(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 642 673**

(51) Int. CI.:

G06F 21/72 (2013.01)
G06F 21/33 (2013.01)
G06F 21/62 (2013.01)
B61L 15/00 (2006.01)
B61L 27/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.03.2012 PCT/EP2012/055460**

(87) Fecha y número de publicación internacional: **11.10.2012 WO12136525**

(96) Fecha de presentación y número de la solicitud europea: **28.03.2012 E 12715542 (2)**

(97) Fecha y número de publicación de la concesión europea: **30.08.2017 EP 2658764**

(54) Título: **Sistema y procedimiento para una gestión de claves de un sistema de protección de trenes**

(30) Prioridad:

05.04.2011 DE 102011006772

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.11.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

SISTEMA Y PROCEDIMIENTO PARA UNA GESTIÓN DE CLAVES DE UN SISTEMA DE PROTECCIÓN DE TRENES

DESCRIPCIÓN

La presente invención se refiere a un sistema y a un procedimiento para una gestión de claves de un sistema de protección de trenes

Estado de la técnica

Un sistema de protección utilizado en el tráfico ferroviario para la protección de trenes es el llamado sistema europeo de control de trenes ("ETCS", European Train Control System). Este sistema de gestión del tráfico utiliza usualmente la transmisión de datos por radio, por ejemplo mediante GSM-R, para intercambiar mensajes de conducción y mensajes de protección entre locomotoras ferroviarias y/o sus ordenadores de protección, como por ejemplo en European Vital Computer (EVC, ordenador vital europeo) y centrales de control de línea fijas, las centrales de bloque de radio ("RBC", Radio Block Centres). Para proteger los datos durante la transmisión frente a manipulaciones inadvertidas y errores de transmisión, están protegidos los mismos con una suma de prueba criptográfica, para calcular y/o comprobar la cual es necesaria una clave criptográfica.

Usualmente se utilizan procedimientos criptográficos simétricos, con lo que tanto la locomotora ferroviaria como también su central de control de línea deben poseer al menos una clave. Puesto que el vehículo ferroviario se mueve sobre su ruta predeterminada a través de zonas de competencia de distintas centrales de control de línea fijas a lo largo del trayecto, es necesario que a cada una de las centrales de control de línea temporalmente competentes se les comunique una clave adecuada para la comunicación con el vehículo ferroviario. La distribución de claves a las centrales de control de línea es por lo tanto un problema fundamental de un sistema de protección de trenes efectivo, para garantizar la comunicación del vehículo ferroviario con todas las centrales de control de línea y dado el caso también con centrales de control de línea de otros operadores de líneas, de una forma segura frente a la manipulación.

La figura 1 muestra la estructura básica de un sistema de conducción de un vehículo ferroviario 10 en una representación esquemática. Un vehículo ferroviario 4, por ejemplo un tren con una locomotora que puede controlarse, que tiene a bordo un EVC, se mueve a lo largo de una ruta 5 a través de distintos dominios A, B y C, que se encuentran bajo el control de distintos operadores de línea y que están delimitados ópticamente entre si mediante las líneas de puntos. Los dominios A, B y C pueden ser por ejemplo países como Alemania, Austria e Italia con respectivas redes ferroviarias propias y el tren 4 puede por ejemplo tener una ruta 5 planificada desde Munich hasta Venecia, que lo conduce a través de los tres países Alemania, Austria e Italia.

Cada operador de línea tiene una central de gestión de claves o puesto de adjudicación de claves 1a, 1b y 1c, respectivamente, denominado también KMC ("Key Management Centre"). Es decir, en el dominio A es responsable el KMC 1a de la gestión de las claves, en el dominio B el KMC 1b y en el dominio C el KMC 1c. Bajo la égida de los KMCs 1a, 1b y 1c se encuentran respectivas centrales de control de línea 3, las llamadas RBCs, que pueden recibir códigos de mensajes de claves, los llamados KMACs ("Key Message Authentication Codes", códigos de autentificación de mensajes de claves), de los KMCs. Los KMACs pueden incluir entonces claves de comunicación, que pueden servir para la comunicación segura de los RBCs 3 con el tren 4.

Las centrales de control de línea o RBCs 3 son localmente responsables de forma fija para determinados cantones de bloqueo de la red ferroviaria. Un RBC 3 puede estar entonces asociado a un respectivo grupo de claves 2a, 2b, 2c, al que suministran claves de comunicación los correspondientes KMCs 1a, 1b y 1c supraordinados de los respectivos dominios A, B o C. Puede estar previsto entonces que varios RBCs 3 estén asociados al mismo grupo de claves. Por ejemplo están asociados en el dominio A y en el dominio C en cada caso dos RBCs 3 a un grupo de claves 2a y 2c respectivamente. Alternativamente puede ser también que un RBC 3 forme simultáneamente también su propio grupo de claves, tal como por ejemplo se representa en el dominio B con el grupo de claves 2b. Cada grupo de claves 2a, 2b, 2c recibe del KMC 1a, 1b, 1c supraordinado una clave de comunicación específica del grupo.

El vehículo ferroviario 4 comunica entonces a través de enlaces de comunicación 5a con RBCs 3 en el primer dominio A, a través de enlaces de comunicación 5b con el RBC 3 en el segundo dominio B y a través de enlaces de comunicación 5c con RBCs 3 en el tercer dominio A. Entonces se protegen los enlaces de comunicación 5a, 5b y 5c en cada caso mediante las claves de comunicación proporcionadas por los KMCs 1a, 1b, 1c.

Una posibilidad para distribuir claves correspondientes a claves de comunicación a las distintas centrales de control de línea 3 consiste en una distribución manual de las claves de comunicación mediante un empleado del operador del tren o del correspondiente operador de la línea. En este caso puede ser que el empleado solicite antes del comienzo del viaje claves de comunicación específicas del dominio de cada uno de los KMCs 1a, 1b, 1c e instale esas claves de comunicación específicas del dominio en el

ordenador de control, la llamada OBU (“On-Board Unit”, unidad de a bordo) del tren 4. La instalación puede realizarse por ejemplo mediante introducción manual a través de una interfaz de entrada, por ejemplo un teclado o una pantalla táctil, a través de una conexión local de red, una memoria utilizada localmente, por ejemplo un diskette o un lápiz USB o una conexión de telemantenimiento inalámbrica protegida.

