(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 657 505**

(51) Int. CI.:

H04L 12/40 (2006.01)
H04L 29/06 (2006.01)
B60R 16/023 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.12.2013 PCT/EP2013/003635**

(87) Fecha y número de publicación internacional: **11.06.2015 WO15081969**

(96) Fecha de presentación y número de la solicitud europea: **02.12.2013 E 13799484 (4)**

(97) Fecha y número de publicación de la concesión europea: **01.11.2017 EP 3078167**

(54) Título: **Procedimiento, elemento seguro y sistema para supervisar dispositivos de red de área de controlador**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.03.2018

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

VUPPU, VIDYARANYA y
NAGAMPALLI, UDAIKAMAL

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimiento, elemento seguro y sistema para supervisar dispositivos de red de área de controlador

La invención se refiere a un procedimiento, un elemento seguro y un sistema para supervisar dispositivos de red de área de controlador.

El bus de red de área de controlador, para abreviar CAN, es un protocolo basado en mensajes diseñado originalmente para aplicaciones de automoción. Un bus CAN es un bus serie estándar para conectar unidades de control electrónicas, en adelante denominadas dispositivos de red de área de controlador, para enviar y/o recibir datos, tales como datos de sensores, información de estado y similares.

En la actualidad la tecnología CAN se aplica también a otros campos técnicos, tales como técnicas aeroespaciales, médicas y/o de automatización industrial, por ejemplo máquina a máquina, para abreviar M2M, también conocidas como SCADA o telemetría. M2M se refiere a una técnica de comunicación en la que los dispositivos se intercomunican dentro del denominado Internet de las cosas, para abreviar IOT, para enviar y/o recibir datos entre diferentes aparatos. M2M existe en formas y aplicaciones muy diferentes, por ejemplo para aumentar la eficiencia de productos, para supervisar sistemas, para medir valores característicos y/o para retransmitir información a un aparato remoto.

Debido a que un bus CAN es un protocolo de red de bajo nivel, en la tecnología CAN no se incorpora de manera intrínseca compatibilidad con funcionalidades adicionales, por ejemplo la supervisión o el control de dispositivos, la autenticación, el análisis del tráfico de datos, la provisión de una mayor seguridad y/o el diagnóstico de fallos, se espera que los dispositivos CAN implementen sus propios mecanismos para obtener esas funcionalidades adicionales.

El documento WO 2013/037996 A1 de la técnica anterior describe un vehículo que proporciona un acceso seguro a datos relacionados con la seguridad. Los datos de seguridad se incorporan en el almacenamiento de datos de una tarjeta universal de chip integrado, para abreviar UICC, normalizada. El almacenamiento de datos es accesible sobre un bus CAN a través de un traductor de bus CAN. Por lo tanto, el traductor de bus CAN convierte un mensaje CAN en un mensaje del protocolo de cable único para acceder al almacenamiento de datos para almacenar datos relacionados con la seguridad de manera segura. La UICC se utiliza únicamente como un almacenamiento de datos seguro y no tiene funcionalidades adicionales. Por lo tanto, las averías de los dispositivos CAN no se detectan en la misma.

El documento US 2008/0092227 A1 da a conocer un procedimiento y un aparato que proporcionan seguridad para un vehículo conectado en red en el que un conjunto predefinido de operaciones permitidas relacionadas con recursos protegidos se pueden iniciar de manera remota desde otro lugar en la red, mientras que la seguridad se mantiene para los recursos protegidos evitando el inicio remoto de cualquier otra operación en una unidad de procesamiento de datos que esté conectada a los recursos protegidos. Uno de un par de componentes de pasarela se ejecuta en cada una de dos unidades de procesamiento de datos dentro del vehículo, estando conectada la primera unidad de procesamiento a las unidades de control de dispositivos del vehículo y estando conectada la segunda unidad de procesamiento a la red externa. Los componentes de pasarela controlan los tipos de comunicaciones que se pueden pasar desde el lado conectado a la red hasta la primera unidad de procesamiento de tal manera que solo se pueden solicitar operaciones permitidas y no se puede iniciar de manera remota ninguna operación no autorizada.

El documento US 7.519.455 B2 da a conocer un procedimiento y un dispositivo para un servicio de telemática relacionado con vehículos. Se utiliza el mismo protocolo de aplicación para el servicio de telemática tanto para la interfaz aérea como para la comunicación en el vehículo y posiblemente en el centro de servicios.

El documento US 2010/0250053 A1 da a conocer un tacógrafo y una unidad de peaje a bordo como compañeros de comunicación, teniendo cada uno de ellos una interfaz de datos para una comunicación de datos a través de un bus de datos del vehículo al que están conectados los compañeros de comunicación. El tacógrafo y/o la unidad de peaje a bordo se implementan como un transmisor de datos para determinar un valor de comprobación criptográfica como una función de datos de usuario, que se van a transmitir al compañero de comunicación, y para transmitir el valor de comprobación criptográfica además de los datos de usuario al compañero de comunicación.

El documento WO 2013/144962 A1 da a conocer un sistema de seguridad para proteger un sistema electrónico del vehículo interviniendo selectivamente en el trayecto de comunicaciones con el fin de evitar la llegada de mensajes maliciosos a las ECU, en particular a las ECU de seguridad crítica. El sistema de seguridad incluye un filtro que evita que los mensajes ilegales enviados por cualquier sistema o dispositivo que se comunique sobre un bus de comunicaciones del vehículo alcancen su destino. El filtro puede, a su discreción conforme a las normas configuradas previamente, enviar los mensajes tal cual, bloquear los mensajes, cambiar el contenido de los mensajes, solicitar autenticación o limitar la velocidad con la que se pueden entregar dichos mensajes, almacenando

los mensajes y enviándolos únicamente en intervalos configurados previamente.

El documento US 2011/0093639 A1 da a conocer una codificación y decodificación cifradas de datos de identificación de dispositivos de bus CAN para comunicaciones entre ellos que proporciona disuasión de robo y acceso no autorizado de estos dispositivos de bus CAN seguros. Utilizando un código de cifrado único almacenado en cada uno de los dispositivos de bus CAN "autorizados", los nodos de bus CAN no autorizados no podrán comunicarse con los nodos de bus CAN autorizados, es decir, seguros, que funcionan en un sistema CAN.

Un objetivo de la invención es dar a conocer un bus CAN que proporcione una mayor robustez, un mayor nivel de seguridad que el bus CAN estándar y una mayor flexibilidad. El bus CAN debería incorporarse fácilmente en topologías de bus CAN existentes. Otro objetivo de la invención es detectar eventos creados por dispositivos CAN en un entorno no modificable para implementar acciones apropiadas y evitar averías o daños.

El objetivo identificado anteriormente se soluciona mediante un procedimiento para supervisar dispositivos CAN según la reivindicación 1. Se soluciona adicionalmente mediante un elemento seguro según la reivindicación 10. Se soluciona adicionalmente mediante un sistema CAN según la reivindicación 15.

Realizaciones ventajosas de la invención se definen en las reivindicaciones dependientes correspondientes.

El procedimiento de la invención comprende las siguientes etapas: recibir un mensaje de red de área de controlador; convertir dicho mensaje de red de área de controlador en un mensaje de elemento seguro; y proporcionar dicho mensaje de elemento seguro a un elemento seguro. Según la invención, el procedimiento comprende la etapa adicional de filtrar, en dicho elemento seguro, dicho mensaje de red de área de controlador incluido en dicho mensaje de elemento seguro dependiendo de un estado de registro de dicho mensaje de red de área de controlador.

