(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 780 902**

(51) Int. CI.:

B61L 27/00 (2006.01)
B61L 15/00 (2006.01)
G06F 11/16 (2006.01)
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.04.2015 PCT/US2015/025022**

(87) Fecha y número de publicación internacional: **22.10.2015 WO15160603**

(96) Fecha de presentación y número de la solicitud europea: **09.04.2015 E 15717773 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.01.2020 EP 3131804**

(54) Título: **Sistemas críticos de seguridad ferroviaria con redundancia de tareas y capacidad de comunicaciones asimétricas**

(30) Prioridad:

16.04.2014 US 201414254332

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.08.2020

(73) Titular/es:

SIEMENS MOBILITY, INC. (100.0%)
16th floor, 498 Seventh Avenue
New York, NY 10018, US

(72) Inventor/es:

WEBER, CLAUS y
EGEL, ZOLTAN

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Sistemas críticos de seguridad ferroviaria con redundancia de tareas y capacidad de comunicaciones asimétricas

Antecedentes de la divulgación

1. Campo de la invención

La invención se refiere a sistemas críticos de seguridad de control ferroviario. Más particularmente, la presente invención se refiere a sistemas de control en sistemas de aplicación críticos de seguridad ferroviaria con índices de riesgo bajos, tal como se necesita en la industria ferroviaria. Los sistemas de aplicación críticos de seguridad ferroviaria ("sistemas críticos de seguridad") incluyen a modo de ejemplo no limitativo sistemas de gestión de tren, servidor de soporte administrativo, unidades a bordo para intervención automática si un tren supera límites de velocidad de salvaguardia, registrador de datos que registran información operacional, velocidad de tren y equipo de determinación de la posición, control de acelerador y frenos, diagnósticos y estado de subsistema, comunicaciones de datos inalámbricos intercambiadas entre lado de la vía/lado de tierra y lado de tren (por ejemplo, a través de comunicaciones de radio inalámbricas) y comunicaciones entre la tripulación del tren. Tal como se usa en el presente documento, el término "tren" es sólo una locomotora, locomotora con vagones, o una locomotora/vehículo de vagón integrado, (por ejemplo, ferrocarril ligero o ferrocarril subterráneo).

2. Descripción de la técnica anterior

Los trenes de ferrocarril están equipados con sistemas críticos de seguridad que se requiere que tengan disponibilidad alta y índices de riesgo bajos (un "riesgo" se entiende habitualmente como "situación física con potencial para que se produzca lesión humana y/o daño al medio ambiente" (norma IEC 62278)). "Los operadores ferroviarios y reguladores gubernamentales a menudo requieren índices de riesgo extremadamente bajos que satisfacen su alta demanda para seguridad operacional."). Los sistemas críticos de seguridad se hacen funcionar normalmente con sistemas de control electrónicos. A lo largo del tiempo estos sistemas son atraídos a sistemas electrónicos digitales operados por procesador o controlador que se comunican entre sí a través de uno o más buses de datos de comunicaciones.

Con el fin de cumplir los objetivos de seguridad ferroviarios, el hardware de sistema de control a menudo es de diseño dedicado de propiedad con pruebas y validación documentadas. Los sistemas operativos de controlador electrónico digital y los softwares de aplicación también se validan. Las comunicaciones de datos electrónicos utilizan códigos de seguridad validados para verificaciones de integridad de datos, tales como códigos de direccionamiento o uniones criptográficas, con el fin de garantizar la integridad de datos tras la transmisión entre los sistemas. Los procedimientos de validación requieren tiempo y gastos. Dada la demanda relativamente limitada y el volumen de ventas de los sistemas críticos de seguridad ferroviaria, en comparación con la demanda de comercios generales y electrónica de consumidor (por ejemplo, hardware, software y sistemas operativos de ordenador personal), los controladores y equipos relacionados de sistemas críticos de seguridad ferroviaria son caros de fabricar y tienen mayores ciclos de vida de producto que los vendidos en los campos generales de aplicaciones de electrónica.

Sin embargo, los ordenadores personales (PC) de consumidor y comerciales no pueden sustituirse directamente por sistemas de control de sistemas críticos de seguridad ferroviaria existentes. Los PC a menudo sólo tienen una tasa de fallo de datos de no más de 10^{-4} por hora de funcionamiento, lo cual es insuficiente para cumplir con los riesgos requeridos por sistemas ferroviarios. Adicionalmente, el software de sistema comercial de PC no está validado para su uso en sistemas críticos de seguridad ferroviaria.