Una tal distribución de claves es costosa, susceptible de errores e ineficiente. En particular es necesaria para ello una conexión permanente entre KMCs de distintos dominios, para garantizar el intercambio permanente de claves de comunicación entre los KMCs.

La solicitud de patente alemana DE 10 2007 041 177 A describe un procedimiento para la gestión de claves online, en el que cada KMC individual genera datos de clave para su dominio. Un vehículo ferroviario lleva asociada entonces una “KMC cooperativa", que autoriza a transmitir datos de claves al vehículo ferroviario. Si ha de recorrer un vehículo ferroviario dominios de otros KMCs, entonces se solicitan previamente los correspondientes datos de claves del KMC cooperativo y se envían al vehículo ferroviario.

Existe por lo tanto necesidad de soluciones más sencillas para una distribución de claves correspondiente a claves de distribución en sistemas de protección para vehículos ferroviarios de ámbito más amplio que el del dominio.

Resumen de la invención

Este objetivo se logra mediante el procedimiento para distribuir claves de comunicación de acuerdo con la reivindicación 1, así como mediante el equipo para distribuir claves de comunicación de acuerdo con la reivindicación 10. Una idea de la presente invención es elaborar un plan de distribución de claves en base a una ruta planificada para el tren y configurar automáticamente las claves de comunicación necesarias para recorrer esa ruta. Para ello pueden generarse desde un puesto de adjudicación de claves central responsable claves de comunicación, que están ajustadas a la ruta planificada. Estas claves de comunicación pueden proporcionarse a los puestos de adjudicación de claves que participan correspondientes a otros dominios u operadores de línea, con lo que las claves de comunicación generadas centralmente y de forma automática pueden distribuirse selectivamente a los trenes y las centrales de control de línea.

Una de las ventajas de esta forma de proceder es que se simplifica considerablemente la definición de un plan de distribución de claves. Además puede limitarse en el espacio y en el tiempo de manera sencilla la validez de las claves de comunicación en cuanto a trayectos y a la duración del trayecto del tren, con lo que el plan de distribución de claves correspondiente a la invención es menos sensible a errores que los planes de distribución de claves tradicionales.

Otra ventaja adicional es la posibilidad de automatizar el plan de distribución de claves mediante la posibilidad de generar y verificar el plan automáticamente a partir de planes de trayectos aportados externamente.

Una forma de realización de la presente invención consiste por lo tanto en un procedimiento para distribuir claves de comunicación para encriptar mensajes de conducción del tráfico de un sistema de protección de vehículos ferroviarios, con las etapas de generación de una clave de comunicación en un primer puesto de adjudicación de claves de un primer operador de línea en función de un trayecto planificado de un vehículo ferroviario, de aportación de una clave de comunicación a un segundo puesto de adjudicación de claves de un segundo operador de línea, de aportación de la clave de comunicación al vehículo ferroviario por parte del primer puesto de adjudicación de claves y de encriptado de mensajes de conducción del tráfico del vehículo ferroviario con la clave de comunicación para la comunicación segura frente a manipulaciones del vehículo ferroviario con centrales de control de línea del primer operador de línea y con centrales de control de línea del segundo operador de línea.

Ventajosamente se realiza la aportación de la clave de comunicación a primeras centrales de control de línea por parte del primer operador de línea y la aportación de la clave de comunicación a segundas centrales de control de línea por parte del segundo operador de línea.

Según una forma de realización preferida, incluye la clave de comunicación una pluralidad de claves de comunicación específicas de la central de control de línea, incluyendo la aportación de la clave de comunicación al segundo puesto de adjudicación de claves la aportación de un grupo de claves de comunicación específicas de la central de control de línea que están asociadas a las segundas centrales de control de línea del segundo operador de línea al segundo puesto de adjudicación de claves. Esto tiene la ventaja de que distintas centrales de control de línea utilizan distintas claves de comunicación, con lo que cuando se publica por descuido o cuando se manipula una de las claves de comunicación, sólo queda comprometida una central de control de línea del sistema completo.

Según una forma de realización, la generación de la clave de comunicación en un primer puesto de adjudicación de claves se realiza con la deducción de la clave de comunicación específica de la central de control de línea a partir de una clave de comunicación principal mediante un procedimiento de deducción de claves. Esto ofrece la ventaja de que la deducción de la clave de comunicación específica de la central de control de línea puede realizarla un ordenador de control propio del vehículo ferroviario.

Según una forma de realización preferida, la deducción de la clave de comunicación específica de la central de control de línea se realiza mediante el primer puesto de adjudicación de claves sólo para las primeras centrales de control de línea y la deducción de la clave de comunicación específica de la central de control de línea mediante el segundo puesto de adjudicación de claves sólo para las segundas centrales de control de línea. De esta manera, cuando hay una elevada afluencia de vehículos, puede limitarse ventajosamente la gestión de claves en un puesto de adjudicación de claves sólo a aquellas claves de comunicación deducidas que se necesitan realmente en ese puesto de adjudicación de claves. Ventajosamente se limita así la afluencia de datos al proporcionar la clave de comunicación por parte del primer puesto de adjudicación de claves a otros puestos de adjudicación de claves.

Según una forma de realización ventajosa, incluye la clave de comunicación una pluralidad de claves de comunicación específicas del vehículo ferroviario, incluyendo la aportación de la clave de comunicación al vehículo ferroviario la aportación de una clave de comunicación específica del vehículo ferroviario de entre la pluralidad de claves de comunicación específicas de vehículos ferroviarios. Esto ofrece la ventaja de que por ejemplo cuando se ensamblan dos vehículos ferroviarios de distintos operadores de vehículos ferroviarios, es posible una comunicación segura entre los vehículos ferroviarios acoplados cuando los correspondientes vehículos ferroviarios ajustan entre sí sus claves de comunicación específicas del vehículo.

Ventajosamente puede proporcionar el trayecto planificado para el vehículo ferroviario un sistema de conducción para el control de la circulación, con lo que el primer puesto de adjudicación de claves realiza automáticamente la generación y la aportación de la clave de comunicación. Con ello, por un lado se acelera considerablemente la generación y distribución de la clave de comunicación y por otro puede comprobarse automáticamente si a lo largo del trayecto planificado se han generado y distribuido todas las claves de comunicación necesarias. Así pueden detectarse tempranamente y con fiabilidad desviaciones y entradas incorrectas.

