(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 647 673**

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.05.2012 PCT/EP2012/059051**

(87) Fecha y número de publicación internacional: **29.11.2012 WO12159940**

(96) Fecha de presentación y número de la solicitud europea: **15.05.2012 E 12726036 (2)**

(97) Fecha y número de publicación de la concesión europea: **16.08.2017 EP 2684154**

(54) Título: **Procedimiento y unidad de control para la detección de manipulaciones en una red de vehículo**

(30) Prioridad:

24.05.2011 DE 102011076350

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.12.2017

(73) Titular/es:

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

(72) Inventor/es:

BEYER, RALF y
FALK, RAINER

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

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

DESCRIPCIÓN

Procedimiento y unidad de control para la detección de manipulaciones en una red de vehículo

La invención se refiere a una vigilancia de la seguridad de información o de la integridad para mantener la seguridad de funcionamiento / “safety” y para mantener la seguridad contra ataques / “security” para la protección contra daños por manipulación.

Una transmisión de datos basada en Ethernet o basada en IP se usa crecientemente para realizar tareas de control y de vigilancia. Así, diferentes vehículos, especialmente vehículos ferroviarios, disponen de redes de datos para realizar el control de vehículo, así como para funciones de operación.

La realización exacta correcta de tareas de control y de vigilancia de un vehículo o de un vehículo ferroviario de un conjunto de tren requiere que la red de control y los componentes de control conectados a través de esta, tales como un ordenador de control, subsistemas o componentes de campo con sensores y actores, funcionen correctamente. En caso de manipulaciones en la red de control, esto sin embargo no está garantizado, porque se pueden modificar datos de control y de medición transmitidos. Por ello se ve perjudicado el funcionamiento correcto. Eventualmente, ya no pueden cumplirse correctamente funciones necesarias para la seguridad de funcionamiento del vehículo.

Se conocen medidas de protección para redes de vehículo en diferentes formas. Por ejemplo, se pueden instalar redes de control con protección de acceso. Esto se realiza por ejemplo en cajas de cables especiales, de tal forma que no están accesibles para personas ajenas y por tanto se pueden evitar manipulaciones. Sin embargo, esto es muy costoso y a causa de la instalación y la realización complejas de trabajos de mantenimiento generalmente no es viable. Las medidas de protección físicas sencillas pueden franquear de manera relativamente sencilla, por ejemplo si sólo hay que retirar o desatornillar una cubierta.

Generalmente, las redes de control están cerradas lógicamente, es decir que no están conectadas o no están conectadas directamente a redes externas. Mediante un llamado “firewall” se puede limitar al menos el tráfico de datos, en el sentido de que se seleccionan datos que pueden intercambiarse con redes externas. De esta manera, no es posible o sólo es posible con un gran esfuerzo un ataque a la red desde fuera.

Mediante las medidas descritas, sin embargo, no se establece ninguna protección contra manipulaciones en el vehículo, de manera que sí se pueden manipular datos dentro de una red de vehículo.

Además, se conoce el modo de proteger datos durante la transmisión mediante una suma de control como por ejemplo un “valor CRC / Cyclic Redundancy Check”, una prueba de redundancia cíclica. Estas sumas de control resultan adecuadas solamente para detectar errores de transmisión aleatorios. De esta manera, no se consigue una protección contra la manipulación intencionada, ya que el atacante puede calcular de manera sencilla el valor CRC para los datos manipulados por el.

Igualmente se conocen sumas de control criptográficas, como por ejemplo un “Message-Authentication-Code” (código de autenticación de mensaje) o una “firma digital”. En este caso, los datos transmitidos, por ejemplo datos de control para un vehículo, se complementan con una suma de control criptográfica durante la emisión. Esta se comprueba durante la recepción. Se siguen procesando datos comprobados correctamente. Se puede codificar por ejemplo la comunicación con “MACsec”, “IPsec” o “SSL/TLS”. Los datos transmitidos están protegidos por una suma de control criptográfica. Una protección criptográfica de este tipo puede realizarse posteriormente sólo de forma complicada, como integración en componentes de automatización. Un componente preconectado de codificación separado es igualmente complicado. Además, el cálculo y la comprobación de una suma de control criptográfica conduce a un retardo por las operaciones criptográficas que requieren mucho cálculo, lo que no es deseable especialmente en el caso de tareas de control y de regulación críticas en tiempo real.

