(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 437**

(51) Int. CI.:

B61L 3/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.05.2015 PCT/EP2015/061697**

(87) Fecha y número de publicación internacional: **30.12.2015 WO15197286**

(96) Fecha de presentación y número de la solicitud europea: **27.05.2015 E 15725327 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2019 EP 3137363**

(54) Título: **Verificación de la autenticidad de una baliza**

(30) Prioridad:

27.06.2014 DE 102014212516

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.07.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

DEICHMANN, UWE;
FRIEDRICHS, WERNER;
GEDUHN, NORBERT;
GOLEBNIAK, UDO;
KÄPPEL, JOCHEN y
SCHULZ, DIRK

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Verificación de la autenticidad de una baliza

La presente invención hace referencia a un procedimiento para el funcionamiento de un vehículo ferroviario, a un procedimiento para verificar un identificador proporcionado por una baliza, a un procedimiento para proporcionar un identificador mediante una baliza, a un equipamiento de línea ETCS, así como a un vehículo ferroviario.

El sistema de control de trenes europeo "European Train Control System" (ETCS) es un componente de un sistema de control de tráfico ferroviario que fue desarrollado bajo la abreviatura ERTMS. El segundo componente técnico de esa tecnología ferroviaria digital es el sistema de comunicaciones móviles ferroviario GSM-R. El sistema ETCS debe reemplazar la pluralidad de los sistemas de protección de trenes utilizados en los países, emplearse a medio plazo en el tráfico de alta velocidad e implementarse a largo plazo en todo el tráfico ferroviario europeo.

Un dispositivo de vehículo ETCS comprende por ejemplo un ordenador ETCS (EVC, European Vital Computer, ordenador vital europeo, denominado también como ordenador de vehículo (OBU, On-board Unit, unidad de a bordo)), una unidad de visualización del puesto del conductor (DMI, Driver Machine Interface), un dispositivo de medición de recorrido, un dispositivo de transmisión GSM-R (incluyendo Euroradio), un lector de balizas y un acceso de frenado (http://de.wikipedia. org/wiki/ETCS).

El sistema nivel 1 de ETCS utiliza balizas como medio de transmisión. La información transmitida por las balizas se trata de gradientes de líneas, velocidades límite en una sección de la línea, y el punto en el cual el vehículo debe detenerse nuevamente. Junto con un modo ETCS, la misma constituye la Movement Authority (MA), lo cual traducido significa "autorización para el movimiento" o "permiso para circular". De este modo, el equipamiento ETCS correspondiente al vehículo puede monitorear de forma continua el cumplimiento de la velocidad permitida (y dirección), y activar a tiempo un frenado de control.

Al final de la MA ("End of Authority" fin de la autorización de movimiento, EoA) - por ejemplo una señal que indica DETENCIÓN - el vehículo ferroviario tiene que detenerse.

Junto con los niveles ETCS también están definidos modos ETCS. Los modos describen los estados en los cuales puede encontrarse el EVC (véase también: http://de.wikipedia. org/wiki/ETCS).

En el nivel 2 de ETCS casi toda la información se transmite al vehículo mediante Euroradio, desde el puesto de control central (Radio Block Center, RBC). De manera adicional existe la posibilidad de transmitir información desde el tren hacia la línea, y la información también puede intercambiarse en el estado de detención. De este modo, la capacidad de utilización de la línea puede aumentarse un poco en comparación con el nivel 1. Antes de que RBC pueda calcular la información necesaria para un permiso de circulación (MA), el mismo debe saber dónde se encuentra precisamente el tren y en qué dirección circula el mismo. El ordenador del vehículo se encarga de la determinación de la posición y la dirección; el mismo la transmite regularmente a la línea mediante GSM-R. Sin embargo, para la determinación se necesitan puntos de referencia en la línea. Para ello se utilizan eurobalizas que por ejemplo están colocadas en vías de salida de estaciones, así como a distancias (por ejemplo irregulares) sobre líneas libres. Entre esos puntos de referencia, la posición se determina de forma odométrica mediante radar Doppler en el piso del vehículo de tracción y en transmisores de impulsos de las ruedas en los ejes del vehículo a tracción. Parcialmente también se utilizan sensores de aceleración.