Según otra forma de realización, logra la invención un equipo de control en un primer puesto de adjudicación de claves de un primer operador de línea de la red ferroviaria para distribuir claves de comunicación para encriptar mensajes de conducción del tráfico de un sistema de protección de vehículos ferroviarios con un equipo de generación que está diseñado para generar una clave de comunicación en función de un trayecto planificado para un vehículo ferroviario y un equipo de aportación que está diseñado para proporcionar la clave de comunicación generada a un segundo puesto de adjudicación de claves de un segundo operador de línea y al vehículo ferroviario, estando diseñada la clave de comunicación para encriptar mensajes de conducción del tráfico del vehículo ferroviario para la comunicación segura frente a manipulaciones del vehículo ferroviario con centrales de control de línea del primer operador de línea y con centrales de control de línea del segundo operador de línea.

Según otra forma de realización, logra la invención un sistema de protección de vehículos ferroviarios con un equipo de control de acuerdo con la invención, un primer puesto de adjudicación de claves en el que está dispuesto el equipo de control, una pluralidad de primeras centrales de control de líneas que están diseñadas para que las alimente el primer puesto de adjudicación de claves con una clave de comunicación generada por el equipo de control para encriptar mensajes de conducción del tráfico de un vehículo ferroviario, un segundo puesto de adjudicación de claves y una pluralidad de segundas centrales de control de línea, que están diseñadas para que las alimente el segundo puesto de adjudicación de claves con una clave de comunicación generada por el equipo de control para encriptar mensajes de conducción del tráfico de un vehículo ferroviario.

Otras modificaciones y variaciones resultan de las características de las reivindicaciones dependientes.

Breve descripción de las figuras

A continuación se describirán con más precisión diversas formas de realización y variantes de la presente invención con referencia a los dibujos adjuntos, en los cuales muestra la

figura 1 una representación esquemática de una estructura de un sistema de conducción de un vehículo ferroviario;
figura 2 una representación esquemática de un sistema de protección de un vehículo ferroviario según una forma de realización de la invención;
figura 3 una representación esquemática de un sistema de protección de un vehículo ferroviario según otra forma de realización de la invención;
figura 4 una representación esquemática de un sistema de protección de un vehículo ferroviario según otra forma de realización de la invención;

figura 5 una representación esquemática de un sistema de protección de un vehículo ferroviario según otra forma de realización de la invención y

figura 6 una representación esquemática de un procedimiento para distribuir claves de comunicación para encriptar mensajes de conducción del tráfico de un sistema de protección de un vehículo ferroviario según otra forma de realización de la invención.

Las variantes y perfeccionamientos descritos pueden combinarse entre sí, siempre que ello tenga sentido. Otras variantes, perfeccionamientos e implementaciones posibles de la invención incluyen también combinaciones no citadas explícitamente de características de la invención descritas previamente o a continuación en relación con los ejemplos de realización.

Los dibujos adjuntos deben transmitir una comprensión mayor de las formas de realización de la invención. Los mismos visualizan formas de realización y sirven en relación con la descripción para clarificar principios y conceptos de la invención. Otras formas de realización y muchas de las citadas ventajas resultan en relación con los dibujos. Los elementos de los dibujos no se muestran necesariamente con exactitud a escala uno respecto a otro. Las mismas referencias designan entonces componentes iguales o que actúan de la misma forma.

Descripción detallada de la invención

Las claves de comunicación en el sentido de la presente invención incluyen todas las informaciones y unidades de datos criptográficas que son adecuadas para encriptar datos en formato explícito y a partir de ellos generar datos seguros frente a una escucha y/o lectura en formato secreto y/o que son adecuados para proteger la integridad de datos en formato explícito y calcular una suma de prueba criptográfica y que son además adecuados para, conociendo las informaciones criptográficas, recuperar y/o comprobar a partir de los datos en formato secreto los datos en formato explícito, tal que los datos no se manipulen durante el trasporte. Las claves de comunicación en el sentido de la invención pueden contener por ejemplo pares de claves simétricos, pares de claves asimétricos o procedimientos criptográficos similares. Las claves de comunicación pueden utilizarse entonces por ejemplo con procedimientos como AES, DES, KDF, IPsec, SSL/TLS, MACsec, L2TP, PPTP, PGP, S/MIME o una técnica similar con la correspondiente gestión de claves, como por ejemplo IKE, EAP u otros procedimientos.

La figura 2 muestra una representación esquemática de un sistema de protección de un vehículo ferroviario 20. El sistema de protección de un vehículo ferroviario 20 se diferencia del sistema de conducción de un vehículo ferroviario 10 mostrado en la figura 1 en que en cada uno de los puestos de adjudicación de claves 1a, 1b y 1c (KMCs) está dispuesto un equipo de control 7, que está diseñado para generar y distribuir claves de comunicación para encriptar mensajes de conducción del tráfico. El equipo de control 7 puede ser por ejemplo un módulo de software, que está alojado en los KMCs y que se ejecuta.

El equipo de control 7 incluye un equipo de generación para generar claves de comunicación 6 para la protección criptográfica de mensajes de conducción del tráfico de un vehículo ferroviario 4. En los siguientes ejemplos se supone que el vehículo ferroviario 4 está asociado al dominio A, con lo que el KMC 1a es el llamado " KMC doméstico" del vehículo ferroviario 4, es decir, que la generación y distribución de claves de comunicación se realiza bajo el control del KMC 1a. Los demás KMCs 1b y 1c dependen en este caso del control a través del KMC 1a. Evidentemente es posible también que los otros KMC 1b y 1c en los otros casos, por ejemplo para otros vehículos ferroviarios, asuman el papel del KMC doméstico. Los equipos de control 7 de los KMCs 1b y 1c tienen entonces la misma constitución que el equipo de control 7 del KMC 1a. Es además evidente que la cantidad de KMCs 1a, 1b y 1c no queda limitada a la cantidad indicada de tres. Es igualmente posible cualquier otra cantidad de KMCs. Los KMCs 1a, 1b, 1c pueden ser operados entonces en particular por distintos operadores de línea.

El equipo de generación puede estar diseñado para en una etapa 8a generar una clave de comunicación 6 en función de un trayecto planificado para el vehículo ferroviario 4. Entonces puede estar diseñado el equipo de generación para que le ponga a disposición el trayecto planificado automáticamente un sistema de control de la circulación (no mostrado) o un sistema de información del trayecto.

