(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 905 641**

(51) Int. CI.:

H04L 12/26 (2006.01)
B61L 19/06 (2006.01)
B61L 27/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.09.2018 PCT/EP2018/073989**

(87) Fecha y número de publicación internacional: **04.04.2019 WO19063259**

(96) Fecha de presentación y número de la solicitud europea: **06.09.2018 E 18781963 (6)**

(97) Fecha y número de publicación de la concesión europea: **10.11.2021 EP 3661830**

(54) Título: **Concepto para monitorizar un tráfico de red entrante en un puesto de enclavamiento**

(30) Prioridad:

29.09.2017 DE 102017217422

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.04.2022

(73) Titular/es:

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

(72) Inventor/es:

AUST, FRANK y
SEIFERT, MATTHIAS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Concepto para monitorizar un tráfico de red entrante en un puesto de enclavamiento

La invención se refiere a un dispositivo y a un procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación. La invención se refiere además a un programa informático.

Un dispositivo de tipo genérico y un procedimiento de tipo genérico se conocen por el documento KENDELBACHER D. ET AL: *"Ein Kommunikationsbasissystem für ETCS (Teil 1)"*, SIGNAL+ DRAHT, DW, n.º 94, 1 de junio de 2002 (2002-06-01), páginas 6-11, XP002495555, ISSN: 0037-4997. En el dispositivo de tipo genérico allí descrito o en el procedimiento de tipo genérico allí descrito se utilizan funciones de transmisión específicas, en particular, protocolos de transmisión específicos, que garantizan la autenticidad y la integridad de conexiones y datos.

Además, por el documento WO 2016/119946 A1 se conoce un sistema de control, por ejemplo, a bordo de un automóvil, que está conectado a un bus de datos, a través del cual puede comunicar con otros sistemas de control o aparatos de control, y que respalda un análisis de error mejorado.

En un centro de control de una instalación de servicio ferroviario se utilizan habitualmente estaciones de trabajo de ordenador para el ajuste de itinerarios y para la monitorización de un tráfico ferroviario.

Las acciones de mando que se efectúan, por ejemplo, mediante las estaciones de trabajo de ordenador y que repercuten, por ejemplo, en un estado de un tramo ferroviario, se monitorizan por regla general mediante un puesto de enclavamiento de la instalación de servicio ferroviario, que asume la responsabilidad de la seguridad antes de que tenga lugar una modificación de señales, itinerarios o liberaciones de marcha.

Dado que generalmente las estaciones de trabajo de ordenador y el puesto de enclavamiento están en distintos lugares, estos están conectados entre sí habitualmente a través de una red de comunicación.

Esto significa por lo tanto que puede accederse al puesto de enclavamiento, por ejemplo, a través de una red de comunicación.

En este aspecto existe una necesidad de proteger el puesto de enclavamiento de un tráfico de red entrante a través de la red de comunicación que podría poner en peligro una seguridad de un funcionamiento de la instalación de servicio ferroviario.

Por lo tanto, el objetivo en el que se basa la invención puede verse en facilitar un concepto eficiente para monitorizar de manera eficiente un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

Este objetivo se resuelve mediante el objeto respectivo de las reivindicaciones independientes. Diseños ventajosos de la invención son objeto de reivindicaciones subordinadas dependientes.

Según un aspecto se facilita un dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación, que comprende:

una red TAP para leer el tráfico de red entrante a través de la red de comunicación en el puesto de enclavamiento y

para emitir el tráfico de red entrante leído a un procesador para verificar el tráfico de red entrante leído y

un equipo de separación de red para la separación del puesto de enclavamiento de la red de comunicación,

en donde el procesador está configurado para controlar el equipo de separación de red, basándose en un resultado de la verificación del tráfico de red entrante leído, de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación y

en donde el procesador para verificar el tráfico de red entrante leído está configurado para comprobar que no haya comandos no permitidos en un flujo de comandos incluido en el tráfico de red entrante leído y cuando se detecta un comando no permitido, controlar el equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

Según otro aspecto se facilita un procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación, que comprende las siguientes etapas:

leer el tráfico de red entrante en el puesto de enclavamiento a través de la red de comunicación,

verificar el tráfico de red entrante leído y separar el puesto de enclavamiento de la red de comunicación basándose en un resultado de la verificación del tráfico de red entrante leído,

en donde un procesador para verificar el tráfico de red entrante leído comprueba que no haya comandos no permitidos en un flujo de comandos incluido en el tráfico de red entrante leído, y cuando se detecta un comando no permitido, controla un equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

Según un aspecto adicional se facilita un programa informático, que comprende un código de programa para llevar a cabo el procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación, cuando el programa informático se ejecuta en un ordenador, por ejemplo, en el dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

La invención se basa en el conocimiento de que el objetivo anterior se resuelve porque una red TAP lee el tráfico de red entrante y se emite a un procesador con el fin de verificar el tráfico de red entrante. Dependiendo de un resultado de la verificación, el puesto de enclavamiento se separa de la red de comunicación o no.

El uso de la red TAP ofrece la ventaja técnica, en particular, de que esta no puede verse en la red de comunicación, y por consiguiente, también no puede ser detectada ni atacada por un atacante.

Adicionalmente, el uso de una red TAP presenta la ventaja técnica de que puede llevarse a cabo una lectura y en este aspecto una verificación correspondiente del tráfico de red entrante capta en tiempo real sin un retardo de tiempo considerable comparado con una denominada puerta de enlace al nivel de aplicación ("*application level gateway* (ALG))". Si bien, una puerta de enlace al nivel de aplicación de este tipo puede comprobar también un tráfico de red, sin embargo, en este sentido genera siempre un desfase en el tiempo considerable y modifica habitualmente una rapidez de respuesta prevista originalmente. La ventaja de tiempo depende, por ejemplo, de la amplitud de la verificación que se lleva a cabo. Esto, en algunas ALG, puede situarse sin más en el intervalo de varios milisegundos hasta 500 ms, lo que no sería tolerable cuando se exige una transmisión exenta de retardos. En una ALG deben copiarse datos de manera múltiple de un lado a otro y conducirse mediante el procesador, lo que produce en sí ya pérdidas de tiempo. Después se añade también el "*processing-time*" propiamente dicho, es decir, el tiempo de procesamiento por parte del procesador. Por lo tanto, la ALG no son especialmente ventajosas.

