(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 845 899**

(51) Int. CI.:

B61L 15/00 (2006.01)
B61L 27/00 (2006.01)
G06F 21/00 (2013.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.12.2018 E 19217919 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.10.2020 EP 3656643**

(54) Título: **Sistemas de seguridad cibernética ferroviaria**

(30) Prioridad:

15.05.2018 US 201862671622 P
04.09.2018 US 201862726444 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.07.2021

(73) Titular/es:

CYLUS CYBER SECURITY LTD. (100.0%)
23 Yehuda Halevi, 21st Floor
6513601 Tel Aviv, IL

(72) Inventor/es:

SHMUELI, GAL;
SHIFMAN, MICHAEL y
LEVINTAL, AMIR

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Sistemas de seguridad cibernética ferroviaria

Campo

La presente invención se refiere a un sistema de seguridad cibernética y un conglomerado de seguridad cibernética, para proporcionar seguridad cibernética a un sistema ferroviario.

Antecedentes

Los primeros sistemas ferroviarios señalaban visualmente a los conductores de trenes y los trenes controlados que operaban en los sistemas utilizando dispositivos mecánicos de señalización y control para gobernar el movimiento de los trenes a lo largo de tramos fijos de vía, denominados "bloques". Cada bloque era responsabilidad de un señalizador que operaba el equipo de control y señalización para autorizar y controlar el movimiento de los trenes dentro y fuera del bloque del señalizador. Por lo general, un señalizador opera desde el punto de vista de un segundo piso de un pequeño edificio de dos pisos denominado caja de señales que era lo suficientemente alta para ofrecerle al señalizador una vigilancia visual del bloque del que era responsable. Por ejemplo, en los interruptores de las vías del ferrocarril en los que se dirigen los trenes para que avancen por diferentes vías, los interruptores de las vías y el equipo de señalización se establecieron manualmente en las posiciones requeridas por los señalizadores que accionaban palancas o manijas ubicadas en una caja de señales. Y los primeros dispositivos automáticos, "al borde del camino", eran dispositivos mecánicos que operaban por contacto físico directo con los trenes. Por ejemplo, las paradas de tren, que funcionaban para detener automáticamente un tren que pasaba si no tenía autoridad para pasar de una manzana a la siguiente, comprendían un brazo que activaba una válvula en el tren que pasaba para activar el sistema de frenos del tren y detener el tren.

Sin embargo, el crecimiento, la urbanización y la globalización de la población mundial generó la necesidad y el despliegue de sistemas ferroviarios capaces de proporcionar grandes capacidades de transporte que abarcan continentes, lo que la tecnología de control y señalización convencional más antigua no podía soportar. La llegada de los modernos procesadores digitales, sensores, sistemas de comunicaciones y sistemas globales de navegación por satélite (GNSS) han puesto a disposición tecnologías que son capaces de soportar los nuevos requisitos de los sistemas ferroviarios. Los sistemas avanzados de gestión del tráfico ferroviario (ARTMN) basados en las nuevas tecnologías que se despliegan y/o están en desarrollo en varios niveles de sofisticación proporcionan un seguimiento en tiempo real y una gestión flexible del movimiento de trenes que se adapta a los contextos operativos de los trenes. Los sistemas pueden proporcionar funcionalidades de control de trenes como Protección Automática de Trenes (ATP), Operación Automática de Trenes (ATO) y/o Supervisión Automática de Trenes (ATS) según se define en varias normas técnicas nacionales e internacionales, como por ejemplo la IEEE. 1474 o IEC 61375. Un sistema ARTMN también puede incluir la gestión y el control de las infraestructuras de las instalaciones de pasajeros, como estaciones de tren, sistemas de seguridad y alarma contra incendios, y servicios de pasajeros, como sistemas automáticos de emisión de billetes y visualización de información.

El Sistema Europeo de Gestión del Tráfico Ferroviario (ERTMS) es un ejemplo de un sistema ARTMN que es un sistema de comando, señalización y comunicación ferroviaria basado en software, adoptado por la Unión Europea como estándar para el control ferroviario. El sistema comprende un ATP conocido como Sistema Europeo de Control de Trenes (ETCS) que opera para proporcionar el cumplimiento de la operación del tren con las regulaciones de velocidad, seguridad y espaciado entre trenes; y un sistema de comunicaciones ferroviarias, denominado Sistema Global para Ferrocarriles de Comunicaciones Móviles (GSM-R), para servicios de voz y datos.

La US 2014 107 875 A1 divulga un sistema de seguridad cibernética para proporcionar seguridad a un ferrocarril, mediante el cual se detecta un ataque cibernético comparando la huella digital de al menos una red de vehículos con información de referencia.

Sumario

La presente invención se define por las características de las reivindicaciones independientes. Las modalidades preferidas de la invención se definen por las reivindicaciones dependientes.

La invención se refiere al proporcionamiento de un sistema de seguridad cibernética, en lo sucesivo también denominado "Rail-Eye", que funciona para proporcionar protección a un ferrocarril contra ataque cibernéticos.

Proporcionar protección contra un ataque cibernético puede comprender identificar un intento de perpetrar, la vulnerabilidad y/o la presencia de un ataque cibernético. La referencia a un ataque cibernético puede referirse a cualquiera o cualquier combinación de más de un intento de perpetrar, vulnerabilidad y/o ataque cibernético.

En una realización, Rail-Eye comprende un concentrador de procesamiento y monitoreo de datos, opcionalmente basado en la nube, y una red distribuida y sincronizada de agentes de recolección de datos y nodos agregadores. Los agentes de recopilación de datos que pueden denominarse "detectores cibernéticos" comprenden detectores cibernéticos de infraestructura y material rodante, "incorporado", detectores cibernéticos. Los detectores de

infraestructura se configuran para monitorear las comunicaciones generadas por y/o las operaciones del equipo de infraestructura. Los detectores incorporados se configuran para monitorear las comunicaciones generadas por y/o las operaciones de los equipos incorporados. Un detector de infraestructura y/o material rodante puede operar y proporcionar funciones de toma de red. Por conveniencia de la presentación, las comunicaciones de monitoreo y/o las operaciones de una pieza de equipo se denominan genéricamente comunicaciones de monitoreo del equipo. Los nodos agregadores, también denominados simplemente agregadores, comprenden nodos agregadores integrados y nodos agregadores de infraestructura. Los agregadores incorporados se encuentran incorporados en el material rodante, y los agregadores de infraestructura, también denominados agregadores RBC, se instalan normalmente en ubicaciones fijas en los centros de bloques de radio ferroviarios (RBC).

En una realización, la red de detectores cibernéticos, agregadores y concentrador Rail-Eye se configuran en una topología lógica jerárquica. Los detectores cibernéticos incorporados transmiten los datos que adquieren de las comunicaciones que supervisan a los nodos agregadores incorporados en mensajes de datos. Los nodos agregadores incorporados pueden reenviar los datos recibidos y/o procesados, opcionalmente para identificar la presencia de un ataque cibernético, a los agregadores de RBC. Los detectores cibernéticos de infraestructura también transmiten datos que adquieren de las comunicaciones que monitorean a los agregadores de RBC en mensajes de datos. Los agregadores de RBC, a su vez, pueden reenviar los datos tal como los reciben y/o procesan los agregadores de RBC, opcionalmente para determinar la presencia de un ataque cibernético al concentrador Rail-Eye para su almacenamiento y/o procesamiento, opcionalmente para determinar la presencia de un ataque cibernético. En una realización, el concentrador y/o un agregador que determina que se indica un ataque cibernético pueden configurarse para emprender una respuesta al ataque cibernético indicado.

De acuerdo con la invención, el sistema Rail-Eye se sincronizó con una hora de reloj de red común, opcionalmente basada en una frecuencia de referencia y en la información de temporización de la hora del día (TOD) proporcionada por las transmisiones desde un GNSS. Los datos que un detector cibernético incorporado y/o de infraestructura transmite en un mensaje de datos a un agregador pueden tener una marca de tiempo con una hora basada en la hora del reloj de la red a la que el detector cibernético recibe la comunicación monitoreada que comprende los datos. El sello de tiempo asociado con los datos que transmite un detector cibernético incorporado en un mensaje de datos puede comprender un lapso de tiempo entre el comienzo de un giro de un bus de vehículo multifuncional (MVB) comprendido en una red de comunicación de trenes (TCN) del tren en el cual se encuentra el detector cibernético incorporado.

Para facilitar el procesamiento de los datos monitoreados, de acuerdo con una realización de la divulgación, los detectores cibernéticos y/o los nodos agregadores en el sistema Rail-Eye pueden ser provistos con algoritmos configurados para generar mensajes de datos en respuesta a los diferentes tipos de comunicaciones que pueden monitorear. de acuerdo con un protocolo común de relator de Rail-Eye.

En una realización, para minimizar la interferencia que un detector cibernético o un agregador puede tener en el funcionamiento del equipo incorporado y/o de infraestructura, el detector cibernético y/o el agregador pueden operar en un modo sigiloso en el que el detector cibernético y/o el agregador cumplen con las normas que rigen la interferencia con el funcionamiento de equipos ferroviarios. A modo de ejemplo, un detector cibernético que supervisa un dispositivo incorporado o de infraestructura puede configurarse para adquirir datos del dispositivo durante los períodos de inactividad del dispositivo. Para aumentar el funcionamiento sigiloso y reducir el ancho de banda que la actividad de los detectores cibernéticos y agregadores requiere para la transmisión de datos, un protocolo de relator de acuerdo con una realización puede comprimir datos que configura para su transmisión en mensajes de datos.

En una realización, Rail-Eye mantiene una base de datos de referencia, en lo sucesivo también denominada "base de datos anónima" (ANDAT), de registros de eventos anómalos que están asociados con, o han estado bajo sospecha de estar asociados con, un ataque cibernético y han sido procesados para eliminar u ocultar elementos de información que podrían permitir la identificación de un objetivo del ataque cibernético. Los registros de eventos almacenados en la base de datos anonimizada que se han procesado para eliminar u ocultar la información de identificación del objetivo pueden denominarse registros de eventos anonimizados y un evento para el que se generó un registro de eventos anonimizados puede denominarse evento anonimizado. En una realización, la base de datos anonimizada se configura para permitir que entidades distintas de una entidad determinada que fue el objetivo de un ataque cibernético asociado con un registro de eventos anonimizado accedan al registro de eventos anonimizados, por ejemplo, con fines de análisis, sin poder identificar la entidad objetivo dada a partir de los datos de la base de datos.

Este sumario se proporciona para presentar una selección de conceptos en una forma simplificada que se describen más adelante en la Descripción detallada. Este sumario no pretende identificar características clave o características esenciales del tema reclamado, ni está destinado a limitar el ámbito del tema reclamado

Breve descripción de las figuras

A continuación, se describen ejemplos no limitantes de realizaciones de la invención con referencia a las Figuras adjuntas que se enumeran a continuación de este párrafo. Las características idénticas que aparecen en más de una figura generalmente se etiquetan con la misma etiqueta en todas las Figuras en las que aparecen. Se puede utilizar una etiqueta que etiquete un icono que representa una característica dada de una realización de la invención en una

figura para hacer referencia a la característica dada. Las dimensiones de las características que se muestran en las Figuras se eligen por conveniencia y claridad de presentación y no necesariamente se muestran a escala.

La Figura 1A muestra esquemáticamente un sistema Rail-Eye que comprende un centro de procesamiento y monitoreo de datos basado en la nube y una distribución de detectores cibernéticos que operan para proteger un sistema ferroviario de incursiones cibernéticas, de acuerdo con una realización de la divulgación;

La Figura 1B muestra esquemáticamente una imagen ampliada de una parte del sistema ferroviario mostrado en la Figura 1A, de acuerdo con una realización de la divulgación.

