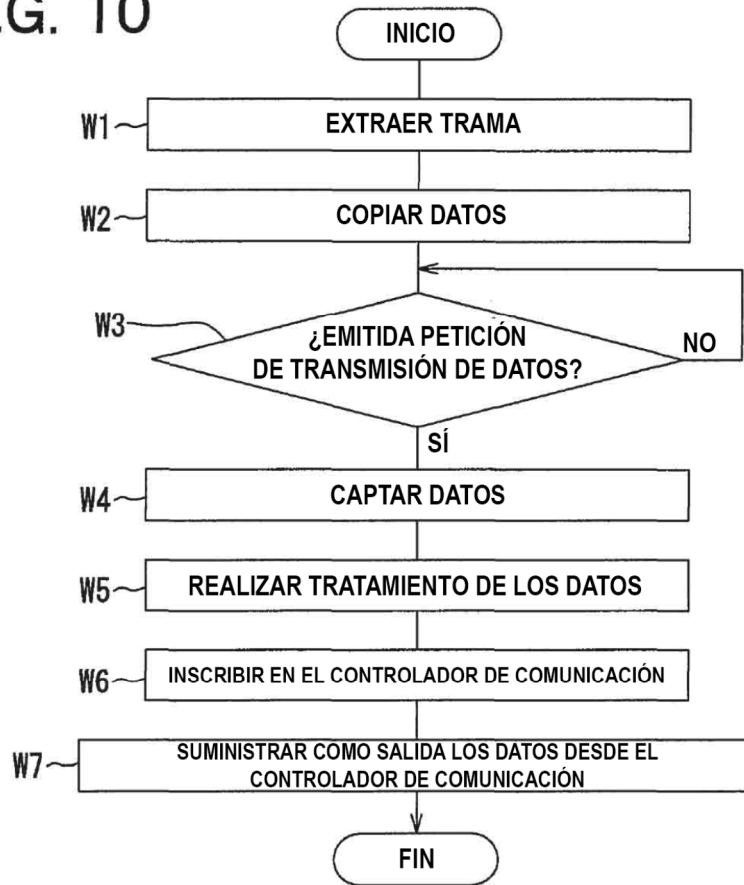


FIG. 11

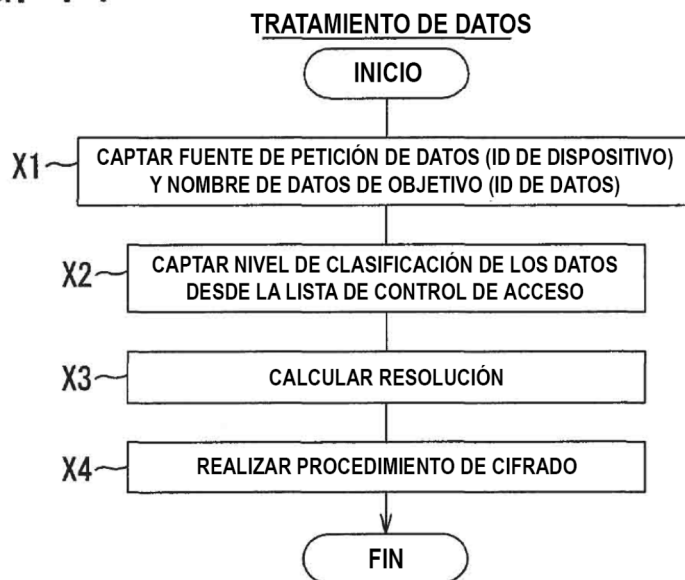


FIG. 12A

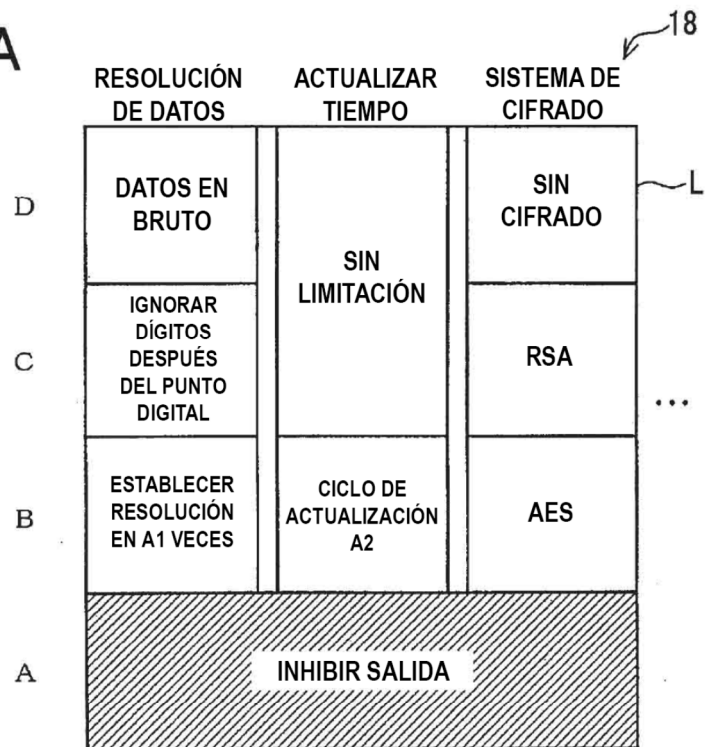


FIG. 12B

