

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 923 182**

51 Int. Cl.:

B61L 19/06 (2006.01)

B61L 21/06 (2006.01)

B61L 27/00 (2012.01)

B61L 25/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA MODIFICADA
TRAS OPOSICIÓN

T5

96 Fecha de presentación y número de la solicitud europea: **12.06.2018 E 18177217 (9)**

97 Fecha y número de publicación de la concesión europea modificada tras oposición: **12.02.2025 EP 3549842**

54 Título: **Sistema de control de tráfico de tren y método para visualizar con seguridad una indicación de estado de un sistema de control de rutas y trenes**

30 Prioridad:

06.04.2018 DE 102018205235

06.04.2018 EP 18166202

45 Fecha de publicación y mención en BOPI de la traducción de la patente modificada:
17.06.2025

73 Titular/es:

HITACHI RAIL GTS DEUTSCHLAND GMBH
(100.00%)

Thalesplatz 1
71254 Ditzingen, DE

72 Inventor/es:

SCHÄFER, MICHAEL y
TIPLÉ, ABHAY

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 923 182 T5

DESCRIPCIÓN

Sistema de control de tráfico de tren y método para visualizar con seguridad una indicación de estado de un sistema de control de rutas y trenes

5

Antecedentes de la invención

La invención se refiere a un sistema de control de tráfico de trenes que comprende un sistema de control de rutas y trenes, una estación de trabajo de operador con una pantalla y un componente de indicación de estado seguro con nivel de seguridad SIL>0, en particular SIL4, para indicar información relacionada con la seguridad concerniente al estado de elementos del sistema de control de rutas y trenes en la pantalla de la estación de trabajo de operador. La invención se refiere además a un método para visualizar con seguridad una indicación de estado de un sistema de control de rutas y trenes.

10

15 Un sistema de control de tráfico de trenes acorde se conoce a partir de [1].

Los sistemas de control de rutas y trenes están adaptados para gestionar de forma segura las rutas y las autoridades de movimiento en las redes ferroviarias para los trenes en circulación y para controlar, proteger y proteger los trenes para que no avancen demasiado rápido o más allá de su límite de autoridad de movimiento. Los sistemas típicos de control de rutas y trenes son, por ejemplo, sistemas de enclavamiento, centros de bloqueo de radio o sistemas similares.

20

El control remoto para controlar sistemas de enclavamiento y otros sistemas de control de rutas y trenes a través de sistemas de gestión de tráfico es cada vez más importante. Los sistemas de gestión de tráfico comprenden interfaces hombre-máquina para operar sistemas de control de rutas y trenes por un operador humano. El sistema de control de rutas y trenes recibe comandos del sistema de gestión de tráfico concerniente a la operación regular, así como concerniente a las operaciones críticas para la seguridad. Las operaciones críticas para la seguridad se llevan a cabo utilizando el sistema de control de rutas y trenes en situaciones operativas especiales o en caso de perturbaciones. A diferencia de las operaciones regulares cuya admisibilidad se puede comprobar en cualquier momento por el sistema de control de rutas y trenes, las operaciones críticas para la seguridad se instruyen por el operador al tiempo que pasa por alto elementos del sistema de control de rutas y trenes (por ejemplo, el centro de bloqueo de radio o el sistema de enclavamiento). Es decir, las operaciones críticas para la seguridad son acciones del operador, por ejemplo, despeje de ruta crítica de seguridad, cambio de punto crítico de seguridad, etc. con los que el operador puede eludir una configuración segura del sistema.

25

30

35

Para controlar operaciones críticas para la seguridad, se tienen que cumplir requisitos de alta seguridad. En algunos casos, los clientes requieren no solo una operación crítica para la seguridad de un sistema de control de rutas y trenes, sino también una indicación de estado seguro de los estados del sistema de control de rutas y trenes, por ejemplo, en el caso de operaciones críticas para la seguridad que pasa por alto el sistema de enclavamiento, tales como "schriftlicher Befehl" y el funcionamiento de una "Ersatzsignal". "Schriftlicher Befehl" es una orden del operador para pasar por alto un sistema de control de rutas y trenes manualmente, que se tiene que entregar al personal del tren o registrar de forma escrita en caso de, por ejemplo, un fallo operativo. "Ersatzsignal" es una señal adicional que reemplaza la orden de pasar una señal de alto. Ejecutando tales operaciones críticas para la seguridad, el operador puede eludir una configuración segura del sistema. La base para la decisión del operador de si ejecutar tal operación crítica para la seguridad es el estado del sistema de control de rutas y trenes indicado en la pantalla de la estación de trabajo de operador. Por lo tanto, es un requisito esencial que el estado del sistema de control de rutas y trenes se muestre correctamente. Según las estaciones de trabajo del operador, que cumplen con el nivel de integridad de seguridad requerido (típicamente SIL2, a veces incluso SIL4), se han desarrollado [1], [2], [3].

40

45

50

Los clientes ahora requieren cada vez más la integración de funcionalidades adicionales no relacionadas con la seguridad o funciones SIL0 en las estaciones de trabajo del operador [4]. Sin embargo, esto da como resultado grandes esfuerzos, porque se debe garantizar que los componentes de SIL0 no sean intrusivos ("ruckwirkungsfrei") para el entorno SIL>0 de la estación de trabajo de operador. Sin embargo, esto da como resultado altos costes de hardware para este ordenador dedicado y también altos costes de desarrollo, integración y prueba de software, porque todos estos componentes tienen que ser desarrollados según un alto nivel de integridad de seguridad (típicamente SIL4) según la norma EN 50128 [5].