La Figura 2A muestra esquemáticamente un tren, componentes del tren TCN y detectores cibernéticos y agregadores conectados al TCN, de acuerdo con una realización de la divulgación.

La Figura 2B muestra esquemáticamente una locomotora del tren mostrado en la Figura 2A y detectores cibernéticos y agregadores conectados a dispositivos en la locomotora, de acuerdo con una realización de la divulgación.

La Figura 2C muestra esquemáticamente un vagón del tren mostrado en la Figura 2A y detectores cibernéticos y agregadores conectados a dispositivos en el vagón, de acuerdo con una realización de la divulgación.

La Figura 3 muestra esquemáticamente una pluralidad de tres sistemas Rail-Eye que cooperan para usar una base de datos común, anónima, opcionalmente basada en la nube, ANDAT, de acuerdo con una realización de la divulgación; y

La Figura 4 ilustra esquemáticamente un escenario de ejemplo en el que, Rail-Eye identifica un evento anómalo indicativo de un ataque cibernético en una parte de un ferrocarril, genera y carga en ANDAT datos anónimos relevantes para el evento anómalo, de acuerdo con una realización de la divulgación.

Descripción detallada

En la siguiente descripción detallada, los componentes de un sistema Rail-Eye que opera para proporcionar seguridad cibernética a un sistema ferroviario en un área de operaciones de trenes se analizan con referencia a las Figuras. 1A y 1B. Las Figuras 2A-2C muestran esquemáticamente los detalles de una red de comunicación de trenes (TCN) que comprende opcionalmente un bus de tren de alambre (WTB) de "ancho de tren" que abarca la longitud de un tren y se acopla a buses de vehículos multifuncionales (MVB), cada uno de los cuales admite comunicaciones para dispositivos incorporados en un solo vagón del tren. La colocación y el funcionamiento de los detectores cibernéticos incorporados y los agregadores incorporados ubicados en el tren de acuerdo con una realización de la divulgación se describen con referencia a las figuras.

En la discusión, a menos que se indique lo contrario, se entiende que adjetivos como "sustancialmente" y "acerca de" modificar una condición o relación característica de una característica o características de una realización de la divulgación, significan que la condición o característica se define dentro de las tolerancias que son aceptables para el funcionamiento de la realización para una aplicación para la que está destinada la realización. A menos que se indique lo contrario, la palabra "o" en la descripción y las reivindicaciones se considera que es inclusiva "o" en lugar de exclusiva o, e indica al menos uno de, o cualquier combinación de elementos que une.

La Figura 1A muestra esquemáticamente una vista en perspectiva del sistema Rail-Eye 20, que funciona para proporcionar protección cibernética a un sistema ferroviario 200, de acuerdo con una realización de la divulgación. La Figura 1B muestra esquemáticamente una parte ampliada del sistema ferroviario 200 y Rail-Eye 20, de acuerdo con una realización de la divulgación.

El sistema ferroviario 200 comprende una infraestructura de vías 202 a lo largo de las cuales se mueven los trenes 300 para transportar pasajeros y mercancías, y equipos de infraestructura que cooperan para controlar el movimiento de los trenes en un área de operaciones representada esquemáticamente por un rectángulo 204 punteado. El equipo de infraestructura comprende interruptores (no mostrados) en los cruces 206 de las vías, aparatos de señalización representados por el equipo 208 de señales de luz de color a lo largo de las vías y en los cruces 206 y cruces 207 de las vías, sistemas de enclavamiento 210 en los cruces de las vías, balizas 218 en la vía, RBC 230, cada uno representado por una casa y una torre de antena de radio, y estaciones de tren representadas por grupos de iconos humanos 260.

Un aparato de señalización 208 denominado convencionalmente "señal" es un dispositivo de vía, típicamente un dispositivo de luz de color como se muestra esquemáticamente en la Figura 1A, operable para transmitir visualmente a un conductor de tren por el color de las luces que muestra la señal, información relacionada con el estado de la vía por delante de un tren que conduce el maquinista. Por ejemplo, una señal 208 podría informar al maquinista de la velocidad a la que el tren puede avanzar de forma segura o, si la vía delante del tren está ocupada por otro tren, indicar al maquinista que detenga el tren. Un sistema de enclavamiento 210, al que se hace referencia convencionalmente como "enclavamiento", controla la señalización y los conmutadores en un cruce de vías 206 para evitar movimientos conflictivos y proporcionar un paso seguro de trenes a través del cruce. Una baliza 218, como la baliza europea

utilizada por el ERTMS, es una baliza electrónica pasiva montada en una traviesa de vía entre los rieles de una vía. La baliza recibe energía de un tren que pasa sobre la baliza y usa la energía para transmitir información al tren a través de una señal conocida como telegrama. El telegrama generalmente comprende una identificación única de la baliza y, por lo tanto, la ubicación del tren a medida que pasa sobre la baliza, límites de velocidad, pendientes, y si la baliza es una baliza denominada baliza transparente, se puede operar para proporcionar autoridad de movimiento.

Un centro de bloque de radio, RBC 230, es un centro de control de radio que se comunica con los trenes 300 y el equipo de infraestructura a través de un sistema de comunicaciones ferroviarias, como GSM-R, en un área denominada área de control de RBC para la cual el RBC tiene radio cobertura y es responsable de la operación segura de los trenes. A modo de ejemplo, las áreas de control para dos glóbulos rojos adyacentes 230 se indican esquemáticamente mediante límites hexagonales discontinuos 231. Un RBC 230 recibe datos relevantes para el estado y la ubicación de los trenes 300 en el área de control 231 del RBC a través de transmisiones de radio GSM-R de los trenes y datos relevantes para el estado de los equipos de infraestructura, tales como enclavamientos 210 en el área de control de RBC 231 vía cable. y/o comunicación por radio. El RBC procesa los datos y la información recibidos para formular y transmitir las autoridades de movimiento a los trenes 300 y los datos a los enclavamientos 210 para que los utilicen los enclavamientos para controlar la señalización y la conmutación en los cruces de vía 206 en los que se encuentran respectivamente los enclavamientos. Las autoridades de movimiento que un RBC genera y transmite a los trenes están determinadas a proporcionar distancias entre trenes que mantengan los intervalos seguros (distancias entre trenes y próximos trenes) y, en general, también una capacidad de transporte ventajosa.

Los trenes 300 comprenden una locomotora 310 y opcionalmente uno o más vehículos 330 de tren, también denominados coches 330. Las imágenes ampliadas y los detalles de un tren 300, una locomotora 310 y un vagón 330 se muestran esquemáticamente en las Figuras. 2A y 2B y 2C respectivamente. Generalmente, un tren 300 tiene una red de comunicaciones de trenes, TCN 331 (Figuras. 1B, 2A-2C), que comprende un bus de todo el tren, WTB 336, que recorre la longitud del tren, y para cada vagón 330 y locomotora 310, un bus 332 MVB conectado al WTB por una pasarela 334 de vehículos de tren. El MVB 332 en un vagón 330 o locomotora 310 dados admite comunicaciones entre y con dispositivos incorporados, referenciados genéricamente en las Figuras. 2A-2C por la etiqueta 360 (Figuras. 2A-2C), en el vagón o locomotora. Por ejemplo, en un vagón de tren 330, los actuadores de control de puertas, el aire acondicionado, la iluminación y los dispositivos de información para los pasajeros se conectan al MVB 332. Las transmisiones sobre MVB 332 por dispositivos 360 conectados a MVB 332 son controladas por al menos un bus maestro 335 que controla el acceso al MVB 332 durante periodos de tiempo secuenciales denominados turnos. El WTB 336 admite comunicaciones entre los coches 330 y entre los coches 330 y la locomotora 310. El aparato de control de freno 362 (Figura 2C) en cada vagón 330 y locomotora 310 está típicamente conectado directamente a WTB de modo que la aplicación y liberación de los frenos en el tren 300 pueden sincronizarse adecuadamente. La locomotora 310 comprende típicamente un módulo de comunicación 312 (Figura 1B) que tiene un extremo frontal adecuado y una antena que admite comunicaciones GSM-R con RBC 230 (Figuras 1A y 1B) y equipo en tierra, un receptor GSNS (Sistema de navegación por satélite global) 313 y un lector de balizas 314 (Figuras 2A, 2B) configurado para interactuar con balizas 218 (Figuras 1A, 1B).

La locomotora tiene el mandato de incluir un registrador de eventos, que, en los sistemas europeos de control de trenes, ETCS, es una Unidad de Registro Jurídico (JRU). El registrador de eventos o JRU, en lo sucesivo denominado genéricamente JRU, es un registrador de "caja negra" de material rodante, que recibe y almacena datos relevantes para eventos de interés específico que pueden ocurrir durante la operación del tren 300 para facilitar el análisis del comportamiento del tren y accidentes en los que pueda verse involucrado el tren. El ERTMS ha definido un conjunto de eventos específicos, en lo sucesivo también denominados eventos JRU, que desencadenan la transmisión a la JRU de datos relevantes para los eventos en paquetes de mensajes formateados, denominados mensajes de datos JRU que identifican los eventos. Un mensaje de datos de JRU asociado con un evento de JRU dado incluye la fecha y hora en que ocurrió en UTC del evento y otros elementos de información que identifican el evento de JRU. Se proporciona una lista de eventos JRU en una especificación de interfaz funcional (FIS) ERTMS/ETCS titulada Registro jurídico FIS.

El sistema Rail-Eye 20 comprende opcionalmente un concentrador 22 de monitorización y procesamiento de datos (Figura 1A y 1B), que puede, como se muestra en las Figuras. 1A y 1B, estar basado en la nube, y una red de detectores cibernéticos incorporados representados esquemáticamente por iconos 32 con forma de diamante, y nodos 34 de agregadores incorporados representados esquemáticamente por iconos de forma hexagonal, ubicados en los trenes 300. Por conveniencia de presentación, en las Figuras. 1A y 1B, para adaptarse a las limitaciones de tamaño de las imágenes que se muestran en las figuras, los detectores cibernéticos 32 y los agregadores incorporados 34 se muestran sobre o sobre las imágenes de los trenes 300, y un solo detector cibernético incorporado 32 y/o agregador incorporado 34 asociado con un tren 300 o parte de un tren 300 en las Figuras. 1A y 1B representan uno o más detectores cibernéticos y/o uno o más agregadores integrados, respectivamente. Las Figuras 2A-2C muestran esquemáticamente los detalles que se discuten a continuación de las posibles ubicaciones de los detectores cibernéticos incorporados 32 y los agregadores incorporados 34 en un tren 300 y cómo pueden conectarse al TCN 331 del tren (Figura 1B, 2A-2C). Rail-Eye 20 también comprende detectores cibernéticos estacionarios de infraestructura, representados esquemáticamente por iconos 36, y agregadores de RBC 38 (Figuras. 1A-2C) que se comunican con los detectores cibernéticos de infraestructura. Un solo detector cibernético 36 de infraestructura y/o un solo agregador 34 de RBC mostrado en las Figuras. 1A y 1B representan uno o más de un detector cibernético y un agregador de infraestructura, respectivamente.

Los detectores cibernéticos incorporados 32 y 36 y de infraestructura, y los agregadores 34 y 38 pueden configurarse como componentes de metal desnudo separados, como se puede inferir de las Figuras. 1A-2C. Sin embargo, los detectores cibernéticos y los agregadores de acuerdo con una realización de la divulgación pueden definirse por componentes de software y hardware, o solo por componentes de software y, en general, pueden comprender cualquier combinación de componentes de software y/o hardware que respalden las funcionalidades de la cibernética. detectores y agregadores.

