(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 689 294**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 9/48 (2006.01)
H04L 29/08 (2006.01)
H04L 9/08 (2006.01)
H04W 4/00 (2006.01)
G06F 21/60 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.06.2016 PCT/AT2016/050214**

(87) Fecha y número de publicación internacional: **29.12.2016 WO16205845**

(96) Fecha de presentación y número de la solicitud europea: **21.06.2016 E 16740931 (7)**

(97) Fecha y número de publicación de la concesión europea: **11.04.2018 EP 3167593**

(54) Título: **Dispositivo, método y producto de programa de ordenador para la comunicación de datos segura**

(30) Prioridad:

23.06.2015 AT 505242015

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.11.2018

(73) Titular/es:

MAHORKA, DIETHARD (100.0%)
Abt Karl-Strasse 23
3390 Melk, AT

(72) Inventor/es:

MAHORKA, DIETHARD

(74) Agente/Representante:

CONTRERAS PÉREZ, Yahel

DESCRIPCIÓN

Dispositivo, método y producto de programa de ordenador para la comunicación de datos segura

La presente invención se refiere a dispositivos, procedimientos y productos de programa de ordenador para la comunicación de datos segura según un protocolo de red que tiene una pluralidad de capas de comunicación estratificadas en una pila de protocolo.

Una de las arquitecturas de capas más conocidas y antiguas para protocolos de red es el modelo de referencia OSI de la ITU (“International Telecommunication Union”) o ISO (“International organisation for Stardarization”) con siete capas, es decir la capa física (capa 1), la capa de enlace de datos (capa 2), la capa de red (capa 3), la capa de transporte (capa 4), la capa de sesión (capa 5), la capa de presentación (capa 6) y la capa de aplicación (capa 7). El modelo de referencia TCP/IP, en el que la mayoría de los protocolos de internet se basan actualmente, también es un protocolo de red estratificado. En el modelo de referencia TCP/IP se utilizan sólo cuatro capas, estando fusionadas la capa física y la capa de enlace de datos en una capa de acceso al medio y la capa de sesión, la capa de presentación y la capa de aplicación en una capa de aplicación. No obstante, los protocolos de red estratificados se utilizan también en unidades de control electrónicas (ECUs, “Electronic Control Units”), que deben comunicarse de forma segura entre sí por medio de buses, por ejemplo, según la norma IEC 61508 o, en el sector de la automoción, de acuerdo con la norma ISO 26262 que se deriva de la anterior, en varios niveles ASIL (“automotive Safety Integrity Levels”) o en dispositivos de telecomunicaciones para redes de vehículos, véase “car-to-car (car2car)” o “car-to-infrastructure (car2X)”.

Para implementar tales protocolos de red estratificados en terminales, frecuentemente las capas individuales son encapsuladas en módulos o tareas de software independientes, que se comunican entre sí por medio de puntos interfaces o canales de comunicación definidos de forma precisa. El sobreposicionamiento o apilamiento denominado “vertical” de los módulos de software que representan las capas de protocolo individuales también se denominan en este caso “pila de protocolo”.

Las pilas de protocolo tienen que cumplir distintos requerimientos parcialmente contradictorios. Por una parte, deben satisfacer requerimientos de seguridad cada vez más exigentes, lo que se lleva a cabo mediante procedimientos de encriptado criptográficos cada vez más complejos a nivel de las capas de protocolo individuales. Para ello cada uno de los módulos de software en la pila de protocolo requiere también correspondientes claves criptográficas para encriptar y desencriptar el tráfico de datos a nivel de su capa. Por otra parte, las pilas de protocolo deben ser procesadas en sistemas de procesador lo más económicos posible. En su mayoría estos son sistemas de procesador de un único chip embebidos (“embedded”), por ejemplo, para módems de usuario final (“residential gateways”) o dispositivos terminales conectados a internet (véase “internet of things”), en los que la pila de protocolo actúa como el denominado “middleware”. Al mismo tiempo el esfuerzo de transporte de la pila de protocolo desde un sistema de procesador o sistema operativo a otro debe ser lo más pequeño posible lo que requiere un encapsulado correspondiente de los módulos de software por medio de capas de abstracción de hardware o software.