Al separarse el puesto de enclavamiento de la red de comunicación, se consigue, en particular, la ventaja técnica de que ya no puede accederse al puesto de enclavamiento a través de la red de comunicación. Por consiguiente, los atacantes ya no pueden atacar el puesto de enclavamiento a través de la red de comunicación. Por consiguiente, el puesto de enclavamiento está protegido de manera eficiente ventajosamente de los ataques a través de la red de comunicación.

Por consiguiente, se consigue adicionalmente en particular la ventaja técnica de que el tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario puede monitorizarse de manera eficiente a través de una red de comunicación.

Una red TAP en el sentido de la descripción establece un punto de acceso pasivo a una conexión de red, con lo cual las señales de datos transmitidas a través de la conexión de red (es decir, por ejemplo, el tráfico de red entrante) pueden leerse y analizarse para propósitos de análisis. Una red TAP se denomina en inglés "*network-TAP*".

La sigla "TAP" quiere decir "*test access port*".

Una red TAP en el sentido de la descripción funciona en la capa 1 OSI (*OSI-layer 1*) y no presenta ninguna dirección MAC. La red TAP, por consiguiente, no puede verse en la red de comunicación.

La red TAP puede denominarse en este aspecto también red TAP pasiva, siempre que establezca el punto de acceso pasivo descrito anteriormente.

La red TAP puede denominarse, por ejemplo, también TAP Ethernet.

Al estar configurado el procesador para verificar el tráfico de red entrante leído para comprobar que no haya comandos no permitidos en un flujo de comandos incluido en el tráfico de red entrante leído y cuando se detecta un comando no permitido controlar el equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación, se consigue, en particular, la ventaja técnica de que pueden detectarse comandos no permitidos de manera eficiente. En particular, se consigue la ventaja técnica de que puede provocarse una protección eficiente del puesto de enclavamiento ante comandos no permitidos.

En una forma de realización está previsto que el procesador para comprobar el flujo de comandos esté configurado para comparar comandos del flujo de comandos con comandos de referencia de una lista de comandos negativos para detectar comandos no permitidos.

Por esto se consigue, por ejemplo, la ventaja técnica de que los comandos no permitidos puedan detectarse de manera eficiente. La lista de comandos negativos forma por lo tanto una así llamada "*black list*" (lista negra). Los comandos que están incluidos en la lista de comandos negativos son, por lo tanto, comandos no permitidos.

Por consiguiente, mediante la adaptación de la lista de comandos negativos se hace posible reaccionar ventajosamente de manera flexible ante diferentes escenarios de amenaza.

Según otra forma de realización está previsto un equipo de registro para el registro del tráfico de red leído.

Por esto se consigue, por ejemplo, la ventaja técnica de que en un momento posterior puede probarse de manera eficiente que, por ejemplo, se han enviado comandos no permitidos al puesto de enclavamiento, o que han podido impedirse con éxito acciones de mando no permitidas que se corresponden con los comandos no permitidos.

Por lo tanto, esto significa en particular que el equipo de registro graba el tráfico de red leído, es decir, lo almacena.

Según una forma de realización está previsto que la red TAP esté configurada para emitir el tráfico de red entrante leído al equipo de registro.

De acuerdo con una forma de realización adicional está previsto que el procesador esté configurado para emitir el tráfico de red entrante leído al equipo de registro.

En otra forma de realización está previsto que el equipo de separación de red esté configurado para separar físicamente el puesto de enclavamiento de la red de comunicación.

Por esto se consigue, por ejemplo, la ventaja técnica de que se consigue una separación eficiente y segura del puesto de enclavamiento de la red de comunicación.

La separación física comprende, por ejemplo, una separación física de una conexión de comunicación entre la red TAP y el puesto de enclavamiento.

Por ejemplo, la separación física comprende una apertura de un conmutador que en una conexión de comunicación está posicionado entre la red de comunicación y el puesto de enclavamiento, por ejemplo, entre la red TAP y el puesto de enclavamiento.

En otra forma de realización está previsto un equipo de alimentación de comandos para alimentar un comando de prueba en el tráfico de red entrante para examinar el procesador, en donde el procesador no está configurado, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído, para llevar a cabo ningún control del equipo de separación de red de tal manera que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

Por esto, en particular, se consigue la ventaja técnica de que se hace posible una prueba eficiente del procesador. Esto significa, por lo tanto, en particular, que una detección del comando de prueba en el tráfico de red entrante no tiene como consecuencia ninguna separación del puesto de enclavamiento de la red de comunicación.

En una forma de realización está previsto que el equipo de alimentación de comandos esté configurado para alimentar el comando de prueba en intervalos de tiempo predeterminados.

Por esto, por ejemplo, se consigue la ventaja técnica de que el procesador puede examinarse de manera eficiente también durante un espacio de tiempo más largo.

Un intervalo de tiempo predeterminado así se selecciona, por ejemplo, dependiendo de los requisitos de la aplicación. Por ejemplo, está previsto que el comando de prueba se alimente una vez por segundo o una vez por minuto o una vez por hora. Por ejemplo, un verificador oficial predetermina el intervalo de tiempo.