La clave de comunicación 6 puede entonces ponerse a disposición de un segundo KMC 1b por parte del primer KMC 1a en una segunda etapa 8b y a disposición de un tercer KMC 1c en una tercera etapa 8c. Los KMC 1b, 1c, a los que se aporta la clave de comunicación 6, se rigen entonces por el trayecto planificado para el vehículo ferroviario 4. Por ejemplo pueden ser responsables los KMC 1b, 1c de las centrales de control de línea 3, a través de cuya zona de gestión conduce el trayecto planificado para el vehículo ferroviario 4. La aportación de claves de comunicación puede entonces realizarse mediante un equipo de aportación del equipo de control 7.

En una etapa 9a puede entonces distribuirse la clave de comunicación 6 generada a primeras centrales de control de línea 3 (RBCs) en el primer dominio A. Además puede instalarse en la etapa 9a la clave de comunicación 6 en un ordenador de control (EVC) del vehículo ferroviario 4. La clave de comunicación 6

puede proporcionarse en etapas 9b y 9c mediante los KMCs 1b y 1c a los RBCs 3 en el dominio B y el dominio C respectivamente.

El KMC 1a puede confeccionar, tras realizarse la distribución de la clave de comunicación 6, una confirmación de que el vehículo ferroviario 4 está listo para el servicio y puede recorrer los dominios A, B y C. Cuando por ejemplo debido a un bloqueo de un tramo o cualquier otro rodeo del vehículo ferroviario 4 debe recorrerse otro dominio D (no mostrado), para el que la clave de comunicación 6 no ha sido puesta a disposición de las correspondientes centrales de control de línea 3, puede confeccionarse un plan de distribución de claves modificado, retransmitiendo el equipo de control 7, tras la correspondiente autorización de un operador, la clave de comunicación 6 también a un KMC del dominio D, que entonces por su parte retransmite la clave de comunicación a los RBC 3 en su dominio D. Alternativamente puede mostrarse al operador que el vehículo ferroviario 4 tiene autorización para atravesar solamente los dominios A, B y C, pero no otros dominios.

La figura 3 muestra una representación esquemática de un sistema de protección de un vehículo ferroviario 30. El sistema de protección de un vehículo ferroviario 30 se diferencia del sistema de protección de un vehículo ferroviario 20 de la figura 2 en que la clave de comunicación 6 incluye una pluralidad de claves de comunicación 6a, 6b, 6c que han sido generadas específicamente por dominio o específicamente por central de control de línea. Cada una de las claves de comunicación 6a, 6b, 6c puede generarse entonces específicamente por zonas para un RBC 3. Las claves de comunicación 6a, 6b, 6c pueden entonces generarse aleatoriamente o pseudoaleatoriamente o mediante una función de deducción de claves a partir de la clave de base y/o de un parámetro de deducción que depende del RBC. Las claves de comunicación 6a, 6b, 6c se instalan entonces conjuntamente sobre el ordenador de control del vehículo ferroviario 4.

A partir de las claves de comunicación 6a, 6b, 6c se eligen entonces grupos de claves de comunicación que pueden asociarse a los correspondientes RBCs 3 de los respectivos dominios B y C. En las etapas 8b, 8c se transmiten entonces sólo aquellas claves de comunicación 6b y 6c que necesitan los KMCs, 1b, 1c para proporcionarlas a sus RBCs.

El vehículo ferroviario 4 puede elegir cuando atraviesa los dominios A, B y C, en función de la posición actual en cada caso, una de las claves de comunicación 6a, 6b, 6c, para comunicar con el RBC 3 actual en cada momento del correspondiente dominio. La posición en ese momento puede determinarse por ejemplo mediante un sistema de navegación por satélite, como por ejemplo GPS o GA-LILEO, mediante localización de estaciones de base de radio, por ejemplo mediante GSM-R o WLAN, en base a direcciones o códigos de identificación de ordenadores de línea de la red ferroviaria o mediante eurobalizas, como por ejemplo balizas de datos fijos o datos transparentes en el balasto de la vía.

La figura 4 muestra una representación esquemática de un sistema de protección de un vehículo ferroviario 40. El sistema de protección de un vehículo ferroviario 40 se diferencia del sistema de protección de un vehículo ferroviario 30 de la figura 3 en que está prevista una clave de comunicación principal 6 entre los KMCs 1a, 1b y 1c, de la cual puede deducirse mediante una función de deducción de claves una pluralidad de claves de comunicación 6a, 6b, 6c. En las etapas 8b y 8c se retransmite, en lugar de la pluralidad de claves de comunicación 6a, 6b, 6c, la clave de comunicación principal 6 a los KMCs 1b y 1c, que a su vez pueden deducir localmente la pluralidad de claves de comunicación 6a, 6b, 6c. La deducción mediante los KMCs puede realizarse por ejemplo en función de un parámetro específico del tren, por ejemplo el número de identificación del vehículo ferroviario 4. La clave de comunicación principal 6 puede ser entonces por ejemplo válida sólo durante un determinado periodo de tiempo.

Igualmente puede estar previsto que el propio vehículo ferroviario 4 se alimente con la clave de comunicación principal 6, de la cual el propio ordenador de control del vehículo ferroviario 4 deduce la pluralidad de claves de comunicación 6a, 6b, 6c.

La deducción de la pluralidad de claves de comunicación 6a, 6b, 6c a partir de la clave de comunicación principal 6 puede realizarse por ejemplo mediante una función de deducción de claves (Key Derivation Function, KDF) como HMAC (Hash Message Authentication Code, código de autentificación del mensaje Hash) o también AES-CBCMAC (Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code, estándar avanzado de encriptado-código de autentificación de mensajes de encadenamiento de bloques de cifrado) en función de parámetros específicos de RBC, como código de identificación, código de zona, código de sección de línea o parámetros similares.

La ventaja de esta forma de proceder reside en que no tiene que existir un enlace online constante entre los KMCs 1a, 1b, 1c, ya que cada KMC puede deducir autónomamente claves de comunicación 6a, 6b, 6c específicas del RBC a partir de la clave de comunicación principal 6 transmitida una sola vez, sin que para ello sea necesaria una nueva comunicación con el KMC doméstico 1a. Además, cuando existe una pluralidad de vehículos ferroviarios 4 y RBCs 3, sólo tienen que intercambiarse unos pocos datos entre los KMCs 1a, 1b, 1c.