El concepto de las pilas de protocolo como middleware especialmente en el entorno heterogéneo del internet de las cosas (“internet of things”) se describe en la publicación de Bandyopadhyay, S. et al., "Role of Middleware for Internet of Things: A Study", International Journal of Computer Science & Engineering Survey (IJCSES), Vol. 2, Nº 3, Agosto 2011. Una revisión apropiada de los requerimientos de seguridad en tales entornos es proporcionada en la publicación de Kocher, P., et. al., "Security as a New Dimension in Embedded System Design", DAC 2004, 7 - 11 Junio 2004, San Diego, California, Estados Unidos.

La invención tiene por objeto proporcionar dispositivos y procedimientos del tipo mencionado anteriormente que concilien los requerimientos mencionados anteriormente mejor que con las soluciones conocidas.

En un primer aspecto de la invención, este objeto se consigue con un dispositivo para la comunicación de datos segura según un protocolo de red con un pluralidad de capas de comunicación estratificadas en una pila de protocolo, dicho dispositivo teniendo un sistema de procesador en el que un procesador controlado por un programador de tareas ejecuta una pluralidad de módulos de software independientes cada uno de los cuales procesando una capa de comunicación de la pila de protocolo,
tal que el módulo de software está interconectado con la pila de protocolo por medio de canales de comunicación y la pila de protocolo está conectada a un marco de interfaces para la comunicación de datos con una red exterior, y
tal que al menos un módulo de software utiliza una clave criptográfica asignada para asegurar la comunicación de datos en su capa de comunicación,
el dispositivo estando caracterizado por que
el programador de tareas está configurado para distribuir al módulo de software asignado una clave criptográfica obtenida de la red externa por medio del marco de interfaces.

En un segundo aspecto de la invención la invención proporciona para ello un procedimiento para la comunicación de datos segura según un protocolo de red con una pluralidad de capas de comunicación estratificadas en una pila de protocolo,
tal que en un sistema de procesador un procesador controlado por un programador de tareas ejecuta una pluralidad de módulos de software independientes cada uno de los cuales procesando una capa de comunicación de la pila de protocolo,
tal que el módulo de software está interconectado con la pila de protocolo por medio de canales de comunicación y la pila de protocolo está conectada a un marco de interfaces para la comunicación de datos con una red exterior, y
tal que al menos un módulo de software utiliza una clave criptográfica asignada para asegurar la comunicación de datos en su capa de comunicación,
el procedimiento estando caracterizado por que
la al menos una clave criptográfica es obtenida a partir de la red externa por medio del marco de interfaces y distribuida por el programador de tareas al módulo de software asignado.

Por tanto, de acuerdo con la invención el programador de tareas que está implementado en los respectivos módulos de software, en un sistema de procesador único, por ejemplo, en una puerta de enlace de una residencia, una puerta de enlace de seguridad o una electrónica de control del que es responsable un conmutador de tareas entre módulos de software independientes que ejecutan las capas de protocolo individuales, para la distribución de las claves de seguridad criptográficas que proceden, por ejemplo, de una pareja de comunicación o una entidad de generación de claves en la red. Esto permite una implementación especialmente sencilla de cualquier medida de seguridad a nivel de las distintas capas de protocolo, sin perjudicar el encapsulamiento y abstracción de los módulos de software individuales respecto al hardware, el sistema operativo, los controladores periféricos o similares, y sin requerir de recursos especiales para la distribución de claves: El programador de tareas existente es incorporado simplemente para este propósito.

La solución de acuerdo con la invención es adecuada para cualquier tipo de protocolo de red, por ejemplo, según el modelo de referencia TCP/IP en el caso de un módem de internet o protocolos estratificados para la implementación de requerimientos críticos de seguridad de acuerdo con los niveles de seguridad integral de automóviles definidos en la norma ISO 26262 (ASIL, “Automotive Integrity Safety Levels”) para el caso de componentes de vehículos eléctricos. De acuerdo con otra forma de realización de la invención, el protocolo de red está configurado según el modelo de referencia OSI y cada módulo de software ejecuta una capa del modelo de referencia OSI, por ejemplo, para un módem ISDN o un adaptador de interfaces ISDN/IP, también conocido como módem ALL-IP.

Cada uno de los módulos de software puede tener una entrada para al menos un canal de mensajes, que está conectado al programador de tareas para obtener la clave respectiva.

El (al menos un) canal de mensajes del módulo de software puede ser utilizado también para transferir el módulo de software a un modo de inicialización y, por ejemplo, por medio de mensajes de inicialización que son intercambiados a través del canal de mensajes, inicializar y/o, en particular, encender y apagar con tal finalidad de inicializar.