En una forma de realización está previsto que el procesador esté configurado, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído para enviar un mensaje de éxito al equipo de alimentación de comandos de que se ha detectado el comando de prueba, en donde el equipo de alimentación de comandos está configurado para controlar, en ausencia de un mensaje de éxito después de la alimentación del comando de prueba el equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

Por esto, por ejemplo, se consigue la ventaja técnica de que un fallo en el procesador que lleva a una no detección del comando de prueba no tenga ninguna repercusión crítica, en términos de seguridad, en un funcionamiento del puesto de enclavamiento. Esto porque, dado que en un caso así, es decir, cuando no existe ningún mensaje de éxito, el puesto de enclavamiento se separa de la red de comunicación.

Al controlarse de acuerdo con esta forma de realización de manera correspondiente el equipo de separación de red mediante el equipo de alimentación de comandos para separar el puesto de enclavamiento de la red de comunicación,

se consigue, en particular, la ventaja técnica de que, en caso de un fallo en el procesador, el puesto de enclavamiento puede separarse no obstante de la red de comunicación.

En una forma de realización está previsto que el dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación esté configurado para ejecutar o llevar a cabo el procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

En una forma de realización está previsto que el procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación se ejecute o se lleve a cabo mediante el dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

Según un aspecto adicional se facilita una instalación de servicio ferroviario que comprende el puesto de enclavamiento y el dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

Las funcionalidades técnicas del dispositivo resultan de manera análoga a partir de funcionalidades técnicas correspondientes del procedimiento y a la inversa.

Esto significa, por lo tanto, por ejemplo, que resultan características de dispositivo de características de procedimiento correspondientes y a la inversa.

Según una forma de realización el procedimiento comprende que se lleva a cabo la lectura del tráfico de red entrante a través de la red de comunicación en el puesto de enclavamiento mediante la red TAP.

De acuerdo con una forma de realización del procedimiento está previsto que el tráfico de red entrante leído se emita al procesador, por ejemplo, mediante la red TAP.

Según una forma de realización del procedimiento para verificar el tráfico de red entrante leído, está previsto comprobar que no haya comandos no permitidos en un flujo de comandos incluido en el tráfico de red entrante leído, y cuando se detecta un comando no permitido, controlar el equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

En una forma de realización del procedimiento, para comprobar el flujo de comandos está previsto que se comparen comandos del flujo de comandos con comandos de referencia de una lista de comandos negativos para detectar comandos no permitidos.

En una forma de realización del procedimiento está previsto un registro del tráfico de red leído.

En una forma de realización adicional del procedimiento está previsto que el puesto de enclavamiento se separe físicamente de la red de comunicación.

En una forma de realización del procedimiento está previsto que el puesto de enclavamiento se separe físicamente de la red de comunicación mediante el equipo de separación de red.

De acuerdo con una forma de realización del procedimiento está prevista una alimentación de un comando de prueba en el tráfico de red entrante para examinar el procesador, en donde, cuando se detecta el comando de prueba mediante el procesador en el marco de la verificación del flujo de red entrante leído, el procesador no lleva a cabo ningún control del equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

En una forma de realización del procedimiento está previsto que el procesador, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído, envíe un mensaje de éxito al equipo de alimentación de comandos de que se ha detectado el comando de prueba, en donde el equipo de alimentación de comandos, en ausencia de un mensaje de éxito, después de la alimentación del comando de prueba controla el equipo de separación de red de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

En una forma de realización está previsto que el equipo de alimentación de comandos esté configurado, en ausencia del mensaje de éxito después de la alimentación del comando de prueba, para controlar el equipo de separación de red tras haber transcurrido una duración de tiempo predeterminada, de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación.

Esto significa, por lo tanto, en particular que, según esta forma de realización, está previsto que el equipo de alimentación de comandos espere el transcurso de la duración de tiempo predeterminada después de la alimentación del comando de prueba, antes de que el equipo de separación de red se controle de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación, en ausencia del mensaje de éxito.

Cuánto tiempo se espera con la separación después de la ausencia del mensaje de éxito depende, por ejemplo, de la implementación, es decir, del caso individual concreto. Si puede garantizarse, por ejemplo, que dentro de un intervalo de tiempo determinado (la duración de tiempo predeterminada) debía realizarse una respuesta bajo todas las condiciones de funcionamiento posibles, de acuerdo con una forma de realización está previsto que el equipo de separación de red se controle directamente después del transcurso del intervalo de tiempo determinado de tal modo que el equipo de separación de red separa el puesto de enclavamiento de la red de comunicación, en ausencia del mensaje de éxito. De acuerdo con una forma de realización está previsto que el puesto de enclavamiento esté conectado o pueda conectarse a través de un rúter VPN con la red de comunicación.

Esto significa, por lo tanto, en particular que, de acuerdo con una forma de realización, esté previsto un rúter VPN para una conexión del puesto de enclavamiento con la red de comunicación. El puesto de enclavamiento está conectado por ejemplo con el rúter VPN.

En una forma de realización está previsto que la red TAP esté posicionada entre el rúter VPN y el puesto de enclavamiento.

En una forma de realización está previsto que un ordenador de un centro de control de la instalación de servicio ferroviario pueda conectarse o esté conectado a través de la red de comunicación con el puesto de enclavamiento.

Esto significa, por lo tanto, por ejemplo, de acuerdo con una forma de realización, que esté previsto un ordenador de un centro de control de la instalación de servicio ferroviario.

En una forma de realización está previsto que el ordenador del centro de control de la instalación de servicio ferroviario esté conectado o pueda conectarse con la red de comunicación a través de un rúter VPN adicional.

Esto significa, por lo tanto, en particular de acuerdo con una forma de realización que esté previsto un rúter VPN adicional para una conexión del ordenador del centro de control con la red de comunicación. El ordenador está conectado por ejemplo con el rúter VPN adicional.