La figura 5 muestra una representación esquemática de un sistema de protección de un vehículo ferroviario 50. El sistema de protección de un vehículo ferroviario 50 se diferencia del sistema de protección de un vehículo ferroviario 40 de la figura 4 en que está prevista una clave de comunicación principal 6, de la que mediante una función de deducción de claves puede deducirse una pluralidad de claves de comunicación 6a, 6b, 6c, específicas del vehículo ferroviario. De una de las claves de comunicación 6c específica del vehículo ferroviario, que por ejemplo está asociada al vehículo ferroviario 4 de la figura 5, puede a su vez deducirse una pluralidad de claves de comunicación 11 específicas del RBC, que pueden distribuirse a los distintos RBCs 3 mediante los respectivos KMCs 1a, 1b, 1c. Al vehículo ferroviario 4 se le proporciona entonces en cada caso la clave de comunicación 6c específica del vehículo ferroviario, así como la clave de comunicación 11 específica del RBC, con lo que puede realizarse una comunicación con los correspondientes RBCs 3 mediante una elección de una clave de comunicación 11 específica del RBC.

Por ejemplo puede estar previsto que en dos vehículos ferroviarios de distintos operadores y/o distintos KMCs domésticos se instale la misma clave de comunicación 6c específica del vehículo ferroviario, con lo que cuando existe un acoplamiento de los dos vehículos ferroviarios resulta posible una comunicación segura entre vehículos.

La figura 6 muestra una representación esquemática de un procedimiento 60 para distribuir claves de comunicación para encriptar mensajes de conducción del tráfico de un sistema de protección de un vehículo ferroviario. En una primera etapa 61 se genera una clave de comunicación en un primer puesto de adjudicación de claves (KMC) de un primer operador de línea en función de un trayecto planificado para un vehículo ferroviario. En una segunda etapa 62 se proporciona la clave de comunicación a un segundo KMC de un segundo operador de línea. En una tercera etapa 63 se proporciona la clave de comunicación a un vehículo ferroviario mediante el primer KMC. En una cuarta etapa 64 se encriptan mensajes de conducción del tráfico del vehículo ferroviario con la clave de comunicación para la comunicación segura frente a manipulaciones del vehículo ferroviario con RBCs del primer operador de línea y con RBCs del segundo operador de línea. Bajo encriptado de un mensaje de conducción del tráfico se entiende en particular que datos útiles y/o datos de gestión, por ejemplo informaciones de direccionamiento de un mensaje de conducción del tráfico, se protegen criptográficamente frente a escuchas y/o manipulación, por ejemplo sustituyendo datos de texto explícito por los correspondientes datos de código encriptados y/o añadiendo una información de integridad criptográfica (Message Authentication Code).

REIVINDICACIONES

1. Procedimiento para distribuir claves de comunicación (6; 6a, 6b, 6c; 11) para encriptar mensajes de conducción del tráfico de un sistema de protección de vehículos ferroviarios, con las etapas:
generación de una clave de comunicación (6; 6a, 6b, 6c; 11) en un primer puesto de adjudicación de claves (1a) de un primer operador de línea en función de un trayecto planificado de un vehículo ferroviario (4);
aportación de la clave de comunicación (6; 6a, 6b, 6c; 11) al vehículo ferroviario (4) a través del primer puesto de adjudicación de claves y
encriptado de mensajes de conducción del tráfico del vehículo ferroviario (4) con la clave de comunicación (6; 6a, 6b, 6c; 11) para la comunicación segura frente a manipulaciones del vehículo ferroviario (4) con centrales de control de línea (3) del primer operador de línea y con centrales de control de línea (3) de un segundo operador de línea,
caracterizado por la etapa
aportación de la clave de comunicación (6; 6a, 6b, 6c; 11) a un segundo puesto de adjudicación de claves (1b) del segundo operador de línea,
realizándose la generación y distribución de claves de comunicación bajo el control del primer puesto de adjudicación de claves (1a).

2. Procedimiento de acuerdo con la reivindicación 1, además con las etapas:
aportación de la clave de comunicación (6; 6a, 6b, 6c; 11) a primeras centrales de control de línea (2a; 3) por parte del primer operador de línea y aportación de la clave de comunicación (6; 6a, 6b, 6c; 11) a segundas centrales de control de línea (2b; 3) por parte del segundo operador de línea.

3. Procedimiento de acuerdo con la reivindicación 2,
en el que la clave de comunicación incluye una pluralidad de claves de comunicación (6a, 6b, 6c) específicas de la central de control de línea, incluyendo la aportación de la clave de comunicación (6; 6a, 6b, 6c; 11) al segundo puesto de adjudicación de claves (1b) la aportación de un grupo de claves de comunicación (6a, 6b, 6c) específicas de la central de control de línea que están asociadas a las segundas centrales de control de línea (2b; 3) del segundo operador de línea, al segundo puesto de adjudicación de claves (1b).

4. Procedimiento de acuerdo con la reivindicación 3,
en el que la generación de la clave de comunicación (6; 6a, 6b, 6c; 11) en un primer puesto de adjudicación de claves (1a) incluye la deducción de la clave de comunicación (6a, 6b, 6c) específica de la central de control de línea a partir de una clave de comunicación principal (6) mediante un procedimiento de deducción de claves.

5. Procedimiento de acuerdo con la reivindicación 4,
en el que la deducción de la clave de comunicación (6a, 6b, 6c) específica de la central de control de línea se realiza mediante un ordenador de control del vehículo ferroviario (4).

6. Procedimiento de acuerdo con la reivindicación 4,
en el que la deducción de la clave de comunicación (6a, 6b, 6c) específica de la central de control de línea se realiza mediante el primer y el segundo puesto de adjudicación de claves (1a, 1b).

7. Procedimiento de acuerdo con la reivindicación 6,
en el que la deducción de la clave de comunicación (6a, 6b, 6c) específica de la central de control de línea mediante el primer puesto de adjudicación de claves (1a) se realiza sólo para las primeras centrales de control de línea (2a; 3) y la deducción de la clave de comunicación (6a, 6b, 6c) específica de la central de control de línea mediante el segundo puesto de adjudicación de claves (1b), se realiza sólo para las segundas centrales de control de línea (2b; 3).