En particular, una clave adicional obtenida del programador de tareas también puede ser utilizada para encriptar o desencriptar el tráfico de mensajes en el canal de mensajes con objeto de garantizar también en este caso una comunicación segura. Por ejemplo, esta clave adicional puede ser utilizada por el módulo de software para transmitir de forma encriptada la clave que utiliza en su capa de protocolo.

En una forma de realización ventajosa de la invención, el programador de tareas también puede ser parte de un módulo de abstracción de hardware ejecutado por el procesador para los módulos de software, el módulo de abstracción proporcionando un entorno de sistema operativo extraído de hardware a cada uno de los módulos de software y para esta finalidad teniendo ya al menos un canal de mensajes para estos.

Básicamente, la invención es adecuada para todo tipo de terminales de comunicación de datos, incluso si éstos son simplemente interfaces de comunicación en unidades de control, por ejemplo, ECUs que se comunican entre sí por medio de buses de datos. Preferiblemente, el dispositivo es un módem o una ECU y el sistema de procesador es un sistema de procesador individual en el que la pila de protocolo actúa como middleware de seguridad embebido (“Embedded Security Middleware”). Alternativamente este middleware puede estar también embebido en un sistema de procesador múltiple.

En un tercer aspecto, la invención también proporciona un producto de programa de ordenador realizado en un soporte de datos que puede ser leído por una máquina configurada para implementar el procedimiento aquí presentado. La invención se divulga en las presentes reivindicaciones. A continuación la invención se explica con mayor detalle haciendo referencia a un ejemplo de realización representado en los dibujos adjuntos. En los dibujos:

La figura 1 muestra la arquitectura de sistema del dispositivo de la invención en un diagrama de bloques;

La figura 2 muestra en detalle uno de los módulos de software del dispositivo de la figura 1; y

La figura 3 muestra un diagrama de flujo de datos del procedimiento de la invención durante la comunicación de datos de los dos dispositivos de la figura 1 por medio de una red.

En la figura 1 está representado un dispositivo 1 para la comunicación de datos según un protocolo de red estratificado, por ejemplo, según el modelo de referencia OSI o TCP/IP. La figura 3 muestra dos dispositivos 1 de este tipo que se comunican entre sí por medio de una red 2 y (opcionalmente) con un centro de generación de claves 3, como se explica más adelante con más detalle. La red 2 puede ser, por ejemplo, internet, una red WAN ("Wide Area Network"), una red LAN ("Local Area Network"), una red de telefonía móvil y/o una red de telefonía por cable, y el dispositivo 1 puede integrar en la misma un conmutador de red, un enrutador o rúter de red, un módem, una pasarela o puerta de enlace o un terminal. En el caso de una red de telefonía, el protocolo de red normalmente está configurado según el modelo de referencia OSI y el dispositivo 1 es, por ejemplo, un terminal ISDN o un terminal ALL-IP; en el caso de internet, de una red WAN o de una red LAN el protocolo de red está normalmente está configurado según el modelo de referencia TCP/IP y el dispositivo 1 es, por ejemplo, un módem ADSL o un módem de comunicaciones mediante línea de potencia ("powerline"). No obstante, la red 2 puede ser también un bus por medio del que componentes electrónicos se comunican de forma segura entre sí por medio de un protocolo de red estratificado (protocolo de bus), por ejemplo, componentes electrónicos de un vehículo en un bus de a bordo del vehículo. En este caso, el dispositivo 1 puede ser, por ejemplo, una unidad de control electrónica (ECU, "Electronic Control Unit") que se comunica con otros componentes electrónicos por medio del bus de a bordo del vehículo.

El dispositivo 1 mostrado en la figura 1 es implementado en ingeniería informática normalmente en un sistema de procesador de hardware que – de manera conocida en la técnica – comprende fuentes de alimentación PWR, memoria MEM, interfaces I/F y al menos un procesador MP, que procesa componentes de software correspondientes. Los componentes del dispositivo 1 representados en la figura 1 son por tanto componentes de software, que están presentes en la memoria MEM del dispositivo 1 durante el tiempo de ejecución del software y son procesados correspondientemente por el procesador MP, de manera conocida en la técnica.

El sistema de procesador en el que el dispositivo 1 está implementado es normalmente un sistema de procesador de bajo coste con un solo chip y que tiene sólo un procesador principal MP que procesa secuencialmente en forma de tareas los componentes de software mostrados en la figura 1. Para ello está previsto un programador de tareas 4 que transmite periódica y secuencialmente el control de programa del procesador MP a módulos de software individuales L_1, L_2, …, en general L_i, así como a un módulo de marco de interfaces 5, véase bucle de control de secuencia de programa 6. El programador de tareas 4 por su parte es un componente de software y puede ser parte de un módulo de abstracción (OSAM, "operating system abstraction module") de software 7 o de un sistema operativo y/o de hardware que igualmente es procesado u operado normalmente dentro del bucle 6 del procesador MP.