Existe la necesidad en la industria ferroviaria de reemplazar software de sistema operativo y hardware de sistema de control de sistema crítico de seguridad de diseño de propiedad específico de dominio ferroviario con más productos comercialmente disponibles ("COTS") de propósito general fácilmente disponibles, donde sea factible. La sustitución de subsistemas de COTS para subsistemas de diseño de propiedad específicos de dominio ferroviario pueden potencialmente simplificar el diseño del sistema global, acortar ciclos de diseño de sistema, y permite al proveedor principal de sistema crítico de seguridad ferroviaria enfocar sus esfuerzos en la aplicación de sistema global y cuestiones de integración, en el que tiene mayor experiencia que un consumidor general o subvendedor de electrónica COTS.

También existe la necesidad en la industria ferroviaria de reducir costes de adquisición de sistema de control de sistema crítico de seguridad y aumentar el número de subvendedores cualificados sustituyendo productos COTS por productos específicos del dominio ferroviario, cuando la validación de los sustitutos es rentable. El cliente ferroviario y el proveedor principal de sistema crítico de seguridad también pueden beneficiarse del diseño y fabricación externalizados de componentes de subsistema a subvendedores que pueden tener experiencia de diseño más amplia para sus componentes comerciales respectivos.

Existe una necesidad adicional en la industria ferroviaria para optimizar las cronologías de adquisición de sistema

crítico de seguridad simplificando y agregando procedimientos de validación. Por ejemplo, si componentes de hardware y software de sistema de control comercialmente disponibles (COTS) ya cumplen los estándares de validación de fiabilidad reconocidos y documentados; puede no tener que revalidar esos mismos productos para aplicaciones de sistema crítico ferroviario. Más bien, la validación del sistema crítico de seguridad puede consolidarse y simplificarse mediante un proceso de validación de sistema general que incluye contribuciones de productos comercialmente disponibles ya validados, optimizando de ese modo las cronologías de adquisición y procesos. El documento US 2014/074327 A1 describe un sistema de aplicación vital o crítico ferroviario que usa un par de ordenadores personales y sistemas operativos con capacidad de comunicaciones asimétricas. Cada ordenador y sistema operativo puede diferir por redundancia adicional. Ambos ordenadores reciben y verifican datos de mensajes de entrada de sistemas vitales e integridad del código de seguridad y generan de manera independiente datos de salida en respuesta al mensaje de entrada.

Sumario de la invención

Por consiguiente, un objeto de la presente invención es simplificar el diseño global de los sistemas críticos de seguridad ferroviaria reemplazando el hardware de sistema de control de sistema crítico de seguridad de diseño de propiedad y haciendo funcionar el software de sistema con productos comerciales sin propiedad más fácilmente disponibles.

También es un objeto de la presente invención reducir los costes de adquisición de sistema de control de sistema crítico de seguridad y aumentar el número de subvendedores cualificados que pueden tener experiencia de diseño más amplia en sus líneas de productos comerciales respectivas sustituyendo los productos sin propiedad para productos de propiedad cuando la validación para los sustitutos es rentable.

Un objeto adicional de la presente invención es optimizar los costes de adquisición de sistema de control de sistema crítico de seguridad y cronologías de validación, así como aumentar el número de vendedores cualificados simplificando y agregando procesos de validación.

Estos y otros objetos se consiguen según la presente invención mediante un sistema de control para un sistema de aplicación crítico de seguridad ferroviaria (“sistema crítico de seguridad”) y método para hacer funcionar ese sistema de control que sustituye el hardware comercialmente disponible y el software de sistema operativo para componentes de producto de propiedad específicos de dominio ferroviario, aún pueden validarse como en conformidad con los estándares de sistema crítico de seguridad ferroviaria. Por ejemplo, un ordenador personal comercial o un entorno de ordenador virtual con uno o más ordenadores personales y sistemas operativos puede sustituirse por entorno ferroviario específico de dominio ferroviario de propiedad con dos tareas, hilos o nodos independientes, y están configuradas para comunicación asimétrica con otros sistemas críticos de seguridad. Ambas tareas reciben y verifican datos de mensaje de entrada de sistemas críticos de seguridad e integridad de código de seguridad y generar de manera independiente datos de salida en respuesta al mensaje de entrada. Con una arquitectura de comunicación asimétrica, la primera tarea tiene la única capacidad de enviar mensajes de salida de sistema crítico de seguridad que incluyen los datos de salida pero sin código de seguridad de salida, y sólo la segunda tarea tiene la capacidad de generar el código de seguridad de salida necesario. Debido a la redundancia y arquitectura de comunicaciones asimétricas, un fallo de cualquiera o ambas tareas, software o capacidad de procesamiento da como resultado un fallo de transmisión de un mensaje de salida de sistema crítico de seguridad o un mensaje de salida que no puede verificarse (y por tanto, no se usa o no se confía) mediante otros sistemas críticos de seguridad que reciben estos mensajes sin verificar.