Además se conocen los llamados “sistemas de detección de intrusos” que vigilan el tráfico de red producido. En caso de tráfico de red “sospechoso” se activa una alarma. Se pueden detectar patrones de ataque conocidos, las llamadas firmas de ataque, del tráfico de red. De esta manera, sin embargo, se pueden detectar sólo ataques especiales, conocidos ya. Mediante procedimientos heurísticos como por ejemplo la detección de un cambio significativo de magnitudes estadísticas que describen el tráfico de red, se intenta detectar también ataques desconocidos hasta ahora. De esta manera, solamente se pueden detectar ataques mediante la evaluación de un cambio significativo de valores característicos estadísticos como por ejemplo la duración de acceso o la frecuencia de uso de un servicio de red. En caso de variaciones aleatorias se puede detectar de forma ligeramente errónea un supuesto ataque.

Por lo tanto, los procedimientos de detección de ataque basados en el análisis de valores característicos estadísticos no son fiables y se emplean como mucho de forma complementaria en la práctica.

Con una detección de topología automática en la red se detectan por ejemplo por medio de “LLDP”, “CDP”, “SNMP” o “Broadcast Ping” todos los aparatos de red conectados. Por “LLDP” se puede detectar también la topología del cableado de red.

El documento US2006/0180709 con el título “Method and System for IP Train Inauguration” describe una inauguración de tren que se produce en una red de control de tren basada en IP. La topografía del tren que está concebida especialmente para un vehículo guía se determina mediante una detección de red. En función de ello se configuran el “routing” y la conversión de direcciones IP / NAT.

El documento US2007/174608A1 describe una red de comunicación con una arquitectura distribuida. Un nodo usado en esta red presenta una funcionalidad de codificación y una funcionalidad de emisión y de recepción para emitir y recibir paquetes de datos.

La invención tiene el objetivo de detectar modificaciones en una red de vehículo, especialmente en la de un vehículo ferroviario, y evitar una puesta en peligro de la integridad, es decir de la seguridad de funcionamiento / “safety” y de la seguridad contra ataques / “security”.

Este objetivo se consigue mediante la respectiva combinación de características de reivindicaciones formuladas independientemente.

La invención está basada en el conocimiento de que se pueden detectar diversas manipulaciones o vandalismos en una red de vehículo que ponen en peligro la realización correcta de funciones de control en el vehículo. Si no se puede garantizar un estado de funcionamiento seguro no se permite un funcionamiento regular.

Para el funcionamiento regular de un vehículo es necesaria generalmente la integridad de la red de vehículo. Una modificación intencionada o accidental o provocada por fallos técnicos puede producirse en cualquier momento. La integridad incluye la seguridad de funcionamiento / “safety”, la protección contra errores de transmisión, y la seguridad contra ataques / “security”, especialmente la protección contra modificaciones intencionadas.

Una detección de manipulaciones en un vehículo, especialmente un vehículo ferroviario, se realiza de tal forma que se detecta una huella digital de una red de vehículo y se compara con una información de referencia depositada. Una huella digital de una red de vehículo caracteriza la configuración existente actualmente de la red de vehículo, es decir, el número de componentes de red conectados tales como aparatos de control y/o una cantidad de información de identificación de los componentes de red conectados. La información de identificación de un componente de red puede estar dada por ejemplo por su dirección de red como la dirección MAC, la dirección IP, o por su tipo y su número de serie. Una huella digital de una red de vehículo puede comprender también una información que caracteriza la topología de red, es decir que describe qué componente de red está conectado directamente a qué otro u otros componentes de red y a través de qué interfaz. En función del resultado de la comparación, se realiza una adaptación de la función de control de una unidad de control conectada a la red de vehículo observada, que es especialmente un ordenador de control.

En caso de una diferencia en esta comparación se conmuta a un llamado control de seguridad de funcionamiento o un estado de funcionamiento seguro. Por lo tanto, en caso de una manipulación relevante en una red de vehículo, la detección de manipulaciones y la conmutación subsiguiente al control de seguridad de funcionamiento se evita que puedan producirse daños a personas o un daño de una instalación / de un vehículo. Para ello, se pueden usar funciones de seguridad de funcionamiento estándar existentes para contrarrestar un suceso relevante o limitar el daño resultante del mismo.

Una información de comparación determinada se comprueba con respecto a una información de referencia almacenada para determinar si la configuración de red real de la red de vehículo corresponde a la información de referencia. De esta manera, se detecta una manipulación en una red de vehículo.