55

Las soluciones existentes ofrecen poca flexibilidad y no cumplen con los requisitos del cliente. En particular, los clientes solicitan interfaces de usuario basadas en web de operación flexible. Los usuarios deberían tener la posibilidad no solo de operar el RTCS desde la estación de trabajo de operador central, sino también desde dispositivos móviles. Una interfaz de usuario basada en web es una solución adaptable que proporciona la flexibilidad necesaria.

60

65

En [2] se describe un método para la transmisión segura de datos. En [3] se describe un método para verificar

la transferencia correcta de datos.

El documento EP 3 040 862 A1 describe un sistema de control de tráfico de trenes que comprende: un sistema de control de rutas y trenes, una estación de trabajo de operador con una pantalla, en donde la estación de trabajo de operador comprende al menos un componente de indicación de integridad básica, con un nivel de seguridad SIL0 para indicar información con una integridad básica en la pantalla, en donde la estación de trabajo de operador está adaptada para generar datos gráficos de información con integridad básica, componente de indicación de estado seguro con nivel de seguridad SIL>0 configurado para transformar datos de estado concernientes al estado de elementos del sistema de control de rutas y trenes en datos gráficos y, por lo tanto, generar datos de indicación que indican información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de rutas y trenes en la pantalla de la estación de trabajo de operador, en donde el componente de indicación de integridad básica y el componente de indicación de estado seguro son componentes de software, en donde el componente de indicación de estado seguro está funcionalmente separado del componente de indicación de integridad básica, el canal seguro que conecta el componente de indicación de estado seguro y la pantalla para la transmisión segura de información relacionada con la seguridad sobre el estado de los elementos del sistema de control de trenes de ruta.

Objeto de la invención

Es un objeto de la invención sugerir un sistema de control de tráfico de trenes, que por un lado realiza el alto nivel de seguridad requerido para la indicación de estado seguro y por otro lado permite una considerable reducción de costes y flexibilidad.

Descripción de la invención

Este objeto se resuelve mediante un sistema de control de tráfico de trenes según la reivindicación 1 y un método según la reivindicación 9.

Según la invención, la estación de trabajo de operador comprende al menos un componente de indicación de integridad básica con nivel de seguridad SIL0 para indicar información con una integridad básica en la pantalla. Se proporciona un servidor de indicación que comprende un componente de indicación de estado seguro con nivel de seguridad SIL>0, en particular SIL4, para mostrar información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de rutas y trenes en la pantalla de la estación de trabajo de operador, en donde el componente de indicación de estado seguro es funcionalmente independiente de la estación de trabajo de operador. Además, se proporciona un canal seguro que conecta el servidor de indicación de estado seguro y la pantalla para la transmisión segura de información relacionada con la seguridad sobre el estado de los elementos del sistema de control de trenes de ruta.

Los componentes de indicación de integridad básica y el componente de indicación de estado seguro son componentes de software, es decir, bloques de software de construcción encapsulada.

El componente de indicación de integridad básica indica cualquier tipo de información con integridad básica, tal como el retraso de un tren o las condiciones climáticas, de un sistema de control de tráfico de trenes en una pantalla para informar a un operador sobre las condiciones respectivas del sistema de control de tráfico de trenes, el sistema de control de rutas y trenes controlados y sus elementos con un nivel de integridad de seguridad SIL0. Los elementos del sistema de control de rutas y trenes pueden ser, por ejemplo, elementos de campo (puntos, señales, sistemas de detección de vías libres, pasos a nivel, etc.), elementos lógicos (rutas, autoridades de movimiento, sistemas de bloqueo de líneas, etc.), elementos relacionados con el tren (parámetros del tren como velocidad o longitud de un tren, etc.) o elementos relacionados con el área (zonas para restricciones temporales de velocidad, áreas de trabajo del personal de mantenimiento, áreas de responsabilidad de un operador específico, etc.).

El componente de indicación de estado seguro genera datos gráficos (datos de indicación) con el fin de indicar estados relacionados con la seguridad del sistema de control de tráfico de trenes, la ruta controlada y el sistema de control de trenes y sus elementos con un nivel de integridad de seguridad SIL>0, en particular SIL4 para informar a un operador de forma fiable sobre estos estados. Las operaciones relacionadas con la seguridad se pueden ejecutar en base a estas indicaciones.

Según la invención, el componente de indicación de integridad básica está integrado en la estación de trabajo de operador, mientras que el componente de indicación de estado seguro es funcionalmente independiente de la estación de trabajo de operador. En otras palabras, la función para generar datos de indicación de información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de trenes de ruta (datos de estado) se externaliza desde la estación de trabajo de operador, es decir, el componente de indicación de estado seguro está funcionalmente separado del componente de indicación de integridad básica y puede (pero no tiene que) instalarse en ubicaciones separadas. Por tanto, la no intrusión de los componentes de indicación de integridad básica SIL0 en el componente de indicación de estado seguro

se puede garantizar más fácilmente. Dado que la estación de trabajo de operador comprende solo componentes de baja seguridad, la estación de trabajo del operador se puede diseñar con integridad básica (en particular SIL0), que es mucho más económica en comparación con la estación de trabajo de operador de alta seguridad conocida en el estado de la técnica. Por tanto, el sistema de control de tráfico inventivo permite una indicación segura de los estados de los elementos del sistema de control de rutas y trenes en la pantalla de la estación de trabajo de operador a bajo coste.