La etapa de filtrado tiene el efecto técnico de reducir la pluralidad de mensajes CAN a una cantidad menor de mensajes CAN. Por lo tanto, el elemento seguro solo procesa los mensajes CAN que son necesarios para supervisar dicho dispositivo CAN. Esto conduce a un bus CAN que no se ralentiza procesando cada mensaje CAN del elemento seguro.

Como el elemento seguro solo es accesible a través de un canal de comunicación dedicado y opcionalmente mediante derechos de acceso estrictos, una supervisión de los dispositivos CAN se ejecuta en un aparato no modificable. Preferentemente, los datos incorporados en el mensaje CAN son datos de estado, de sensores y/o de autenticación de los dispositivos CAN.

Un elemento seguro según la invención es un elemento de tamaño y capacidad de cálculo reducidos, ya que un microcontrolador incorporado en dicho elemento seguro comprende una potencia de procesamiento muy limitada. Dicho elemento seguro comprende funcionalidades adicionales apropiadas, tales como funciones de seguridad, funciones de autenticación, funciones de firma digital, funciones de generación de contraseñas, almacenamiento seguro de datos, funciones de supervisión, funciones de diagnóstico de fallos y/o funciones de prevención de averías. El elemento seguro es preferentemente una UICC, tal como una tarjeta inteligente, una tarjeta de almacenamiento de testigos y/o un módulo de identificación de abonado, para abreviar SIM. El término SIM también incluye los términos SIM universal, CDMA-SIM, módulo de identidad de usuario extraíble, módulo de identificación M2M o realizaciones equivalentes de un SIM.

En realizaciones preferentes, el elemento seguro es un SIM, en el que el SIM se configura como un componente de hardware y se dispone como un componente integrado. El SIM se incorpora de manera fija para conectarse de manera no extraíble en la topología CAN, tal como un módulo soldado en una tarjeta de circuito impreso, o bien se incorpora de manera extraíble para ser intercambiable, tal como una tarjeta SIM con factor de forma normalizado.

En una realización alternativa el elemento seguro es un componente de software tal como una parte fiable de un núcleo del sistema operativo en la topología CAN. El elemento seguro se configura como un entorno de ejecución seguro para ejecutar programas o aplicaciones en un entorno de ejecución no modificable.

De manera ventajosa, dicho mensaje CAN comprende un estado registrado o bien un estado no registrado como dicho estado de registro. Dicho mensaje CAN registrado se procesa en dicho elemento seguro para supervisar dichos dispositivos CAN. La supervisión segura comprende un diagnóstico de un estado del sistema de bus CAN, una detección de fallos en caso de ocurrencia de mensajes CAN registrados no esperados en el elemento seguro y/o una comprobación de verosimilitud de los mensajes CAN registrados. Por lo tanto, se puede obtener una intervención apropiada en caso de eventos específicos en el bus CAN para evitar averías en el bus CAN. También es posible adaptar los procesos de cada dispositivo CAN. Como el elemento seguro es una unidad independiente en la topología del bus CAN, el bus CAN está protegido contra ataques fraudulentos.

El estado de registro no es una parte del propio mensaje CAN. Es una entrada de base de datos de una base de datos conectada al bus CAN o bien un conjunto de datos independiente. La base de datos que contiene las entradas de los mensajes CAN registrados se incluye en el elemento seguro y se administra mediante el mismo. El elemento

seguro puede añadir más mensajes CAN a la lista de mensajes CAN registrados y/o eliminar entradas de la lista de mensajes CAN registrados. En una realización preferente, la base de datos contiene todos los mensajes CAN posibles transmitidos a través del bus CAN, en la que el elemento seguro solo administra el estado de registro de cada mensaje CAN. Por lo tanto, el propio bus CAN no tiene ninguna influencia en el estado de registro de dicho mensaje CAN, lo que conduce a una mayor seguridad de dicha CAN.

El estado de registro de dichos mensajes CAN se puede cambiar de un estado no registrado a un estado registrado por medio de dicho elemento seguro. Por lo tanto, el elemento seguro obtiene una lista de mensajes CAN necesarios para supervisar dicho dispositivo. Dicha lista se obtiene de un almacenamiento de datos seguro de dicho elemento seguro o, de manera alternativa, mediante un comando de conjunto de instrucciones inalámbrico, para abreviar OTA (over-the-air). La lista está disponible en la CAN para filtrar los mensajes CAN registrados de los mensajes CAN transmitidos.

En una realización preferente, dichos mensajes CAN registrados se proporcionan mediante dicho elemento seguro durante una fase de registro, en la que la supervisión de dichos mensajes CAN registrados ocurre en una fase de supervisión. De manera adicional, el procedimiento de la invención puede comprender una fase de inicialización, en la que un aparato remoto, tal como un servidor OTA, proporciona un conjunto de instrucciones como comandos OTA al elemento seguro. De manera adicional, el procedimiento de la invención puede comprender una fase de actualización, en la que un aparato remoto, tal como un servidor OTA, proporciona correcciones al conjunto de instrucciones como comandos OTA al elemento seguro. También durante la fase de registro, la fase de inicialización y/o la fase de actualización, los mensajes CAN pueden enviarse o recibirse mediante dicho dispositivo CAN, ya que la supervisión de los mensajes CAN se realiza en un canal independiente del canal OTA. En particular, no es necesario reiniciar el elemento seguro después de que se haya realizado un registro/inicialización y/o actualización en el elemento seguro. Esto otorga al registro/inicialización y/o actualización un comportamiento dinámico.

En una realización preferente, dicho mensaje CAN registrado es un mensaje de autenticación utilizado para autenticar dicho dispositivo CAN en otro dispositivo CAN o en otro aparato conectado al bus CAN. Un fallo en el procedimiento de autenticación podría dar lugar a varias clases de ataques, en caso de que un atacante consiga introducir mensajes CAN apropiados en el bus CAN. Como dicho mensaje CAN registrado se proporciona al elemento seguro, dicho mensaje CAN registrado puede revisarse adicionalmente y comprobar su verosimilitud utilizando conjuntos de datos o información específicos del dispositivo CAN, tal como contraseñas, números de serie, etc.

De manera ventajosa, el mensaje CAN registrado contiene un evento definido previamente relacionado con una característica de dicho dispositivo CAN. La característica de dicho dispositivo CAN se supervisa mediante dicho elemento seguro. Preferentemente, dicha característica es un parámetro definido previamente, una salida de un sensor, una frase de contraseña, una pregunta de una autenticación de pregunta-respuesta y/o algún otro valor determinado previamente, enviado por dicho dispositivo CAN. Dicho evento puede constar de o comprender: ausencia de una característica esperada, desviación de una característica (por ejemplo, valor de salida de un sensor, frase de contraseña introducida, etc.) con respecto a una característica esperada (por ejemplo, valor de salida de un sensor esperado, frase de contraseña de referencia, etc.). Por ejemplo, el elemento seguro obtiene la característica de la manera prescrita y compara la característica con un valor esperado de la característica. En caso de un evento, por ejemplo si la característica recibida y la característica esperada difieren entre sí, el elemento seguro reacciona en consecuencia, por ejemplo enviando un mensaje de informe sobre el bus CAN y/o la red de radio móvil; enviando un mensaje de advertencia a un dispositivo CAN dedicado y/o al bus CAN, etc.

De manera ventajosa, un segundo mensaje de elemento seguro se genera mediante el elemento seguro, en el que el mensaje de elemento seguro se convierte en un segundo mensaje CAN y se envía sobre el bus CAN a dicho dispositivo CAN y/o a otro dispositivo CAN dedicado. Por lo tanto, se obtiene una interacción activa entre los dispositivos CAN y el elemento seguro, proporcionando una mayor seguridad en el bus CAN.