Es esencial detectar una manipulación en la red de control de un vehículo. Se puede detectar, por ejemplo, si un aparato de red adicional se conecta a una red de vehículo, por el hecho de que el número de los componentes de red conectados es superior al valor de referencia almacenado. También se puede detectar la sustitución de un aparato de red por otro aparato de red, con la ayuda de la distinta información de identificación del componente de red. También se puede detectar un cambio de conexión del cableado.

La información de comparación o la información de referencia pueden entenderse como huella digital de referencia de la red de vehículo.

Una “huella digital” es respectivamente característica para una red de vehículo 2 individual.

Un control de vehículo realiza un control regular si la huella digital determinada de la red de control empleada para el control del vehículo coincide con una huella digital de referencia almacenada. En caso de una diferencia, el vehículo se hace funcionar de forma limitada o se desactiva, para mantenerlo en un estado de funcionamiento seguro.

Resulta ventajoso usar una red de vehículo basada en Ethernet o IP, que esté conectado sólo a componentes conocidos según un cableado fijo. Esto significa que se trata de una red cerrada con una configuración fija. Esto es válido en caso de que en una red de control de vehículo se ha realizado una detección de manipulaciones, siempre que no se haya detectada ninguna diferencia de la huella digital de la red de control de una huella digital de referencia almacenada. Según la invención, durante una comparación se puede detectar fácilmente una diferencia de esta configuración fija de la red. Resulta ventajoso adaptar el control de vehículo en caso de la aparición de una diferencia de la configuración fija depositada. De esta manera, se puede evitar un control defectuoso incluso en una red de control de vehículo manipulada intencionadamente o accidentalmente. De esta manera, se consigue el objetivo de evitar una puesta en peligro de los pasajeros.

Para la realización de una comparación entre la “huella digital” y una información de referencia, puede ser realizada por una unidad de control misma, por ejemplo, un ordenador de control en el marco de una red de vehículo. Pero, igualmente, el resultado de la comparación puede suministrarse a una unidad de control adicional. Esto puede realizarse a través de la red de control misma o a través de una línea de control separada.

Resulta ventajoso el uso de una unidad de control de programa almacenado. Con esta se puede realizar el control de instalaciones de aire acondicionado, puertas, accionamientos, frenos etc.

Especialmente para un estado de funcionamiento seguro de un vehículo pueden protegerse de forma criptográfica resultados de comparación o de prueba durante una transferencia. Esto puede realizarse por ejemplo mediante un llamado “código de autenticación de mensaje / MAC” o mediante una “firma digital”. De esta manera, esta información adquiere un estado en el que no es manipulable.

Para la detección de una manipulación, de manera ventajosa se puede recurrir a la prueba de la integridad topológica del cableado de red. Por integridad topológica se entiende que la conexión de las interfaces de red de los componentes de red conectados a la red de control del vehículo por cables de red está inalterada. Aunque es posible una comunicación de datos, en el caso de cables de red conectadas de forma incorrecta no se puede descartar por ejemplo una cesión de red en algunas conexiones de red, o una comunicación de control de red crítica en tiempo real en una conexión de red en un cable de red puede ser perturbada por otra comunicación de datos que no existiría en caso de una conexión correcta de los cables de red. Se comprueba si los aparatos están cableados de la manera habitual o si por ejemplo se han cambiado de conexión componentes o cables de red. Asimismo, se puede comprobar si se pueden localizar aparatos regulares y si determinados aparatos no esperados no pueden ser localizados realmente. Se puede comprobar si conexiones de red no ocupados no están ocupados realmente. Durante ello se puede tener en consideración que aparatos de control individuales pueden ser desconectados por un servicio técnico del vehículo. Por lo tanto, la falta de un componente durante la búsqueda de manipulaciones puede clasificarse inmediatamente como negativa, es decir, como diferencia inadmisible.

Asimismo, resulta ventajoso emplear sensores físicos para la vigilancia del cableado de red. Por ejemplo, se pueden vigilar componentes que son controlados de forma digital, es decir, sólo de forma abierta o sólo de forma cerrada.

En otra variante se recurre a parámetros de transmisión físicas para la evaluación. Para ello, se determina una respuesta de impulsos del cableado de red y se compara con un valor de referencia. Por lo tanto, se puede detectar una manipulación en forma de una sustitución de un cable de red o en forma de una manipulación física en un cable de red.