La transmisión de información relacionada con la seguridad sobre el estado de los elementos del sistema de control de trenes de ruta entre el componente de indicación de estado seguro y la pantalla se realiza proporcionando un canal seguro (canal de comunicación entre el servidor de indicación y la pantalla) que transmite datos de indicación gráfica a la pantalla y la información de suma de comprobación al componente de indicación de estado seguro. Los procedimientos para garantizar comunicaciones seguras a través de este canal se implementan según las normas pertinentes (por ejemplo, EN 50159) y el nivel de integridad de seguridad requerido.

En la pantalla de la estación de trabajo de operador, se muestra al operador tanto información con integridad básica como información relacionada con la seguridad, en particular, la indicación de estado seguro del sistema de control de rutas y trenes.

Según la invención, el componente de indicación de estado seguro está integrado en el sistema de control de rutas y trenes, es decir, en un subcentro del sistema de control de tráfico de trenes. En este caso no se requiere ningún ordenador adicional, lo que hace que esta realización sea rentable. Sin embargo, se tiene que integrar una función adicional en todos los sistemas de control de rutas y trenes, que han de ser controlados por el sistema de control de tráfico de trenes.

El componente de indicación de estado seguro se puede integrar en un servidor de indicación. El servidor de indicaciones puede ser parte del sistema de control de rutas y trenes. Esto es, en particular, ventajoso en caso de que no exista un Centro de Control general y solo se tenga que controlar un (pequeño) sistema de control de rutas y trenes.

En una realización alternativa, el sistema comprende un centro de control, en donde el servidor de indicaciones está integrado en el centro de control. Esta realización es ventajosa en los casos en los que se deba controlar el sistema de control de rutas y trenes existente (por ejemplo, de diferentes proveedores), dado que no se tienen que integrar funciones adicionales en el sistema de control de rutas y trenes. Los centros de control son conocidos, por ejemplo, de DB "Betriebszentrale" o "Steuerzentrale" respectivamente y manejan las tareas de control, seguridad y disposición de las operaciones ferroviarias.

En una realización alternativa adicional, el servidor de indicaciones está integrado en un centro de cálculo remoto (remoto de la pantalla). Esto permite el uso de clientes ligeros para la estación de trabajo de operador (para reducir la cantidad de energía necesaria, el ruido y el espacio en el centro de control). El centro de cálculo remoto puede ser parte del centro de control.

Preferiblemente, el servidor de indicaciones está protegido por procedimientos, es decir, el nivel de integridad de seguridad necesario se logra mediante un procedimiento que, por un lado, integra al usuario humano (operador) y, por otro lado, está controlado por un componente del sistema de control de rutas y trenes. Un ordenador industrial común se puede utilizar como servidor de indicaciones.

Alternativamente, el servidor de indicaciones puede ser un servidor compuesto de seguridad contra fallos. Es decir, el servidor de indicaciones es un servidor multicanal que tiene una arquitectura 2002 o 2003. El nivel de seguridad SIL4 se puede lograr con esta realización.

Preferiblemente, la estación de trabajo de operador está integrada en un sistema de gestión de tráfico. El sistema de gestión de tráfico puede comprender funciones adicionales para gestionar la operación del tren, por ejemplo, detección de retrasos, detección de conflictos de ocupación de trenes, resolución (automática) de conflictos, gestión de recursos tales como el personal del área de mantenimiento a lo largo de la ruta, integración de telecomunicaciones y video vigilancia. Integrando la estación de trabajo de operador en un sistema de gestión de tráfico, solo se requiere un conjunto de dispositivos de entrada (ratón, teclado, etc.) para controlar el tráfico de tren. Por lo tanto, un operador es capaz de gestionar la operación del tren de nivel superior así como realizar las operaciones críticas de seguridad que requieren la indicación segura.

En una realización altamente preferida, el canal seguro se enruta a través de la estación de trabajo de operador. En este caso, no se requiere ningún ordenador adicional para la transmisión de la información relacionada con la seguridad. Mientras que, según el estado de la técnica, los datos de estado se transmiten y procesan en la estación de trabajo, lo que conduce a una integridad de seguridad general SIL>0 para la estación de trabajo en sí misma, la presente invención utiliza la estación de trabajo solo como un "canal gris" que está asegurado por un procedimiento que no conduce a necesidades de integridad de seguridad adicionales para la estación de

trabajo en sí misma. Esto reduce los costes de desarrollo.

En una realización altamente preferida, el componente de indicación de estado seguro está adaptado para calcular una primera suma de comprobación de los datos de indicación generados por el componente de indicación de estado seguro y está adaptado además para llevar a cabo una comparación de suma de comprobación y/o una comparación de píxeles de datos de mapa de píxeles.

El componente de indicación de estado seguro está adaptado preferiblemente para descargar un componente vuelto a leer desde un navegador de la estación de trabajo de operador.

La invención también se refiere a un método para mostrar de forma segura información relacionada con la seguridad concerniente a la indicación de estado de un sistema de control de rutas y trenes en una estación de trabajo de operador de un sistema de control de tráfico de trenes como se describió anteriormente, que tiene los pasos de la reivindicación 9.

La información relacionada con la seguridad se transmite desde el sistema de control de rutas y trenes al servidor de indicaciones. El servidor de indicaciones genera datos gráficos (datos de indicación) a partir de la información relacionada con la seguridad, que luego se envían a la pantalla de la estación de trabajo de operador a través del canal seguro.

Sin embargo, los datos gráficos de información con integridad básica se generan dentro de la estación de trabajo de operador. Los datos gráficos de información con integridad básica luego se transmiten dentro de la estación de trabajo de operador a la pantalla.

En una variante altamente preferida, el canal seguro se enruta a través de la estación de trabajo de operador. En este caso, el canal seguro es al menos parcialmente parte de la estación de trabajo de operador.