La información sobre secciones libres de la vía se determina con en el nivel 1 de ETCS, mediante el aviso de vía libre fijado, desde el puesto de maniobra, y se transmite al puesto de control central: La línea - como en la técnica de protección convencional - está dividida en secciones ("bloques"), y el tren sólo puede ingresar a la siguiente sección cuando la misma no está ocupada por otro tren, sino que ha sido informada como "libre". (Fuente: http://de.wikipedia.org/wiki/ European_Train_Control_System.)

La transmisión correcta de un mensaje de la baliza ETCS se asegura mediante un control de redundancia cíclica (CRC, "Cyclic Redundancy Check"). De este modo se determina un valor de control (denominado también como código CRC) para datos, para poder descubrir errores en la transmisión (véase por ejemplo http://de.wikipedia.org/wiki/Zyklische_Redundanzprüfung).

El código CRC es adecuado para poder detectar errores habituales en los canales de comunicaciones. De este modo, se considera una desventaja en el hecho de que los códigos CRC de esa clase no ofrecen ninguna protección frente a una manipulación intencional (maliciosa) de los datos, por ejemplo en forma de diferentes ataques. A modo de ejemplo, las siguientes modificaciones podrían efectuarse en los avisos de la baliza:

- una modificación de la autorización de circulación (MA);

- una modificación de una información proporcionada por la baliza, por ejemplo "continuación del viaje" (Proceed) en lugar de "detención" (Stop);

- una modificación de valores de velocidad, de manera que por ejemplo se transmite una velocidad más elevada que la velocidad máxima verdaderamente prevista;

- una modificación de la señalización que limita la circulación;

- una modificación de valores de distancia.

Las manipulaciones de esa clase se tratan de ataques a datos proporcionados por la baliza, los cuales no pueden detectarse mediante el código CRC. Por ejemplo, los datos manipulados (con los códigos CRC apropiados para los mismos) pueden ser proporcionados por un agresor mientras que el vehículo ferroviario pasa por la baliza. Precisamente eso no se considera deseable para datos relevantes para la seguridad.

En la solicitud EP 2 022 697 A1 y en la solicitud EP 0 735 381 A2 se describen respectivamente sistemas y procedimientos en los cuales se verifica el identificador de balizas a bordo del vehículo ferroviario.

El objeto de la invención consiste en evitar las desventajas antes mencionadas y en particular en crear una posibilidad para una transmisión de datos segura y fiable, desde la baliza hacia el ordenador del vehículo, de un vehículo ferroviario.

Dicho objeto se soluciona según las características de las reivindicaciones independientes. Formas de ejecución preferentes pueden deducirse en particular de las reivindicaciones dependientes.

Para solucionar este objeto se propone un procedimiento para el funcionamiento de un vehículo ferroviario,

- en el cual una información para el funcionamiento del vehículo ferroviario y un identificador se transmiten desde una baliza hacia un ordenador del vehículo, del vehículo ferroviario,

- de manera que mediante el identificador se verifica la autenticidad de la baliza, por el vehículo ferroviario,

- en el cual, en el caso de una verificación exitosa del identificador, la información se utiliza para el funcionamiento del vehículo ferroviario.

Por ejemplo, la información y el identificador se transmiten juntos en un mensaje, desde la baliza, hacia el ordenador del vehículo, del vehículo ferroviario.

La información proporcionada se utiliza en particular de manera que por ejemplo pueden observarse especificaciones contenidas en la información, para el funcionamiento del vehículo ferroviario. En particular, el vehículo ferroviario es controlado en base a la información, en tanto el identificador haya podido verificarse de forma exitosa.

En este caso, cabe señalar que la verificación exitosa del identificador comprende en particular una verificación del identificador. Mediante la verificación del identificador, de este modo, puede asegurarse la autenticidad de la baliza. Con ello, está garantizado que la información obtenida también proviene de la baliza, y se impide que un agresor - disimulado como baliza - sin ser reconocido, transmita la información al vehículo ferroviario.

El identificador no es verificado por el ordenador del vehículo, en caso de que se determine que está presente un identificador o en el caso de que el identificador presente un valor predeterminado.

Por ejemplo, puede prescindirse de una verificación, en caso de que no se encuentre presente ningún identificador. Esto puede determinarse debido a que el identificador presenta un valor predeterminado, por ejemplo, el campo en el que se transmite el identificador está vacío, o presenta o contiene un valor determinado.