La red de comunicación comprende de acuerdo con una forma de realización la Internet.

En una forma de realización la red de comunicación comprende una red de telefonía móvil.

El ordenador del centro de control de acuerdo con una forma de realización está configurado como una estación de trabajo, por ejemplo, como una estación de trabajo de mando.

A través del ordenador del centro de control de la instalación de servicio ferroviario, por ejemplo, se especifica o puede especificarse, por ejemplo, el estado que deben presentar las señales de la instalación de servicio ferroviario o el estado o la posición debe tener una aguja de la instalación de servicio ferroviario o mediante el ordenador se especifica una liberación de marcha. Entre los posibles avisos de un puesto de mando figuran, entre otros, avisos de liberación o de ocupación de secciones de vía y/o protección de flancos de agujas.

En una forma de realización está previsto que el flujo de comandos se transmita en forma de telegramas PDS y/o SBS.

En este sentido, la sigla "PDS" en alemán quiere decir interfaz de datos de proceso.

La sigla "SBS" en alemán quiere decir interfaz de mando estándar.

En una forma de realización está previsto que el flujo de comandos sea un flujo de comandos de uno de los siguientes protocolos de red: SSH, SFTP, SMB.

Un comando no permitido en el sentido de la descripción es, por ejemplo, una liberación de comando. Una liberación de comando de este tipo consigue en el puesto de enclavamiento una anulación de estados de sistema o una cancelación manual del puesto de enclavamiento. Esto significa, por lo tanto, en particular que, con el comando "liberación de comando" se hace posible cancelar manualmente el puesto de enclavamiento para poder continuar, por ejemplo, con un funcionamiento de tren con seguridad limitada, siempre y cuando se haya producido, por ejemplo, una avería en el puesto de enclavamiento que ha llevado a un bloqueo.

Un ejemplo para una liberación de comando de este tipo es el caso de que, aunque se indique una señal "rojo", se emite una orden de marcha al jefe de tren o se libera una entrada en una sección de vía, aunque se haya indicado ya que la sección de vía está ocupada. Esta orden de marcha corresponde en este caso a la liberación de comando. Se invalida por lo tanto la monitorización de seguridad.

Las causas para la necesidad de una liberación de comando de este tipo son, por ejemplo, avisos erróneos de vía libre ordenados por un usuario por separado en una estación de trabajo mediante comandos KF (KF = liberación de comando) y se cancelan manualmente en el puesto de enclavamiento.

De acuerdo con una forma de realización, un dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación comprende el puesto de enclavamiento.

En una forma de realización, un dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación no comprende el puesto de enclavamiento.

En una forma de realización está previsto que, después del transcurso de una duración de tiempo predeterminada adicional, el puesto de enclavamiento se conecte de nuevo con la red de comunicación. En flujos de comando de acuerdo con PDS, SBS la duración de tiempo predeterminada adicional por ejemplo es mayor de 1 minuto, por ejemplo, mayor de 2 minutos. De acuerdo con una forma de realización una acción KF debe finalizar dentro de esta duración de tiempo predeterminada adicional, de lo contrario esta se detecta como inválida.

Esto, por lo tanto, significa por ejemplo que el equipo de separación de red está configurado para conectar, después del transcurso de una duración de tiempo predeterminada adicional, el puesto de enclavamiento de nuevo con la red de comunicación.

Esto, por lo tanto, significa, por ejemplo, que el procesador está configurado para controlar el equipo de separación de red después del transcurso de una duración de tiempo predeterminada adicional, de tal modo que este conecta de nuevo el puesto de enclavamiento con la red de comunicación.

Según una forma de realización está previsto que el equipo de separación de red esté configurado para separar de manera reversible el puesto de enclavamiento de la red de comunicación.

En una forma de realización está previsto que el equipo de separación de red esté configurado para separar de manera irreversible el puesto de enclavamiento de la red de comunicación.

Por lo tanto, por ejemplo, en una separación irreversible mediante el equipo de separación de red, para conectar el puesto de enclavamiento de nuevo con la red de comunicación debe reemplazarse, por ejemplo, el equipo de separación de red.

La expresión "o" comprende, en particular, la expresión "y/o".

Las propiedades, características y ventajas anteriormente descritas de esta invención, así como el modo de lograrlas se aclaran y se comprenden con más claridad en relación con la siguiente descripción de los ejemplos de realización, que se explican con más detalle en relación con los dibujos, en donde

FIG 1 muestra un primer dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación,

FIG 2 un segundo dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación,

FIG 3 un tercer dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación y

FIG 4 un diagrama de flujo de un procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

En lo sucesivo, para las mismas características pueden emplearse las mismas referencias.

La figura 1 muestra un primer dispositivo 101 para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

El primer dispositivo 101 comprende:

una red TAP 103 para leer el tráfico de red entrante a través de la red de comunicación en el puesto de enclavamiento y para emitir el tráfico de red entrante leído a un procesador 105 para verificar el tráfico de red entrante leído,

un equipo de separación de red 107 para la separación del puesto de enclavamiento de la red de comunicación,

en donde el procesador 105 está configurado para controlar, basándose en un resultado de la verificación del tráfico de red entrante leído, el equipo de separación de red 107 de tal modo que el equipo de separación de red 107 separa el puesto de enclavamiento de la red de comunicación.

La figura 1 muestra adicionalmente un puesto de enclavamiento 109 de una instalación de servicio ferroviario (no mostrada adicionalmente en detalle), que está conectado a través de un rúter VPN 111 con una red de comunicación 113.

La red de comunicación 113 es de acuerdo con una forma de realización la Internet.

Adicionalmente, la figura 1 muestra una estación de trabajo de mando 115 de un centro de control no mostrado, en este caso, adicionalmente de la instalación de servicio ferroviario.

La estación de trabajo de mando 115 está conectada a través de un rúter VPN adicional 117 con la red de comunicación 113.