De manera ventajosa, el segundo mensaje de elemento seguro es un mensaje de respuesta a dicho mensaje de elemento seguro y/o un mensaje de comando proactivo generado mediante el elemento seguro para supervisar dicho dispositivo CAN. De manera alternativa, el segundo mensaje de elemento seguro no es un mensaje de repuesta, sin embargo se genera mediante dicho elemento seguro independientemente de los mensajes CAN registrados de dicho dispositivo CAN. Dicho segundo mensaje de elemento seguro se genera preferentemente basándose en un escenario de temporización y/o en un comando recibido mediante una red de radio móvil o un trayecto de comunicación cableado o inalámbrico adicional.

En una realización preferente, el elemento seguro se integra en un dispositivo M2M. El dispositivo M2M comprende además una unidad de módem para establecer una comunicación mediante una red de radio móvil tal como el Sistema global para comunicación móvil, es decir, GSM, el Servicio general de paquetes de radio, es decir, GPRS, el Sistema universal de telecomunicaciones móviles, es decir, UMTS, y/o la Evolución a largo plazo, es decir, LTE.

Preferentemente, el elemento seguro comprende una unidad de interfaz de mensajes para establecer un primer canal de comunicación lógico con la unidad de módem del dispositivo M2M para enviar y recibir mensajes de

elemento seguro dedicados a una unidad de módem del dispositivo M2M. Este primer canal de comunicación lógico se establece preferentemente como un protocolo de datos de UICC normalizado, por ejemplo la norma ISO 7816 o algún otro protocolo de datos apropiado útil para la comunicación entre dicho elemento seguro y dicha unidad de módem de dicho dispositivo M2M.

El dispositivo M2M se conecta también al bus CAN. Dicha unidad de interfaz de mensajes de dicho elemento seguro establece además un segundo canal de comunicación lógico para enviar y recibir mensajes de elemento seguro dedicados a dicho dispositivo CAN. Este segundo canal de comunicación lógico se establece para proporcionar mensajes de elemento seguro obtenidos de mensajes CAN registrados a dicho elemento seguro y viceversa. Protocolos de datos útiles son el Bus serie universal o el Protocolo de cable único.

De manera ventajosa, el elemento seguro se configura para enviar y recibir mensajes de elemento seguro mediante el primer y/o el segundo canales de comunicación lógicos. En consecuencia el elemento seguro puede enviar y/o recibir mensajes de elemento seguro dedicados a dicho dispositivo CAN para supervisar dicho dispositivo CAN. Además el elemento seguro puede enviar y/o recibir mensajes de elemento seguro a aparatos de la red de radio móvil a través de la unidad de módem del dispositivo M2M. De manera ventajosa solo se utiliza un canal de comunicación físico existente para establecer ambos canales de comunicación lógicos. Según una alternativa, el elemento seguro tiene dos canales físicos, por ejemplo ISO y USB, y cada uno de los dos canales lógicos se establece en un canal físico independiente.

De manera ventajosa, el elemento seguro en el dispositivo M2M es un módulo de identificación M2M, para abreviar MIM, y permite la comunicación de dispositivos CAN con aparatos de dicha red de radio móvil. Esto conduce a dispositivos CAN de medición inteligente para comunicar valores de mediciones, tales como un medidor eléctrico inteligente, un medidor de flujo de agua, etc. También conduce a dispositivos CAN de comunicación de estado, en los que dichos aparatos en dicha red de radio móvil obtienen los datos del dispositivo CAN en un entorno fiable y no modificable, protegido mediante dicho elemento seguro.

De manera ventajosa, el mensaje de elemento seguro es del tipo de unidad de datos de protocolo de aplicación, para abreviar APDU. Esta es una comunicación normalizada para dichos elementos seguros. Por lo tanto, no es necesaria ninguna adaptación para incorporar un elemento seguro de este tipo en dicha topología del bus CAN.

Para convertir el mensaje CAN en un mensaje de elemento seguro se utiliza un comando ENVELOPE. Por lo tanto, los datos transmitidos mediante el bus CAN se convierten fácilmente en un comando APDU ENVELOPE y pueden procesarse mediante el elemento seguro fácilmente.

De manera ventajosa, el elemento seguro registra dichos mensajes de elemento seguro en dicho elemento seguro. Esto se utiliza para registrar el tráfico del bus CAN de los mensajes CAN registrados. De manera alternativa, los mensajes de elemento seguro registrados se utilizan para retransmitir secuencias de datos de mensajes CAN registrados. Ambos casos de uso aumentan la seguridad de un bus CAN.

La invención se refiere, además, a un elemento seguro que comprende una interfaz de mensajes y un módulo de procesamiento de mensajes. Según la invención, un módulo de registro se configura para registrar un mensaje CAN como un mensaje CAN registrado para supervisar un dispositivo CAN. El módulo de registro se configura, además, para proporcionar el mensaje CAN registrado al bus CAN, en el que el estado de registro se utiliza para filtrar mensajes CAN registrados de mensajes CAN no registrados.

Preferentemente, el elemento seguro comprende, además, una unidad de puente para convertir dicho mensaje de elemento seguro en un mensaje de red de área de controlador, en el que dicho mensaje de red de área de controlador se envía y/o recibe a través de dicha interfaz. De manera ventajosa, el módulo de registro se implementa como una miniaplicación de elemento seguro, escrita en lenguaje nativo o JAVA. Esta miniaplicación administra dicha lista de mensajes CAN registrados y se la proporciona al bus CAN. La miniaplicación se configura para corregir dicha lista de mensajes CAN registrados conforme a conjuntos de instrucciones proporcionados por aparatos remotos o el propio elemento seguro. Esto conduce a una administración y configuración remotas de dichos mensajes CAN registrados.

Preferentemente, el elemento seguro comprende una unidad de almacenamiento de datos configurada para registrar dichos mensajes de elemento seguro originados en un dispositivo de red de controlador.

La invención se refiere, además, a un sistema CAN, que comprende al menos un dispositivo CAN, una unidad de puente y un elemento seguro. La unidad de puente comprende una base de datos de estado de registro con entradas de los mensajes CAN registrados, en la que un mensaje CAN recibido se convierte en un mensaje de elemento seguro y se proporciona a dicho elemento seguro si se incluye una entrada apropiada en la base de datos de estado de registro.

Las siguientes realizaciones de la invención se describen haciendo referencia a las figuras de los dibujos a modo de ejemplo únicamente. Se utilizan signos de referencia para las mismas características técnicas en figuras diferentes.

En los dibujos:

La figura 1 muestra un sistema CAN según la invención.

La figura 2 muestra un dispositivo M2M según la invención.

La figura 3 muestra un diagrama de bloques de un elemento seguro de la invención.

La figura 4 muestra un diagrama de flujo de un procedimiento para supervisar dispositivos CAN según la invención.

La figura 5 muestra un diagrama de flujo de la invención alternativo.

La figura 6 muestra un diagrama de flujo de la invención alternativo.