Asimismo, resulta ventajoso identificar con la ayuda de direcciones IP o direcciones MAC aparatos ajenos o aparatos de sustitución. Se identifican o se autentican los componentes conectados a la red del vehículo. Durante ello, se determina el tipo de aparato de los mismos según criterios como el fabricante, el modelo, el número de serie etc. Además, puede realizarse una autenticación criptográfica de aparatos. La autenticación de aparatos conectados se realiza por medio de una contraseña, una clave criptográfica o un certificado digital de aparato. Esta consulta puede realizarse en el marco de la detección de manipulaciones misma, o bien, una comunicación que se produce durante la autenticación de otro componente es vigilada y analizada por la detección de manipulaciones. Además, se pueden transmitir datos de prueba a través de la red de vehículo, a fin de verificar su transmisión correcta.

Por medio de una unidad de control se realiza al menos una tarea de control en función del resultado de la comprobación de la red de control. Durante ello, la funcionalidad de un aparato de control se habilita, se habilita de forma limitada o se desactiva para el funcionamiento. Por desactivación se entiende generalmente un estado de funcionamiento con seguridad propia de un vehículo. Como servicio especial se puede enviar un mensaje de habilitación a un aparato de control. De esta manera, se consigue que la instalación no cambie a un estado de funcionamiento no seguro incluso en caso de existir una manipulación de la red de control. Se puede producir un

funcionamiento limitado del vehículo, por ejemplo, a una velocidad de marcha limitada o la conducción a la vista.

Ventajas adicionales resultan del uso de un ordenador de control en caso del acoplamiento de varias redes de vehículo, para limitar la comunicación permitida en un acoplador de red / “gateway”. Generalmente, existen diferentes redes parciales de vehículo como una red de pasajeros, una red de explotador o similares que normalmente están desacopladas totalmente de una red de vehículo que es responsable del control del vehículo. En la secuencia del procedimiento para detecciones de manipulaciones pueden incorporarse cálculos en los que para la continuación del funcionamiento del vehículo deben cumplirse criterios adicionales. Por ejemplo, se puede comprobar que un acoplador de red / “Gateway” con una funcionalidad de “firewall” realmente impida una comunicación no permitida entre una red de control del vehículo y una red de explotador o red de pasajeros conectada a través del acoplador de red / “gateway”. Si no obstante es posible tal comunicación no permitida, por ejemplo, porque los cables de red hacia el acoplador de red / “gateway” están conectados incorrectamente o porque la funcionalidad de “firewall” del acoplador de red / “gateway” no funciona correctamente, se detecta un error, es decir, la detección de manipulaciones detecta una diferencia / manipulación.

Para el seguimiento de mensajes de error puede realizarse una entrada en una memoria de errores. Lo mismo se refiere a resultados positivos de una comprobación.

Además, resultan ventajas si se transmite una transmisión de datos a una unidad situada en tierra, por ejemplo, a través de “WLAN” o una red de telefonía móvil como por ejemplo “GSM”, “GPRS”, “UMTS”, “WIMAX” o similares.

El procedimiento para la detección de manipulaciones puede aplicarse en momentos diferentes y puede ser invocado periódicamente, permanentemente u opcionalmente. El procedimiento puede activarse por ejemplo en las siguientes condiciones:

- al finalizar un modo de mantenimiento para la habilitación para el funcionamiento,
- al activarse la función de control,
- al arrancar el vehículo,
- al cambiar el operario para la autenticación del nuevo operario,
- durante el funcionamiento en marcha.

Un vehículo, especialmente un vehículo ferroviario puede disponer de redes de vehículo, por ejemplo, para realizar diferentes tareas de red de vehículo o tareas de control de vehículo. Cabe mencionar:

- la red de accionamiento,
- la red de frenos,
- la red de seguridad de tren,
- la red de control de clima,
- la red de control de puertas,
- la red de información al pasajero o
- la red de videovigilancia.

La vigilancia también puede referirse a cada una de estas redes de vehículo individualmente. También es posible realizar varias tareas de red de vehículo en una red de vehículo. Por ejemplo, pueden coincidir una red de accionamiento y la red de frenos. Las distintas redes de vehículo pueden estar conectadas a través del acoplador de red / “gateway”.