También puede prescindirse de la verificación en caso de que el identificador no presente un valor predeterminado. En ese caso, la verificación sólo se realiza cuando el identificador es detectado como tal. Para ello es posible que el identificador comprenda un valor adicional, por ejemplo en forma de un patrón de bits, el cual por ejemplo forma parte del identificador y/o se encuentra presente adicionalmente con respecto al mismo. De este modo, el valor adicional puede anticiparse al identificador o puede estar añadido al mismo.

Por ejemplo si un campo de datos, en el cual podría transmitirse el identificador, se usa con otro fin y en el mismo no se encuentra presente ningún identificador, entonces esto es detectado y puede omitirse la verificación del identificador.

Otro perfeccionamiento consiste en el hecho de que la información no se utilice en el caso de que la verificación del identificador no haya sido exitosa.

En tanto el identificador (que se encuentra presente y reconocido como tal) no haya podido verificarse, se supone por ejemplo que la información de la baliza no es válida. Puede entonces iniciarse una acción adecuada, por ejemplo una verificación de la baliza y/o el pasaje del sistema a un estado seguro, por ejemplo un frenado o una detención del vehículo ferroviario.

Se considera especial un perfeccionamiento en el cual la información no se utiliza en el caso de que se haya detectado el identificador y la verificación no haya sido exitosa.

También se considera un perfeccionamiento en el cual el vehículo ferroviario pasa a un estado seguro en el caso de que la verificación del identificador no haya sido exitosa.

También se considera un perfeccionamiento en el cual el identificador comprende al menos una de las siguientes posibilidades:

- datos cifrados;

- datos no cifrados;

- datos que fueron determinados en base a una función hash, en particular en base a una función hash criptográfica;

- datos que fueron determinados en base a un algoritmo MD4;

- una firma;

- un certificado;

- un valor para la identificación del identificador;

- un valor para la identificación de un tipo del identificador.

En el marco de un perfeccionamiento adicional, el identificador se transmite en un bloque 44 de la implementación ETCS conforme a UNISIG.

Un siguiente perfeccionamiento consiste en que

- el identificador es verificado por el vehículo ferroviario, determinando otro identificador mediante la información y comparando el identificador con el otro identificador,

- la verificación del identificador ha sido exitosa en el caso de que el identificador y el otro identificador sean idénticos.

En una configuración,

- el identificador es cifrado (por ejemplo desde la baliza);

- el identificador es descifrado desde el vehículo vehículo ferroviario,

- el vehículo ferroviario, mediante la información, determina otro identificador y compara el identificador descifrado con el otro identificador,

- la verificación del identificador ha sido exitosa en el caso de que el identificador descifrado y el otro identificador sean idénticos.

Una forma de ejecución alternativa consiste en que para el cifrado y para el descifrado se utilice un procedimiento de cifrado simétrico o asimétrico.

En otra configuración, mediante el identificador, el vehículo ferroviario determina qué tipo de verificación del identificador debe realizarse.

Por ejemplo, el identificador puede presentar un valor para la identificación del identificador, por ejemplo en forma de un patrón de bits, mediante el cual puede determinarse que el mismo se trata de un identificador. El identificador puede presentar también un valor para la identificación del tipo de identificador, de modo que puede determinarse mediante qué algoritmo puede verificarse el identificador. El valor para la identificación del identificador y/o el valor para la identificación del tipo de identificador pueden estar codificados en un patrón de bits. El patrón de bits, por ejemplo, puede formar parte del identificador, como cabecera o similares, o también puede transmitirse separado del identificador.

Las ejecuciones, así como las características que hacen referencia al procedimiento antes explicado aplican para las siguientes reivindicaciones, en particular para las categorías de reivindicaciones, de modo correspondiente.

El objeto se soluciona también mediante un procedimiento para verificar un identificador proporcionado desde una baliza,

- en el cual un ordenador del vehículo, de un vehículo ferroviario, recibe el identificador y una información desde la baliza,

- de manera que mediante el identificador se verifica la autenticidad de la baliza, por el ordenador del vehículo.

En una configuración, en el caso de una verificación exitosa del identificador, la información se utiliza para el funcionamiento del vehículo ferroviario.

Además, en una configuración, el identificador se recibe en un bloque 44 de la implementación ETCS, conforme a UNISIG.