La figura 1 muestra un sistema de bus CAN de la invención. Los dispositivos CAN -1-, -1'- están conectados a un bus CAN -2-. Según la invención, un dispositivo M2M está conectado al bus CAN -2-. El dispositivo M2M incorpora un elemento seguro -4- y una unidad de control de telecomunicaciones, TCU. La TCU observa los mensajes CAN -3- transmitidos sobre el bus CAN -2-. El elemento seguro es un MIM. El elemento seguro -4- almacena una lista de mensajes CAN -3- registrados al dispositivo M2M. La lista se utiliza filtrando los mensajes CAN -3- recibidos conforme a un estado de registro de cada mensaje -3- respectivo. De manera más precisa, la lista se utiliza para filtrar los mensajes CAN -3- recibidos registrados y no filtrar los mensajes CAN -3- recibidos no registrados. En ese sentido, todos los mensajes CAN -3- se convierten en mensajes de elemento seguro -5- y se proporcionan al elemento seguro -4- con fines de supervisión. El elemento seguro -4- utiliza la lista para filtrar los mensajes CAN convertidos registrados y procesa únicamente los mensajes CAN filtrados, es decir, registrados. El elemento seguro descarta los mensajes CAN convertidos no registrados. En caso de que el dispositivo CAN -1- se comunique con el dispositivo CAN -1'- sobre el bus CAN -2-, el elemento seguro -4- supervisa dicha comunicación.

En la figura 2 se muestra en mayor detalle una realización de un dispositivo M2M según la figura 1. El bus CAN -2- está conectado a dicha TCU. La TCU según la figura 2 está conectada a una unidad de puente -6-. La unidad de puente -6- convierte los mensajes de bus CAN -3- en mensajes de elemento seguro -5-. El elemento seguro -4- comprende, además, una base de datos de estado de registro -8-. El dispositivo M2M según la figura 2 comprende, además, una unidad de módem -7- para la comunicación con un aparato remoto de una red de radio móvil. Este aparato es un servidor OTA -9- configurado para recibir y enviar mensajes de radio móvil desde la unidad de módem -7-, por ejemplo un OTA-SMS. La unidad de módem -7- está conectada a la TCU para enviar dichos mensajes de radio móvil a dichos dispositivos CAN -1- incluyendo instrucciones o peticiones del servidor OTA -9- a dichos dispositivos CAN -1- y viceversa.

El elemento seguro -4- según la figura 2 es un SIM. Como el SIM se incorpora automáticamente en el dispositivo M2M, no es necesario implementar ningún elemento seguro adicional. El SIM se incorpora de manera fija en el dispositivo M2M soldando el SIM en una tarjeta de circuito impreso de dicho dispositivo M2M. De manera alternativa puede incorporarse de manera extraíble, si el SIM es una tarjeta SIM de uno de los factores de forma normalizados.

El SIM comprende una unidad de interfaz -41- que conecta físicamente el SIM a la unidad de puente -6- y la unidad de módem -7-. La unidad de módem -7- está conectada al elemento seguro -4- mediante un primer canal de comunicación lógico -43- para enviar y recibir mensajes de elemento seguro -5- dedicados a dicho servidor OTA -9-. La unidad de puente -6- está conectada al elemento seguro -4- mediante un segundo canal de comunicación lógico -43- para enviar y recibir mensajes de elemento seguro dedicados al bus CAN -2-. Los canales de comunicación lógicos -43- pueden construirse en el mismo canal de comunicación físico -42- o, de manera alternativa, pueden construirse en canales de comunicación físicos -42- independientes.

Todos los mensajes CAN -3- del bus CAN -2- que se reciben mediante la TCU se pasan a la unidad de puente -6-. La unidad de puente -6- se configura para transformar mensajes CAN -3- en ENVELOPE APDU. En la unidad de puente -6-, todos los mensajes CAN -3- pasados se transforman en envelope APDU y, a continuación, se proporcionan, como envelope APDU, al elemento seguro -4- sobre el segundo canal de comunicación lógico -43-. Una miniaplicación -45- de elemento seguro incluida en dicho elemento seguro -4- puede recibir esos mensajes -5- desde la unidad de puente -6-. El elemento seguro -4- filtra, a continuación, los mensajes CAN transformados registrados por medio de la base de datos -8- ubicada en el elemento seguro -4-.

La miniaplicación -45- de elemento seguro puede enviar, además, un segundo mensaje de elemento seguro -5- al bus CAN -2- a través de la unidad de puente -6-. La miniaplicación -45- de elemento seguro puede activar, además, una función de retrollamada para ejecutarse cuando el bus CAN -2- transmite un mensaje CAN -3- registrado. De manera alternativa, la miniaplicación -45- añade el estado de registro en la base de datos -8- y, además, interpreta los mensajes CAN -3- registrados con fines de supervisión. Adicionalmente, la miniaplicación -45- de elemento seguro puede registrar mensajes de elemento seguro -5- con fines de análisis y/o con fines de retransmisión.

En la figura 3 se muestra un elemento seguro -4- de la invención. El elemento seguro -4- comprende una unidad de

interfaz de mensajes -41- que comprende un canal de comunicación físico -42- y dos canales de comunicación lógicos -43-, o, de manera más precisa -43a-, -43b-. Los canales de comunicación lógicos -43- se pueden separar mediante canales de comunicación físicos -42-.

La unidad de interfaz de mensajes -41- proporciona datos a la red CAN -2- y recibe mensajes de la red CAN -2- mediante una unidad de puente -6-, que obtiene mensajes CAN -3- y convierte los mensajes CAN -3- registrados en mensajes de elemento seguro -5- utilizando comandos ENVELOPE APDU. La unidad de puente -6- puede incorporarse en el elemento seguro -4- o en el dispositivo M2M según la figura 2. El elemento seguro -4- comprende, además, una unidad de procesamiento µP y una unidad de almacenamiento de datos seguros -44-. El elemento seguro -4- comprende, además, una miniaplicación -45- de filtrado y un módulo de registro -46- para proporcionar el estado de registro a la unidad de puente -6- y/o al bus CAN -2-.

Según la figura 3, la unidad de puente -6- y la base de datos -8- se pueden incorporar en el SIM, en el que la miniaplicación -45- de SIM gestiona el filtrado de dichos mensajes CAN -3- y la conversión de dichos mensajes CAN -3- registrados en mensajes de elemento seguro -5-.

Según la figura 4, se ilustra un diagrama de flujo del procedimiento de la invención para supervisar módulos CAN -1-. El procedimiento comprende una etapa de recepción -10- para recibir un mensaje CAN. Todos los mensajes recibidos se convierten en mensajes de elemento seguro según la etapa -11-. A continuación, el mensaje de elemento seguro convertido se proporciona al elemento seguro -4- según la etapa de provisión -12-. El procedimiento de la invención comprende, además, una etapa de filtrado -13- en la que se verifica un estado de registro del mensaje CAN convertido proporcionado. En caso de que el mensaje CAN convertido proporcionado sea un mensaje CAN no registrado, el procedimiento finaliza aquí. Si el mensaje CAN convertido proporcionado es un mensaje CAN registrado, el elemento seguro -4- procesa el mensaje CAN convertido en mensaje de elemento seguro en la etapa de procesamiento -14-.

La etapa de procesamiento -14- puede incluir el registro del mensaje de elemento seguro. De manera alternativa o adicional se construye un segundo mensaje de elemento seguro como respuesta a este mensaje de elemento seguro convertido. Esta respuesta se transmite a través del bus CAN -2- a un módulo CAN dedicado -1-. Un mensaje CAN registrado es por ejemplo un mensaje de autenticación, en el que un dispositivo CAN -1- desea autenticarse en otro dispositivo CAN -1'- o un servicio del servidor OTA -9-, por ejemplo, para transmitir datos al servidor OTA -9- o recibir datos del servidor OTA -9-. Para supervisar el proceso de autenticación mediante el SIM, todos los mensajes CAN de autenticación se proporcionan al SIM para la verificación del proceso de autenticación. Esto incluye una interacción de pregunta-respuesta entre el SIM y el dispositivo CAN dedicado -1-, en la que una suma de verificación o un número aleatorio se compara para comprobar la exactitud de la transmisión y para evitar cualquier ataque fraudulento.