La presente invención presenta un sistema de control para un sistema de aplicación crítico de seguridad ferroviaria (“sistema crítico de seguridad”). El sistema de control tiene al menos un controlador, que comprende un procesador de ordenador y está configurado para ejecutar tareas primera y segunda. La primera tarea puede estar en comunicación bilateral con la segunda tarea y puede enviar y recibir un mensaje de sistemas críticos de seguridad dentro de un sistema de aplicación crítico de seguridad ferroviaria. Ese mensaje incluye un código de seguridad y datos críticos de seguridad. La segunda tarea puede estar en comunicación bilateral con la primera tarea y puede recibir pero no puede enviar el mensaje de sistemas críticos de seguridad al sistema de aplicación crítico de seguridad ferroviaria. La segunda tarea tiene un generador de código de seguridad. El sistema de control tiene una ruta de comunicaciones entre tareas que acopla las tareas primera y segunda. Las tareas primera y segunda están configuradas para recibir un mensaje de sistemas críticos de seguridad de entrada común que incluye datos de sistemas críticos de seguridad de entrada y un código de seguridad de entrada. Ambos están configurados para verificar de manera independiente la integridad de mensaje de entrada y generar de manera independiente datos de sistemas críticos de seguridad de salida. La segunda tarea está configurada para generar un código de seguridad de salida y enviarlo a la primera tarea. La primera tarea está configurada para ensamblar y enviar un mensaje de sistemas críticos de seguridad de salida que incluye los datos de sistemas críticos de seguridad de salida y el código de seguridad de salida de la segunda tarea para su uso dentro del sistema de aplicación crítico de seguridad. El procesador de ordenador está configurado para ejecutar dicha primera tarea y dicha segunda tarea de manera simultánea, virtualmente y en tiempo real en dicho procesador de ordenador.

La presente invención también presenta un sistema ferroviario que comprende una pluralidad de sistemas de control

según la invención.

La presente invención presenta adicionalmente un método para controlar sistemas de control ferroviario crítico de seguridad (tal como sistemas de enclavamiento o sistemas de control de trenes). El método comprende recibir con tareas primera y segunda respectivas que se ejecutan en al menos un controlador, que comprende un procesador de ordenador, un mensaje de entrada de sistemas críticos de seguridad que se genera dentro de un sistema de aplicación crítico de seguridad ferroviaria que incluye un código de seguridad y datos críticos de seguridad, y verificar de manera independiente la integridad de mensaje de entrada. Después, cada una de las tareas genera de manera independiente datos de sistemas críticos de seguridad de salida en respuesta al mensaje de entrada. La segunda tarea genera un código de seguridad de salida que se envía a la primera tarea, que a su vez es responsable de ensamblar y enviar un mensaje de sistemas críticos de seguridad de salida que incluye los datos de sistemas críticos de seguridad de salida y el código de seguridad de salida de la segunda tarea. Dichas tareas primera y segunda se están ejecutando de manera simultánea, virtualmente y en tiempo real en el procesador de ordenador.

Los objetos y características de la presente invención pueden aplicarse conjuntamente o de manera variada en cualquier combinación o subcombinación por los expertos en la técnica.

Breve descripción de los dibujos

Las enseñanzas de la presente invención pueden entenderse fácilmente considerando la siguiente descripción detallada en relación con los dibujos adjuntos, en los que:

la figura 1 es un dibujo esquemático general del sistema de control de trenes a bordo que muestra la interacción de sistemas críticos de seguridad de trenes de la presente invención;

la figura 2 es un esquema de un ordenador o controlador del tipo usado en sistemas de control de sistema crítico de seguridad de trenes de la presente invención;

la figura 3 es un formato de mensaje de sistemas críticos de seguridad a modo de ejemplo usado en los sistemas de control de sistema crítico de seguridad de la presente invención;

la figura 4 es un diagrama de bloques que muestra interacción de comunicaciones entre los sistemas de control de sistema crítico de seguridad de la presente invención;

la figura 5 es un diagrama de tiempo que muestra etapas de procesamiento realizadas por una realización a modo de ejemplo de los sistemas de control de sistema crítico de seguridad de la presente invención; y

la figura 6 es un diagrama de tiempo que muestra etapas de procesamiento realizadas por otra realización a modo de ejemplo de los sistemas de control de sistema crítico de seguridad de la presente invención.