En otra variante, se vigila la integridad de una red de vehículo y en caso de una diferencia se impide o se limita la comunicación de datos con una red de vehículo. Si por ejemplo se detecta que una red de explotador o una red de control por ejemplo para un control de clima o un control de iluminación difiere de la configuración de referencia conocida, porque un aparto adicional o un aparato de mantenimiento está conectado a dicha red de vehículo, un acoplador de red / “gateway” puede conectarse como sustitución a una red parcial adicional, por ejemplo, la red de control o la red de frenos del vehículo. Además, se puede limitar o impedir una comunicación de datos de la red de vehículo observada con otras redes. De esta manera, se evita que modificaciones de cualquier red del vehículo repercutan poniendo en peligro el funcionamiento fiable de otra red del vehículo.

Resulta especialmente ventajoso que una información de referencia no sólo puede estar predefinida fijamente, sino que en una variante también puede ser aprendida. Durante un mantenimiento del vehículo durante el que se recambia un aparato de control defectuoso cambia también la huella dactilar de la red de vehículo. Para que la huella dactilar de referencia no tenga que ser almacenada explícitamente por el personal operativo, al finalizar el mantenimiento o al finalizar un modo de mantenimiento de vehículo puede determinarse la huella dactilar existente actualmente de la red de vehículo y almacenarse como nueva huella dactilar de referencia. Esto puede ser realizado por un aparato de control del vehículo o por un aparato de mantenimiento conectado, por ejemplo, un ordenador portátil de mantenimiento. Durante ello, también es posible modificar la huella dactilar determinada y almacenar la

huella dactilar modificada como huella dactilar de referencia, por ejemplo, para eliminar de la huella dactilar de referencia la información relativa al ordenador portátil de mantenimiento conectado. De esta manera, durante un mantenimiento de vehículos o vehículos ferroviarios se puede registrar y almacenar si para el vehículo se habilita información de referencia para la marcha. Esto sólo es posible en este caso si a través de una interfaz de mantenimiento del vehículo ferroviario se produce un acceso a mantenimiento autorizado.

A continuación, con la ayuda de figuras esquemáticas se describen ejemplos de realización que no limitan la invención:

la figura 1 muestra un vehículo ferroviario con varias redes de vehículo 2 distintas, conectando un acoplador de red / “gateway” GW las redes de vehículo 2 con una red principal de vehículo 3,

la figura 2 muestra una variante de la figura 1, en la que el vehículo ferroviario dispone de varias redes de vehículo 2 que a través de un acoplador de red / “gateway” GW están interconectadas y, al mismo tiempo, a través del acoplador de red / “gateway” GW están acopladas a la red principal de vehículo 3,

la figura 3 muestra un plano de secuencias para la detección de manipulaciones y reacciones correspondientes.

Las figuras 1 y 2 muestran respectivamente un vehículo 1, especialmente un vehículo ferroviario, con un bus de red principal de vehículo 3 que conecta uno o varios acoplamientos eléctricos EK a través de un acoplador de red / “gateway” GW. Como está representado en la figura 1, las redes parciales de vehículo 21 a 26 de la red de vehículo 2 están interconectadas a través de un bus de red de control de vehículo 4, existiendo una conexión al acoplador de red / “gateway” GW. La red de vehículo 2 puede estar realizada especialmente como red Ethernet o red IP o como combinación de estas. En la figura 1 está representada como bus, a través del que están conectados los aparatos de control del vehículo o las redes parciales de vehículo 21 a 24 y el acoplador de red / “gateway” GW. La red de vehículo 2 o un grupo de esta igualmente pueden estar realizados como anillo o como estrella.

La figura 2 muestra una variante en la que están reunidas respectivamente tres redes de control de vehículo o tres redes parciales de control de vehículo 21 a 23 así como 25 a 26. Por lo tanto, las redes parciales de control de vehículo según la figura 2 en parte están conectadas interconectadas entre sí y en parte están interconectadas unas a otras a través del acoplador de red / “gateway” GW y están conectadas individualmente y en conjunto, a través del acoplador de red / “gateway” GW, a la red principal de vehículo 3.