Por ejemplo, un detector cibernético o un agregador puede ser un módulo de hardware desnudo que comprende cualquier circuito de control y/o procesamiento electrónico y/u óptico, para proporcionar y habilitar las funcionalidades que el detector cibernético o el agregador pueden necesitar para respaldar el monitoreo o las funcionalidades de procesamiento del detector cibernético o agregador. El detector cibernético o agregador puede comprender cualquiera, o cualquier combinación de más de uno de, un microprocesador, un circuito de aplicación específica (ASIC), una matriz programable de campo (FPGA) y/o un sistema en un chip (SOC). El detector cibernético o agregador puede comprender una memoria que tenga cualquier circuito electrónico y/u óptico adecuado para almacenar datos y/o instrucciones ejecutables por computadora y puede, a modo de ejemplo, comprender cualquiera o cualquier combinación de más de una memoria flash, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM) y/o memoria de solo lectura programable y borrable (EPROM). Un detector cibernético o agregador puede ser un módulo de software comprendido en cualquiera de varios equipos incorporados y/o de infraestructura de un sistema ferroviario y puede cooperar con hardware y/o software en el equipo del sistema ferroviario para realizar las funcionalidades del detector cibernético y/o agregador. Un detector cibernético o un agregador puede ser una entidad virtual. De manera similar, el concentrador 22 tiene opcionalmente una memoria 23 y un procesador 24 configurado para soportar las funcionalidades del concentrador, puede comprender cualquier combinación de componentes de hardware y software y puede comprender o ser una entidad virtual.

Como se muestra esquemáticamente en las Figuras. 2A-2C, los detectores cibernéticos incorporados 32 y los agregadores incorporados 34 pueden acoplarse a diferentes equipos incorporados en un tren 300 para monitorear las comunicaciones generadas por los dispositivos en el tren y transmitir datos desde las comunicaciones monitoreadas al agregador incorporado 34 del tren para su reenvío a un RBC 230 y/o concentrador 22 para procesamiento y opcionalmente almacenamiento. Y un detector cibernético 32 puede acoplarse de diferentes formas a un dispositivo 360 en el tren 300 y al TCN 331 del tren para adquirir y enviar los datos.

Por ejemplo, un detector cibernético incorporado 32 distinguido por una etiqueta 32-1 ubicada en un vagón 330 (Figura 2C) puede acoplarse directamente a un dispositivo 360 en el vagón para monitorear las comunicaciones generadas por el dispositivo. El detector cibernético 32-1 puede acoplarse a un puerto (no mostrado) del dispositivo 360 para monitorear las comunicaciones propagadas a través del puerto o a un procesador (no mostrado) incluido en el dispositivo para monitorear la actividad del procesador. El detector cibernético 32-1 opcionalmente no está conectado directamente al TCN 331 mediante una conexión a MVB 332 y puede configurarse para usar una conexión que el dispositivo 360 tiene a MVB 332 para transmitir los datos adquiridos de las comunicaciones o actividades monitoreadas al MVB y desde allí. al agregador 34 en el coche 330. Alternativa o adicionalmente, un detector cibernético 32, tal como el detector cibernético que se distingue por una etiqueta 32-2 en la Figura 2C, que monitorea un dispositivo 360 en el vagón 330 puede acoplarse directamente a MVB 332 para transmitir datos al TCN 331 conmutador cibernético 32-2 adquiere de comunicaciones monitoreadas. Un agregador incorporado 34 en la cabina 330 puede estar conectado a MVB 332 para recibir y agregar datos comprendidos en mensajes de datos transmitidos por detectores cibernéticos 32-1 y 32-2 para su reenvío y procesamiento. El agregador incorporado 34 puede procesar los datos agregados para determinar la posible presencia de un ataque cibernético y reenviar datos agregados y/o datos agregados procesados para entrenar la puerta de enlace 334 del vehículo para su transmisión a través de WTB 336 a la locomotora 310 y reenvío por comunicación GSM-R a un RBC 230. Un agregador incorporado, tal como el agregador 34 comprendido en la locomotora 310 mostrada esquemáticamente en la Figura 2B, puede recibir mensajes de datos generados por un detector cibernético distinguido por una etiqueta 32-3 que monitorea WTB 336.

En una realización, para reducir el uso de ancho de banda y la posible interferencia que la actividad de los detectores cibernéticos 32 y 36 y los agregadores 34 y 38 pueden tener en las operaciones de los equipos incorporados y/o de infraestructura del sistema ferroviario 200, un detector cibernético y/o agregador puede comprimir los datos que recibe para su transmisión en un mensaje de datos y/o procesamiento. Opcionalmente, para facilitar el procesamiento de los datos incluidos en los mensajes de datos que los detectores cibernéticos y los agregadores incluidos en Rail-Eye 20 generan y transmiten, los mensajes de datos pueden configurarse de acuerdo con un protocolo común de relator de Rail-Eye. En una realización, un mensaje de datos configurado de acuerdo con el protocolo del relator Rail-Eye puede comprender un campo de mensaje que codifica un vector de ponderación que tiene componentes que indican el grado de relevancia de los datos para diferentes aspectos operativos del sistema ferroviario. El vector de ponderación para un mensaje de datos generado por un agregador de detectores cibernéticos puede, por ejemplo, indicar qué tan relevantes pueden ser los datos para la seguridad de la operación del material rodante y/o equipo de infraestructura, proporcionar un marco de tiempo deseado y/o prioridad para procesar los datos., y/o que se debería dar una alarma para indicar que se recomienda la intervención humana. La ponderación puede depender del contexto.

Los componentes Rail-Eye 20 se sincronizan opcionalmente con un mismo reloj de red representado esquemáticamente por un reloj 25 que genera una frecuencia de referencia y TOD basado en información de temporización y señales TOD recibidas de un sistema GNSS representado esquemáticamente por satélites 50. Los

detectores cibernéticos y los agregadores pueden marcar la fecha y hora de los datos que adquieren con las horas del reloj de la red en las que adquieren los datos. En una realización, el sistema Rail-Eye se sincronizó con una hora de reloj de red común, opcionalmente basada en una frecuencia de referencia y la información de tiempo del día (TOD) proporcionada por las transmisiones desde un GNSS. Como se indicó anteriormente, las transmisiones sobre MVB 332 por dispositivos conectados a MVB son controladas por al menos un bus maestro 335 que controla el acceso a MVB 332 durante turnos de períodos de tiempo secuenciales. En una realización, un detector incorporado 32 puede marcar la fecha y hora de los datos que adquiere de un dispositivo incorporado 360 con un lapso de tiempo, también conocido como lapso de "tiempo de turno", entre un momento en el que el detector cibernético adquirió los datos y un comienzo de un turno durante el cual se adquirieron los datos. Un agregador incorporado y/o RBC, una pasarela de vehículos de tren y/o un concentrador 22 que recibe los datos pueden determinar cuándo se adquirieron los datos en relación con el tiempo de la red utilizando el lapso de tiempo de turno.

En una realización, como se indica en las Figuras 1A y 1B, la red de detectores cibernéticos 32 y 34, los agregadores 36 y 38 y el concentrador Rail-Eye 20 se configuran en una topología lógica jerárquica. Los detectores incorporados 32 transmiten mensajes de datos a los agregadores incorporados 34 para su procesamiento y/o reenvío a los agregadores 38 de RBC. Los agregadores incorporados 34, los detectores 34 de infraestructura y, opcionalmente, los detectores incorporados 32, transmiten datos a los agregadores 38 RBC para su procesamiento. Los agregadores de RBC 38, a su vez, transmiten los datos que reciben y/o han procesado al concentrador Rail-Eye 22 para su procesamiento.

Opcionalmente, Rail-Eye 20 se configura para procesar los datos adquiridos por los detectores cibernéticos incorporados 32 y 34 y de la infraestructura en "capas" homomórficas a la topología de red jerárquica para determinar la presencia de un posible ataque cibernético.

Los agregadores incorporados 34 pueden configurarse para identificar eventos anómalos en respuesta a los datos que reciben y agregar de los detectores incorporados 32 en los respectivos trenes 300 en los que están ubicados los agregadores incorporados. En una realización, un agregador incorporado 34 puede determinar un contexto de tren operativo para el tren. en el que se encuentra el agregador incorporado, e identificar eventos anómalos según el contexto del tren. Un contexto de tren puede comprender, a modo de ejemplo, al menos uno o cualquier combinación de más de uno de velocidad del tren, condiciones de la vía, congestión del tráfico, condiciones climáticas ambientales, carga de pasajeros o mercancías, número de vagones en el tren, número de locomotoras en el tren y especificaciones de locomotoras y vagones. Opcionalmente, al identificar una indicación de un ataque cibernético, el agregador incorporado 34 puede funcionar para emprender una respuesta al ataque.

Por ejemplo, en una realización, los detectores cibernéticos 32 en un vagón 330 de un tren 300 pueden monitorear los dispositivos 360 que controlan las puertas del vagón y generar y transmitir a un agregador incorporado 34 en el vagón mensajes de datos que comprenden datos que indican el estado de las puertas. El agregador incorporado 34 en el vagón que recibe los mensajes de datos puede determinar un contexto operativo para el tren que comprende valores en base a la velocidad y la ubicación del tren para los momentos en los que las marcas de tiempo en los mensajes de datos indican que los datos de estado fueron adquiridos por los detectores cibernéticos. Para una situación en la que los mensajes de datos de los detectores cibernéticos 32 indican que las puertas del vagón 330 están abiertas, el agregador 34 puede generar y transmitir a un agregador de RBC 38 (Figura 1B) un mensaje de datos para el cual un vector de ponderación tiene un valor muy grande de peso para cada uno de la seguridad operacional y la anomalía indicativo de un posible ataque cibernético si el tren 300 transporta pasajeros entre estaciones de tren. Las magnitudes de los pesos grandes pueden depender de la velocidad y/o ubicación del tren indicadas por el contexto operativo del tren. Opcionalmente, el agregador incorporado 34 puede configurarse para responder a la situación en función de las magnitudes de los pesos de seguridad y anomalías. Por ejemplo, si el peso del vector de ponderación para la seguridad operacional o la anomalía excede un umbral predeterminado, el agregador 34 puede generar un aviso de alarma para un conductor del tren y/o el agregador de RBC 38. Por otro lado, los pesos para la seguridad operativa y la anomalía pueden ser relativamente bajos si el contexto del tren determinado por el agregador 34 indica que el vagón 330 está vacío de pasajeros o el tren está en un patio de trenes.

A modo de otro ejemplo, un detector cibernético incorporado 32 se puede acoplar al WTB 336 y una salida de la pasarela 334 del vehículo del tren. El detector cibernético puede generar y transmitir mensajes de datos a un agregador incorporado 34 en respuesta a demoras de tiempo entre la puerta de enlace que recibe una comunicación a través de WTB 336 para activar o liberar los frenos en el vagón y un momento en el que la puerta de enlace transmite una señal de activación correspondiente a los frenos. Si el tiempo de demora excede un máximo predeterminado, podría ser que el detector cibernético pueda determinar la presencia de una anomalía que indique un posible ataque cibernético.