Para facilitar la comprensión, se han usado números de referencia idénticos, donde sea posible, para designar elementos idénticos que son comunes en las figuras.

Descripción detallada

Después de considerar la siguiente descripción, los expertos en la técnica se darán cuenta claramente de que las enseñanzas de la presente invención pueden utilizarse fácilmente en un sistema crítico de seguridad ferroviaria que sustituye el hardware comercial y/o el software de sistema operativo para componentes de productos de propiedad, y aun así se valida para conformarse con estándares de sistemas críticos de seguridad ferroviaria. En algunas realizaciones de la presente invención, el sistema crítico de seguridad utiliza un entorno de ordenador virtual con uno o más ordenadores personales, con dos tareas independientes y sistemas operativos, u otros controladores y sistemas operativos comercialmente disponibles. Cada ordenador, sistema operativo, lenguaje de software y compilador pueden diferir por diversidad adicional. Ambas tareas reciben y verifican datos de mensaje de entrada de sistemas críticos de seguridad e integridad de código de seguridad y generan de manera independiente datos de salida en respuesta al mensaje de entrada. Las tareas emparejadas independientes se comunican asimétricamente. La primera tarea tiene la única capacidad de enviar mensajes de salida del sistema crítico de seguridad, incluyendo los datos de salida y un código de seguridad de salida, pero sólo la segunda tarea tiene la capacidad de generar el código de seguridad de salida. Un fallo cualquiera de hardware, software de ordenador o capacidad de procesamiento da como resultado un fallo de transmisión de un mensaje de salida de sistema crítico de seguridad o transmite un mensaje de salida que no puede verificarse (y por tanto, no se usa o no se confía) por otros sistemas críticos de seguridad que reciben esos mensajes sin verificar.

Descripción general de sistemas críticos de seguridad de trenes

La figura 1 muestra en general un sistema ferroviario con vías 10 fijadas y uno o más trenes 40. La descripción

general en el presente documento acerca de comunicaciones de trenes, interacciones de sistemas de trenes que incluyen sistemas críticos de seguridad o similares, es de una naturaleza general para ayudar en la comprensión de cómo puede utilizarse la presente invención en un tren ferroviario. Las redes de trenes individuales y sistemas de trenes pueden variar de la descripción general a modo de ejemplo explicada en el presente documento. El tren 40 incluye un sistema 42 de datos/comunicaciones inalámbricas que puede transmitir y recibir datos inalámbricos, que está en comunicación con la red inalámbrica de estación de control de vías - trenes del sistema de comunicaciones (no mostrada).

El sistema 42 crítico de seguridad de comunicaciones de transmisor y receptor de tren se acopla de manera comunicativa directa o indirectamente a otros sistemas críticos de seguridad, incluyendo el sistema 50 de gestión de tren de a bordo (TMS) y una unidad 51 a bordo (OBU) que interviene en control de velocidad y frenos del tren en el caso de que el operario del tren falle en seguir las órdenes de parada y velocidad de vía locales. Normalmente, el tren 40 también tiene un sistema 60 de registro de datos a bordo (DRS) de diseño conocido, con un registrador 62 y uno o más dispositivos 64 de almacenamiento de memoria asociados, para entre otras cosas adquirir, procesar, organizar, formatear y registrar datos de sucesos. Como con cualquier otro sistema crítico de seguridad, la función de DRS 60 puede incorporarse como un subsistema dentro de otro sistema vital a bordo de tren, tal como el sistema 50 de gestión de tren (TMS), en vez de como un dispositivo autónomo independiente.

Como también se muestra en la figura 1, el tren 40 tiene generalmente otros subsistemas críticos de seguridad, que incluyen un sistema 72 de impulsión que proporciona fuerza motriz a uno o más carros de ruedas, y sistema 74 de frenos para modificar la velocidad del tren. El sistema 50 de gestión de tren a bordo (TMS) es el dispositivo de control electrónico principal para todos los otros subsistemas de trenes controlados, incluyendo el sistema 82A de posición de navegación (NPS) con el sistema 82B de detección de ubicación de tren asociado que proporciona información de velocidad y posición de tren. Otros subsistemas incluyen control de acelerador que hace que el sistema 72 de impulsión (por ejemplo, más o menos velocidad regulada) y recibe órdenes del TMS 50. El sistema 74 de frenos hace que los frenos frenen el tren 40. El sistema 74 de frenos también recibe órdenes del TMS 50. Otros vagones de tren y/o locomotoras 40' en tándem pueden estar opcionalmente en comunicación con el TMS 50 u otros subsistemas en el tren 40, tal como para la coordinación de frenos y control del acelerador. El tren 40 también tiene una interfaz 90 de máquina-hombre de tripulación de tren que tiene una pantalla 91 de visualización electrónica y controles de freno B y acelerador T accionados por operarios (uno o ambos de los que usa el operario dependiendo de las condiciones de operación del tren), de modo que el operario del tren puede conducir el tren. La HMI 90 se comunica con el TMS 50 a través de un bus 92 de datos de comunicaciones, aunque otras rutas de comunicaciones conocidas pueden sustituirse por el bus de datos cuando se implementan otras arquitecturas de sistema de control conocidas. La HMI 90 comunica las órdenes de control de acelerador T y frenos B respectivos de operario de tren al control 72 de motor respectivo y el sistema 74 de frenos.