Además, el objeto se soluciona mediante un procedimiento para proporcionar un identificador mediante una baliza,

- en el cual se crea un identificador en base a una información,

- en el cual el identificador y la información se proporcionan a un vehículo ferroviario al pasar por la baliza,

- de manera que mediante el identificador puede verificarse la autenticidad de la baliza, por el vehículo ferroviario.

De manera adicional, el objeto se soluciona mediante un equipamiento de línea ETCS

- con al menos una baliza,

- donde al menos una baliza está configurada de modo que al ser pasada por un vehículo ferroviario proporciona un identificador y una información, donde el identificador fue creado en base a la información, de modo que mediante el identificador se verifica la autenticidad de la baliza, por el vehículo ferroviario.

En un perfeccionamiento, el identificador puede determinarse mediante una función hash (o función hash) criptográfica y el identificador puede almacenarse en un bloque 44 de la implementación ETCS, conforme a UNISIG.

El objeto se soluciona también mediante un vehículo ferroviario con un ordenador del vehículo, el cual está configurado de manera que

- el identificador y una información son recibidos desde la baliza,

- mediante el identificador se verifica la autenticidad de la baliza, por el vehículo ferroviario.

El ordenador del vehículo mencionado puede estar realizado en particular como una unidad de procesador y/o como una disposición de conmutación al menos cableada de forma fija o lógica, la cual por ejemplo está configurada de modo que el procedimiento puede realizarse del modo aquí descrito. El ordenador del vehículo mencionado puede ser o comprender cualquier clase de procesador, ordenador o computadora con la periferia necesaria correspondiente (memorias, interfaces de entrada/salida, aparatos de entrada-salida). El ordenador del vehículo puede formar parte de una unidad de control del vehículo ferroviario.

El objeto antes mencionado se soluciona también mediante un sistema de que comprende al menos uno de los dispositivos aquí descritos.

Las propiedades, características y ventajas de esta invención, antes descritas, así como el modo de alcanzarlas, se aclaran de forma más comprensible con relación a la siguiente descripción esquemática de ejemplos de ejecución que se explican en detalle con relación a los dibujos. Con el fin de una mayor claridad, los elementos idénticos o que actúan del mismo modo pueden estar provistos de los mismos símbolos de referencia.

Muestran:

Figura 1: un diagrama a modo de ejemplo, el cual comprende un vehículo ferroviario con un ordenador del vehículo que está conectado a una antena de balizas, donde el vehículo ferroviario se desplaza sobre una línea, en dirección de dos balizas;

Figura 2: un diagrama secuencial, a modo de ejemplo, de una comunicación entre la baliza y el ordenador del vehículo, del vehículo ferroviario.

Cabe señalar que el vehículo ferroviario (denominado también como "tren"), presenta al menos uno, en particular al menos dos vagones, donde los vagones pueden tratarse de una unidad de tracción, de un vagón de pasajeros, de un vagón de carga o de una combinación de compartimentos o funciones de esa clase. La unidad de tracción presenta una cabina del conductor (denominada también como puesto de mando), y puede estar realizada con o sin accionamiento. La unidad de tracción en particular puede ser una locomotora. Cada vagón del vehículo ferroviario puede estar equipado con un ordenador del vehículo; si el ordenador del vehículo (eventualmente con la interfaz de comunicaciones móvil), proporciona una función ETCS, el mismo puede denominarse eventualmente como vagón ETCS. En principio es posible que sólo las unidades de tracción presenten en cada caso un ordenador del vehículo (eventualmente con la interfaz de comunicaciones móvil), así como que también los vagones individuales que no sean unidades de tracción presenten ordenadores del vehículo de esa clase (eventualmente con la interfaz de comunicaciones móvil).

La solución aquí propuesta posibilita en particular una transmisión protegida de información, relevante en cuanto a la seguridad, hacia el vehículo ferroviario, por ejemplo desde una baliza hacia el vehículo ferroviario.

Por ejemplo, para ello puede utilizarse un así llamado paquete 44 de la implementación ETCS conforme a UNISIG (SUBSET-026-7), para transmitir un mensaje protegido (por ejemplo desde la baliza), hacia el ordenador del vehículo, del vehículo ferroviario. De este modo, el paquete 44 permite la transferencia transparente de (cualquier) información. El mensaje protegido, de este modo, puede transmitirse en el paquete 44.