En este punto cabe señalar que el rúter VPN 117 adicional, la Internet como una red de comunicación 113 posible y el rúter VPN 111 de acuerdo con una forma de realización no son forzosamente necesarios. El dispositivo 101 está instalado de acuerdo con una forma de realización en la red local de un cliente y no tiene que estar conectado, por ejemplo, obligatoriamente a través de la Internet y rúter VPN al puesto de enclavamiento 109.

La red TAP 103 está posicionada entre el rúter VPN 111 y el puesto de enclavamiento 109.

Adicionalmente, el equipo de separación de red 107 está posicionado entre la red TAP 103 y el puesto de enclavamiento 109.

Un modo de funcionamiento a modo de ejemplo del primer dispositivo 101 se describe a continuación:

> La red TAP 103 lee un flujo de comandos que se envía desde el rúter VPN 111 al puesto de enclavamiento 109 y emite el flujo de comandos leído al procesador 105. La red TAP 103 lee, por tanto, el tráfico de red entrante en el puesto de enclavamiento 109 (flujo de comandos).
>
> El procesador 105 comprueba que no haya comandos no permitidos o secuencias de comandos no permitidas o tipos de comandos no permitidos, por ejemplo, una liberación de comando en el flujo de comandos que se transmite de acuerdo con una forma de realización en forma de telegramas PDS y/o SBS.

Si el procesador 105 detecta un tipo de comando o secuencia de comandos así o un comando no permitido, el procesador 105 controla el equipo de separación de red 107 de tal modo que el equipo de separación de red 107 separa la conexión de red entre la red TAP 103 y el puesto de enclavamiento 109. Por esto, el puesto de enclavamiento 109 se separa de la red de comunicación 113.

Es habitual que las acciones de mando que se efectúan empleando la estación de trabajo de mando 115 y que repercuten en un estado de una sección ferroviaria (no mostrada) de la instalación de servicio ferroviario, se monitoricen mediante el puesto de enclavamiento 109, que asume la responsabilidad de la seguridad, antes de que tenga lugar una modificación de señales o itinerarios o liberaciones de marcha. Esto es válido habitualmente para todos los comandos excepto los que se denominan "liberación de comando". Tales comandos cancelan manualmente el puesto de enclavamiento 109.

Al prever tales "liberaciones de comando" en el caso de una avería debe ser posible continuar con un funcionamiento de tren con seguridad limitada, y anular, dado el caso, estados de sistema en el puesto de enclavamiento 109 que han llevado a un bloqueo.

No obstante, por ello pueden eludirse funciones de seguridad que están integradas en el puesto de enclavamiento 109, lo que puede representar un alto riesgo en el caso de un error en el manejo intencionado o involuntario. Esto es válido, por ejemplo, sobre todo cuando tales comandos pueden dispararse intencionadamente o con intención a través de un accionamiento a distancia.

Sin embargo, dado que la comunicación en remoto, es decir, por ejemplo, la conexión entre la estación de trabajo de mando 115 y el puesto de enclavamiento 109 se diseña o se configura o está configurada únicamente para una monitorización de posición, y en particular, no está prevista para una ejecución de órdenes de liberación de comando, es válido prevenir que se impida dar órdenes del tipo "liberación de comando" o por completo o al menos su efecto. En este sentido, debe prestarse especial atención a que un equipo de monitorización no se desactive.

En el curso de una nueva legislación sobre seguridad se exigen en este caso altas medidas de protección adicionales, y al mismo tiempo nuevas funcionalidades por parte del cliente. El concepto de acuerdo con la invención considera esta situación de dos requisitos contradictorios.

Esto, por lo tanto, dado que a través de la red TAP 103 el flujo de comandos, que se envía por ejemplo desde la estación de trabajo de mando 115 a través de la red de comunicación 113 al puesto de enclavamiento 109, se lee y se emite al procesador 105 para propósitos de verificación. El procesador 105 puede comprobar la existencia de comandos del tipo "liberación de comando" por consiguiente, ventajosamente en este flujo de comandos, y cuando se detecta un comando de este tipo, activar el equipo de separación de red 107.

Por esto, en particular, se consigue la ventaja técnica de que mediante un error en el manejo intencionado o involuntario en correspondencia no tenga lugar un peligro elevado, al menos puede reducirse un riesgo correspondiente.

Al no ser visible la red TAP 103 en la red, esta no puede ser atacada y, dado el caso, desactivarse.

Por consiguiente, puede accederse al puesto de enclavamiento 109 a través de la red de comunicación 113, lo que se exige, por ejemplo, del lado del cliente.

Al mismo tiempo, sin embargo, también se ponen en práctica, en este caso, de manera eficiente medidas de protección adicionales exigidas por la nueva legislación de seguridad.

Por consiguiente, a pesar de todo, pueden cumplirse dos requisitos realmente contradictorios de acuerdo con la invención.

La figura 2 muestra un segundo dispositivo 201 para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

El segundo dispositivo 201 está configurado de manera esencialmente análoga al primer dispositivo 101 de acuerdo con la figura 1.

Adicionalmente, al dispositivo 101 de acuerdo con la figura 1, el segundo dispositivo 201 comprende un equipo de registro 205 para el registro del tráfico de red leído.

La red TAP 103 está configurada en este aspecto para emitir el tráfico de red leído al equipo de registro 205.

Los elementos adicionales mostrados en la figura 2 y su modo de funcionamiento son idénticos a los elementos mostrados en la figura 1 a o sus modos de funcionamiento. Se remite a las realizaciones hechas anteriormente para evitar repeticiones.

Mediante el equipo de registro 205 se hace posible ventajosamente poder demostrar también en un momento posterior si el flujo de comandos comprendía comandos no permitidos.