En esta realización a modo de ejemplo de la figura 1, cada uno del sistema 50 de control de tren TMS, la OBU 51, el sistema 60 de registro de datos (DRS) y la HMI 90 tienen plataformas 100 de ordenador/controlador internas de diseño conocido que se comunican entre sí a través del bus 92 de datos. Sin embargo, el número de controladores de ordenador, su ubicación y sus funciones distribuidas pueden modificarse como una cuestión de elección de diseño. En esta realización a modo de ejemplo, el control general de subsistemas de tren 40 se realiza mediante el TMS 50 y la plataforma 100 de controlador en el mismo; las funciones de intervención se realizan mediante la OBU 51 y la plataforma 100 de controlador en la misma; las funciones de registro de datos se realizan mediante el sistema 60 de registro de datos y la plataforma 100 de controlador en la misma; y las funciones de la HMI se realizan mediante la HMI 90 y la plataforma 100 de controlador en la misma, aunque cualquiera de estos sistemas 50, 51, 60, 90 pueden combinarse en parte o en su totalidad.

Descripción general de tareas de sistemas ferroviarios críticos de seguridad y su comunicación

Haciendo referencia a la figura 2, una plataforma 100 de controlador física o virtual incluye un procesador 110 y un bus 120 de controlador en comunicación con la misma. El procesador 110 está acoplado a uno o más dispositivos 130 de memoria interna o externa que incluyen en el mismo un sistema 140 operativo y conjuntos de instrucción de módulo de software de programa 150 de aplicación a los que se accede y se ejecutan por el procesador, y hacen que su dispositivo de control respectivo (por ejemplo, TMS 50, OBU 51, DRS 60 o HMI 90, etc.) realice operaciones de control sobre sus respectivos subsistemas críticos de seguridad asociados.

Aunque se hace referencia a una arquitectura e implementación de una plataforma 100 de controlador a modo de ejemplo mediante módulos de software ejecutados por el procesador 110, también se entiende que la presente invención puede implementarse en diversas formas de hardware, software, firmware, procesadores con propósitos especiales o una combinación de los mismos. Preferiblemente, se implementan aspectos de la presente invención en software como un programa incluido de manera tangible en un dispositivo de almacenamiento de programa. El programa puede subirse a, y ejecutarse mediante, una máquina que comprende cualquier arquitectura adecuada. Preferiblemente, la máquina se implementa en una plataforma de ordenador que tiene hardware tal como una o más unidades centrales de procesamiento (CPU), una memoria de acceso aleatorio (RAM), e interfaz/interfaces de entrada/salida (I/O). La plataforma 100 de ordenador también incluye un sistema operativo y un código de microinstrucción. Los diversos procesos y funciones descritos en el presente documento pueden ser o bien parte del

código de microinstrucción o bien parte del programa (o combinación de los mismos) que se ejecuta a través del sistema operativo. Además, pueden conectarse otros diversos dispositivos periféricos a la plataforma 100 de ordenador/controlador.

Debe entenderse que debido a que algunos de los componentes del sistema y etapas de método representados en las figuras adjuntas se implementan preferiblemente en software, las conexiones reales entre los componentes de sistema (o las etapas de proceso) pueden diferir dependiendo de la manera en que la presente invención se programa. Específicamente, cualquiera de las plataformas o dispositivos de ordenador pueden interconectarse usando cualquier tecnología de red existente o descubierta últimamente y todas pueden también conectarse a través de un sistema de red más grande, tal como una red de empresa, red metropolitana o una red global tal como Internet.

La plataforma 100 de ordenador/controlador recibe comunicaciones de entrada desde uno o más dispositivos I de entrada a través de rutas I' de comunicaciones respectivas a través de la interfaz 160 de entrada, que a su vez puede distribuir la información de entrada a través del bus 120 de controlador. La interfaz 180 de salida facilita la comunicación con uno o más dispositivos O de salida a través de rutas O' de comunicaciones asociadas. La plataforma 100 de controlador también tiene una interfaz 170 de comunicaciones para la comunicación con otros controladores en un bus de datos externos compartido, tales como el bus 92 de datos que se describió anteriormente.