El mensaje protegido se trata por ejemplo de un identificador. El identificador puede comprenden por ejemplo al menos una de las siguientes posibilidades (valores, así como datos):

- datos cifrados;

- datos no cifrados;

- datos que fueron determinados en base a una función hash, en particular en base a una función hash criptográfica;

- datos que fueron determinados en base a un algoritmo MD4;

- una firma;

- un certificado;

- un valor para la identificación del identificador;

- un valor para la identificación de un tipo del identificador.

Por ejemplo, el identificador puede determinarse en base a una función hash criptográfica. Ejemplos de funciones hash criptográficas son los así llamados algoritmos hash de mensajes, por ejemplo "MD2" o "MD4" (véase por ejemplo RFC 1320 del Network Working Group, http://tools.ietf.org/html/rfc1320).

El identificador puede estar incorporado en el paquete 44 y, junto con otra información, puede transmitirse como parte del mensaje de la baliza, desde la baliza hacia el ordenador del vehículo, del vehículo ferroviario. Mediante el

identificador, el ordenador del vehículo puede autentificar la baliza, es decir, determinar si la información obtenida proviene de la baliza proporcionada para ello.

Gracias a esto, los mensajes pueden protegerse adicionalmente contra manipulaciones intencionales de datos (en particular contra los así llamados ataques de intermediario, véase por ejemplo http://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff).

El identificador puede comprender también el valor de una función hash. La función hash (denominada también como función de valor de dispersión) es una representación que representa un conjunto de entrada de gran tamaño (las claves) en un conjunto-diana más reducido (los valores hash). La función hash no es forzosamente inyectiva. En particular, el conjunto de entrada puede contener también elementos con diferentes longitudes, mientras que los elementos del conjunto-diana presentan en particular una longitud fija. Una así llamada colisión se produce entonces cuando a diferentes datos de entrada se asocia el mismo valor hash.

El identificador puede comprender también el valor de una función hash criptográfica (denominada también como función hash criptológica (véase http://de.wikipedia. org/wiki/Kryptologische_Hashfunktion). En este caso se trata de una forma especial de la función hash, la cual es resistente a colisiones y/o es una función unidireccional. La función unidireccional, de forma teórica, puede calcularse "fácilmente" en cuanto su complejidad, pero es "difícil" de invertir. Las funciones unidireccionales también son funciones para las cuales hasta el momento no es conocida ninguna inversión que pueda realizarse de forma práctica en un tiempo adecuado.

Existen funciones hash criptográficas sin clave y funciones hash criptográficas que dependen de claves.

También es posible que el identificador comprenda una firma digital. Una firma digital, también un procedimiento de firma digital, es un criptosistema asimétrico, en el cual un emisor, con la ayuda de una clave de firma secreta (la clave privada), para un mensaje digital (es decir, cualquier dato deseado), calcula un valor que igualmente se denomina como firma digital. Ese valor permite a cualquiera verificar la integridad del mensaje, con la ayuda de la clave de verificación pública (la clave pública) (véase http://de.wikipedia.org/wiki/ Digitale_Signatur).

Por ejemplo, de este modo el ordenador del vehículo, mediante la clave pública de la baliza, puede verificar el mensaje de la baliza (o una parte del mensaje de la baliza). Para el cifrado, la baliza usa su clave de firma secreta, la cual preferentemente está almacenada en la baliza del modo más seguro posible contra manipulaciones y sólo puede ser usada por la propia baliza.

Una posibilidad consiste en almacenar en el paquete 44 un valor hash del mensaje o una parte del mensaje, y en transmitirlo al ordenador del vehículo, del vehículo ferroviario. El ordenador del vehículo determina ahora un valor hash en base al mensaje o una parte del mensaje, y compara ese valor hash con el valor hash recibido en el paquete 44. Si los dos valores hash son idénticos se supone que el mensaje no fue manipulado de forma intencional.

Una posibilidad alternativa consiste en que la baliza marque el valor hash de la información que debe transmitirse (por tanto de forma cifrada con la clave privada de la baliza), y que el identificador se almacene en el paquete 44. La información y el identificador (por ejemplo como mensaje), se transmiten al ordenador del vehículo, del vehículo ferroviario. El ordenador del vehículo determina ahora un valor hash en base a la información y decodifica el identificador mediante la clave pública de la baliza (la misma opcionalmente también puede ser transmitida desde la baliza). El valor hash determinado por el ordenador del vehículo se compara con el valor hash creado por la baliza; si los dos son idénticos, entonces el identificador se ha verificado de forma exitosa; la información proporcionada por la baliza puede utilizarse o procesarse de modo posterior, de modo correspondiente.