Por ejemplo, está previsto que el equipo de registro 205 esté configurado para registrar una separación del puesto de enclavamiento 109 de la red de comunicación 113.

Un registro comprende, por ejemplo, una memoria.

La figura 3 muestra un tercer dispositivo 301 para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación.

El tercer dispositivo 301 está configurado de manera esencialmente análoga al segundo dispositivo 201 de acuerdo con la figura 2.

Adicionalmente al segundo dispositivo 201 mostrado en la figura 2, el tercer dispositivo 301 de acuerdo con la figura 3 comprende también un equipo de alimentación de comandos 303 para alimentar un comando de prueba en el tráfico de red entrante para examinar el procesador 105.

De acuerdo con esta forma de realización, el procesador 105 está configurado entonces, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído, para no llevar a cabo ningún control del equipo de separación de red 107 de tal modo que el equipo de separación de red 107 separa el puesto de enclavamiento 109 de la red de comunicación 113.

En una forma de realización está previsto que el tercer dispositivo 301 no comprenda el equipo de registro 205. De acuerdo con esta forma de realización el tercer dispositivo 301 está configurado de manera esencialmente análoga al primer dispositivo 101 de acuerdo con la figura 1. De acuerdo con esta forma de realización, el tercer dispositivo 301 comprende adicionalmente al primer dispositivo 101 mostrado en la FIG 1 el equipo de alimentación de comandos 303.

En una forma de realización, está previsto que el procesador 105 esté configurado, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído, para enviar un mensaje de éxito al equipo de alimentación de comandos 303 de que se ha detectado el comando de prueba, estando configurado el equipo de alimentación de comandos 303 para controlar el equipo de separación de red 107, en ausencia de un mensaje de éxito después de la alimentación del comando de prueba, en particular, en ausencia de un mensaje de éxito después de la alimentación del comando de prueba tras haber transcurrido una duración de tiempo predeterminada, por ejemplo, como máximo de 3 s, de tal modo que el equipo de separación de red 107 separa el puesto de enclavamiento 109 de la red de comunicación 113.

De acuerdo con una forma de realización, un dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación comprende el puesto de enclavamiento.

En una forma de realización, un dispositivo para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación no comprende el puesto de enclavamiento.

La figura 4 muestra un diagrama de flujo de un procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento de una instalación de servicio ferroviario a través de una red de comunicación, que comprende las siguientes etapas:

leer 401 el tráfico de red entrante a través de la red de comunicación en el puesto de enclavamiento,

verificar 403 el tráfico de red entrante leído, separar 405 el puesto de enclavamiento de la red de comunicación basándose en un resultado de la verificación del tráfico de red entrante leído.

Según una forma de realización está previsto que el procedimiento mostrado y descrito en la figura 4 se lleve a cabo o se ejecute mediante uno de los tres dispositivos 101, 201, 303.

Esto significa, por lo tanto, por ejemplo, que la lectura 401 se lleva a cabo mediante la red TAP 103.

La red TAP 103 emite, por ejemplo, al procesador 105el tráfico de red leído.

La verificación 403 se lleva a cabo, por ejemplo, mediante el procesador 105.

La separación 405 se lleva a cabo, por ejemplo, mediante el equipo de separación de red 107. Para ello, el procesador 105 controla de manera correspondiente el equipo de separación de red 107.

En una forma de realización está previsto que, tras haber transcurrido una duración de tiempo predeterminada, el puesto de enclavamiento 109 se conecte de nuevo con la red de comunicación 113.

Esto significa, por lo tanto, por ejemplo, que el equipo de separación de red 107 esté configurado para conectar de nuevo el puesto de enclavamiento 109 con la red de comunicación 113, tras haber transcurrido una duración de tiempo predeterminada.

Esto significa, por lo tanto, por ejemplo, que el procesador 105 está configurado para conectar el puesto de enclavamiento 109 con la red de comunicación 113, tras haber transcurrido una duración de tiempo predeterminada.

Según una forma de realización está previsto que el equipo de separación de red 107 esté configurado para separar de manera reversible el puesto de enclavamiento 109 de la red de comunicación 113.

En una forma de realización está previsto que el equipo de separación de red 107 esté configurado para separar de manera irreversible el puesto de enclavamiento 109 de la red de comunicación 113.

Aunque la invención se ha ilustrado y descrito en detalle mediante los ejemplos de realización preferidos, la invención no está limitada por los ejemplos divulgados y el experto, a partir de estos, puede derivar otras variaciones en este caso, sin abandonar el ámbito de protección de la invención.

REIVINDICACIONES

1. Dispositivo (101, 201, 301) para monitorizar un tráfico de red entrante en un puesto de enclavamiento (109) de una instalación de servicio ferroviario a través de una red de comunicación,

caracterizado por

una red TAP (103) para leer el tráfico de red entrante a través de la red de comunicación (113) en el puesto de enclavamiento (109) y para emitir a un procesador (105) el tráfico de red entrante leído para verificar el tráfico de red entrante leído y

un equipo de separación de red (107) para la separación del puesto de enclavamiento (109) de la red de comunicación (113),

en donde el procesador (105), basándose en un resultado de la verificación del tráfico de red entrante leído, está configurado para controlar el equipo de separación de red (107) de tal modo que el equipo de separación de red (107) separa el puesto de enclavamiento (109) de la red de comunicación (113), y en donde el procesador (105) está configurado para verificar el tráfico de red entrante leído, para comprobar que no haya comandos no permitidos en un flujo de comandos incluido en el tráfico de red entrante leído, y cuando se detecta un comando no permitido, controlar el equipo de separación de red (107) de tal modo que el equipo de separación de red (107) separa el puesto de enclavamiento (109) de la red de comunicación (113).