Los agregadores de RBC 38 pueden configurarse para identificar eventos anómalos que indiquen un posible ataque cibernético en respuesta a los datos que los agregadores de RBC 38 reciben de los detectores de infraestructura 34 y los detectores incorporados 32 y/o agregadores incorporados 34 ubicados en las respectivas áreas de control 231 (Figura 1) de los RBC 230 en los que se encuentran los agregadores de RBC. Un agregador de RBC 38 puede configurarse para determinar un contexto de área de control de RBC para material rodante y/o equipo de infraestructura en su área de control 231 e identificar eventos anómalos, opcionalmente basándose en el contexto de RBC. Un contexto de área de control de RBC puede comprender al menos una o cualquier combinación de más de una de las medidas relacionadas con las condiciones de la vía, como el estado de reparación y adherencia de la

cabeza del carril, las condiciones meteorológicas, como la visibilidad y la precipitación, y el estado del material rodante, como como congestión y tipos de material rodante en movimiento en una zona de control 231 de un RBC 230. Un contexto de área de control también puede comprender la demanda de transporte ferroviario de los clientes, como lo demuestra el número de personas físicamente presentes en las estaciones de ferrocarril y/o la compra de boletos para viajar en tren en el área de control de RBC. Opcionalmente, un agregador de RBC 38 puede configurarse para emprender una respuesta a un posible ataque cibernético identificado.

Por ejemplo, situaciones anómalas en un solo tren 300, tales como estados de puerta anómalos o retrasos de tiempo discutidos anteriormente con respecto a un tren 300, pueden deberse a un mal funcionamiento del dispositivo en el tren más que a un ataque cibernético. Sin embargo, en una realización, un agregador de RBC 38 se configura para correlacionar mensajes de datos de diferentes detectores cibernéticos incorporados y de infraestructura en un área de control 231 de RBC 230 con el que está asociado el agregador de RBC 38. Si el agregador de RBC recibe datos de agregadores incorporados 34 que informan anomalías similares en el estado de la puerta o retrasos de tiempo para una pluralidad de trenes 300 diferentes en el área de control 231 de RBC 230, el agregador de RBC puede correlacionar los datos para determinar con mayor confiabilidad que los datos son indicativo de un ataque cibernético.

A modo de otro ejemplo, en una realización, un agregador de RBC 38 puede determinar que un ataque cibernético posiblemente esté presente en respuesta a los mensajes de datos recibidos de los ataques cibernéticos 36 de la infraestructura que monitorean las luces de señal 208, las balizas 218 y los enclavamientos 210 en una intersección de pistas 206 (Figura 1B). Por ejemplo, el control de interruptores y señales 208 en una intersección de vías 206 en un área de control 231 (Figura 1B) de un RBC 230 para permitir que los trenes se muevan a través de la intersección de manera segura generalmente implica una coreografía cuidadosamente cronometrada de señales y eventos orquestados por el RBC en cooperación con un enclavamiento 210 ubicado en la intersección. Los trenes 300 que se acercan y salen de un vecindario de la intersección informan sus ubicaciones basándose en telegramas de baliza y/o ubicaciones GNNS a través de GSM-R a RBC 230. Basándose en la información de ubicación y un parámetro de contexto del área de control del RBC, como la congestión del tren, el RBC determina las autorizaciones de movimiento para los trenes y las secuencias de control correspondientes para el interruptor y la señal 208 que se mediarán mediante el enclavamiento 210 para permitir el paso seguro de un tren a través de la intersección. Para el paso de un tren 300 dado a través de la intersección, el agregador de RBC 38 puede procesar mensajes de datos recibidos de los detectores cibernéticos incorporados 32 a través de un agregador incorporado 34 en el tren y el equipo de monitoreo de los detectores cibernéticos 36 en el tren se comporta con un escenario normativo de señalización y movimiento de un tren a través de la intersección. Si los eventos asociados con el paso del tren no se corresponden con un escenario normativo, el agregador de RBC 38 puede determinar que se indica la presencia de un posible ataque cibernético. Los escenarios normativos para su uso por el agregador de RBC pueden almacenarse en una base de datos (no mostrada) incluida en el agregador de RBC o en una base de datos, por ejemplo, la base de datos 23 incluida en el concentrador 22, a la que tiene acceso el agregador de RBC.

El concentrador Rail-Eye 22 puede operar para identificar eventos anómalos que indiquen un posible ataque cibernético en respuesta a los datos que el concentrador recibe de los ataques cibernéticos 32 y 34 y de los agregadores 36 y 38 en el área geográfica 204 de operaciones ferroviarias en cuyo sistema ferroviario 200 para el cual Rail- Eye 20 es el responsable de las operaciones. Opcionalmente, el concentrador 22 se configura para generar un contexto de sistema para las operaciones del sistema ferroviario en el área 204 de operaciones ferroviarias e identificar eventos anómalos que indiquen un posible ataque cibernético basado en el contexto del sistema. Un contexto de sistema puede comprender al menos uno o cualquier combinación de más de uno de hora del día, temporada, feriado, eventos especiales en el área de operaciones, clima y/o estado de una red eléctrica que suministra energía al sistema ferroviario 200. En una realización, el concentrador 22 puede configurarse para identificar, basándose en los datos que recibe el concentrador, eventos anómalos indicativos de un posible ataque cibernético en un tren dado 300, en un área de control de RBC dada 231, así como un posible sistema: amplio ataque cibernético en el área de operaciones ferroviarias 204 del sistema ferroviario 200. El Hub 22 puede configurarse para responder a un posible ataque cibernético identificado.

Como en el caso de un agregador de RBC 38 que puede correlacionar los datos recibidos de una pluralidad de trenes en un área de control del RBC 230 del agregador para mejorar la confiabilidad de la identificación de un posible ataque cibernético, el concentrador 22 puede operar para correlacionar los datos recibidos de una pluralidad de agregadores 38 de RBC para mejorar la fiabilidad de una identificación de un ataque cibernético. Por ejemplo, como en el caso de un mal funcionamiento del equipo incorporado de un tren que da lugar a la sospecha de un ataque cibernético, el mal funcionamiento y/o las condiciones meteorológicas pueden afectar el funcionamiento del equipo de vía y/o un RBC 230 y dar lugar al agregador de RBC 38 determina que existe una sospecha de un ataque cibernético. Al correlacionar los datos recibidos de una pluralidad de agregadores de RBC 38, el concentrador 22 puede mejorar la fiabilidad de una determinación de que la sospecha se debe a un ataque cibernético real.

A modo de otro ejemplo, en una realización del centro de divulgación 22 puede configurarse para determinar patrones normativos geográficos y/o temporales para la actividad del sistema ferroviario 200 en el área de operaciones ferroviarias 204 y almacenar los patrones normativos en la memoria 23 del centro. El centro puede comparar patrones de actividad en tiempo real del sistema ferroviario en base a los datos que recibe en mensajes de datos de ataque cibernéticos y agregadores con patrones normativos para determinar si existe un ataque cibernético. Por ejemplo, la actividad del sistema ferroviario 200 puede exhibir patrones normativos de actividad diurna, mensual y/o estacional y

si un patrón de actividad en tiempo real difiere de un patrón normativo, el centro 22 puede determinar que la diferencia indica la presencia de un ataque cibernético.

A modo de ejemplo específico, el tráfico ferroviario de pasajeros normativo en una región suburbana determinada de un área de control de RBC particular 231 puede ser alto por la mañana, ya que la gente de la región suburbana viaja para trabajar en una metrópolis en otra área de control de RBC, que disminuye durante al final de la mañana y al principio de la tarde y aumenta de nuevo hacia la noche a medida que la gente regresa del trabajo. Se espera que las velocidades y los avances normativos de los trenes en la región suburbana dada se correlacionen con el tráfico. Se puede esperar que las velocidades de los trenes sean altas y los avances relativamente cortos durante las horas de la mañana y al final de la tarde para proporcionar una capacidad ventajosa para atender el tráfico pesado de pasajeros. Se espera que las velocidades de los trenes sean respectivamente relativamente bajas y largas distancias durante las últimas horas de la mañana y las primeras horas de la tarde cuando el tráfico es relativamente ligero. Si los datos procesados por el concentrador 22 indican que las magnitudes de las velocidades y/o los avances del tren en tiempo real varían de las magnitudes de las velocidades y los avances normativos del tren, respectivamente, o están desfasados con el tráfico de pasajeros, el concentrador 22 puede determinar que existe un ataque cibernético.

Un sistema Rail-Eye de acuerdo con una realización de la divulgación puede comprender y/o tener acceso a una base de datos anónima (ANDAT), en la que se pueden almacenar datos relevantes para un ataque cibernético que un ferrocarril determinado ha encontrado, de modo que los datos pueden ser accesibles a otros ferrocarriles, pero no se asocian fácilmente con el ferrocarril dado. Los datos de ataque cibernéticos que no se asocian fácilmente con un ferrocarril determinado pueden denominarse datos anónimos. Los datos anonimizados pueden cargarse en ANDAT después de que los datos hayan sido procesados para anonimizar los datos o cargados y almacenados en ANDAT antes de la anonimización y procesados para ser anonimizados antes de ser descargados por una entidad autorizada para acceder a los datos en ANDAT. Al permitir el intercambio de datos de ataque cibernéticos entre los ferrocarriles que cooperan y que tienen acceso a ANDAT, ANDAT proporciona a los ferrocarriles que utilizan la base de datos acceso a una mayor cantidad de datos de ataque cibernéticos de los que normalmente estaría disponible para un solo ferrocarril. Como resultado, un ferrocarril, utilizando la base de datos de ANDAT, puede generar un análisis mejorado de los ataques cibernéticos para su propio uso a fin de reforzar su capacidad para detectar y contrarrestar ataques cibernéticos. La anonimización de los datos de ataque cibernéticos hace que sea más difícil para un ciberdelincuente analizar los datos para identificar y explotar las vulnerabilidades cibernéticas de ferrocarriles particulares que utilizan ANDAT.

La Figura 3 muestra esquemáticamente una pluralidad de opcionalmente tres sistemas Rail-Eye 121, 122 y 123, que operan para proteger los ferrocarriles 131, 132, 133 respectivamente y cooperan para usar un ANDAT 100 común, opcionalmente basado en la nube, en el que cada uno de los sistemas Rail-Eye que cooperan pueden almacenar y/o recibir datos de ataque cibernéticos anónimos relacionados con escenarios de ataque cibernéticos que Rail-Eye ha encontrado. Se supone que cada Rail-Eye, a modo de ejemplo, comprende componentes similares a los del Rail-Eye 20 (Figura 1A), y además tiene un anonimizador 102 que se comprendió en, o que se comunica con el concentrador 22 del Rail-Eye. En la Figura 3, los anonimizadores 102 se muestran, a modo de ejemplo, configurados para comunicarse con sus respectivos concentradores 22 pero separados de ellos. Una pluralidad de sistemas Rail-Eye que cooperan de acuerdo con una realización, tales como los sistemas Rail-Eye 121, 122 y 123, pueden denominarse conglomerado Rail-Eye.

Un anonimizador 102 funciona para "eliminar" elementos de información de los datos que un sistema Rail-Eye 121, 122 o 123 carga para su almacenamiento en ANDAT 100 o descarga desde ANDAT, de modo que los datos no puedan asociarse fácilmente con uno determinado de los sistemas Rail-Eye 121, 122 o 123 o los ferrocarriles que protegen. Para facilitar la presentación, se asume que un anonimizador borra los datos de ataque cibernéticos de su Rail-Eye asociado antes de que Rail-Eye cargue los datos. La depuración puede implicar eliminar, encriptar o disfrazar, genéricamente, encriptar, elementos de información de datos relacionados con un ataque cibernético para aumentar la dificultad de asociar los datos del ataque cibernético con un Rail-Eye en particular o un ferrocarril que el Rail- Eye protege, que se encontró con el ataque cibernético. Mientras que la limpieza de información de acuerdo con la realización funciona para cifrar elementos de información, generalmente está restringida a mantener la integridad de la información relevante para determinar si un evento anómalo indica un ataque cibernético y/o es relevante para identificar ataques cibernéticos que pueden estar indicados por eventos anómalos similares.