Por ejemplo, en el paquete 44 puede estar contenida una marcación, por ejemplo en forma de una combinación de bits, la cual indica al ordenador del vehículo, del vehículo ferroviario, si el paquete 44 puede utilizarse para la verificación o la autenticación del mensaje. Si es ése el caso, por ejemplo pude tener lugar uno de los controles (verificaciones) antes explicados. En cambio, si el paquete 44 está vacío o no presenta ninguna de eventualmente una pluralidad de combinaciones de bits predeterminadas, entonces no tiene lugar una verificación en base a los datos del paquete 44. Ese principio, de este modo, también es compatible con otras posibilidades de utilización del paquete 44.

También es una opción que, dependiendo del caso de aplicación, pueda exigirse que se autentifique cada baliza. En un caso de esa clase puede estar proporcionado al menos un campo de datos que se utiliza para transmitir el identificador, de modo que mediante el identificador puede autentificarse la baliza emisora. Si no puede verificarse una baliza, entonces puede realizarse una acción adecuada, la cual por ejemplo comprende una de las siguientes posibilidades: emisión de un aviso de advertencia, pasaje del sistema y/o de al menos un vehículo ferroviario a un estado seguro (por ejemplo detención), monitoreo y eventualmente mantenimiento de la baliza, etc.

Otra opción consiste en que una combinación de bits de esa clase en el paquete 44 puede presentar diferentes valores, de los cuales a cada uno se encuentra asociado una clase de verificación determinada. Por ejemplo, una combinación de bits predeterminada puede indicar que en el paquete 44 fue almacenado un valor hash; además, mediante el valor de la combinación de bits puede estar predeterminado qué función hash fue utilizada para crear el valor hash. Además, otro valor de la combinación de bits puede indicar que está almacenada una firma electrónica, o según qué algoritmo fue generada la firma electrónica.

La utilización del paquete 44 para la transferencia transparente de datos que pueden utilizarse para verificar el mensaje sólo debe entenderse como un ejemplo. En principio es posible utilizar otros campos de datos o campos de datos adicionales para transmitir la información relevante para la verificación aquí descrita, desde un emisor hacia el ordenador del vehículo, del vehículo ferroviario. La transmisión de los datos puede tener lugar por ejemplo de forma inalámbrica (por ejemplo mediante radio, mediante comunicación de campo próximo, mediante una red de telecomunicaciones, etc.) o por cables.

La figura 1 muestra un diagrama a modo de ejemplo, el cual comprende un vehículo ferroviario 101 con un ordenador del vehículo 102 que está conectado a una antena de balizas 103. El vehículo ferroviario 101 se desplaza sobre una línea 104, en una dirección de circulación 105. En la dirección de circulación 105, el vehículo ferroviario 101 pasa primero por una baliza 106, después por una baliza 107.

Las balizas 106 y 107 se tratan por ejemplo de euro-balizas, donde por ejemplo la baliza 106 es una baliza de datos transparentes y la baliza 107 es una baliza de datos fijos (véase http://de.wikipedia. org/wiki/Eurobalise).

La baliza de datos trasparentes (Transparent Data Balise o Controllable Balise - baliza controlable) está conectada, por ejemplo con un cable, a una unidad electrónica del lado de la línea (LEU, Lineside Electronic Unit). La unidad LEU transmite a la baliza el mensaje que respectivamente debe transferirse.

Cabe señalar en este punto que el término baliza comprende aquí también una pluralidad de balizas proporcionadas unas detrás de otras, de un así llamado grupo de balizas.

Al pasar por la respectiva baliza, la baliza 106 y/o la baliza 107, mediante la antena de balizas 103 y el ordenador del vehículo 102, proporciona al vehículo ferroviario 101 un mensaje (de balizas) que presenta un campo de datos (por ejemplo en forma del paquete 44 antes descrito), en el cual está contenido por ejemplo el identificador. Mediante el campo de datos es posible verificar la integridad o la autenticidad de los datos contenidos. De este modo, en particular puede asegurarse que la información provenga efectivamente de la baliza 106 y/o 107, y que no haya sido falsificada.