2. Dispositivo (101, 201, 301) según la reivindicación 1, en donde el procesador (105) para comprobar el flujo de comandos está configurado para comparar comandos del flujo de comandos con comandos de referencia de una lista de comandos negativos para detectar comandos no permitidos.

3. Dispositivo (101, 201, 301) según una de las reivindicaciones anteriores, que comprende un equipo de registro (205) para el registro del tráfico de red leído.

4. Dispositivo (101, 201, 301) según una de las reivindicaciones anteriores, en donde el equipo de separación de red (107) está configurado para separar físicamente el puesto de enclavamiento (109) de la red de comunicación (113).

5. Dispositivo (101, 201, 301) según una de las reivindicaciones anteriores, que comprende un equipo de alimentación de comandos (303) para alimentar un comando de prueba en el tráfico de red entrante para examinar el procesador (105), en donde el procesador (105) está configurado, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído, para no llevar a cabo ningún control del equipo de separación de red (107) de tal modo que el equipo de separación de red (107) separa el puesto de enclavamiento (109) de la red de comunicación (113).

6. Dispositivo (101, 201, 301) según la reivindicación 5, en donde el procesador (105) está configurado, cuando se detecta el comando de prueba en el marco de la verificación del tráfico de red entrante leído, para enviar un mensaje de éxito al equipo de alimentación de comandos (303) de que se ha detectado el comando de prueba, en donde el equipo de alimentación de comandos (303) está configurado para controlar el equipo de separación de red (107) en ausencia de un mensaje de éxito después de la alimentación del comando de prueba de tal modo que el equipo de separación de red (107) separa el puesto de enclavamiento (109) de la red de comunicación (113).

7. Procedimiento para monitorizar un tráfico de red entrante en un puesto de enclavamiento (109) de una instalación de servicio ferroviario a través de una red de comunicación (113),

caracterizado por

las siguientes etapas:

leer (401) el tráfico de red entrante a través de la red de comunicación (113) en el puesto de enclavamiento (109),

verificar (403) el tráfico de red entrante leído y

separar (405) el puesto de enclavamiento (109) de la red de comunicación (113) basándose en un resultado de la verificación del tráfico de red entrante leído,

en donde un procesador (105) para verificar el tráfico de red entrante leído comprueba que no haya comandos no permitidos en un flujo de comandos incluido en el tráfico de red entrante leído, y cuando se detecta un comando no permitido, controla un equipo de separación de red (107) de tal modo que el equipo de separación de red (107) separa el puesto de enclavamiento (109) de la red de comunicación (113).

8. Procedimiento según la reivindicación 7, en donde después de una separación del puesto de enclavamiento (109) de la red de comunicación (113), el puesto de enclavamiento (109) después del transcurso de una duración de tiempo predeterminada adicional se conecta de nuevo con la red de comunicación (113).

9. Programa informático, que comprende un código de programa para llevar a cabo el procedimiento según la reivindicación 7 u 8, cuando el programa informático se ejecuta en un ordenador.