Por ejemplo, las comunicaciones ERTMS/ETCS se basan en variables, paquetes y mensajes que están anidados, definidos y configurados de acuerdo con sintaxis específicas; las variables ERTMS/ETCS se utilizan para codificar valores de datos individuales. Los paquetes ERTMS/ETCS pueden incluir más de una variable y comprenden un encabezado que identifica el paquete por un número de tipo de paquete único, denominado paquete NID. El encabezado puede incluir variables administrativas que puedan identificar un ferrocarril, como un código de país, NID_C ", un código RBC," NID_RBC ", un código de conductor de tren" Driver_ID ", una identidad de usuario" NID_USER "," Q_DIR "que especifica una dirección de ejecución de un grupo Eurobaliza y una "Q_SCALE", que especifica una escala de distancia que caracteriza la información de distancia que puede incluirse en la carga útil de un paquete. Los mensajes ERTMS/ETCS normalmente agrupan una pluralidad de variables y/o paquetes ERTMS/ETCS. Como en el caso de un paquete ERTMS/ETCS, un mensaje ERTMS/ETCS comprende un encabezado que incluye un número de identificación denominado NID_MESSAGE, que identifica el tipo de mensaje y las variables administrativas. Las variables administrativas pueden incluir una hora, "T_TRAIN", de acuerdo con un reloj de tren, un

número de identidad de grupo de baliza "NID_LRBG" y/o un perfil de pendiente de la vía. Un telegrama es un tipo de mensaje que se transmite mediante un dispositivo de un solo punto, como una baliza.

De acuerdo con una realización, el anonimizador 102 de Rail-Eye 121, 122 o 123 puede borrar un mensaje ERTMS/ETCS que el anonimizador o Rail-Eye carga en ANDAT 100 para proporcionar un registro anónimo de un ataque cibernético y cifrar la identificación. variables de entre las variables, como se indicó anteriormente, en el registro que pueden usarse para identificar el Rail-Eye o el ferrocarril 131, 132 o 133 que protege Rail-Eye.

Además de borrar los datos, la anonimización de datos incluye opcionalmente ocultar la identidad de un Rail-Eye 121, 122, 123 y actualizar los datos anonimizados a ANDAT 100. En una realización, el anonimizador 102 asociado con los sistemas Rail-Eye 121, 122 y 123 cooperan para ocultar la identidad de un Rail-Eye que actualiza datos anónimos a ANDAT100. Por ejemplo, en una realización, los anonimizadores 102 pueden comunicarse entre sí a través de una red de comunicación en anillo representada esquemáticamente por flechas discontinuas 222 que conectan los anonimizadores 102 y referidos por el número 222. Cuando un Rail-Eye, 121, 122 o 123 determinado genera datos anonimizados listos para cargar en ANDAT 100, el Rail-Eye dado establece un período de retraso que tiene una duración aleatoria y transmite los datos anonimizados a los otros anonimizadores en la red de anillo. Cuando otro de los anonimizadores recibe los datos anonimizados, descarga los datos anonimizados, establece un retraso aleatorio y retransmite los datos anonimizados en el anillo. Opcionalmente, una vez que el anonimizador dado recibe los datos anonimizados que él mismo ha generado y transmitido, elimina los datos anonimizados de la circulación en el anillo. Cada anonimizador 102 carga los datos anonimizados en ANDAT 100 a la vez después de un tiempo en el que el anonimizador generó o recibió los datos anonimizados del anillo retrasado por el retraso aleatorio que el anonimizador ha establecido. En una realización, cada uno de los anonimizadores 102 establece su retardo aleatorio en respuesta a un algoritmo que opera para proporcionar a cada uno de los anonimizadores un retardo aleatorio diferente y para el cual el orden en el que los diferentes anonimizadores 102 cargan los datos anonimizados también es aleatorio. Dado que todos los anonimizadores cargan los mismos datos anónimos en diferentes momentos aleatorizados, es ventajosamente difícil determinar cuál de los sistemas Rail-Eye 131, 132, 133 es la fuente de los datos aleatorizados.

Se observa que mientras que en la descripción anterior los anonimizadores 102 se describen como comunicando a través de una topología de anillo y cargando datos anonimizados a ANDAT 100, en una realización, los componentes de los sistemas Rail-Eye distintos de los anonimizadores pueden configurarse para comunicarse a través de una topología de anillo. y operar para cargar datos anónimos a ANDAT 100.

La Figura 4 ilustra esquemáticamente un escenario de ejemplo en el que, a modo de ejemplo, Rail-Eye 122 que protege el ferrocarril 132 (Figura 3), identifica un evento anómalo indicativo de un ataque cibernético en una parte del ferrocarril, genera y carga en ANDAT 100 un informe anónimo del evento.

En el escenario de ejemplo de la Figura 4, se muestra esquemáticamente una locomotora 310 (Figura 2B) de un tren 300 (sin vagones para facilitar la presentación) pasando sobre una sección curva 400 de la vía en el ferrocarril 132. La sección de vía 400 comprende grupos de balizas 411, 412 y 413, en la región 421, 422 y 423 respectivamente de la sección de vía 400. A modo de ejemplo, se supone que cada grupo de balizas comprende dos balizas, B1 y B2. La locomotora 310 se muestra en las ubicaciones 421, 422 y 423 a lo largo de la vía 400 mientras se mueve a lo largo de la vía en una dirección indicada por una flecha 401 de bloque. Un ciberdelincuente ha instalado un grupo de balizas falsas, "FB", que comprende balizas falsas FB-1 y FB-2 en una ubicación "X" entre las ubicaciones 412 y 413. El grupo de balizas falso FB se configura para enmascarar y asumir la identidad del grupo de balizas 413.

A medida que la locomotora 310 se mueve a lo largo de la vía 400 a través de la región 421, el lector 314 de balizas de locomotora encuentra, pasa y energiza las balizas B1 y B2 en el grupo de balizas 411. En respuesta a la activación, cada baliza del grupo de balizas responde transmitiendo un telegrama representado esquemáticamente por una línea 411-1 de doble punta de flecha al lector de balizas 314. Cada telegrama comprende elementos de información como N_PIG, que identifica la baliza, B1 o B2 en el grupo de balizas 411 que transmite el telegrama, N_TOTAL, el número total de balizas en el grupo de balizas 411 y NID_C, que identifica el país en el que se encuentra situado el grupo de balizas 411. En respuesta a la recepción de los telegramas de baliza 411-1 de B1 y B2 en el grupo de balizas 411, la locomotora 310 transmite un mensaje ERTMS/ETCS Reporte de Posición del Tren 136 representado esquemáticamente por una flecha de rayo 411-2, al RBC 230 para informar la posición de locomotora 310. El mensaje 136 puede comprender paquetes que proporcionen respectivamente un NID_Message, L_Message, T_Train, mencionado anteriormente, y NID_Engine, que identifica al proveedor de equipos de motor, y NID-LRBG que identifica el grupo de balizas 411. El RBC 230 responde con un Mensaje 3 de autorización de movimiento, indicado esquemáticamente por una flecha de rayo 411-3, que el RBC transmite a la locomotora 310. El mensaje 3 comprende el identificador de mensaje NID_Message, T_Train, M_ACK, NID_LBRG. la identidad del último grupo de balizas (grupo de balizas 411) informado por la locomotora 310 al RBC 230, y un paquete 15 que proporciona una Autoridad de Movimiento de nivel 2/3 que informa a la locomotora 310 que está autorizada a avanzar por la vía 400. La secuencia de la vía para entrenar la locomotora 310, el tren de la locomotora 310 al RBC 230 y el RBC 230 para entrenar las comunicaciones de la locomotora 310 que proporcionan al tren una autoridad de movimiento en la ubicación 421 se repite en la ubicación 422 con un conjunto de mensajes 412-1, 412- 2 y 412-3 similar a los mensajes 411-1, 411-2 y 411-3.

Al pasar sobre el grupo de balizas falso FB en la ubicación X, el grupo de balizas FB telegrama la identificación del grupo de balizas 413 haciendo que la locomotora 310 envíe un informe de posición falso Mensaje 136, representado esquemáticamente como un mensaje "sombrero negro" 136X, que había recibido un telegrama del grupo de balizas 413. Como resultado, RBC 230 concluye incorrectamente que la locomotora 319 está ubicada en la región 423 donde el grupo de balizas 413 está ubicado cuando la locomotora está realmente ubicada en la región X. Dado que la región X está más cerca que la región 423 de la región 422 desde donde la locomotora 310 informó su última posición, RBC 230 puede concluir incorrectamente que la locomotora 310 viaja mucho más rápido de lo que debería viajar. Como resultado, el RBC 23 puede, por ejemplo, emprender acciones para mantener la seguridad del Ferrocarril 132, tales como negar la autoridad de movimiento de la locomotora 310 y/u operar para efectuar una parada de emergencia de la locomotora 310. Alternativamente, a modo de ejemplo, el RBC 23 puede transmitir una autoridad de movimiento incorrecta. Las acciones de RBC 230 en respuesta a recibir la ubicación incorrecta de la locomotora 310 pueden generar una interrupción grave y/o peligrosa del servicio proporcionado por el ferrocarril.

En una realización, un detector cibernético 36 de infraestructura que supervisa las comunicaciones en las que participa el RBC 230 puede reenviar comunicaciones entre la locomotora 310 y el RBC 230, tales como los mensajes 411-2, 411-3, 412-2, 412-3 y 136X al agregador de RBC 38 para análisis y/o reenvío al concentrador 22. El agregador 38 también puede recibir mensajes de los detectores cibernéticos incorporados 32 comprendidos en la locomotora 310 a través de un agregador incorporado 34 en la locomotora y, opcionalmente, reenviar los mensajes al concentrador 22. En una realización, un detector incorporado que funciona como una toma de red puede reflejar las comunicaciones entrantes a la JRU de la locomotora para reenviar mensajes tales como los mensajes 411-1, 411-2, 411-3, 412-1, 412-2, 412-3 y 136X al agregador de RBC 38 para su análisis y/o reenvío al concentrador 22. El agregador de RBC 38 y/o el concentrador 22 pueden procesar los mensajes de los ataques cibernéticos y determinar que el mensaje de sombrero negro 136X es un mensaje anómalo que puede haber sido generado como resultado de un ataque cibernético.

Por ejemplo, el agregador de RBC 38 y/o el concentrador 22 pueden determinar que los detectores cibernéticos incorporados 32 que generan señales que responden a la rotación de la rueda de la locomotora, la temperatura de un motor de tracción eléctrico en la locomotora 310 y/o señales de los sonidos generados por el funcionamiento de la locomotora entran en conflicto con la conclusión de que la locomotora 310 se desplaza por encima de un límite de velocidad seguro. Si en respuesta al mensaje de sombrero negro 136X, el RBC 230 no funciona para detener el movimiento de la locomotora 310 a lo largo de la vía 400, una posición válida Mensaje 136 recibido por el RBC 230 de la locomotora 310 cuando la locomotora pasa y recibe telegramas del grupo de balizas 413 en la región 423 puede confirmar que el mensaje de sombrero negro 136X es falso y puede ser indicativo de un ataque cibernético. En la Figura 4, los telegramas de las balizas B1 y B2 en el grupo de balizas 413 están representados por la línea de punta de flecha doble 413-1, y el Mensaje 136 de la locomotora 310 en la región 423 está representado por la flecha de iluminación 413-2.