Haciendo referencia a las figuras 2-4, las comunicaciones entre plataformas 100 de ordenador/controlador y sus sistemas críticos de seguridad (SCS1-SCSn) respectivos se consiguen a través de un mensaje 200 de sistemas críticos de seguridad (SCSM) portado en el bus 92 de datos. Cada SCSM 200 se formatea y transmite según un protocolo conocido que se aprueba para la integridad de datos críticos de seguridad en sistemas críticos ferroviarios, incluyendo un código de seguridad conocido generado por protocolos conocidos CHECK-SUM, HASH, etc. El SCSM 200 a modo de ejemplo mostrado en la figura 3 incluye un sello 210 de tiempo, y si se requiere, un número de secuencia e identificadores de fuente y destino (no mostrados), datos 220 de sistema crítico de seguridad (datos de SCS) y un código 230 de seguridad (SC). Para facilitar la descripción en el presente documento, un mensaje de sistemas críticos de seguridad (SCSMI) entrante o de entrada comprende datos de entrada críticos de seguridad (DI) y un código de seguridad de entrada (SI). De manera similar, un mensaje de sistemas críticos de seguridad (SCSMO) saliente o de salida comprende datos de salida críticos de seguridad (DO) y un código de seguridad de salida (SO). Cuando un sistema crítico de seguridad SCS1-SCSn recibe un SCSMI su integridad de datos se verifica con un módulo de análisis SCI 240 conocido dentro de las tareas (T1, T2). Si la integridad de datos de SCSMI verifica los DI se utilizan mediante las tareas para preparar un mensaje de salida de respuesta SCSMO que incluye datos de salida DO y un código de seguridad de salida generado en el módulo de generación SCO 250. Como con el módulo SCI 240, la función de generación de módulo SCO 250 se implementa en hardware, firmware, software o cualquier combinación de los mismos. El SCSMO generado posteriormente se comunica a una o más plataformas de controlador SCS destinatarias que a su vez tratan el mensaje como un SCSMI.

Operación y sistema de control redundante

En la figura 4, las tareas de sistema crítico de seguridad SCS1 y SCS2 comprenden respectivamente un conjunto emparejado de tareas T1 300 y T2 320 que están en comunicación bilateral entre sí a través de una interfaz 330 de datos entre controladores. Las tareas 300, 320 se ejecutan en dispositivos de consumidor o comerciales industriales comercialmente disponibles, tales como por ejemplo controladores lógicos programables industriales, placas madre de ordenador/controlador independientes o unificados, u ordenadores personales/placas madre comercialmente disponibles. Las tareas 300, 320 se ejecutan virtualmente en un procesador de ordenador. Las tareas T1 y T2 independientes, se ejecutan ambas de manera simultánea, virtualmente y en tiempo real, en un procesador 100 de ordenador común, con las subtareas SCI 240 y SCO 250 respectivas también implementadas virtualmente.

La tarea T1 300 puede realizar comunicación bilateral con el bus 92 de datos de sistema crítico a través de la ruta 340 de comunicaciones, que puede comprender un puerto de comunicaciones habilitado en la interfaz 170 de comunicaciones de plataforma 100 de tareas. La tarea 300 tiene un módulo 240 de verificación de código de seguridad entrante que le permite verificar la integridad de datos de un SCSMI, pero no tiene la capacidad de generar un código de seguridad SCO de SCSMO saliente.

La tarea T2 320 tiene un generador 250 de código de seguridad SCO saliente habilitado, pero no puede transmitir un SCO y datos de salida críticos directamente a la interfaz 92 de datos de sistema crítico. La tarea 320 sólo puede transmitir el SCO a la tarea 300 a través de la interfaz 330 de datos interna: sólo puede recibir un SCSMI a través de una ruta 350 de comunicaciones entrante unilateral y puede verificar la integridad de datos con el módulo 240 de verificación de SCI. Dicho de otro modo, la tarea T2 320 no puede transmitir directamente SCSMO al bus 92 de datos.

Tal como puede entenderse por referencia a las figuras 5 y 6, las tareas T1 300 y tarea T2 320 respectivas en SCS1 están en una relación emparejada mutuamente dependiente con implementaciones de comunicaciones asimétricas. La primera tarea T1 300 puede recibir un SCSMI y enviar un SCSMO de respuesta, pero no puede crear el mensaje

de respuesta hasta que recibe el SCO desde la segunda tarea T2 320. La tarea T2 no puede realizar comunicación externa con el bus 92 de datos de sistema crítico, y debe apoyarse en la tarea T1 para enviar cualquier mensaje.