En la figura 5 se muestra un diagrama de flujo alternativo del procedimiento de la invención. En esta se muestran un elemento seguro -4-, una red CAN -2-, un primer dispositivo CAN -1- y un segundo dispositivo CAN -1'-. La línea de puntos en la figura 4 ilustra una miniaplicación -45- de filtrado del elemento seguro -4- para ejecutar el procedimiento de la invención. El primer dispositivo CAN -1- envía un mensaje CAN -3- que se recibe en el elemento seguro -4-. El mensaje CAN -3- se convierte en un mensaje de elemento seguro -5- en la etapa -11-. El mensaje de elemento seguro -5- se filtra en una etapa de filtrado -13- con el fin de filtrar los mensajes CAN -3- incluidos en los mensajes de elemento seguro -5-. En esta, se comprueba el estado de registro de cada mensaje CAN -3- con el fin de filtrar los mensajes CAN -3- registrados. Los mensajes CAN registrados se filtran en la etapa -13- y se procesan en la etapa -14-. A continuación, se construye un segundo mensaje de elemento seguro -5- y se convierte en un segundo mensaje CAN -3- en la etapa -11'-. El segundo mensaje CAN -3- se envía sobre la red CAN -2- al dispositivo CAN -1-. De manera adicional o alternativa, el segundo mensaje CAN -2- se envía al segundo dispositivo CAN -1'-, como se ilustra mediante las líneas de puntos.

El mensaje de elemento seguro -5- es una unidad de datos de protocolo de aplicación, para abreviar APDU, que es un tipo de mensaje normalizado para la comunicación con UICC. La conversión -11- de los datos incorporados en un mensaje CAN -3- en datos incorporados en un mensaje de elemento seguro -5- se obtiene mediante un comando ENVELOPE. Por lo tanto, los mensajes CAN se transforman en ENVELOPE APDU y se proporcionan al elemento seguro -4-.

Como se puede deducir de la figura 5, la miniaplicación -45- de filtrado utiliza una unidad de puente -6- incorporada en el elemento seguro -4-. De manera alternativa, la figura 6 muestra un diagrama de flujo de un procedimiento de la invención, en el que la unidad de puente -6- es externa al elemento seguro -4-. Según la figura 6, se muestran un servidor OTA -9-, una miniaplicación -45- de elemento seguro, una unidad de puente -6- y una red CAN -2-. La red CAN -2- conecta los dispositivos CAN -1-, -1'-, lo que no se ilustra.

El diagrama de flujo según la figura 6 se divide en cuatro fases diferentes A a D, en donde las fases A y D son opcionales. Durante la fase de inicialización A, la fase de registro B y la fase de actualización C, no se transmite ningún mensaje CAN -3- sobre el bus CAN -2- para garantizar una correcta supervisión del bus CAN -2-.

Comenzando con una fase de inicialización A, el servidor OTA -9- proporciona instrucciones a la miniaplicación -45- de elemento seguro. Las instrucciones obtienen una lista de mensajes CAN -3- que debe supervisar la miniaplicación -45-. De manera adicional o alternativa, las instrucciones obtienen la información de identificación o la información de la transacción de un dispositivo CAN específico -1-, -1'- que se tiene que supervisar.

Después de recibir todas las instrucciones en la etapa -16- comienza la fase de registro B. En esta, la miniaplicación -45- de elemento seguro proporciona listas de estados de registro de los mensajes CAN -3- a la unidad de puente -6- externa. La unidad de puente -6- almacena la lista proporcionada en la base de datos -8-. De manera alternativa se proporciona una lista de eventos y/o mensajes CAN -3- registrados a la unidad de puente -6-. Estos eventos o mensajes CAN -3- proporcionados son parámetros para situaciones ambientales, por ejemplo, la transmisión de un valor de temperatura, agua, voltaje o vibración. De manera alternativa, estos eventos son eventos relacionados con la seguridad, tales como eventos del procedimiento de autenticación o eventos del procedimiento de verificación de la contraseña. De manera alternativa, estos eventos son eventos relativos a parámetros operativos de un dispositivo CAN -1-, por ejemplo un informe de estado, que podría incluir el estado de actividad, el estado de inactividad y el estado de espera. Como se ha mencionado, un evento puede implicar la entrada de un valor (por ejemplo, un valor de autenticación, un valor de un parámetro, ...), la ausencia de un valor esperado, o similares.

Después de la finalización de la fase de registro B, comienza la fase de supervisión C. Todos los mensajes CAN -3- transmitidos en el bus CAN -2- se obtienen en la unidad de puente -6-. La unidad de puente -6- filtra los mensajes CAN -3- según el estado de registro o el evento proporcionado en la fase de registro B en la etapa -13-. En caso de que el mensaje CAN -3- sea un mensaje CAN -3- registrado, la unidad de puente -6- convierte el mensaje CAN en un mensaje de elemento seguro -5- en la etapa -11-. Por lo tanto, se utilizan ENVELOPE APDU. Según la etapa -14-, la APDU se procesa en el elemento seguro -4-. Esto incluye el diagnóstico, la supervisión, el registro, la reacción de dicho mensaje de elemento seguro -5-. De manera opcional, se construye una respuesta como un comando proactivo. Esta respuesta es un segundo mensaje de elemento seguro -5- y se convierte en la unidad de puente -6-. A continuación, se obtiene un segundo mensaje CAN -3- y se envía sobre el bus CAN -2-.

En caso de que el servidor OTA -9- proporcione un conjunto de instrucciones actualizado al elemento seguro -4-, comienza la fase de actualización opcional D. De manera similar a la fase de inicialización A, se proporciona una lista actualizada de mensajes CAN -3- o información de identificación o información de la transacción de un dispositivo CAN específico -1-, -1'-.

Durante la fase de inicialización B, el elemento seguro -4- se registrará en los eventos para los que se deben recibir notificaciones en el elemento seguro -4-. La miniaplicación -45- en el elemento seguro -4- reacciona a los mensajes CAN recibidos consecuentemente. La miniaplicación -45- se puede escribir en lenguaje de programación nativo o en lenguaje de programación JAVA.

En un primer caso de uso la miniaplicación -45- asiste en el diagnóstico del bus CAN -2- localmente o bien mediante instrucciones del servidor OTA -9-. Basándose en los mensajes CAN -3- recibidos de la red CAN -2-, la miniaplicación -45- diagnostica el estado del sistema y lleva a cabo las acciones oportunas. Los procedimientos de diagnóstico en el bus CAN -2- y las acciones derivadas de los mismos son intercambiables en la fase de inicialización A o en la fase de actualización B en tiempo de ejecución proporcionando diferentes conjuntos de instrucciones a través de comandos OTA.

En un segundo caso de uso la miniaplicación -45- supervisa el bus CAN -2- en busca de tráfico disciplinado. Si se detectan actividades maliciosas durante la etapa de procesamiento -14-, la miniaplicación -45- realiza acciones correctivas inmediatamente enviando los paquetes correctos sobre el bus CAN -2-.

En un tercer caso de uso se implementa una acción correctiva para un dispositivo CAN defectuoso -1- utilizando miniaplicaciones alternativas que se descargan mediante OTA o ignorando los mensajes CAN -3- fallidos. Un primer dispositivo CAN -1- con un sensor envía un mensaje CAN -3- sobre la red -2-. El dispositivo CAN -1'- detecta el mensaje enviado y realiza o inicia una acción apropiada. Suponiendo que el sensor del dispositivo CAN -1- está averiado y no se puede sustituir inmediatamente, el dispositivo CAN -1'- no debe considerar el mensaje CAN -3- procedente del dispositivo CAN -1-. Mediante el servidor OTA -9- se carga un conjunto de instrucciones apropiado en el elemento seguro -4- en la fase A o D. El elemento seguro registra este mensaje CAN -3- fallido en la unidad de puente -6-. El mensaje CAN -3- se convierte y se proporciona al elemento seguro -4-. El elemento seguro -4- sustituye los datos del sensor averiado por datos de sensor correctivos en la etapa de procesamiento -14- y se los proporciona al bus CAN -2- para recuperar el comportamiento predeterminado del dispositivo CAN -1'-.