Preferiblemente, los datos de estado se transforman en datos de indicación de mapa de píxeles y los datos de indicación de mapa de píxeles se transmiten a la pantalla usando un método para verificar la transferencia correcta de datos de mapa de píxeles. El método para verificar la transferencia correcta de datos de mapa de píxeles comprende preferiblemente:

a) modificar al menos una propiedad de un número fijo de píxeles seleccionados a partir de los datos de indicación del mapa de píxeles en una primera memoria, la selección que se realiza de forma aleatoria,

b) transferir los datos de indicación de mapa de píxeles que comprenden los píxeles modificados desde la primera memoria a una segunda memoria,

c) volver a leer los píxeles modificados de la segunda memoria, y

d) comparar los píxeles modificados vueltos a leer con los píxeles modificados de la primera memoria para verificar la transferencia correcta de los datos de indicación del mapa de píxeles, en donde la al menos una propiedad se modifica de tal manera que la modificación no es observable cuando se muestran los píxeles modificados en la pantalla gráfica. Un método correspondiente se describe en [3].

En una variante altamente preferida, los datos de indicación generados por el componente de estado seguro se muestran en un navegador web de la estación de trabajo de operador para proporcionar la flexibilidad necesaria.

Con el fin de verificar que la visualización de los datos de indicación en el navegador es realmente lo que se pretendía mostrar, una variante preferida prevé que los datos de indicación mostrados se vuelvan a leer, en particular mediante la generación de datos de mapa de píxeles.

En una variante altamente preferida, el componente de indicación de estado seguro genera una primera suma de comprobación de los datos de indicación, el navegador genera una segunda suma de comprobación de los datos vueltos a leer y transmite la segunda suma de comprobación al componente de indicación de estado seguro a través del canal seguro, y el componente de indicación de estado seguro compara la primera suma de comprobación y la segunda suma de comprobación. Por tanto, se puede comprobar si la transmisión de los datos de indicación al navegador y la visualización de los datos de indicación transmitidos ha sido correcta. Según esta realización, la comparación de la suma de comprobación se lleva a cabo de forma remota desde la estación de trabajo de operador para separar la comparación relacionada con la seguridad de la estación de trabajo de operador de SIL0.

Alternativamente o además, el navegador transmite los datos vueltos a leer al componente de indicación de estado seguro a través del canal seguro y el componente de indicación de estado seguro compara los datos vueltos a leer con los datos de indicación (comparación de píxeles).

Para evitar una comparación de errores de falsos positivos, se utilizan algoritmos que comprueban solo unos pocos píxeles (por ejemplo, según [3]) o algoritmos de comparación morfológica (por ejemplo, según [6]).

La presente invención realiza una indicación gráfica segura basada en procedimientos de un estado del sistema de control de rutas y trenes en un sistema de gestión de tráfico SIL0. Por tanto, los sistemas de control de rutas y trenes relacionados con la seguridad, por ejemplo, enclavamientos, los sistemas de señalización se pueden controlar desde los sistemas de gestión de tráfico SIL0.

El sistema de control de tráfico inventivo permite la ejecución de operaciones críticas para la seguridad en un sistema crítico para la seguridad con un coste reducido, en particular la ejecución de operaciones críticas para la seguridad que requieren una visualización segura del estado del sistema de control de rutas y trenes, por ejemplo, porque se pasa por alto el sistema de control de rutas y trenes ejecutando la respectiva operación crítica de seguridad.

Se pueden extraer ventajas adicionales de la descripción y el dibujo adjunto. Las realizaciones mencionadas no se han de entender como una enumeración exhaustiva sino más bien que tienen carácter ejemplar para la descripción de la invención.

Dibujos

La invención se muestra en el dibujo.

Fig. 1 muestra la arquitectura de un sistema de control de tráfico según el estado de la técnica.

Fig. 2 muestra la arquitectura de un sistema de control de tráfico que no pertenece a la invención con un servidor de indicaciones integrado en un centro de control.

Fig. 3 muestra la arquitectura de un sistema de control de tráfico según la invención con un servidor de indicaciones integrado en el sistema de control de rutas y trenes.

Fig. 4 muestra la arquitectura de un sistema de control de tráfico según la invención, en donde un componente de indicación de estado seguro está integrado en el sistema de control de rutas y trenes sin servidor de indicaciones.

Fig. 5 muestra la arquitectura de un sistema de control de tráfico que no pertenece a la invención con un servidor de indicaciones integrado en un centro de cálculo remoto.

Fig. 6 muestra la arquitectura de un sistema de control de tráfico que no pertenece a la invención con un componente de integración de estado seguro adaptado para revelar errores en la transmisión y/o visualización de los datos de indicación y una estación de trabajo de operador basada en web.

La Fig. 1 muestra una arquitectura de un sistema de control de tráfico según el estado de la técnica. El sistema de control de tráfico comprende un sistema de control de rutas y trenes RTCS y una estación de trabajo de operador OW' con una pantalla D. La estación de trabajo de operador OW' comprende componentes de indicación de integridad básica BIC con nivel de seguridad SIL0 para la indicación de información en la pantalla D con una integridad básica (datos de gestión del tráfico ferroviario). La estación de trabajo de operador OW' comprende además un componente de indicación de estado seguro SSC con nivel de seguridad SIL>0 para el procesamiento de datos de estado (información relevante para la seguridad concerniente a estados de elementos del sistema de control de rutas y trenes RTCS). Los datos de estado se transmiten desde el sistema de control de rutas y trenes RTCS al componente de indicación de estado seguro SSC de la estación de trabajo de operador OW'. El componente de indicación de estado seguro SSC transforma los datos de estado en datos gráficos y, por tanto, genera datos de indicación, que luego se muestran en la pantalla D.