El módulo de abstracción 7 proporciona también un entorno de operación para el módulo de software L_i, por ejemplo, para proporcionar temporizadores, para gestionar requerimientos de memoria dinámicos, etc. Así como para establecer canales de comunicación 8, 9, por medio de los cuales se comunican entre sí o con el módulo de marco de interfaces 5, y para canales de mensajes 10, por medio de los cuales pueden recibir mensajes de control del módulo de abstracción 7 o de su programador de tareas 4.

El procesador MP del dispositivo 1 puede ser también parte de un sistema de procesador múltiple que forma una combinación de dispositivos individuales 1. En este caso, una pluralidad de dispositivos 1 pueden compartir un procesador MP o un dispositivo 1 puede tener una pluralidad de procesadores MP. En tal sistema de procesador múltiple, el intercambio de datos entre los dispositivos 1 puede realizarse, en particular, también por medio de los canales de comunicación 8, 9 de uno o más módulos de software L_i.

En este caso, cada módulo de software L_i puede tener una entrada para más de un canal de mensajes 10. El canal o los canales de mensajes 10 de un módulo de software L_i pueden ser utilizados adicionalmente también para inicializar o a estos efectos para encender y apagar el respectivo módulo de software L_i – localmente o desde otra red conectada -.

La figura 2 muestra en detalle la estructura interna de uno de los módulos de software L_i. Cada módulo de software L_i es responsable de una de las capas de comunicación del protocolo de red estratificado, el cual maneja el dispositivo 1 o el procedimiento ejecutado por éste. En el caso del modelo de referencia OSI existen siete módulos de software L_i (i=1,… 7), cada uno de los cuales ejecuta una de las siete capas OSI. Los módulos de software L_i están "encapsulados" o "independizados" al estar interconectados a una "pila" individualmente por medio de los

canales de mensajes 8, 9; el conjunto de módulos de software L_i apilados uno encima del otro se denomina pila de protocolo 11.

Cabe entender que en el caso de otros protocolos de red, por ejemplo, del modelo de referencia TCP/IP de cuatro capas, sólo son necesarios cuatro módulos de software L_1 (i=1,… 4), cada uno de los cuales es responsable de la funcionalidad de una capa de comunicación.

Para ello, según la figura 2 cada módulo de software L_i tiene un programa de control 12 correspondiente y recursos para su ejecución (proporcionados por el módulo de abstracción 7), en particular, una cola de espera de mensajes 13 interna, la cual recoge mensajes de comunicación que llegan a través de los canales de comunicación 8, 9 así como mensajes de control que llegan a través del canal de mensajes 10 para su procesado por el programa de control 12.

El módulo de software L_i que está más abajo en el orden de las capas de la pila de protocolo 11, aquí el módulo de software L_1 para la capa física del modelo de referencia OSI o la capa de acceso al medio del modelo de referencia TCP/IP, está conectado al módulo de de interfaces 5 por medio de sus canales 8, 9 de comunicación, por medio de los cuales es procesado el tráfico de datos físico a la red 2. Las interfaces I/F físicas requeridas para ello son presentadas por el entorno operativo de hardware o de software o abstraídas por el módulo de marco de interfaces 5 a la pila de protocolo 11 o a sus módulos de software L_i.

El código fuente de un módulo de software L_i puede ser utilizado tanto en un entorno específico embebido como también en la forma de un controlador de modo privilegiado (“kernel mode”) de un sistema operativo de PC, sin tener que transferir el código fuente del módulo de software L_i. Esto tiene la ventaja adicional de que el código fuente puede desarrollarse inicialmente para sistemas embebidos en sistemas operativos de PC, probados y sólo entonces poder ser compilados para cualquier sistema específico embebido, sin tener que ser transferido el código fuente para el módulo de software L_i (“portability wihtout porting”). Mediante el alto grado de reutilización de código de los módulos de software L_i se consigue también una mejora continua en la calidad del código mediante optimización por reutilización de diseño (“design reuse”). Esto también proporciona la ventaja adicional de poder tener en cuenta requerimientos de rendimiento del sistema específico embebido, tales como rendimientos de procesador y requerimientos de la memoria, incluso antes del desarrollo del sistema específico embebido o de la ECU. Debido a que las interfaces y los canales de comunicación del módulo de software L_i están especificados, estos pueden también ser reutilizados de forma fácil en equipos compartidos de grandes empresas de desarrollo.