8. Procedimiento de acuerdo con la reivindicación 2,
en el que la clave de comunicación incluye una pluralidad de claves de comunicación (6; 6a, 6b, 6c; 11) específicas del vehículo ferroviario, incluyendo la aportación de la clave de comunicación (6; 6a, 6b, 6c; 11) al vehículo ferroviario (4) la aportación de una clave de comunicación específica del vehículo ferroviario (4) de entre la pluralidad de claves de comunicación (11) específicas de vehículos ferroviarios.

9. Procedimiento de acuerdo con la reivindicación 8,
además con las etapas:
deducción en cada caso de una pluralidad de claves de comunicación (11) específicas de la central de control de línea de la pluralidad de claves de comunicación (6a, 6b, 6c) específicas del vehículo ferroviario y
aportación de un grupo de claves de comunicación (11) específicas de la central de control de línea en cada caso de una de la pluralidad de claves de comunicación (11) específicas de la central de control de línea que están asociadas específicamente para el vehículo ferroviario a las

segundas centrales de control de línea (2b; 3) del segundo operador de línea al segundo puesto de adjudicación de claves (1b).

10. Procedimiento de acuerdo con la reivindicación 9,
en el que la deducción de la pluralidad de claves de comunicación (11) específicas de la central de control de línea de la pluralidad de claves de comunicación (6a, 6b, 6c) específicas del vehículo ferroviario se realiza mediante un ordenador de control del vehículo ferroviario (4).

11. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10,
en el que el trayecto planificado para el vehículo ferroviario (4) lo aporta un sistema de conducción para el control de la circulación y en el que el primer puesto de adjudicación de claves (1a) realiza automáticamente la generación y la aportación de la clave de comunicación (6; 6a, 6b, 6c; 11).

12. Equipo de control (7) en un primer puesto de adjudicación de claves (1a) de un primer operador de línea de la red ferroviaria para distribuir claves de comunicación (6; 6a, 6b, 6c; 11) para encriptar mensajes de conducción del tráfico de un sistema de protección de vehículos ferroviarios con:
un equipo de generación, que está diseñado para generar una clave de comunicación (6; 6a, 6b, 6c; 11) en función de un trayecto planificado para un vehículo ferroviario (4) y
un equipo de aportación, que está diseñado para proporcionar la clave de comunicación generada (6; 6a, 6b, 6c; 11) al vehículo ferroviario (4), estando diseñada la clave de comunicación (6; 6a, 6b, 6c; 11) para encriptar mensajes de conducción del tráfico del vehículo ferroviario (4) para la comunicación segura frente a manipulaciones del vehículo ferroviario (4) con centrales de control de línea (2a; 3) del primer operador de línea y con centrales de control de línea (2b; 3) de un segundo operador de línea;
caracterizado porque
el equipo de aportación está diseñado para proporcionar la clave de comunicación (6; 6a, 6b, 6c; 11) generada al segundo puesto de adjudicación de claves (1b) del segundo operador de línea,
realizándose la generación y distribución de claves de comunicación bajo el control del primer puesto de adjudicación de claves (1a).

13. Sistema de protección de vehículos ferroviarios (20; 30; 40; 50) con
un equipo de control (7) de acuerdo con la reivindicación 12;
un primer puesto de adjudicación de claves (1a) en el que está dispuesto el equipo de control (7);
una pluralidad de primeras centrales de control de línea (2a; 3), que están diseñadas para que las alimente el primer puesto de adjudicación de claves (1a) con una clave de comunicación (6; 6a, 6b, 6c; 11) generada por el equipo de control (7) para encriptar mensajes de conducción del tráfico de un vehículo ferroviario (4);
un segundo puesto de adjudicación de claves (1b) y
una pluralidad de segundas centrales de control de línea (2b; 3), que están diseñadas para que las alimente el segundo puesto de adjudicación de claves (1b) con una clave de comunicación (6; 6a, 6b, 6c; 11) generada por el equipo de control (7) para encriptar mensajes de conducción del tráfico de un vehículo ferroviario (4).

FIG 1

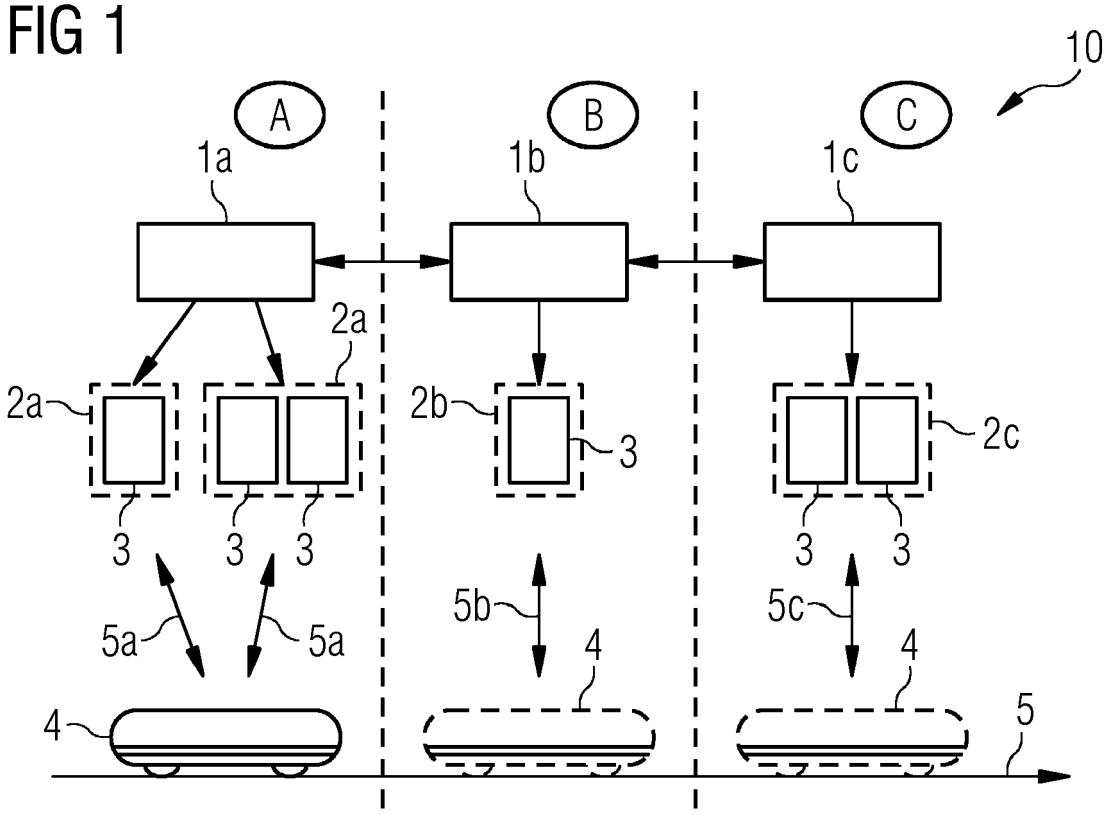
10
A
B
C
1a
1b
1c
2a
2a
2b
2c
3
3
3
3
3
3
5a
5a
5b
5c
4
4
4
5