Según la invención, el sistema de control de tráfico comprende una estación de trabajo de operador OW que no involucra ningún componente con nivel de seguridad SIL>0, es decir, la estación de trabajo de operador solo comprende componentes con nivel de seguridad SIL0 o menos, tales como los componentes de indicación de integridad básica BIC. Dado que el componente de indicación de estado seguro SSC se intercambia fuera de la estación de trabajo de operador OW y es funcionalmente independiente de la estación de trabajo de operador OW, es decir, se implementa de una manera diferente, se puede asegurar la no intrusión de la estación de trabajo de operador SIL=0 al componente de indicación de estado seguro SSC SIL>0.

La información con integridad básica se transmite desde el sistema de control de rutas y trenes RTCS a la estación de trabajo de operador OW a través del canal C1. Sin embargo, la información relevante para la seguridad (datos de estado) se transmite al componente de indicación de estado seguro SSC a través de un canal C2 separado con el fin de generar los datos de indicación gráfica correspondientes. El canal de transmisión C2 es un canal seguro, por ejemplo, asegurado por medio de una pasarela de seguridad con el fin de evitar la manipulación de

los datos de estado. Los datos de indicación se transfieren desde el componente de indicación de estado seguro SSC a la pantalla D de la estación de trabajo de operador. Con el fin de evitar la falsificación de los datos de indicación debido al mal funcionamiento del hardware o software, la transferencia de datos se lleva a cabo a través de un canal seguro C3.

El componente de indicación de estado seguro SSC se puede o bien ejecutar por un servidor de indicación IS como se muestra en la Fig. 2, Fig. 3 y Fig. 5 (es decir, se proporciona un ordenador adicional para ejecutar el componente de indicación de estado seguro SSC) o mediante una partición segura de un ordenador ya existente del sistema de control de tráfico, como se muestra en Fig. 4.

En una realización que no pertenece a la presente invención, mostrada en Fig. 2, el componente de indicación de estado seguro SSC está integrado en un centro de control CC junto con la estación de trabajo de operador OW. La no intrusión entre la estación de trabajo de operador OW y el componente de indicación de estado seguro SSC se asegura proporcionando un ordenador separado (servidor de indicación IS) para ejecutar el componente de indicación de estado seguro SSC.

En lugar de integrar el componente de indicación de estado seguro SSC en el centro de control CC, también es posible integrar el componente de indicación de estado seguro SSC en el sistema de control de rutas y trenes RTCS, o bien ejecutable por el servidor de indicación (Fig. 3) o por un ordenador existente del RTCS en sí mismo (Fig. 4). Si varios sistemas de control de rutas y trenes RTCS se operan por el sistema de control de tráfico, cada uno de los sistemas de control de rutas y trenes RTCS tiene que ser equipado con un componente de indicación de estado seguro SCC correspondiente.

En un ejemplo, no perteneciente a la presente invención, que se muestra en Fig. 5, el servidor de indicación IS con el componente de indicación de estado seguro SSC está integrado en un centro de cálculo RZ, que se puede ubicar remoto de la estación de trabajo de operador OW.

La Fig. 6 muestra la arquitectura de un sistema de control de tráfico, que no pertenece a la presente invención, que utiliza una estación de trabajo de operador basada en la web. La estación de trabajo de operador comprende un navegador B y un componente vuelto a leer R. El componente de indicación de estado seguro SSC está adaptado para descargar el componente vuelto a leer R desde la estación de trabajo de operador OW. Ejecutando el componente vuelto a leer R, los datos de indicación mostrados se vuelven a leer (datos vueltos a leer) y se transmiten al componente de indicación de estado seguro SSC.

Los pasos a continuación describen la realización de una variante altamente preferida del método inventivo por medio del sistema de control de tráfico mostrado en la Fig. 6. Los pasos del método correspondientes se ejecutan preferiblemente cada vez que el operador usa el navegador para ejecutar comandos críticos para la seguridad. Los comandos críticos para la seguridad también se podrían ejecutar explícitamente bajo demanda a través de un mecanismo de interacción de usuario dedicado (botón, botón desplegable, etc.). Los pasos del método preferido son de la siguiente manera:

1. El componente de indicación de estado seguro tiene la funcionalidad de convertir los datos de estado en datos de indicación gráfica. El componente de indicación de estado seguro envía estos datos de indicación a través del canal seguro al navegador de la estación de trabajo de operador. El navegador muestra estos datos de indicación en la pantalla. Los datos mostrados se vuelven a leer y el navegador calcula una primera suma de comprobación de los datos vueltos a leer.

2. Los datos vueltos a leer (datos de mapa de píxeles) junto con la primera suma de comprobación se envían al componente de indicación de estado seguro a través del canal seguro.

3. El componente de indicación de estado seguro luego compara la primera suma de comprobación generada por el navegador con una segunda suma de comprobación calculada por el componente de indicación de estado seguro. La segunda suma de comprobación es la suma de comprobación de los datos de indicación generados por el componente de indicación de estado seguro. Por lo tanto, se verifica que los datos de indicación enviados al navegador y los datos de mapa de píxeles vueltos a leer resultantes enviados desde el navegador a través del canal seguro no se corrompieron de ninguna manera en el camino.