Preferentemente, la respectiva baliza 106, así como 107, está realizada de modo que desde el exterior no pueda lograrse un acceso a un área de memoria segura o que el mismo sólo pueda lograrse con una inversión muy elevada. En un área de memoria asegurada de ese modo puede estar almacenada una clave privada que se utiliza para crear la firma. De manera preferente, esa clave debe asegurarse de forma adecuada frente a accesos desde el exterior.

Una opción consiste en que la baliza, en el mensaje (por ejemplo en el campo de datos o en el paquete 44), transmita también la clave pública de la baliza (denominada también como clave de verificación pública o certificado). Preferentemente, el vehículo ferroviario puede verificar si la clave pública cuadra con la posición de la baliza. Preferentemente, sólo entonces y sólo cuando la verificación de los datos ha sido exitosa, los datos del mensaje son procesados de forma posterior por el ordenador del vehículo, del vehículo ferroviario.

La figura 2 muestra un diagrama secuencial, a modo de ejemplo, de una comunicación entre la baliza 106, 107 y el ordenador del vehículo 102, del vehículo ferroviario 101.

En un paso 201, la baliza 106, 107 crea el mensaje o recibe desde la unidad LEU el mensaje que debe retransmitirse. En una etapa 202, la baliza crea un valor hash mediante una función hash criptográfica (por ejemplo MD4) y almacena el valor hash en el paquete 44 de la implementación ETCS conforme a UNISIG (SUBSET-026-7). En una etapa 203, el mensaje se transmite desde la baliza 106, 107 hacia el ordenador del vehículo 102. El ordenador del vehículo 102, mediante el mensaje (en base a datos predeterminados del mensaje, por ejemplo todos los datos sin el paquete 44), en una etapa 202, determina un valor hash mediante una función hash criptográfica, que también fue utilizada por la baliza 106, 107. En una etapa 205, el ordenador del vehículo 102 compara el valor hash determinado con el valor hash leído desde el paquete 44. Si los dos valores hash son idénticos, entonces se supone que los datos del mensaje no fueron falsificados y se inicia una acción (por ejemplo un control del vehículo ferroviario 101) en base a esos datos. Si los dos valores hash no fueran idénticos, entonces puede mostrarse un aviso de error, por ejemplo al vehículo ferroviario y/o a un puesto de maniobra. En particular, en ese caso el funcionamiento del vehículo ferroviario puede pasarse a un estado seguro, y a continuación puede controlarse si la baliza 106, 107 se encuentra defectuosa o si ha tenido lugar un intento de manipulación.

Si bien la invención fue ilustrada y descrita en detalle mediante al menos un ejemplo de ejecución mostrado, la invención no está limitada al mismo y el experto puede deducir de éste otras variaciones, sin abandonar el alcance de protección de la invención, que está definido por las reivindicaciones.

REIVINDICACIONES

1. Procedimiento para el funcionamiento de un vehículo ferroviario (101),

- en el cual una información para el funcionamiento del vehículo ferroviario (101) y un identificador se transmiten desde una baliza (106, 107) hacia un ordenador del vehículo (102) del vehículo ferroviario (101),

- de manera que mediante el identificador se verifica la autenticidad de la baliza (106, 107), por el vehículo ferroviario (101),

- en el cual, en el caso de una verificación exitosa del identificador, la información se utiliza para el funcionamiento del vehículo ferroviario (101).

2. Procedimiento según la reivindicación 1, en el cual la información no se utiliza en el caso de que la verificación del identificador no haya sido exitosa.

3. Procedimiento según la reivindicación 1, en el cual la información no se utiliza en el caso de que se haya detectado el identificador y la verificación no haya sido exitosa.

4. Procedimiento según una de las reivindicaciones precedentes, en el cual el vehículo ferroviario pasa a un estado seguro en el caso de que la verificación del identificador no haya sido exitosa.

5. Procedimiento según una de las reivindicaciones precedentes, en el cual el identificador comprende al menos una de las siguientes posibilidades:

- datos cifrados;

- datos no cifrados;

- datos que fueron determinados en base a una función hash, en particular en base a una función hash criptográfica;

- datos que fueron determinados en base a un algoritmo MD4;

- una firma;

- un certificado;

- un valor para la identificación del identificador;

- un valor para la identificación de un tipo del identificador.