Otros casos de uso son la observación de la autenticación y la prevención de ataques. No se excluyen otros casos de uso.

La invención se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para supervisar dispositivos de red de área de controlador (1), comprendiendo el procedimiento las siguientes etapas:

- recibir (10) un mensaje de red de área de controlador (3);
- convertir (11) dicho mensaje de red de área de controlador (3) en un mensaje de elemento seguro (5); y
- proporcionar (12) dicho mensaje de elemento seguro (5) a un elemento seguro (4);

caracterizado por que:

- dicho mensaje de red de área de controlador (3) se recibe desde un dispositivo de red de área de controlador (1) a supervisar y se transmite sobre un bus de red de área de controlador (2); y
- dicho mensaje de red de área de controlador (3) se filtra (13) dependiendo de un estado de registro de dicho mensaje de red de área de controlador (3).

2. Procedimiento, según la reivindicación 1, en el que:

- dicho mensaje de red de área de controlador (3) comprende uno de un estado registrado y un estado no registrado como dicho estado de registro; y
- dicho mensaje de red de área de controlador se procesa (14) en dicho elemento seguro (4) para supervisar dichos dispositivos de red de área de controlador (1).

3. Procedimiento, según la reivindicación 1 o 2, en el que el estado de registro se proporciona mediante dicho elemento seguro (4), y en el que dicho mensaje de red de área de controlador registrado contiene un evento definido previamente que define una característica de dicho dispositivo de red de área de controlador (1) y se observa mediante dicho elemento seguro (4).

4. Procedimiento, según una de las reivindicaciones precedentes, en el que se genera un segundo mensaje de elemento seguro mediante dicho elemento seguro (4), en el que el segundo mensaje de elemento seguro se convierte en un segundo mensaje de red de área de controlador y se envía (10) sobre la red de área de controlador (2) a un dispositivo de red de área de controlador dedicado (1).

5. Procedimiento, según la reivindicación 4, en el que el segundo mensaje de elemento seguro es un mensaje de respuesta a dicho mensaje de elemento seguro (5) y/o un mensaje de comando proactivo generado mediante el elemento seguro (4) para supervisar dicho dispositivo de red de área de controlador (1).

6. Procedimiento, según una de las reivindicaciones precedentes, en el que dicho elemento seguro (4) se integra en un dispositivo máquina a máquina, en el que dicho elemento seguro (4) comprende una interfaz (41) para establecer:

- un primer canal de comunicación lógico (43a) para enviar y recibir mensajes de elemento seguro (5) dedicados a una unidad de módem (7) de un dispositivo máquina a máquina; y
- un segundo canal de comunicación lógico (43b) para enviar y recibir mensajes de elemento seguro (5) dedicados a los dispositivos de red de área de controlador (1).

7. Procedimiento, según una de las reivindicaciones precedentes, en el que dicho mensaje de elemento seguro (5) es una unidad de datos de protocolo de aplicación (APDU) y en el que el mensaje de red de área de controlador (3) se convierte (11) mediante un comando Envelope.

8. Procedimiento, según una de las reivindicaciones precedentes, en el que dicho estado de registro de dicho mensaje de red de área de controlador (3) se puede cambiar de un estado no registrado a un estado registrado.

9. Procedimiento, según una de las reivindicaciones precedentes, en el que dicho mensaje de elemento seguro (5) se registra en dicho elemento seguro (4).

10. Elemento seguro (4) que comprende:

- una interfaz (41) configurada para enviar y/o recibir (10) un mensaje de elemento seguro (5); y
- un módulo de procesamiento (µP) configurado para procesar (14) dicho mensaje de elemento seguro (5);

caracterizado por que:

dicho mensaje de elemento seguro (5) se convierte de un mensaje de red de área de controlador (3) que se recibe desde un dispositivo de red de área de controlador (1) a supervisar y se transmite sobre un bus de red de área de controlador (2);
el elemento seguro (4) comprende, además, un módulo de registro (46) configurado para:

- registrar (15) un mensaje de red de área de controlador (3) como un mensaje de red de área de controlador registrado para supervisar un dispositivo de red de área de controlador (1);
y
- proporcionar el mensaje de red de área de controlador registrado al dispositivo de área de controlador (1) mediante una red de área de controlador (2), en el que el estado de registro se utiliza para filtrar los mensajes de red de área de controlador registrados de los mensajes de red de área de controlador no registrados.

11. Elemento seguro, según la reivindicación 10, que comprende además una unidad de puente (6) para convertir dicho mensaje de elemento seguro (5) en el mensaje de red de área de controlador (3), en el que dicho mensaje de red de área de controlador (3) se envía y/o se recibe (10) a través de dicha interfaz (41).

12. Elemento seguro, según la reivindicación 10 u 11, en el que el módulo de registro (46) se implementa como una miniaplicación (45) de elemento seguro, en el que la miniaplicación (45) preferentemente se puede configurar y actualizar con comandos inalámbricos, OTA (over the air), mediante un servidor OTA (9).

13. Elemento seguro, según cualquiera de las reivindicaciones 10 a 12, en el que el elemento seguro (4) comprende además una unidad de almacenamiento de datos (44) configurada para registrar dichos mensajes de elemento seguro (5) que se originan en un dispositivo de red de controlador (1).

14. Elemento seguro, según cualquiera de las reivindicaciones 10 a 13, en el que la interfaz (41) se configura para establecer:

- un primer canal de comunicación lógico (43a) configurado para enviar y recibir mensajes de elemento seguro (5) dedicados a una unidad de módem (7) de un dispositivo máquina a máquina en un primer canal de comunicación físico (42a); y
- un segundo canal de comunicación lógico (43b) configurado para enviar y recibir mensajes de elemento seguro (5) dedicados a una red de área de controlador (2) en el primer canal de comunicación físico (42a) o en un segundo canal de comunicación físico (42b).

15. Sistema de red de área de controlador que comprende:

- al menos un dispositivo de red de área de controlador (1) configurado para enviar y/o recibir (10) un mensaje de red de área de controlador (3);
- una unidad de puente (6) configurada para convertir (11) dicho mensaje de red de área de controlador (3) en un mensaje de elemento seguro (5); y
- un elemento seguro (4) configurado para recibir (12) dicho mensaje de elemento seguro (5); **caracterizado por que**,

dicho mensaje de red de área de controlador (3) se recibe desde un dispositivo de red de área de controlador (1) a supervisar y se transmite sobre un bus de red de área de controlador (2); y

- el elemento seguro (4) comprende una base de datos de estado de registro (8) con entradas de mensajes de red de área de controlador registrados, en el que el mensaje de red de área de controlador (3) recibido se filtra (13) verificando si una entrada apropiada está incluida en la base de datos de estado de registro (8), y se convierte en dicho mensaje de elemento seguro (5) y se proporciona a dicho elemento seguro (4) si una entrada apropiada está incluida en la base de datos de estado de registro (8).