4. Luego, el componente de indicación de estado seguro realiza una comparación de suma de comprobación y (si es aplicable, en particular si la comparación de suma de comprobación es exitosa) una comparación de píxeles entre los datos vueltos a leer enviados por el navegador y los datos de indicación que el componente de indicación de estado seguro en sí mismo generó en base a los datos de estado. Si la comparación es exitosa, envía una notificación de éxito a la estación de trabajo de operador a través del canal seguro. Si no es así, enviará una notificación de fallo.

5. Según la respuesta del componente de indicación de estado seguro, el comando crítico que se inició por

el operador o bien continuará o bien terminará.

La solución inventiva se basa en la idea de externalizar el componente de indicación de estado seguro SSC SIL>0 de la estación de trabajo de operador OW y configurar un canal seguro C3 (por ejemplo, mediante la aplicación de protocolos de escritorio remoto) mejorado con medidas de seguridad, en particular según la norma EN50159. Este canal seguro C3 se enruta preferentemente a través de la estación de trabajo de operador OW en donde se utiliza un método para verificar la transferencia de datos correcta. Por tanto, la invención realiza una indicación gráfica segura de los estados de los elementos del sistema de control ferroviario (por ejemplo, enclavamiento, RBC,...) en una estación de trabajo de operador OW, en particular dentro de un sistema de gestión de tráfico TMS que proporciona (solo) un entorno SIL0.

Documentos citados

[1] EP 0 443 377 A2 (Lorenz)

[2] EP 2 683 589 B1 (Siemens)

[3] EP 2 244 188 A1 (Thales)

[4] Antweiler: "Bahn-Betriebsleitsystem ILTIS" Signal & Draht, 87 (1995) 10, Páginas 337 - 340

[5] EN 50128 "Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme" Edición: 2012-03

[6] Mantere, Timo: "Electronic Imaging & Signal Processing – Image comparison base on morphological transforms " 29 de noviembre de 2007, SPIE Newsroom. DOI: 10.1117/2.1200711.0926

Lista de signos de referencia

BIC	componente de indicación de integridad básica
C1	canal de transmisión de información con integridad básica
C2	canal de transmisión de información relevante para la seguridad (datos de estado)
C3	canal de transmisión seguro para datos de indicación gráfica
CC	centro de control
D	pantalla
ES	servidor de indicaciones
OW	estación de trabajo de operador
RTCS	sistema de control de rutas y trenes
RZ	centro de cálculo
SSC	componente de indicación de estado seguro
TMS	sistema de gestión de tráfico

REIVINDICACIONES

1. Sistema de control de tráfico de trenes que comprende

- 5 un sistema de control de rutas y trenes (RTCS),

una estación de trabajo de operador (OW) con una pantalla (D), en donde la estación de trabajo de operador (OW) comprende al menos un componente de indicación de integridad básica (BIC) con nivel de seguridad SIL0 para indicar información con una integridad básica en la pantalla (D), en donde la
10 estación de trabajo de operador está adaptada para generar datos gráficos de información con integridad básica, y en donde la estación de trabajo de operador (OW) comprende solo componentes con nivel de seguridad SIL0 o menos, y

un componente de indicación de estado seguro (SSC) con nivel de seguridad SIL>0, en particular SIL4, configurado para transformar los datos de estado concernientes al estado de los elementos del sistema de control de rutas y trenes (RTCS) en datos gráficos y, por lo tanto, generar datos de indicación que indiquen información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de rutas y trenes (RTCS) en la pantalla de la estación de trabajo de operador (OW),
15

en donde el componente de indicación de integridad básica y el componente de indicación de estado seguro son componentes de software, esto es, bloques de software de construcción encapsulada,

en donde se proporciona un canal (C1) que conecta el sistema de control de rutas y trenes (RTCS) y la estación de trabajo de operador (OW), para transmitir información con integridad básica desde el sistema de control de rutas y trenes (RTCS) hasta la estación de trabajo de operador (OW),
20

en donde el componente de indicación de estado seguro (SSC) es funcionalmente independiente de la estación de trabajo de operador (OW), y el componente de indicación de estado seguro (SSC) está funcionalmente separado del componente de indicación de integridad básica (BIC), en donde la función para generar datos de indicación de la información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de trenes de ruta se externaliza de la estación de trabajo de operador, y
25

además del canal (C1), un canal seguro (C3) que conecta el componente de indicación de estado seguro (SSC) y la pantalla (D) para la transmisión segura de información relacionada con la seguridad sobre el estado de los elementos del sistema de control de trenes de ruta (RTCS),

en donde el componente de indicación de estado seguro (SSC) está integrado en el sistema de control de rutas y trenes (RTCS).
30
35
40
2. Sistema de control de tráfico de trenes según la reivindicación 1 caracterizado por que el componente de indicación de estado seguro (SSC) está integrado en un servidor de indicación (IS).
3. Sistema de control de tráfico de trenes según la reivindicación 2 caracterizado por que el sistema comprende un centro de control (CC), en donde el servidor de indicaciones (IS) está integrado en el centro de control.
4. Sistema de control de tráfico de trenes según la reivindicación 2 o 3 caracterizado por que el servidor de indicaciones (IS) está integrado en un centro de cálculo remoto (RZ).
5. Sistema de control de tráfico de trenes según cualquiera de las reivindicaciones 2 a 4, caracterizado por que el servidor de indicaciones (IS) está protegido por procedimientos.
6. Sistema de control de tráfico de trenes según cualquiera de las reivindicaciones 2 a 4, caracterizado por que el servidor de indicaciones (IS) es un servidor compuesto de seguridad contra fallos.
7. Sistema de control de tráfico de trenes según una de las reivindicaciones anteriores, caracterizado por que la estación de trabajo de operador (OW) está integrada en un sistema de gestión de tráfico (TMS).
8. Sistema de control de tráfico de trenes según una de las reivindicaciones anteriores, caracterizado por que el canal seguro (C3) se enruta a través de la estación de trabajo de operador (OW).
9. Método para la visualización segura de información relacionada con la seguridad concerniente al estado de un sistema de control de rutas y trenes (RTCS) en una estación de trabajo de operador (OW) de un sistema de control de tráfico de trenes que comprende un sistema de control de rutas y trenes (RTCS), una estación de trabajo de operador (OW) con una pantalla (D), en donde la estación de trabajo de operador (OW) comprende al menos un componente de indicación de integridad básica (BIC) con nivel de seguridad SIL0 para indicar
60
65