En una realización, el anonimizador 102 comprendido en Rail-Eye 122 elimina el mensaje de sombrero negro 136X y los mensajes recibidos por el agregador de infraestructura 38 o el concentrador 22 que están asociados con el mensaje de sombrero negro 136X, cifrando elementos de información en los mensajes que identifican el sombrero y mensajes asociados con el ferrocarril 132. Opcionalmente, después de la depuración, Rail-Eye 122 carga a través de la red de anillo 222 (Figura3) los mensajes depurados a ANDAT 100 para proporcionar un registro de eventos anónimo para el mensaje de sombrero negro 136X al que se puede acceder mediante Rail-Eye 121 y 123.

A modo de ejemplo, los mensajes de limpieza asociados con el mensaje 136X de sombrero negro pueden comprender normalizar los tiempos de tren T_Train en los mensajes a una escala de tiempo en la que el tiempo de primer tren T_Train es 0, y/o eliminar valores para al menos uno o cualquier combinación de las variables NID-C, NID-LRBG y NID-Engine de los mensajes.

Por lo tanto, se proporciona de acuerdo con una realización de la divulgación, un sistema de seguridad cibernética para proporcionar seguridad a un ferrocarril, comprendiendo el sistema: un centro de procesamiento y monitoreo de datos; una red que comprende una pluralidad de agentes de recopilación de datos sincronizados con un mismo reloj de red y configurados para monitorear dispositivos de infraestructura ferroviaria y dispositivos incorporados en el material rodante que tienen una red de comunicación de trenes (TCN), y reenviar datos monitoreados al concentrador para que los procese el concentrador a detectar anomalías en la operación ferroviaria que sean indicativas de un ataque cibernético; en el que un agente de la pluralidad de agentes de recopilación de datos que monitorean un dispositivo incorporado conectado al TCN de un material rodante dado recibe señales propagadas hacia o desde el dispositivo a través del TCN y las reenvía al concentrador datos en base a una señal recibida dada junto con un tiempo sello que comprende la hora del reloj de la red en la que el agente recibe la señal recibida dada.

Opcionalmente, el TCN comprende un bus de vehículo multifuncional (MVB) acoplado a un bus de tren cableado (WTB) y el sello de tiempo comprende un valor de un lapso de tiempo entre el comienzo de un giro del MVB durante el cual la señal recibida dada se propaga sobre el TCN. Opcionalmente, la red de agentes de recopilación de datos se sincroniza en función de una frecuencia de referencia y la información de tiempo del día (TOD) proporcionada por las transmisiones del sistema de navegación por satélite global (GNSS). Opcionalmente, la información de tiempo comprende una frecuencia de referencia y una hora del día (TOD). Opcionalmente, el agente que monitorea el

dispositivo integrado comprende un reloj de tiempo de referencia primario (PRTC) que proporciona la frecuencia de referencia y ToD.

En una realización de la divulgación, un agente de la pluralidad de agentes de recopilación de datos es un agente sigiloso configurado para operar en modo sigiloso, en cuyo modo sigiloso el agente interrumpe mínimamente el funcionamiento en tiempo real de un dispositivo que el agente supervisa. Opcionalmente, en el modo sigiloso, la operación del agente sigiloso satisface los límites de interrupción establecidos por un estándar internacional. Opcionalmente, el agente de modo sigiloso se configura para monitorear un dispositivo solo durante el tiempo de inactividad del dispositivo. Adicional o alternativamente, el agente sigiloso puede comprender una antena configurada para proporcionar una conexión inalámbrica a un dispositivo monitoreado a través de la cual el agente invisible recibe señales del dispositivo monitoreado con una interrupción mínima del funcionamiento en tiempo real del dispositivo. Opcionalmente, el agente sigiloso se configura para recibir una secuencia de código de expansión para demodular una señal que el agente sigiloso recibe del dispositivo. Opcionalmente, la antena se configura para proporcionar una conexión inalámbrica a un cable coaxial radiante de un Euroloop.

En una realización de la divulgación, los agentes se configuran para codificar datos supervisados en un protocolo común para reenviarlos al concentrador.

En una realización de la divulgación, el concentrador genera un espectro de frecuencia de aparición de señales que proporciona una serie de señales de un tipo particular que es recibido por el concentrador en función del tiempo. El concentrador puede procesar el espectro de frecuencia de ocurrencia para identificar anomalías que pueden ser indicativas de un ataque cibernético. Adicional o alternativamente, el espectro de frecuencia de aparición proporciona varias señales recibidas durante un período de tiempo dado en función del tipo de señales.

En una realización de la divulgación, el concentrador genera un espectro de frecuencias de aparición de señales para cada uno de al menos dos materiales rodantes diferentes y procesa los espectros para identificar anomalías que podrían ser indicativas de un ataque cibernético. En una realización de la divulgación, el concentrador procesa los datos que recibe de los agentes para identificar anomalías temporales en el funcionamiento de la infraestructura y/o los dispositivos incorporados que podrían ser indicativos de un ataque cibernético. En una realización de la divulgación, el concentrador procesa los datos que recibe para generar un contexto para el funcionamiento de una infraestructura o dispositivo de material rodante y determina si el funcionamiento del dispositivo entra en conflicto con el contexto para identificar anomalías que podrían ser indicativas de un ataque cibernético.

En una realización de la divulgación, la seguridad cibernética puede comprender al menos un anonimizador configurado para eliminar elementos de información de los datos que el concentrador recibe de un agente de recopilación de datos de la pluralidad de agentes de recopilación de datos que se pueden usar para identificar el sistema de seguridad cibernética o el ferrocarril para el que el sistema proporciona seguridad.

Se proporciona además de acuerdo con la invención, un conglomerado de seguridad cibernética que comprende: una pluralidad de sistemas de seguridad cibernética según las reivindicaciones 1 a 7, cada uno de los cuales proporciona seguridad a un sistema ferroviario diferente de una pluralidad de sistemas ferroviarios; para cada sistema de seguridad cibernética, al menos un anonimizador operable para eliminar elementos de información de los datos que el centro del sistema de seguridad cibernética recibe de un agente de recopilación de datos de la pluralidad de agentes de recopilación de datos que se pueden usar para identificar el sistema de seguridad cibernética y/o el ferrocarril para el que el sistema de seguridad cibernética proporciona seguridad; y un sistema de comunicaciones de topología en anillo sobre el cual los sistemas de seguridad cibernética de la pluralidad de sistemas de seguridad cibernética se configuran para comunicarse para compartir datos depurados.

Opcionalmente, el conglomerado de seguridad cibernética comprende una base de datos configurada para recibir y almacenar datos que cada uno de los al menos un anonimizador elimina. Opcionalmente, los sistemas de seguridad cibernética se configuran para compartir datos borrados por al menos un anonimizador de un sistema de seguridad cibernético dado de la pluralidad de sistemas de seguridad cibernética con cada uno de los otros sistemas de seguridad cibernética mediante transmisión a través del sistema de comunicaciones de topología en anillo. Opcionalmente, cada sistema de seguridad cibernética se configura para transmitir datos depurados que genera o recibe a través de la red de topología en anillo a la base de datos. Cada uno de los sistemas de seguridad cibernética puede configurarse para transmitir datos depurados que genera o recibe a través de la red de topología en anillo a la base de datos. Cada sistema de seguridad cibernética puede configurarse para transmitir a la base de datos los mismos datos compartidos en un momento aleatorio diferente en relación con un momento en el que el sistema de seguridad cibernética ha generado o recibido los datos compartidos.

En una realización, cada sistema de seguridad cibernética de la pluralidad de sistemas de seguridad cibernética se configura para acceder a la base de datos para recibir datos depurados de la base de datos.

En una realización, los datos depurados comprenden datos que son indicativos de un ataque cibernético asociado con un ferrocarril protegido por un sistema de seguridad cibernética de la pluralidad de sistemas de seguridad cibernética.

En la descripción y las reivindicaciones de la presente solicitud, cada uno de los verbos, "comprender", "incluir" y "tener", y sus conjugados, se utilizan para indicar que el objeto u objetos del verbo no son necesariamente una lista completa de componentes, elementos o partes del sujeto o sujetos del verbo.

Las descripciones de las realizaciones de la invención en la presente solicitud se proporcionan a modo de ejemplo y no pretenden limitar el ámbito de la invención. Las modalidades descritas comprenden diferentes características, no todas las cuales son necesarias en todas las modalidades de la invención. Algunas realizaciones utilizan solo algunas de las características o posibles combinaciones de las características.

REIVINDICACIONES

1. Un sistema de seguridad cibernética (20) para proporcionar seguridad a un ferrocarril (200), comprendiendo el sistema:

un centro de procesamiento y monitoreo de datos (22);

una red que comprende una pluralidad de agentes de recopilación de datos (32, 34) sincronizados con un mismo reloj de red y configurados para monitorear dispositivos de infraestructura ferroviaria y dispositivos incorporados en el material rodante que tienen una red de comunicación de trenes (331), y enviar datos monitoreados al concentrador para procesamiento por parte del concentrador para detectar anomalías en la operación ferroviaria que sean indicativas de un ataque cibernético; y

al menos un anonimizador (102) configurado para eliminar elementos de información de los datos que el concentrador recibe de un agente de recopilación de datos de la pluralidad de agentes de recopilación de datos que se pueden usar para identificar el sistema de seguridad cibernética o el ferrocarril para el que el sistema proporciona seguridad.

2. El sistema de seguridad cibernética de acuerdo con la reivindicación 1, en el que la red de comunicación del tren comprende un bus de vehículo multifuncional (332) acoplado a un bus de tren cableado (336) y el sello de tiempo comprende un valor de un lapso de tiempo entre el comienzo de un turno del multifuncional bus de vehículo durante el cual la señal recibida dada se propaga a través de la red de comunicación del tren.

3. El sistema de seguridad cibernética de acuerdo con la reivindicación 2, en el que la red de agentes de recopilación de datos está sincronizada en base a una frecuencia de referencia y la información de tiempo del día proporcionada por las transmisiones del Sistema de navegación por satélite global.

4. El sistema de seguridad cibernética de acuerdo con la reivindicación 3, en el que el agente que supervisa el dispositivo incorporado comprende un reloj de tiempo de referencia principal que proporciona la frecuencia de referencia y la hora del día.

5. El sistema de seguridad cibernética de acuerdo con cualquiera de las reivindicaciones anteriores, en el que un agente de la pluralidad de agentes de recopilación de datos es un agente sigiloso configurado para operar en modo sigiloso, en cuyo modo sigiloso el agente interrumpe mínimamente el funcionamiento en tiempo real de un dispositivo que el agente supervisa.

6. El sistema de seguridad cibernética de acuerdo con la reivindicación 5, en el que, en el modo sigiloso, el funcionamiento del agente sigiloso satisface los límites de interrupción establecidos por un estándar internacional.

7. El sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que los agentes se configuran para codificar datos monitoreados en un protocolo común para reenviarlos al concentrador.

8. Un conglomerado de seguridad cibernética que comprende:

una pluralidad de sistemas de seguridad cibernética de acuerdo con cualquiera de las reivindicaciones 1 a 7, cada uno de los cuales proporciona seguridad a un sistema ferroviario diferente de una pluralidad de sistemas ferroviarios; y

un sistema de comunicaciones de topología en anillo sobre el cual los sistemas de seguridad cibernética de la pluralidad de sistemas de seguridad cibernética se configuran para comunicarse para compartir datos depurados.

9. El conglomerado de seguridad cibernética de acuerdo con la reivindicación 8 y que comprende una base de datos (100) configurada para recibir y almacenar datos que cada uno de los al menos un anonimizador depura.

10. El conglomerado de seguridad cibernética de acuerdo con la reivindicación 9, en el que los sistemas de seguridad cibernética se configuran para compartir datos depurados por al menos un anonimizador de un sistema de seguridad cibernético dado de la pluralidad de sistemas de seguridad cibernética con cada uno de los otros sistemas de seguridad cibernética a través de la transmisión a través del sistema de comunicaciones de topología en anillo.