Los signos de referencia de las figuras significan en concreto:

1 Vehículo
2 Redes de vehículo / VCS red de control de vehículo
3 Bus principal de vehículo
4 Bus parcial de vehículo / bus de red de control de vehículo

Redes parciales de vehículo:

21 Red de control
22 Red de frenos / aparato de control de frenos
23 Red de clima / aparato de control de clima / control HVAC
24 Red de seguridad de tren ATP
25 Red de información al pasajero PIS-S
26 Red de información al pasajero AIS-D

Figura 3:

31 Inicio
32 Determinación de la huella dactilar de una red de vehículo
33 Comparación con información de referencia
34 Decisión: manipulación sí/no
35 No
36 Sí
37 Activación de un modo de control regular
38 Activación de un modo de control de funcionamiento seguro
39 Fin

GW Acoplador de red / “gateway”
EK Acoplamiento eléctrico.

El vehículo ferroviario representado en la figura 1 contiene varios aparatos de control de vehículo que están interconectados. El aparato de control de vehículo de la red de control 21 realiza en este caso una función de guía como “Vehicle Control Server (VCS)” (servidor de control de vehículo) y puede excitar subsistemas / redes parciales de vehículo / aparatos de control de vehículo 22 a 24 individuales. Entre los subsistemas figuran en este caso:

- el aparato de control de frenos o la red de frenos 22,
- el aparto de control de clima o la red de climatización 23, HVAC, calefacción, ventilación, aire acondicionado, y
- el aparato de control de seguridad de tren o la red de seguridad de tren 24, Automatic Train Protection, ATP.

La red de control 21 del vehículo 1 se conecta a través del acoplador de red / “gateway” GW al bus de red principal de vehículo 3. Dicho bus de red principal de vehículo 3 puede ser una red Ethernet o una red IP o una combinación de estas. Una red principal existente de un tren es por ejemplo el “Ethernet Train Backbone” ETB / Ethernet / red base de tren.

En el caso de la detección de manipulación en la red de control de vehículo 2, cuando se detecta una manipulación se adapta el control de vehículo, es decir, la funcionalidad de control realizada. La detección de manipulaciones puede estar realizada en el acoplador de red / “gateway” GW o como parte del “Vehicle Control Server VCS”, es decir, de la red o el aparato de control de vehículo 21. En una variante, es parte del aparato de control de seguridad de tren 24 / “Automatic Train Protección” ATP (protección automática de tren).

Según otro ejemplo de realización, el resultado de la detección de manipulación puede transmitirse a otro vehículo a través del bus principal de vehículo 3 y un acoplamiento eléctrico EK. Existe la posibilidad de visualizar el resultado de la detección en un pupitre de mando.

La figura 2 representa una variante en la que el equipamiento del vehículo ferroviario presenta un mayor número de redes parciales de vehículo 21 a 26. Estas están unidas a través del acoplador de red / “gateway” GW.

En la figura 2 son: una red de control 21 que comprende un aparato de control de vehículo como “Vehicle Control Server” (VCS) así como un aparato de control de frenos 22 y un aparato de control de clima con una red de control de clima 23. Además, existen una red de seguridad de tren con un aparato de control de seguridad de tren 24 y una red de control de información al pasajero con dos aparatos de control de información al pasajero 25 PIS-S y 26 PIS-D.

La figura 3 muestra el esquema de secuencias para una detección de manipulaciones. Después del inicio 31 se hace funcionar la detección 32 de una llamada huella digital para una red actual. A continuación, el resultado se compara 33 con una información de referencia almacenada. Si la detección de manipulaciones 34 arroja que no existe ninguna diferencia en esta prueba, es decir que procede la ramificación izquierda con la respuesta No 35, se hace funcionar la activación 37 de un modo de control regular. Si existe una diferencia entre una información de referencia y una huella dactilar determinada de una red de vehículo, se va a la ramificación derecha con un Sí 36 y se produce la activación 38 de un modo de control de funcionamiento seguro. A continuación, este procedimiento para la detección de manipulaciones ha llegado al fin 39.

REIVINDICACIONES

1. Procedimiento para la detección de manipulaciones en al menos una red de vehículo (2) de un vehículo (1), presenta los siguientes pasos:

- la determinación de una huella digital de la al menos una red de vehículo (2),
- la comparación de la huella digital de la al menos una red de vehículo (2) con información de referencia para la detección de una manipulación,
- la adaptación del funcionamiento de la al menos una red de vehículo (2) en función del resultado de la comparación, de tal forma que queda garantizada la seguridad de funcionamiento / “safety”,
- la activación (37) de un modo de control regular, si no se ha detectado ninguna manipulación en la al menos una red de vehículo (2) o la activación (38) de un modo de control de funcionamiento seguro, si se ha detectado una manipulación en la al menos una red de vehículo (2),

2. Procedimiento según la reivindicación 1, **caracterizado por que** la adaptación de la al menos una red de vehículo (2) se realiza por medio de una unidad de control.

3. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se usan funciones de seguridad depositadas en el modo de funcionamiento seguro.

4. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** para la detección de una manipulación en la al menos una red de vehículo (2) se usa el resultado de la comparación de la información de referencia con la huella digital de la red de vehículo.

5. Procedimiento según la reivindicación 4, **caracterizado por que** un modo de control regular en una red de control de vehículo (21) se realiza sólo si la huella digital determinada de la red de control de vehículo (21) empleada para el control del vehículo (1) coincide con una información de referencia almacenada.

6. Procedimiento según la reivindicación 4, **caracterizado por que** en caso de una diferencia entre la huella digital tomada y una información de referencia, la al menos una red de vehículo (2) se hace funcionar en un modo limitado o se desactiva para mantener el vehículo en un estado de funcionamiento seguro.

7. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** una red de control de vehículo (21) es una Ethernet o una red de control de vehículo basada en IP.

8. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se usa una red de vehículo (2) cerrada con una configuración de red fija, de manera que se puede detectar fácilmente una diferencia de esta configuración fija de la red.

9. Procedimiento según la reivindicación 8, **caracterizado por que** en caso de una diferencia en la comparación entre una configuración de red de referencia fija y la huella digital de al menos una red de vehículo (2) se adapta el control de la al menos una red de vehículo (2).

10. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** en caso de que se detecta una manipulación o un vandalismo en una red de control de un vehículo, que pone en peligro una realización correcta de la funcionalidad de un control, no se inicia un funcionamiento regular del vehículo (1).

11. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se comprueba una integridad topológica del cableado de red.

12. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se emplean sensores físicos y se consultan estados bipolares de elementos de conmutación.

13. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se evalúan parámetros de transmisión físicos y se comparan con valores de referencia.

14. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se detectan aparatos ajenos existentes en la red de vehículo.

15. Procedimiento según la reivindicación 14, en el que el identificador de un aparato está protegido por medio de una clave criptográfica.

16. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** una información de referencia puede ser aprendida.

17. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** una detección de manipulaciones se realiza permanentemente o en momentos seleccionados o eventos seleccionados o estados de funcionamiento seleccionados.

18. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se realiza una vigilancia en redes parciales de vehículo (21 a 26) individuales.

19.Unidad de control para la detección de manipulaciones en al menos una red de vehículo (2) de un vehículo (1), **caracterizado por que** una realización de tareas de control se realiza en función del resultado de una comparación de una huella digital determinada previamente de al menos una red de vehículo (2) con informaciones de referencia de una red de control (21) se realiza de tal forma que queda garantizada la seguridad de funcionamiento / “safety”, activándose un modo de control regular si no se detecta ninguna manipulación en la al menos una red de vehículo (2) o activándose un modo de control de funcionamiento seguro si se ha detectado una manipulación en al menos una red de vehículo (2).

20. Unidad de control según la reivindicación 19, **caracterizado por que** la unidad de control está concebida de tal forma que se puede realizar una autoprueba.

21. Unidad de control según una de las reivindicaciones 19 a 20, **caracterizado por que** la unidad de control puede liberar, habilitar de forma limitada o desactivar al menos un aparato de control para el funcionamiento regular.

22. Unidad de control según una de las reivindicaciones 19 a 21, **caracterizado por que** la unidad de control comprende un ordenador de control que limita una comunicación admisible a través de un acoplador de red / “Gateway” (GW), para el acoplamiento de varias redes de vehículo (2).

23. Unidad de control según una de las reivindicaciones 19 a 22, **caracterizado por que** un mensaje de alama que indica una detección de manipulación puede desactivarse y se puede iniciar un funcionamiento regular.

24. Unidad de control según una de las reivindicaciones 19 a 23, **caracterizado por que** existe una memoria de errores para el almacenamiento de resultados de prueba.

25. Unidad de control según una de las reivindicaciones 19 a 24, **caracterizado por que** una comunicación de datos para la detección de manipulaciones puede transmitirse a una unidad situada en tierra, a través de una red de telefonía móvil estándar.

26. Unidad de control según una de las reivindicaciones 19 a 25, **caracterizado por que** existen varias redes de vehículo (2) o redes parciales de vehículo (21 a 26) que están conectadas a través de un acoplador de red / “gateway” (GW).