En la figura 5, uno de los sistemas críticos de seguridad SCS2-SCSn está enviando un SCSMI en la etapa 400, que comprende un DI y un SCI para SCS1 en el momento t1, donde se reciben por tanto T1 como T2. En el momento t2, tanto T1 como T2 verifican la integridad de datos de SCSMI en la etapa 410 y en la etapa 420 ambos generan datos DO (t3) en respuesta a los datos DI de entrada. En la etapa 430, T2 genera el código de seguridad de salida SCO en el momento t4 y lo envía a T1 en la etapa 440. En la etapa 450 (t5), T1 ensambla ahora y verifica opcionalmente los DO (proporcionados por T2 en la etapa anterior) con sus propios DO generados antes de transmitir el SCSMO a través del bus 92 de datos de sistemas críticos en la etapa 460 (t6) a otros sistemas críticos de seguridad. Si los DO no se corroboran entre sí durante la etapa 450 (es decir, los datos de salida son sospechosos) no se transmitirá el SCSMO. Alternativamente, si T1 no se permite que verifique los DO o si T1 y /o T2 no funcionan correctamente, puede transmitir un SCSMO corrompido, pero la corrupción se identificará cuando el mensaje se reciba por otro sistema crítico de seguridad.

La realización de la figura 6 tiene todas las etapas y procesos que la realización de la figura 5, pero añade una etapa 415 de verificación de SCSMI de comparación, en la que T1 y T2 comprueban los resultados de verificación respectivos entre sí. Si los resultados comparados no son los mismos, SCS1 marca un fallo. Esta realización también añade una etapa 425 de comparación de datos de salida DO antes de que T2 genere el código de salida de seguridad SCO en la etapa 430. De nuevo, si los resultados comparados no son los mismos, SCS1 marca un fallo.

La redundancia de software y las características de generación/transmisión de código de seguridad de salida de comunicación asimétrica mutuamente dependientes del sistema de control ferroviario de la presente invención para sistemas críticos de seguridad garantiza un mayor nivel de seguridad que cualquier par de procesamiento individual o independientemente paralelo de controladores u ordenadores personales comercialmente disponibles. Un único ordenador es susceptible a múltiples formas de fallo que no se detectarían necesariamente por otros sistemas críticos de seguridad que reciben SCSMO del ordenador que falla. Dos ejecuciones T1 y T2 de tareas independientes y paralelas, ya se implementen en una o múltiples plataformas de ordenador, alimentando idénticos SCSMO a otros sistemas críticos de seguridad o que corroboran mensajes de salida antes de su transmisión, pueden generar ambas mensajes de salida incorrectos idénticos. Tales errores de transmisión de modo de fallo no son posibles con el sistema de control de la presente invención.

Cuando se analizan posibles modos de fallo de los sistemas de control de sistemas críticos de seguridad de la presente invención SCS1, si T1 calcula un DO incorrecto y T2 calcula un DO y SCO correctos, entonces durante la etapa de verificación 450, T1 marcará una discordancia entre su propio DO y el DO y marca un error. Si T1 no verifica el SCSMO en la etapa 450, otros sistemas críticos de seguridad que reciben ese mensaje marcarán el error cuando verifican el mensaje recibido. En cambio, si el DO de T1 es correcto, pero o bien el DO de T2 o bien el SCO son incorrectos, T2 u otro SCS que reciben el SCSMO identificarán el error. Si tanto T1 como T2 no funcionan correctamente y generan DO y/o SCO con fallos, la discordancia del DO y SCO se observará mediante otros sistemas críticos que reciben posteriormente el mensaje corrompido.

Aunque diversas realizaciones que incorporan las enseñanzas de la presente invención, se han mostrado y se describen con detalle en el presente documento, los expertos en la técnica pueden idear fácilmente muchas otras realizaciones variadas que todavía incorporan estas enseñanzas.