FIG 2

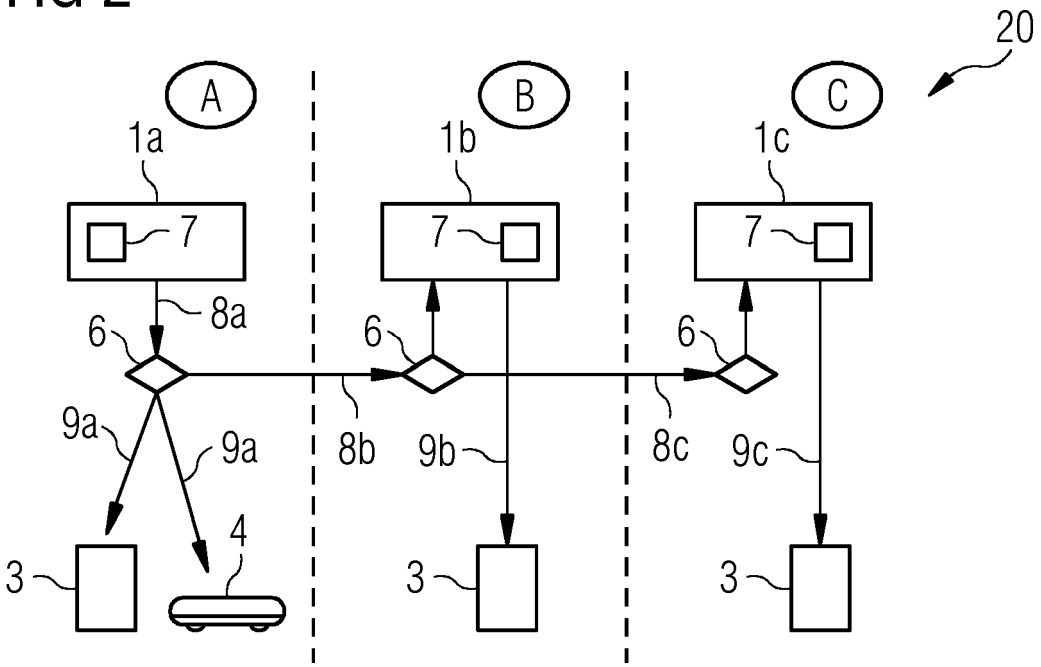
20
A
B
C
1a
1b
1c
7
7
7
8a
6
6
6
9a
9a
8b
9b
8c
9c
4
3
3
3

FIG 3

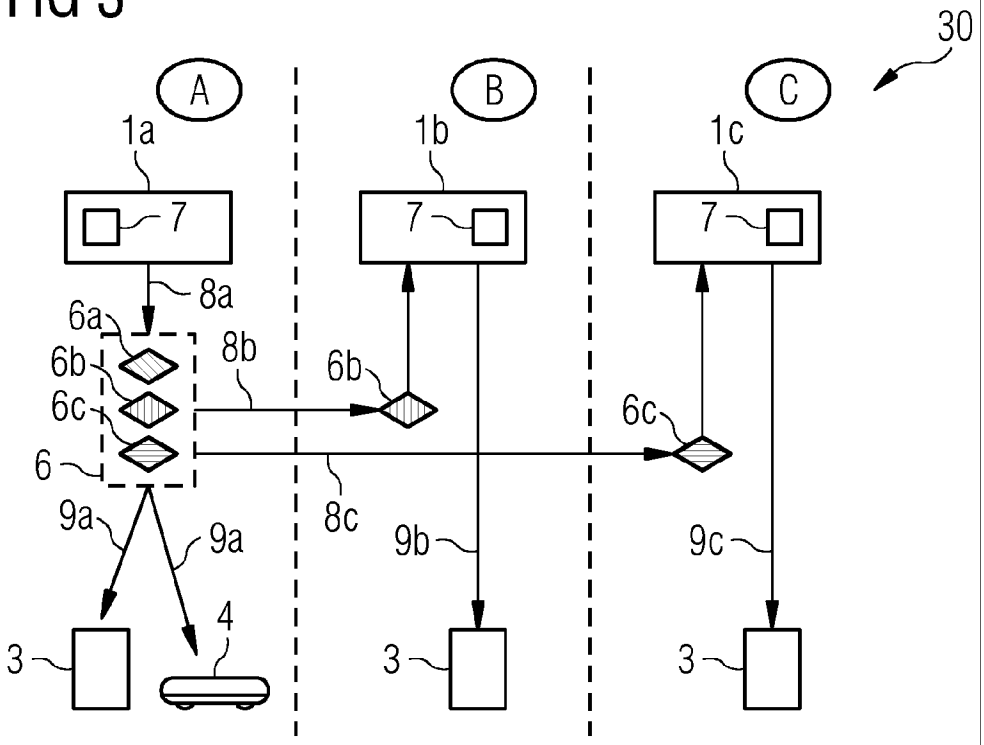
30
A
B
C
1a
1b
1c
7
8a
6a
6b
6c
6
8b
8c
9a
9b
9c
4
3