información con una integridad básica en la pantalla (D), en donde la estación de trabajo de operador está adaptada generar datos gráficos de información con integridad básica; y en donde la estación de trabajo de operador (OW) comprende solo componentes con nivel de seguridad SIL0 o menos, y un componente de indicación de estado seguro (SSC) con nivel de seguridad SIL>0, en particular SIL4, para transformar datos de estado concernientes al estado de los elementos del sistema de control de rutas y trenes (RTCS) en datos gráficos y, por lo tanto, generar datos de indicación que indican información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de rutas y trenes (RTCS) en la pantalla de la estación de trabajo de operador (OW), en donde el componente de indicación de integridad básica y el componente de indicación de estado seguro son componentes de software, esto es, bloques de software de construcción encapsulada, en donde se proporciona un canal (C1) que conecta el sistema de control de rutas y trenes (RTCS) y la estación de trabajo de operador (OW), para transmitir información con integridad básica desde el sistema de control de rutas y trenes (RTCS) hasta la estación de trabajo de operador (OW), en donde el componente de indicación de estado seguro (SSC) es funcionalmente independiente de la estación de trabajo de operador (OW), y el componente de indicación de estado seguro (SSC) está funcionalmente separado del componente de indicación de integridad básica (BIC), en donde la función para generar datos de indicación de información relacionada con la seguridad concerniente al estado de los elementos del sistema de control de trenes de ruta se externaliza desde la estación de trabajo de operador; el sistema de control de tráfico de trenes que comprende además un canal seguro (C3) adicional que conecta el componente de indicación de estado seguro (SSC) y la pantalla (D) para la transmisión segura de información relacionada con la seguridad sobre el estado de los elementos del sistema de control de trenes de ruta (RTCS), en donde el componente de indicación de estado seguro (SSC) está integrado en el sistema de control de rutas y trenes (RTCS).

el método comprende

la generación de datos gráficos de información con integridad básica dentro de la estación de trabajo de operador,

la transformación de datos de estado que comprenden la información relevante para la seguridad en datos de indicación gráfica dentro del componente de indicación de estado seguro (SSC) con nivel de seguridad SIL>0 que es funcionalmente independiente de los componentes de indicación de integridad básica (BIC) con nivel de seguridad SIL0 de la estación de trabajo de operador (OW), y

la transmisión de los datos de indicación a una pantalla (D) a través del canal seguro (C3).

10. Método según la reivindicación 9, caracterizado por que el canal seguro se enruta a través de la estación de trabajo de operador (OW).

11. Método según la reivindicación 9 o 10, caracterizado por que los datos de indicación son datos de mapa de píxeles y en donde los datos de indicación se transmiten a la pantalla (D) usando un método para verificar la transferencia correcta de datos de mapa de píxeles.

12. Método según cualquiera de las reivindicaciones 9 a 11, caracterizado por que los datos de indicación se muestran en un navegador web de la estación de trabajo de operador.

13. Método según la reivindicación 12, caracterizado por que los datos de indicación mostrados se vuelven a leer.

14. Método según la reivindicación 13, caracterizado por

que el componente de indicación de estado seguro genera una primera suma de comprobación de los datos de indicación;

que el navegador genera una segunda suma de comprobación de los datos vueltos a leer y transmite la segunda suma de comprobación al componente de indicación de estado seguro a través del canal seguro; y

que el componente de indicación de estado seguro compara la primera suma de comprobación y la segunda suma de comprobación.

15. Método según la reivindicación 13 o 14, caracterizado por

que el navegador transmite los datos vueltos a leer al componente de indicación de estado seguro a través del canal seguro; y

que el componente de indicación de estado seguro compara los datos vueltos a leer con los datos de indicación.