Para implementar mecanismos de seguridad criptográficos en el protocolo de red manejado por el dispositivo 1 se utilizan, en uno o más de los módulos de software L_i, respectivamente, una o más claves criptográficas 14, por ejemplo, claves privadas o públicas de procedimientos de encriptado públicos o privados (“public/private key”), los cuales intercambian dos parejas de comunicación por medio de la red 2, o claves comunes de procedimientos de encriptado de clave compartida (“shared key”) que, por ejemplo, son generadas por el centro de generación de claves 3 y distribuidas por medio de la red 2 o similares.

El módulo de software L_i responsable de las capas de comunicación correspondientes por tanto requiere conocer la o las claves 14 que son necesarias en su capa de comunicación para el correspondiente encriptado o desencriptado.

Para esta finalidad, el programador de tareas 4 está configurado para distribuir tales claves obtenidas 14 desde la red externa 2 en el módulo de software correspondiente L_i por medio de la red 2 y el módulo de marco de interfaces 5, concretamente por medio de su canal de mensajes 10. Estas claves 14 pueden ser también sólo componentes de una clave compuesta o completa que sea requerida para el encriptado o desencriptado en la capa de protocolo del módulo de software L_i. En este caso, varias claves 14 obtenidas de este modo en el módulo de software L_i por el programador de tareas 4 son ensambladas para formar la clave completa requerida.

Las claves 14 pueden ser solicitadas (“pull”) u obtenidas (“push”), por ejemplo, del módulo de abstracción 7 por medio del módulo de marco de interfaces 5 de la pareja de comunicación en la red 2, por ejemplo, de otro dispositivo 1 o del centro de generación de claves 3, y el programador de tareas 4 es utilizado únicamente para la correspondiente distribución o entrega de la clave o las claves 14 así obtenidas al módulo o módulos de software L_i correctos respectivos en el trascurso del programa 6. Alternativamente, el programador de tareas 4 por sí mismo solicita o recibe la clave o las claves 14 desde la red 2 y las envía al módulo de software L_i respectivo. Otra posibilidad es que uno de los módulos de software L_i de más alto nivel, en particular, un módulo de software L_i de una capa con una aplicación específica más alta en el curso de una aplicación, reciba una o más claves para un módulo de software L_i de más bajo nivel y las pase al módulo de software correspondiente de más bajo nivel L_i por medio del programador de tareas 4 o el módulo de abstracción 7. Asimismo en este caso, el programador de tareas 4 actúa de nuevo – en el curo de la ejecución del bucle de control 6 – como entregador de la respectiva clave 14 al módulo de software L_i correspondiente por medio de su canal de mensajes 10. Una clave 14 obtenida del programador de tareas 4 puede ser utilizada también en un módulo de software L_i para encriptar o desencriptar la

comunicación en su (al menos un) canal de mensajes 10, por ejemplo, para asegurar la transmisión de una clave 14 a continuación.

La invención no se limita a las formas de realización representadas sino que comprende todas las variantes, combinaciones y modificaciones de las mismas que se encuentran en el ámbito de las reivindicaciones adjuntas. Por ejemplo, el canal de mensajes 10 del dispositivo descrito anteriormente puede ser utilizado también para inicializar o para encender y apagar –localmente o por medio de otra red – un módulo de software L_i, tal que el intercambio de información a través del canal 10 correspondiente al procedimiento descrito anteriormente puede también ser encriptado.

REIVINDICACIONES

1. Dispositivo para la comunicación de datos segura según un protocolo de red con un pluralidad de capas de comunicación estratificadas en una pila de protocolo (11), dicho dispositivo teniendo un sistema de procesador en el que un procesador (MP) controlado por un programador de tareas (4) ejecuta una pluralidad de módulos de software independientes (L_i) cada uno de los cuales procesando una capa de comunicación de la pila de protocolo (11),
tal que el módulo de software (L_i) está interconectado con la pila de protocolo (11) por medio de canales de comunicación (8, 9) y la pila de protocolo (11) está conectada a un marco de interfaces (5) para la comunicación de datos con una red exterior (2), y
tal que al menos un módulo de software (L_i) utiliza una clave criptográfica asignada (14) para asegurar la comunicación de datos en su capa de comunicación,
caracterizado por que
el programador de tareas (4) está configurado para distribuir al módulo de software (L_i) asignado una clave (14) criptográfica obtenida de la red (2) externa por medio del marco de interfaces (5).