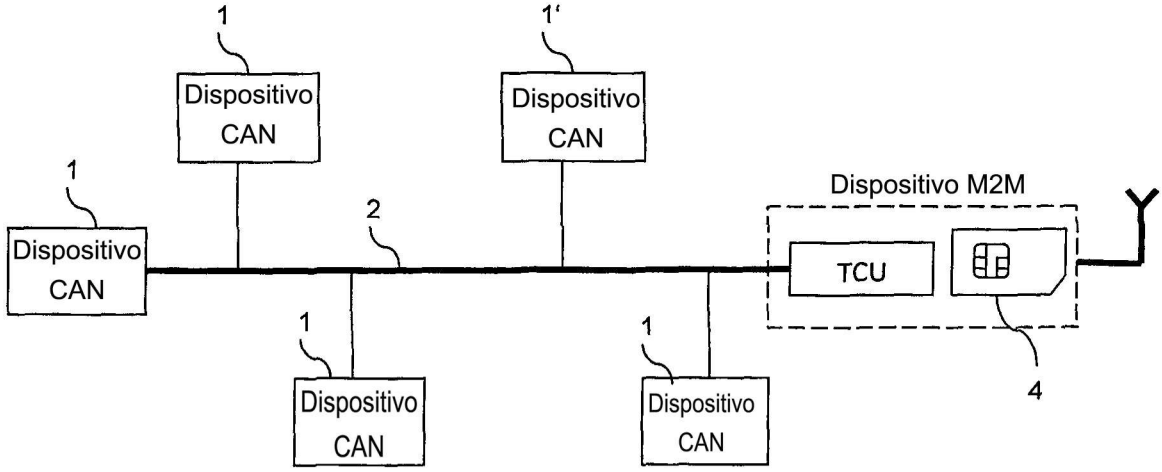
1
Dispositivo CAN
1'
Dispositivo CAN
1
Dispositivo CAN
2
Dispositivo M2M
TCU
1
Dispositivo CAN
1
Dispositivo CAN
4

Fig. 1

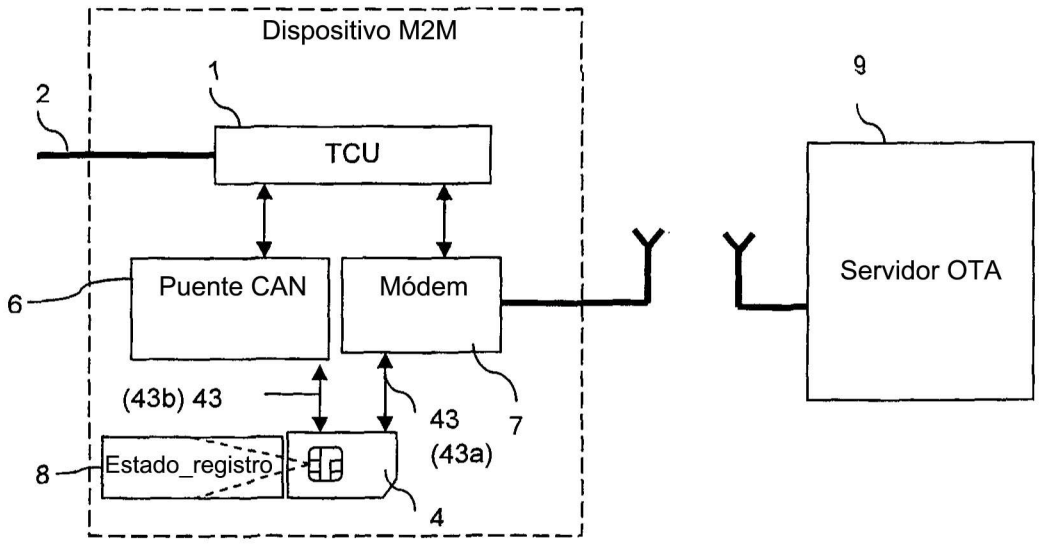
Dispositivo M2M
1
2
TCU
9
Servidor OTA
6
Puente CAN
Módem
(43b) 43
43
(43a)
7
8
Estado_registro
4

Fig. 2

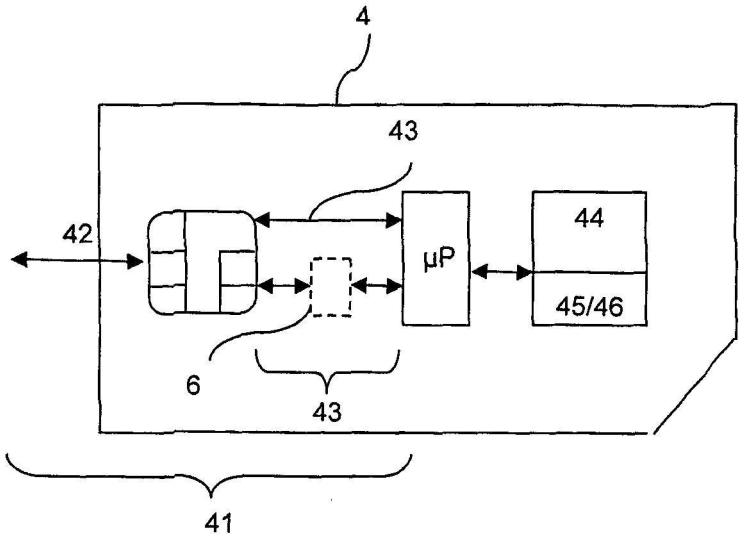
4
43
42
μP
44
45/46
6
43
41

Fig. 3

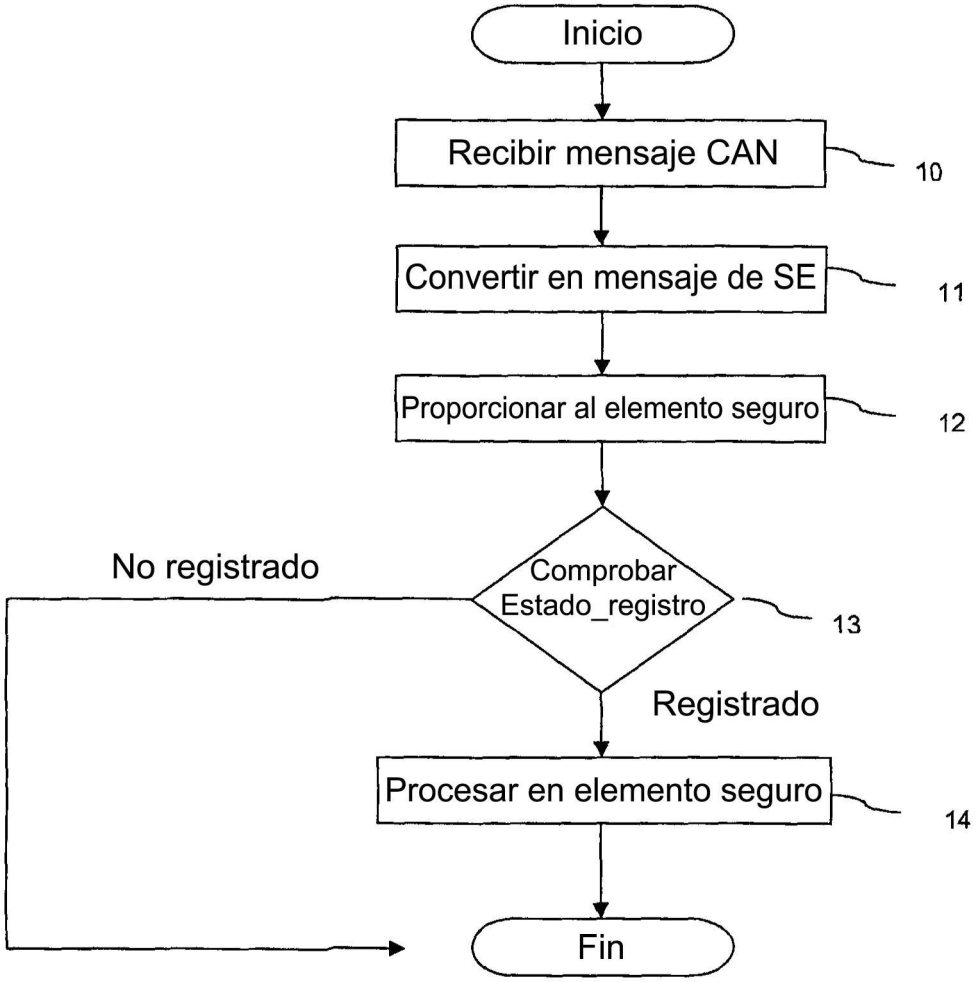
Inicio
Recibir mensaje CAN
10
Convertir en mensaje de SE
11
Proporcionar al elemento seguro
12
Comprobar Estado_registro
13
No registrado
Registrado
Procesar en elemento seguro
14
Fin