FIG 1

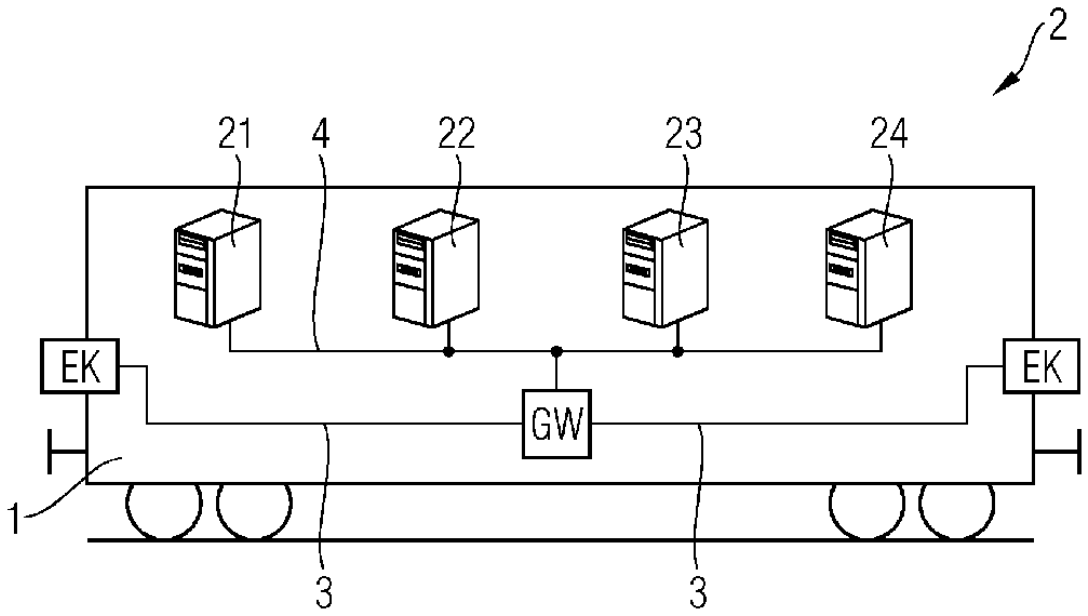

FIG 2

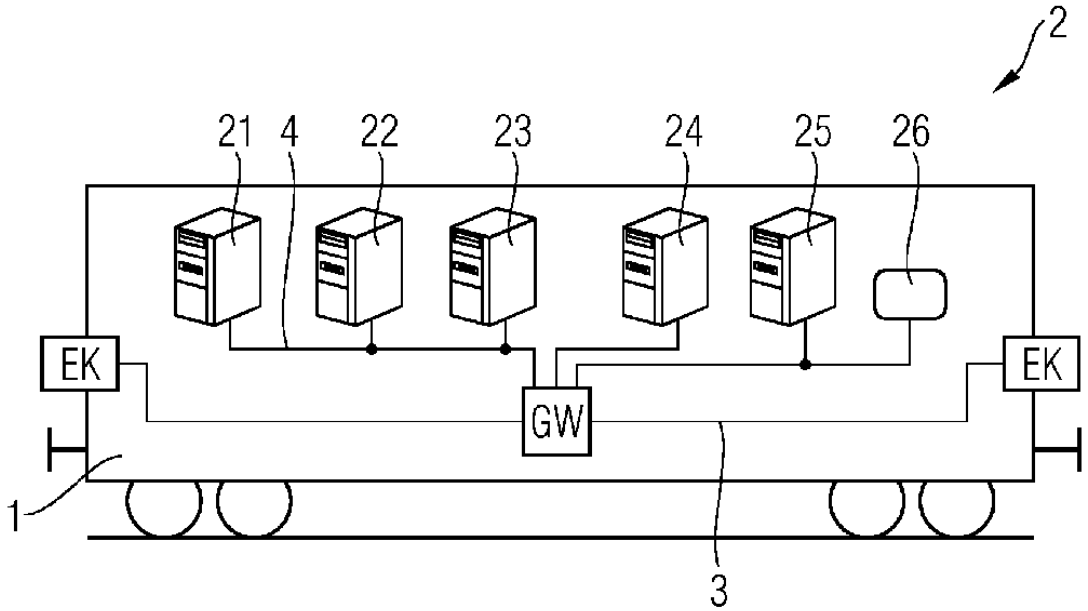

FIG 3