11. El conglomerado de seguridad cibernética de acuerdo con la reivindicación 10, en el que cada sistema de seguridad cibernética se configura para transmitir datos depurados que genera o recibe a través de la red de topología en anillo a la base de datos.

12. El conglomerado de seguridad cibernética de acuerdo con la reivindicación 11, en el que cada uno de los sistemas de seguridad cibernética se configura para transmitir datos depurados que genera o recibe a través de la red de topología en anillo a la base de datos.

13. El conglomerado de seguridad cibernética de acuerdo con la reivindicación 12, en el que cada sistema de seguridad cibernética se configura para transmitir a la base de datos los mismos datos compartidos en un momento aleatorio diferente con respecto a un momento en el que el sistema de seguridad cibernética ha generado o recibido los datos compartidos.

14. El conglomerado de seguridad cibernética de acuerdo con cualquiera de las reivindicaciones 8-13, en el que cada sistema de seguridad cibernética de la pluralidad de sistemas de seguridad cibernética se configura para acceder a la base de datos para recibir datos depurados de la base de datos.

15. El conglomerado de seguridad cibernética de acuerdo con cualquiera de las reivindicaciones 8-14, en el que los datos depurados comprenden datos que son indicativos de un ataque cibernético asociado con un ferrocarril protegido por un sistema de seguridad cibernética de la pluralidad de sistemas de seguridad cibernética.

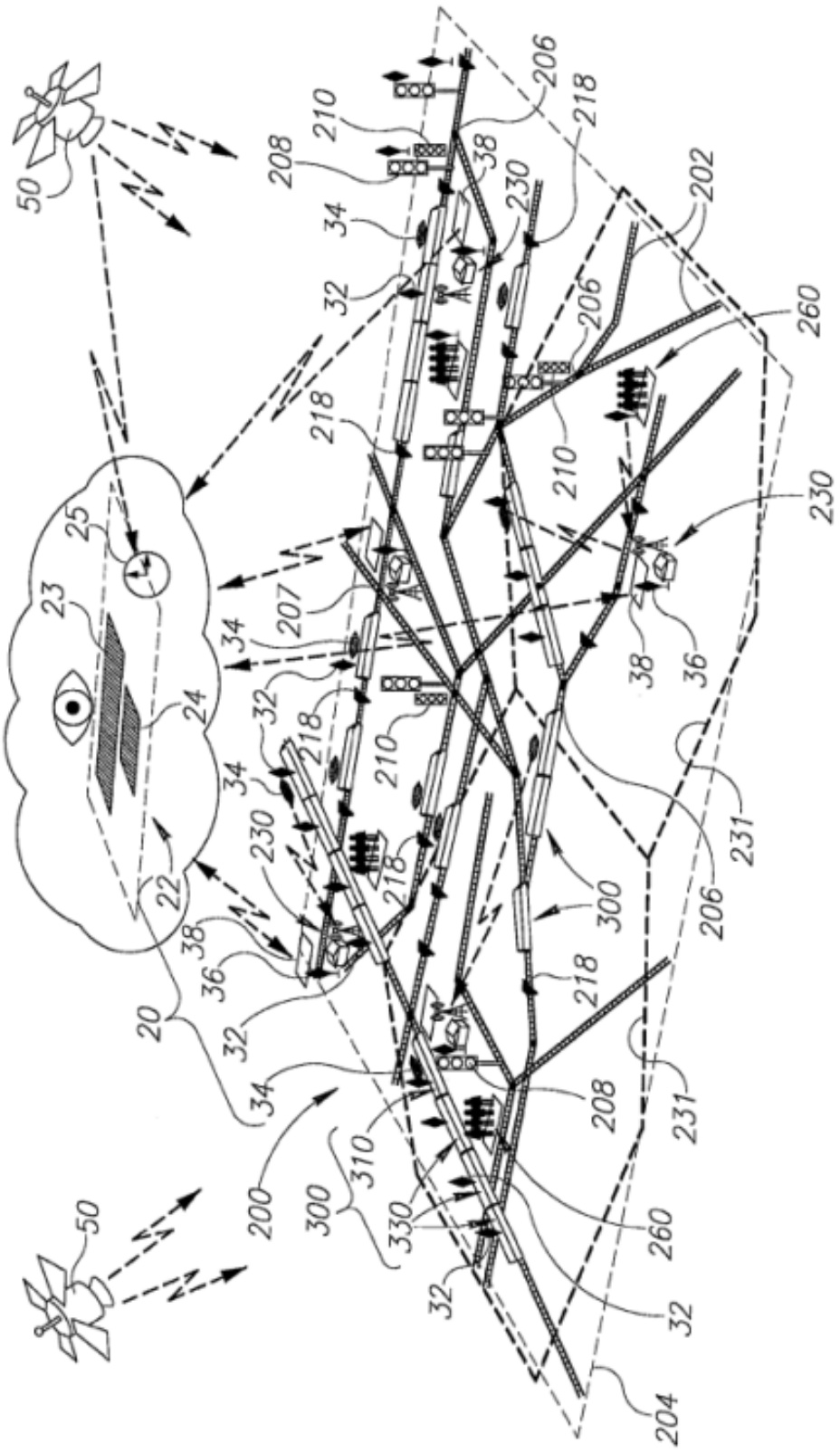
50
208
210
206
218
38
230
202
34
32
260
207
25
23
24
22
20
36
231
300
310
330
200
204

FIGURA 1A

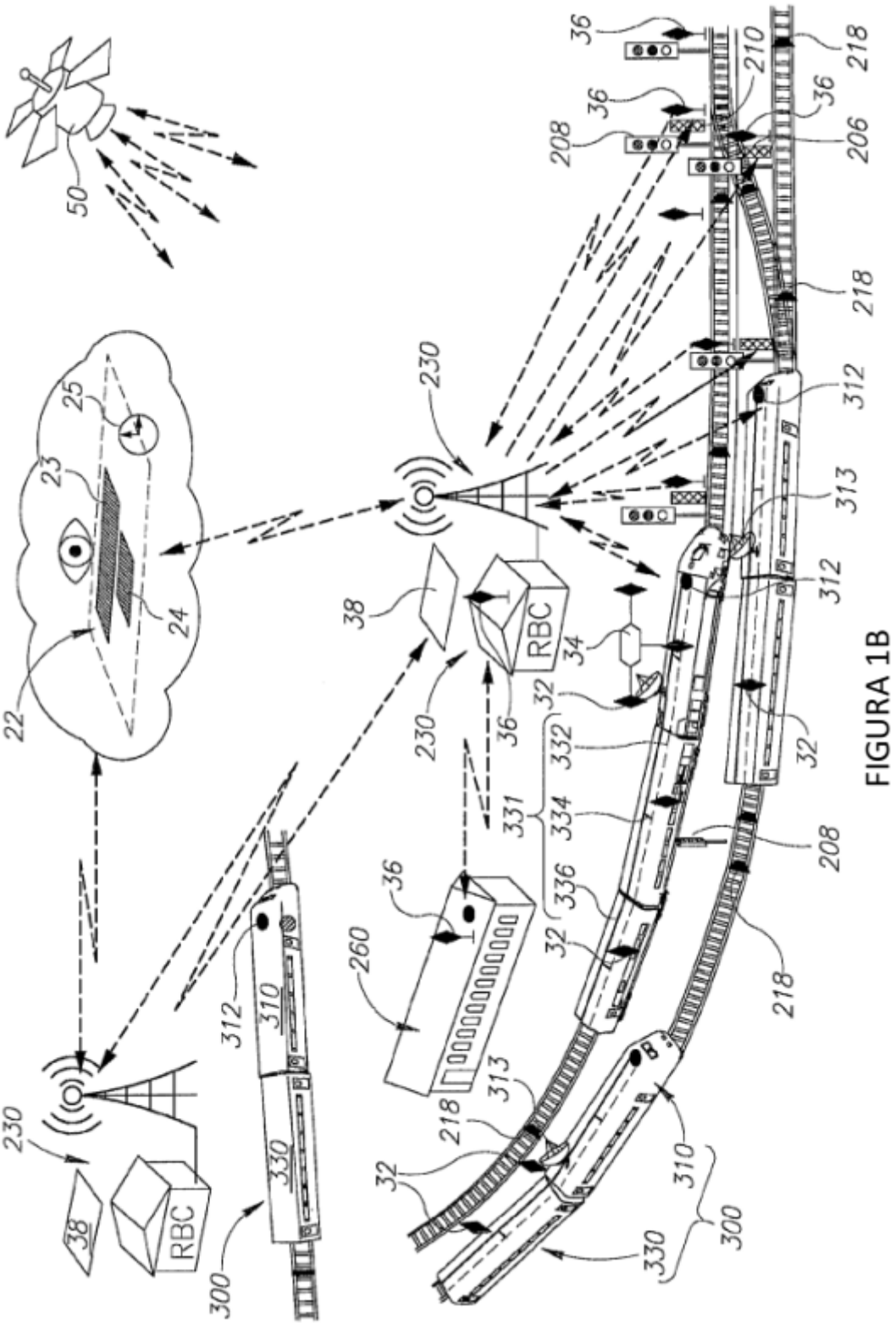
50
22
25
23
24
230
38
RBC
34
36
32
332
331
334
336
260
313
312
310
330
300
218
208
206
210