Fig. 4

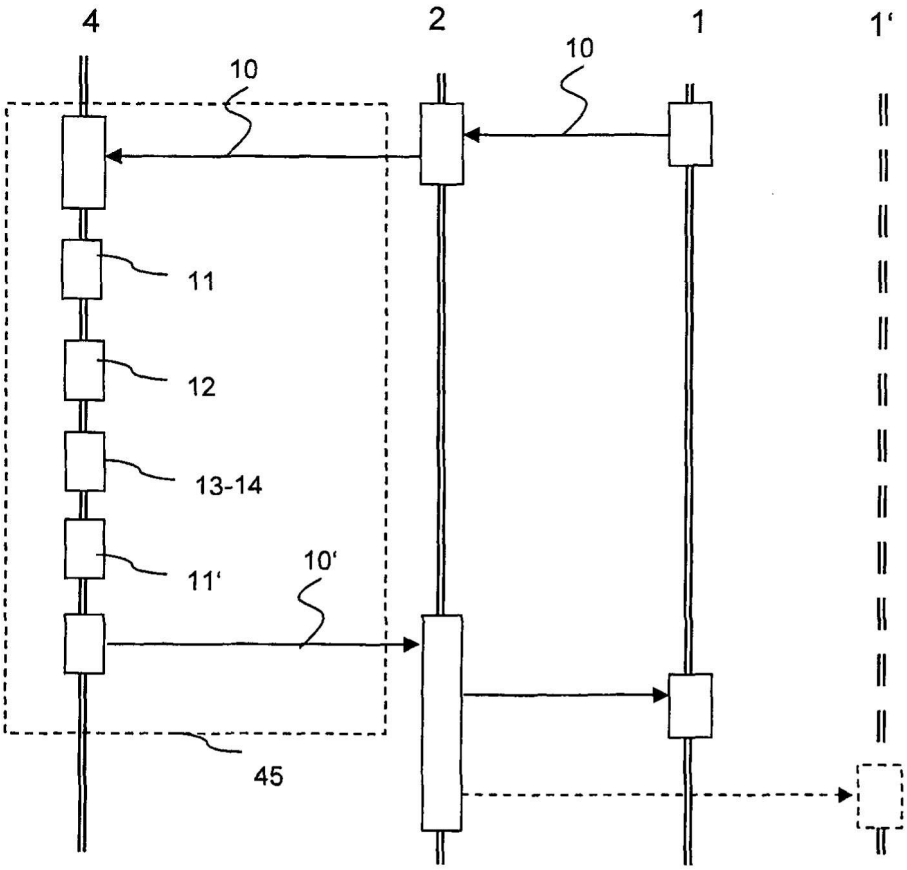

Fig. 5

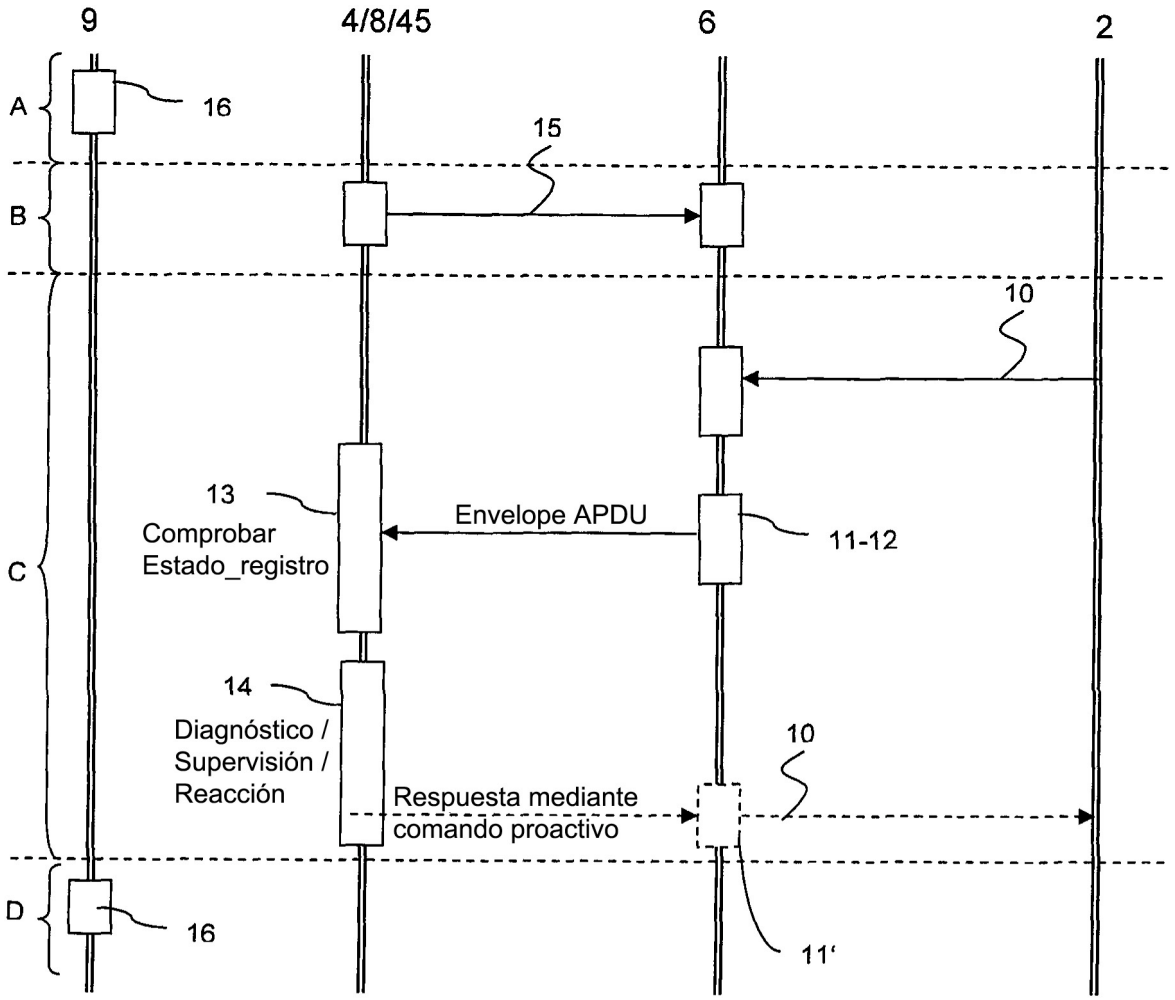
9
4/8/45
6
2
A
B
C
D
16
15
10
13
Comprobar
Estado_registro
Envelope APDU
11-12
14
Diagnóstico /
Supervisión /
Reacción
10
Respuesta mediante
comando proactivo
16
11'

Fig. 6