6. Procedimiento según una de las reivindicaciones precedentes, en el cual el identificador se transmite en un bloque 44 de la implementación ETCS conforme a UNISIG.

7. Procedimiento según una de las reivindicaciones precedentes,

- en el cual el identificador es verificado por el vehículo ferroviario (101) determinando otro identificador mediante la información y comparando el identificador con el otro identificador,

- en el cual la verificación del identificador ha sido exitosa en el caso de que el identificador y el otro identificador sean idénticos.

8. Procedimiento según una de las reivindicaciones 1 a 6,

- en el cual se cifra el identificador,

- en el cual el identificador es descifrado por el vehículo ferroviario (101),

- en el cual el vehículo ferroviario (101), mediante la información, determina otro identificador y compara el identificador descifrado con el otro identificador,

- en el cual la verificación ha sido exitosa en el caso de que el identificador descifrado y el otro identificador sean idénticos.

9. Procedimiento según la reivindicación 8, en el cual para el cifrado y el descifrado se utiliza un procedimiento de cifrado simétrico o asimétrico.

10. Procedimiento según una de las reivindicaciones precedentes, en el cual, mediante el identificador, el vehículo ferroviario (101) determina qué clase de verificación del identificador debe realizarse.

11. Procedimiento para verificar un identificador proporcionado por una baliza (106, 107),

- en el cual un ordenador del vehículo (102) de un vehículo ferroviario (101) recibe el identificador y una información desde la baliza (106, 107),

- de manera que mediante el identificador se verifica la autenticidad de la baliza (106, 107), por el ordenador del vehículo (102).

12. Procedimiento según la reivindicación 11, en el cual, en el caso de una verificación exitosa, la información se utiliza para el funcionamiento del vehículo ferroviario.

13. Procedimiento según una de las reivindicaciones 11 ó 12, en el cual el identificador se recibe en un bloque 44 de la implementación ETCS conforme a UNISIG.

14. Procedimiento para proporcionar un identificador mediante una baliza (106, 107),

- en el cual se crea un identificador en base a una información,

- en el cual el identificador y la información se proporcionan a un vehículo ferroviario (102, 101) al pasar por la baliza (106, 107),

- de manera que mediante el identificador se verifica la autenticidad de la baliza (106, 107), por el vehículo ferroviario (101, 102).

15. Equipamiento de línea ETCS

- con al menos una baliza (106, 107),

- donde al menos una baliza (106, 107) está configurada de manera que la misma, al ser pasada por un vehículo ferroviario (101), proporciona un identificador y una información, donde el identificador fue creado en base a la información, de manera que el vehículo ferroviario (101) verifica la autenticidad de la baliza (106, 107) mediante el identificador.

16. Equipamiento de línea ETCS según la reivindicación, en el cual el identificador puede determinarse mediante una función hash criptográfica, y en el cual el identificador puede almacenarse en un bloque 44 de la implementación ETCS conforme a UNISIG.

17. Vehículo ferroviario (101) con un ordenador del vehículo (102) que está configurado de manera que

- el identificador y una información son recibidos desde la baliza (106, 107),

- mediante el identificador se verifica la autenticidad de la baliza (106, 107), por el vehículo ferroviario (101).

FIG 1

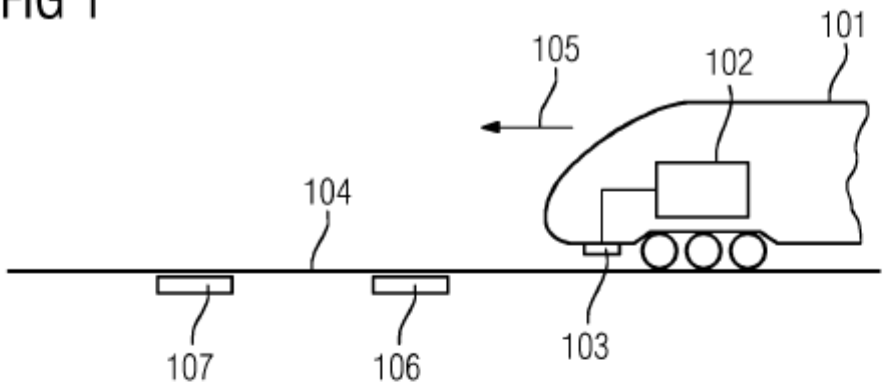

FIG 2