2. Dispositivo según la reivindicación 1, **caracterizado por que** el protocolo de red está configurado según el modelo de referencia OSI y cada módulo de software (L_i) procesa una capa del modelo de referencia OSI.

3. Dispositivo según la reivindicación 1 ó 2, **caracterizado por que** cada módulo de software (L_i) tiene una entrada para al menos un canal de mensajes (10), que está conectado al programador de tareas (4) para obtener así la clave (14).

4. Dispositivo según la reivindicación 3, **caracterizado por que** el módulo de software (L_i) puede ser inicializado y/o encendido y apagado por medio de un canal de mensajes (10).

5. Dispositivo según la reivindicación 3 ó 4, **caracterizado por que** el módulo de software (L_i) está configurado para utilizar una clave adicional obtenida del programador de tareas (4) para el tráfico de mensajes seguro en el canal de mensajes (10).

6. Dispositivo según una de las reivindicaciones 1 a 5, **caracterizado por que** el programador de tareas (4) es parte de un módulo de abstracción (7) para los módulos de software (L_i) que está procesado por el procesador (MP).

7. Dispositivo según una de las reivindicaciones 1 a 6, **caracterizado por que** el dispositivo (1) es un módem o una ECU y el sistema de procesador es un sistema de procesador individual.

8. Procedimiento para la comunicación de datos segura según un protocolo de red con un pluralidad de capas de comunicación estratificadas en una pila de protocolo,
tal que en un sistema de procesador un procesador (MP) controlado por un programador de tareas (4) ejecuta una pluralidad de módulos de software independientes (L_i) cada uno de los cuales procesando una capa de comunicación de la pila de protocolo,
tal que el módulo de software (L_i) está interconectado con la pila de protocolo (11) por medio de canales de comunicación (8, 9) y la pila de protocolo (11) está conectada a un marco de interfaces (5) para la comunicación de datos con una red exterior (2), y
tal que al menos un módulo de software (L_i) utiliza una clave criptográfica asignada (14) para asegurar la comunicación de datos en su capa de comunicación,
caracterizado por que
la al menos una clave criptográfica (14) es obtenida a partir de la red (2) externa por medio del marco de interfaces (5) y distribuida por el programador de tareas (4) al módulo de software asignado (L_i).

9. Procedimiento según la reivindicación 8, **caracterizado por que** el protocolo de red está configurado según el modelo de referencia OSI y cada módulo de software (L_i) procesa una capa del modelo de referencia OSI.

10. Procedimiento según la reivindicación 8 ó 9, **caracterizado por que** dicho módulo de software (L_i) obtiene la clave (14) del programador de tares (4) por medio de un canal de mensajes (10)

11. Procedimiento según la reivindicación 10, **caracterizado por que** el módulo de software (L_i) puede ser inicializado y/o encendido y apagado por medio de un canal de mensajes (10).

12. Procedimiento según la reivindicación 10 u 11, **caracterizado por que** el módulo de software (L_i) obtiene una clave adicional del programador de tareas (4) y la utiliza para asegurar el tráfico de mensajes en el canal de mensajes (10).

13. Procedimiento según una de las reivindicaciones 8 a 12, **caracterizado por que** el programador de tareas (4) es parte de un módulo de abstracción (7) para los módulos de software (L_i) que está procesado por el procesador (MP).

14. Producto de programa de ordenador, realizado en un soporte de datos que puede ser leído por una máquina y que implementa el procedimiento según una de las reivindicaciones 8 a13.