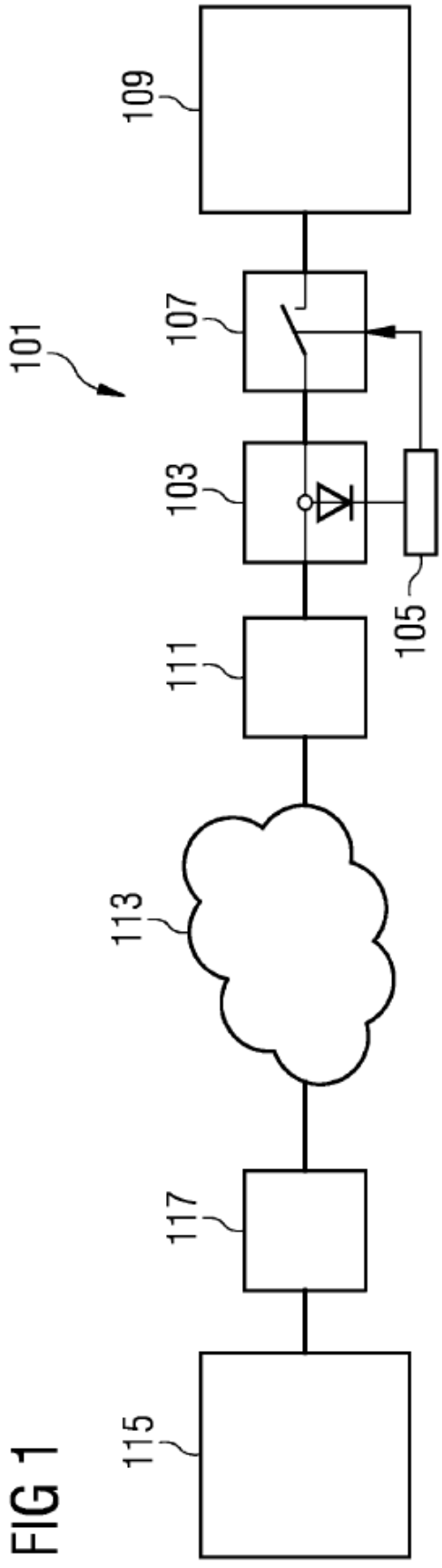

FIG 1

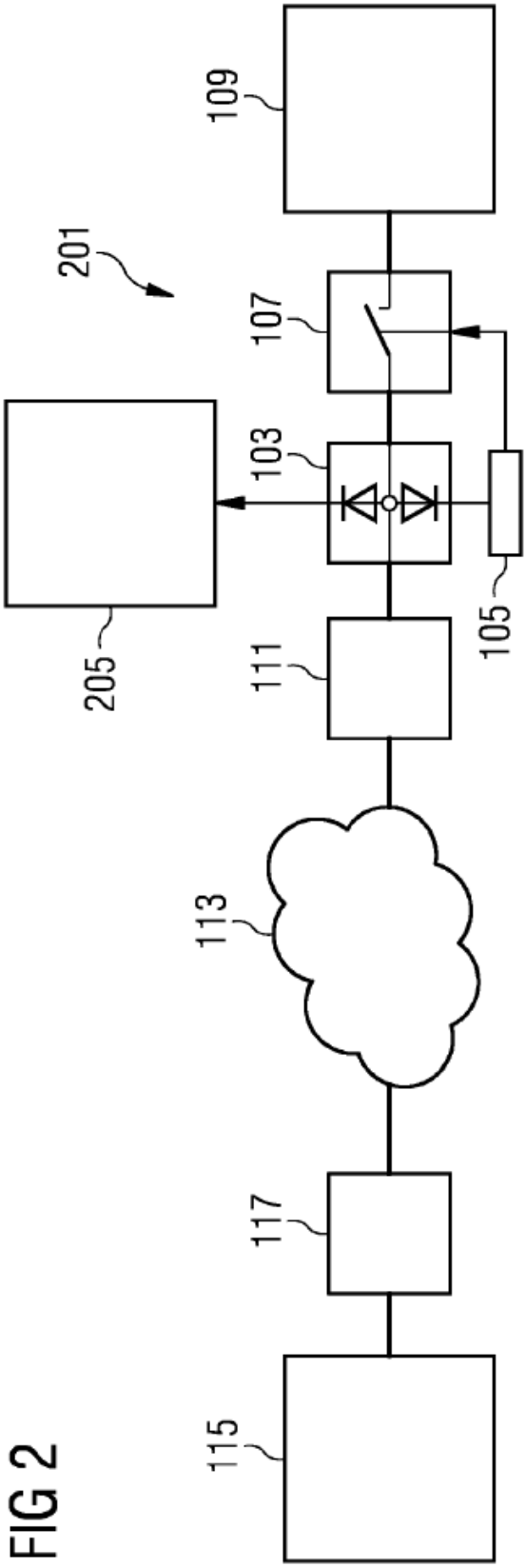

FIG 2

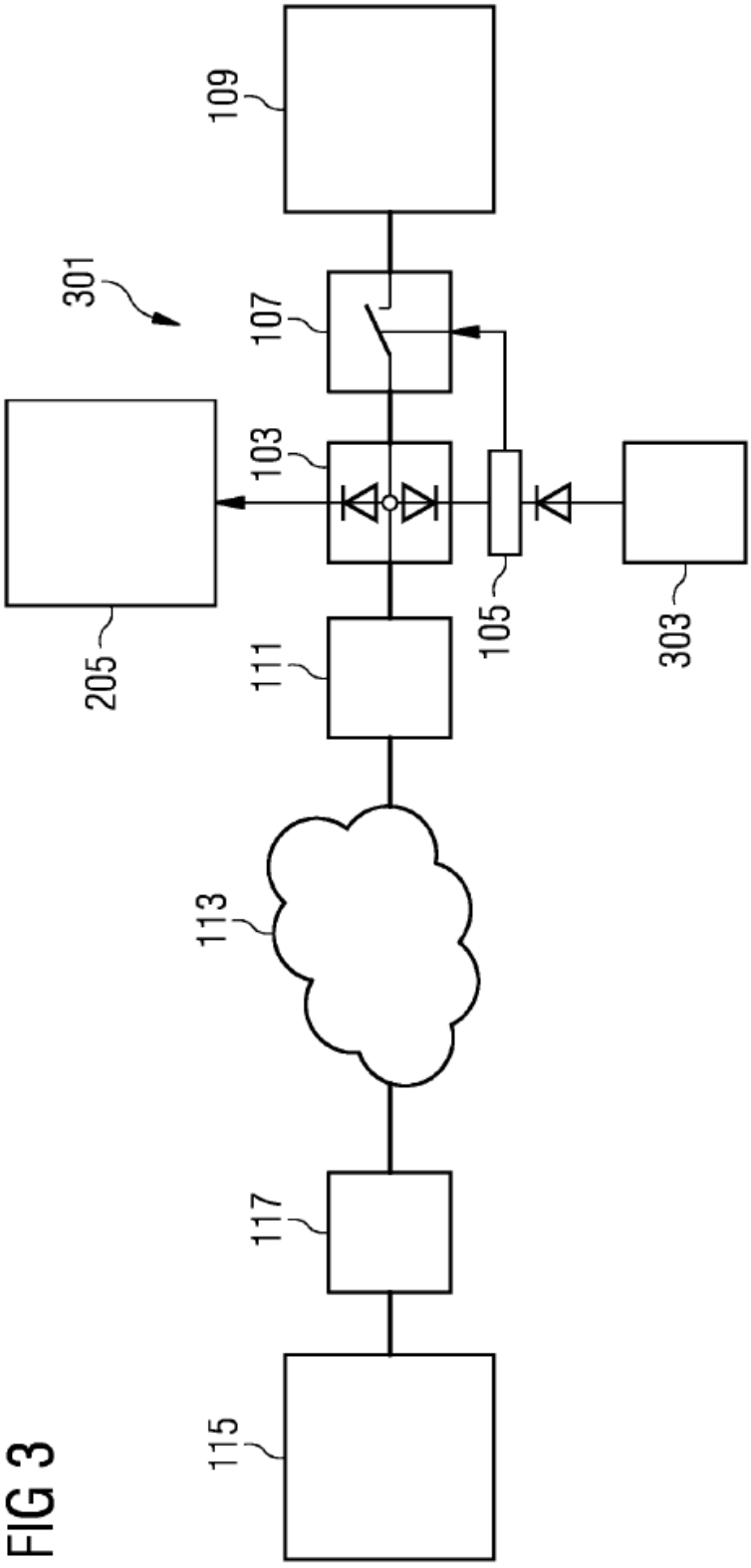

FIG 3

FIG 4