FIG 4

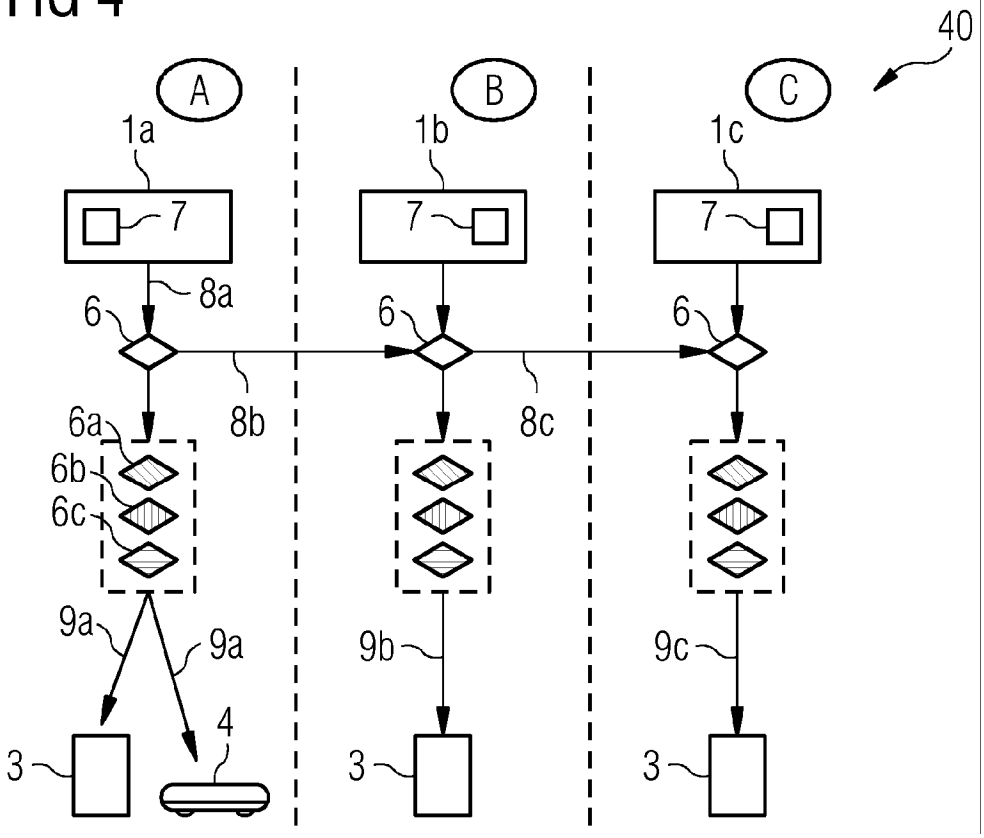
40
A
B
C
1a
1b
1c
7
8a
6
8b
8c
6a
6b
6c
9a
9b
9c
4
3

FIG 5

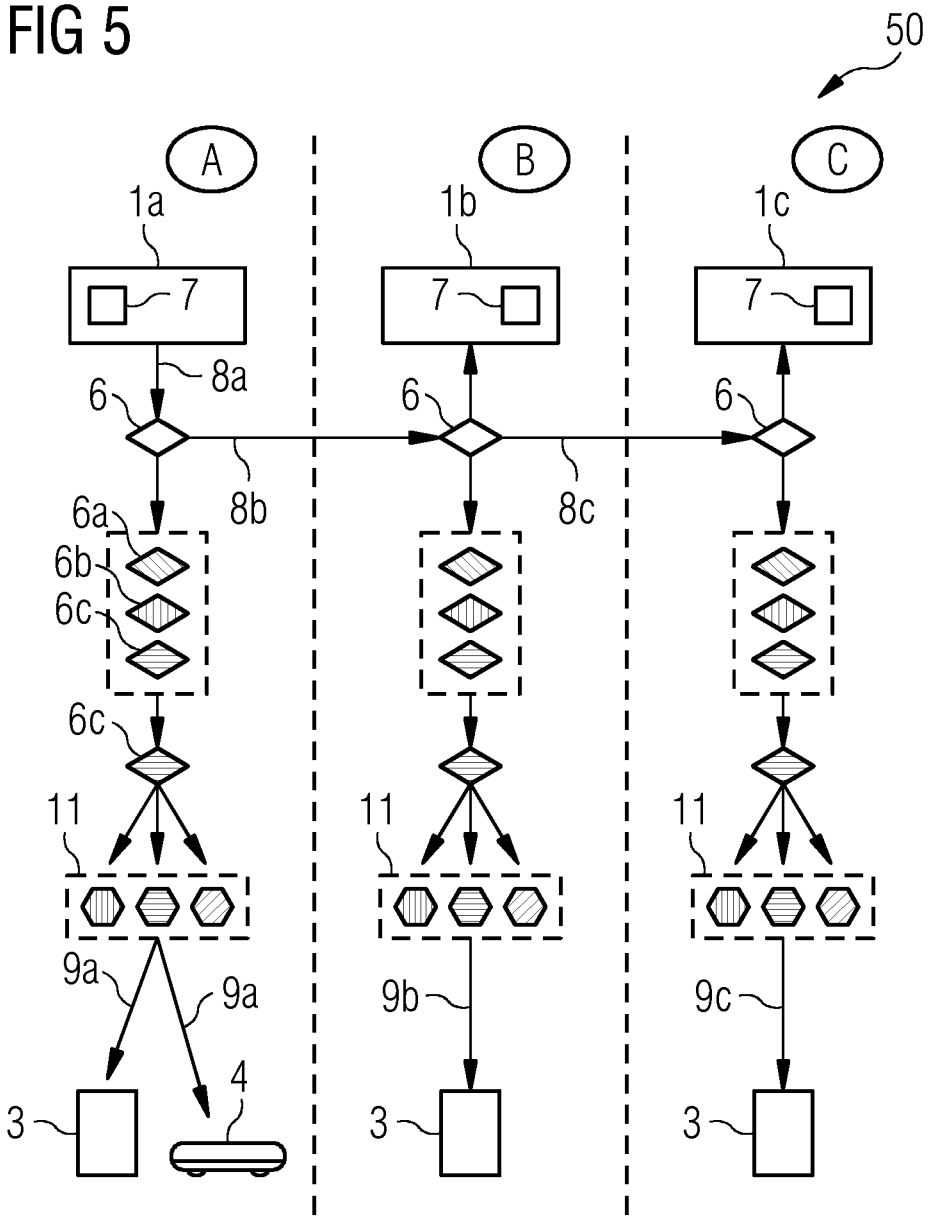

FIG 6