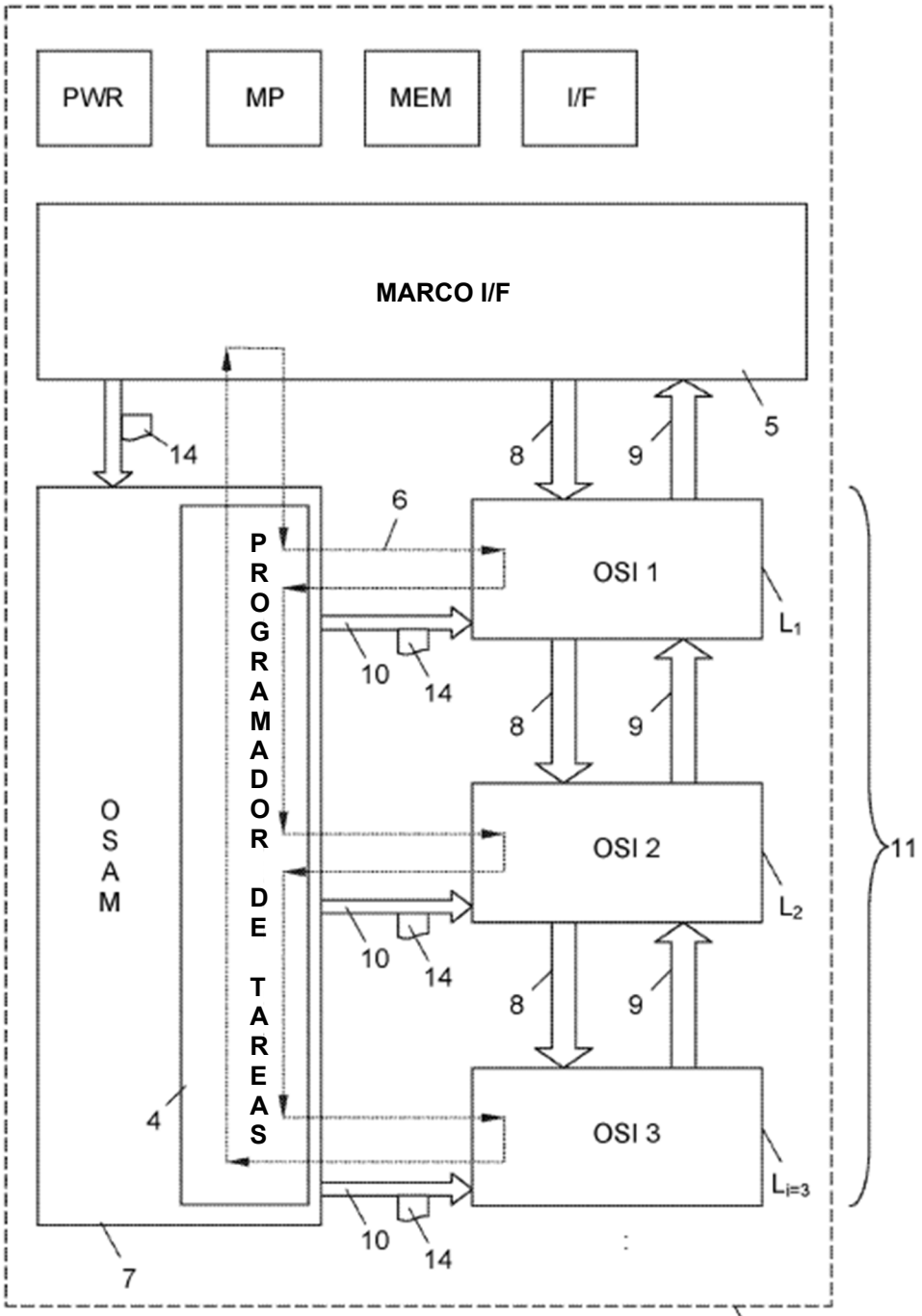
PWR
MP
MEM
I/F
MARCO I/F
14
8
9
5
6
PROGRAMADOR DE TAREAS
OSI 1
L_1
10
14
OSAM
OSI 2
L_2
11
4
OSI 3
$L_{i=3}$
7
1