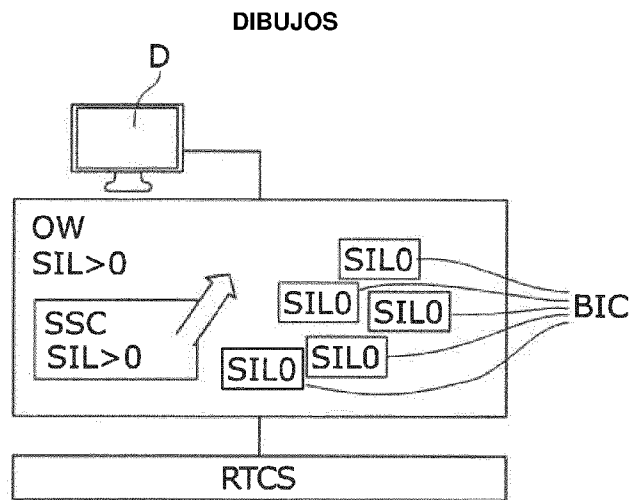


Fig. 1

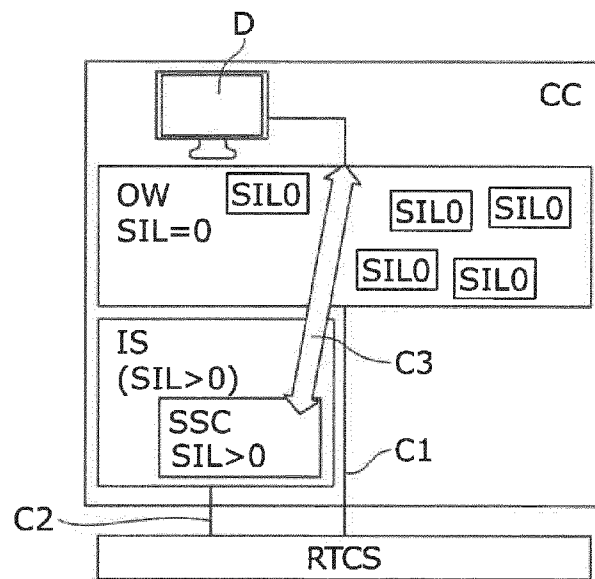


Fig. 2

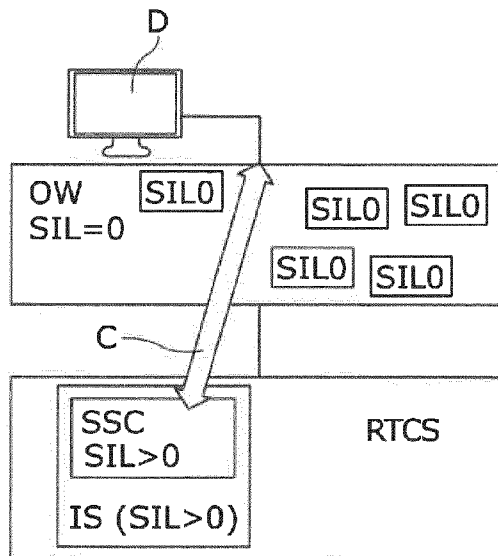


Fig. 3

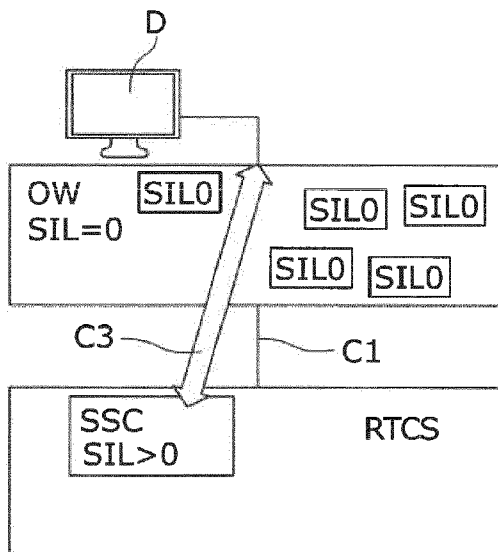


Fig. 4

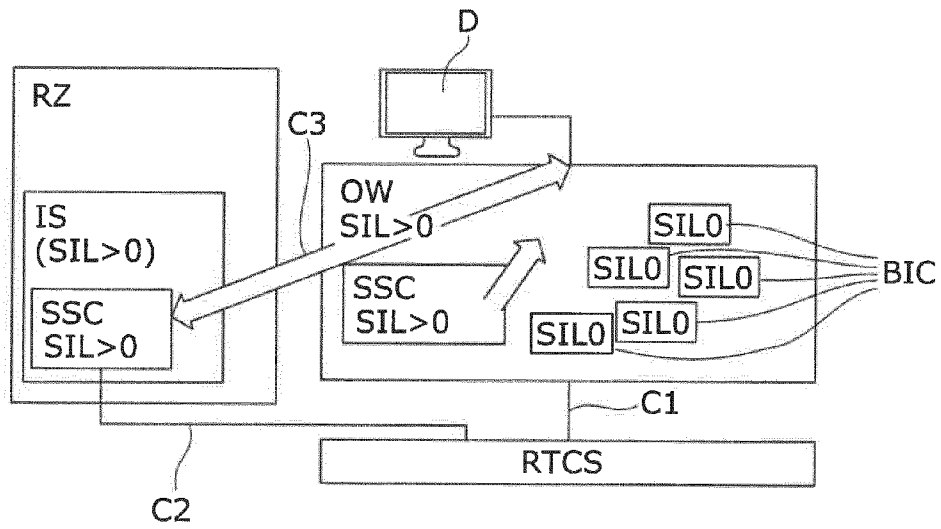


Fig. 5

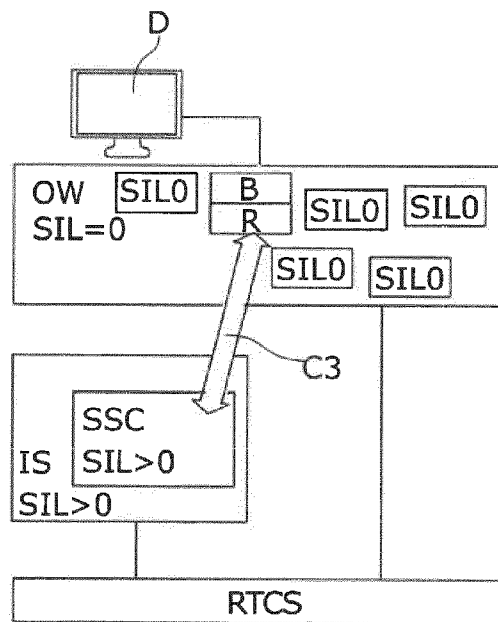


Fig. 6