FIGURA 1B

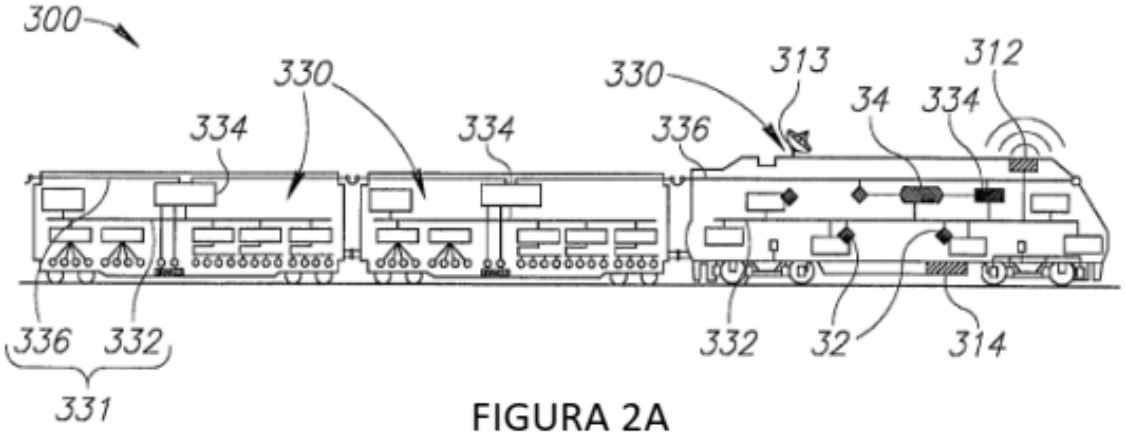

FIGURA 2A

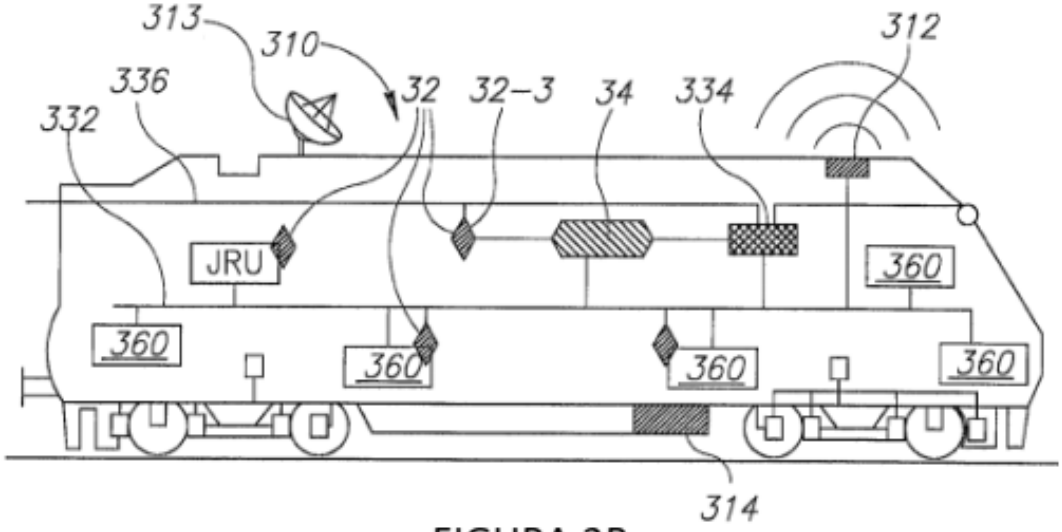

FIGURA 2B

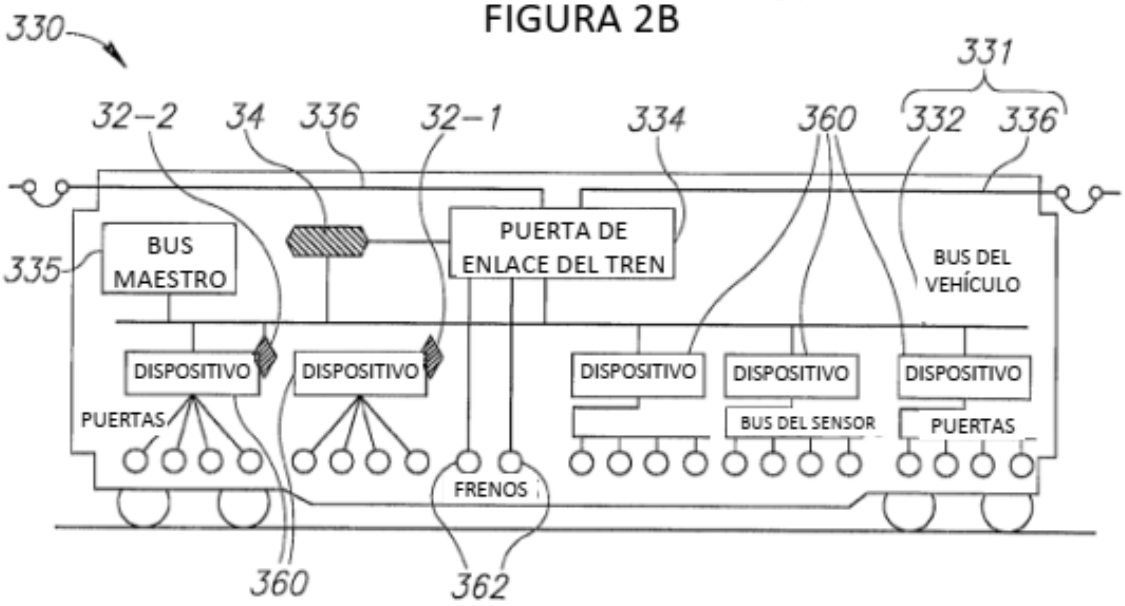

FIGURA 2C

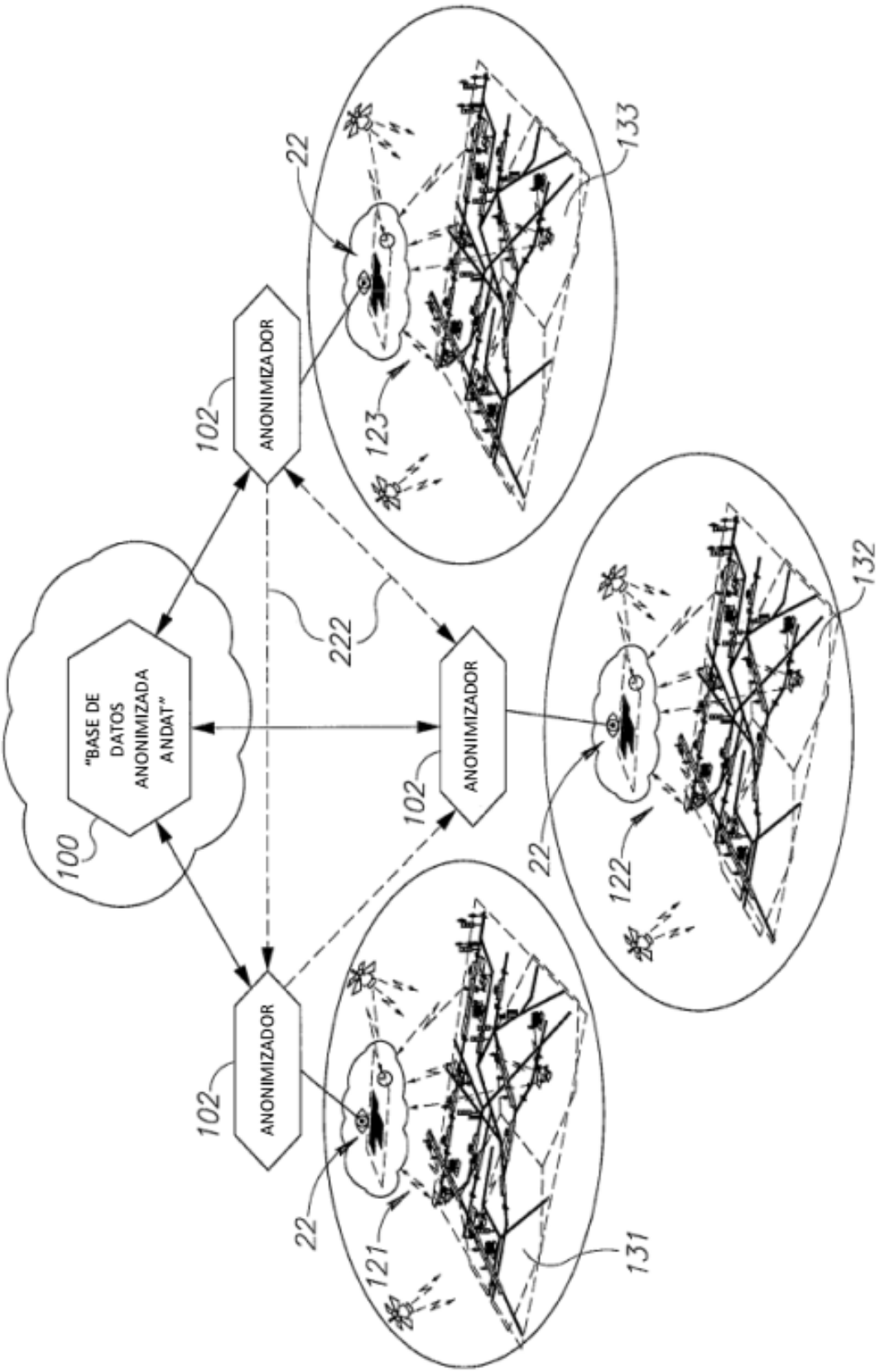
"BASE DE DATOS ANONIMIZADA ANDAT"
100
ANONIMIZADOR
102
ANONIMIZADOR
102
ANONIMIZADOR
102
222
22
123
133
22
122
132
22
121
131

FIGURA 3

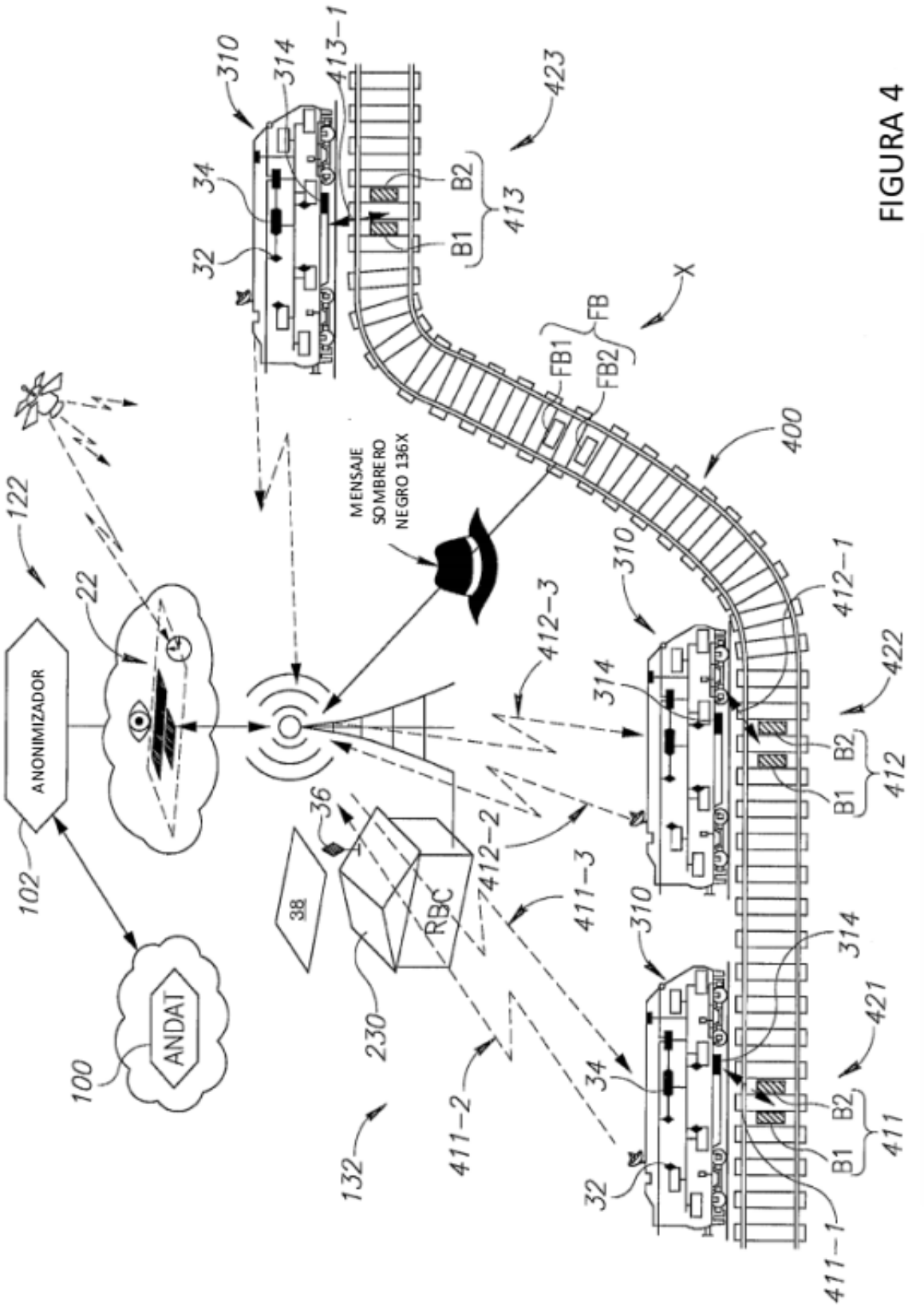
ANONIMIZADOR
ANDAT
MENSAJE
SOMBRERO
NEGRO 136X
RBC
FB
FB1
FB2
B1
B2
X
122
22
102
100
36
38
230
132
32
34
310
314
413-1
413
423
400
412-3
412-2
411-3
411-2
412-1
422
412
421
411
411-1

FIGURA 4