Fig. 1

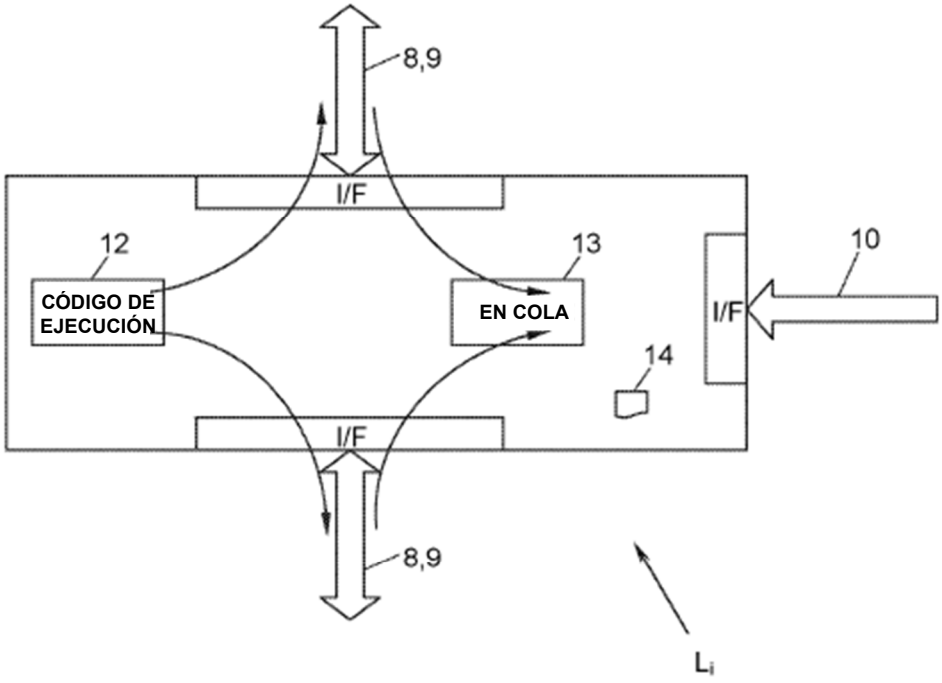

Fig. 2

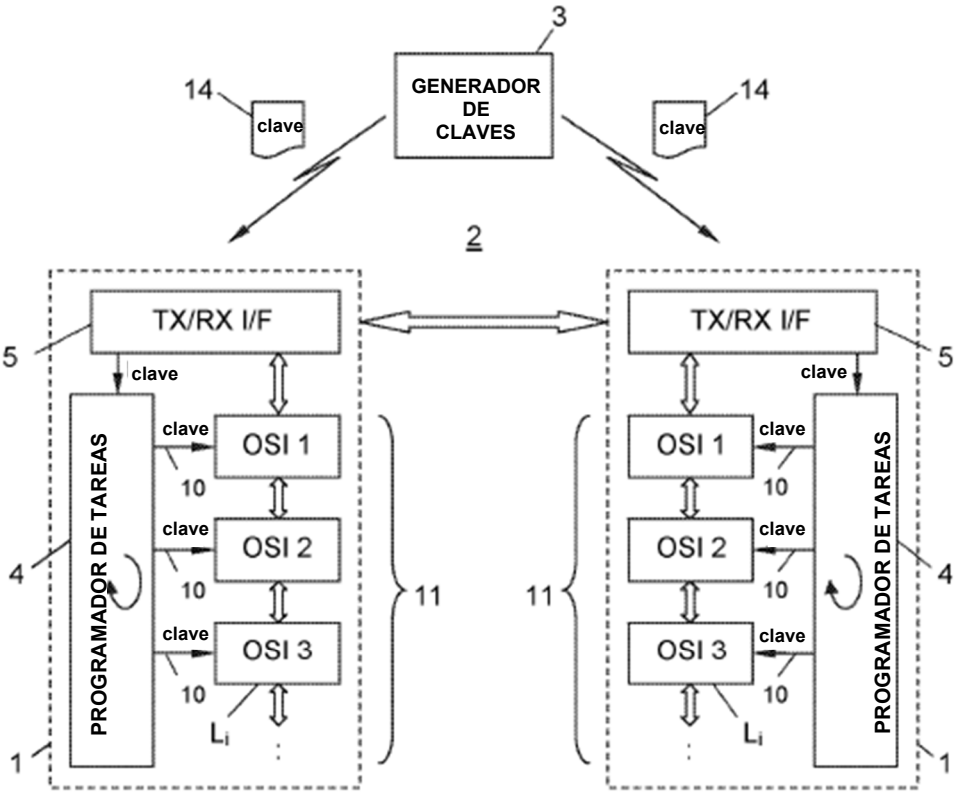
3
GENERADOR DE CLAVES
14
clave
14
clave
2
TX/RX I/F
TX/RX I/F
5
5
clave
clave
PROGRAMADOR DE TAREAS
PROGRAMADOR DE TAREAS
4
4
clave
OSI 1
10
clave
OSI 2
10
clave
OSI 3
10
Li
11
11
1
1

Fig. 3

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Literatura diferente de patentes citada en la descripción

- **BANDYOPADHYAY, S. et al. "**Role of Middleware for Internet of Things: A Study". International Journal of Computer Science & Engineering Survey (IJCSES), Agosto 2011, Vol. 2, Nº 3. **[0005]**

- **KOCHER, P. "**Security as a New Dimension in Embedded System Design". *DAC 2004,* 07. Junio 2004. **[0005]**