REIVINDICACIONES

1. Sistema de control para un sistema de aplicación crítico de seguridad ferroviaria, que comprende:

al menos un controlador, que comprende un procesador de ordenador y está configurado para ejecutar tareas primera y segunda;

pudiendo la primera tarea estar en comunicación bilateral con la segunda tarea y pudiendo enviar y recibir un mensaje de sistemas críticos de seguridad dentro de un sistema de aplicación crítico de seguridad ferroviaria, incluyendo el mensaje un código de seguridad y datos críticos de seguridad;

pudiendo la segunda tarea estar en comunicación bilateral con la primera tarea y pudiendo recibir un mensaje de sistemas críticos de seguridad, pero no pudiendo enviar el mensaje de sistemas críticos de seguridad al sistema de aplicación crítico de seguridad ferroviaria, teniendo la segunda tarea un generador de código de seguridad;

comprendiendo además el sistema de control una ruta de comunicaciones entre tareas que acopla las tareas primera y segunda;

en el que las tareas primera y segunda están configuradas cada una para

recibir un mensaje de sistemas críticos de seguridad de entrada común que incluye datos de sistemas críticos de seguridad de entrada y un código de seguridad de entrada,

verificar de manera independiente la integridad de mensaje de entrada y

generar de manera independiente datos de sistemas críticos de seguridad de salida,

la segunda tarea está configurada para generar un código de seguridad de salida y para enviarlo a la primera tarea, y

la primera tarea está configurada para ensamblar y enviar un mensaje de sistemas críticos de seguridad de salida que incluye los datos de sistemas críticos de seguridad de salida y el código de seguridad de salida de la segunda tarea para su utilización dentro del sistema de aplicación crítico de seguridad ferroviaria,

caracterizado por estar dicho procesador de ordenador configurado para ejecutar dicha primera tarea y dicha segunda tarea de manera simultánea, virtualmente y en tiempo real en dicho procesador de ordenador.

2. Sistema según la reivindicación 1, en el que las tareas primera y segunda comparan sus verificaciones de integridad de mensaje de entrada respectivas antes de generar datos de sistemas críticos de seguridad de salida respectivos.

3. Sistema según la reivindicación 2, en el que las tareas primera y segunda comparan sus datos de sistemas críticos de seguridad de salida respectivos, en particular antes de la generación del código de seguridad de salida.

4. Sistema según la reivindicación 1, en el que la primera tarea verifica la integridad de datos de sistemas críticos de seguridad de salida antes de enviar el mensaje de sistemas críticos de seguridad de salida.

5. Sistema según la reivindicación 1, en el que las tareas primera y segunda se ejecutan en al menos un ordenador personal, las tareas ejecutadas además mediante al menos uno de diferentes sistemas operativos o conjuntos de instrucciones de software.

6. Sistema de aplicación crítica de seguridad ferroviaria que comprende un sistema de control según la reivindicación 1 ó 5.

7. Sistema ferroviario que comprende: una pluralidad de sistemas de control según cualquiera de las reivindicaciones 1 a 5.

8. Sistema ferroviario según la reivindicación 7, en el que las tareas primera y segunda comparan sus verificaciones de integridad de mensaje de entrada respectivas antes de generar datos de sistemas críticos de seguridad de salida respectivos.

9. Sistema ferroviario según la reivindicación 8, en el que las tareas primera y segunda comparan sus datos de sistemas críticos de seguridad de salida respectivos antes de, en particular, la generación del código de

seguridad de salida.

10. Sistema ferroviario según la reivindicación 7, en el que la primera tarea verifica la integridad de datos de sistemas críticos de seguridad de salida antes de enviar el mensaje de sistemas críticos de seguridad de salida.

11. Sistema ferroviario según la reivindicación 7, en el que dentro de cada sistema de control respectivo, las tareas primera y segunda se ejecutan en al menos un ordenador personal, ejecutándose además las tareas mediante al menos uno de diferentes sistemas operativos o conjuntos de instrucciones de software, en particular en el que cada sistema de control respectivo, las tareas primera y segunda se ejecutan en ordenadores que tienen diferentes construcciones de hardware y diferentes sistemas operativos.

12. Método para controlar un sistema de control de aplicación crítica de seguridad ferroviaria que comprende:

recibir con tareas primera y segunda respectivas que se ejecutan en al menos un controlador, que comprende un procesador de ordenador, un mensaje de entrada de sistemas críticos de seguridad que se genera dentro de un sistema de aplicación crítica de seguridad ferroviaria que incluye un código de seguridad y datos críticos de seguridad, y verificando de manera independiente la integridad del mensaje de entrada;

generar de manera independiente datos de sistemas críticos de seguridad de salida en respuesta al mensaje de entrada con las tareas primera y segunda respectivas;

generar un código de seguridad de salida sólo con la segunda tarea y enviar el código de seguridad de salida generado a la primera tarea; y

ensamblar y enviar un mensaje de sistemas críticos de seguridad de salida que incluye los datos de sistemas críticos de seguridad de salida y código de seguridad de salida de la segunda tarea con la primera tarea.

en el que dicha primera tarea y dicha segunda tarea se ejecutan de manera simultánea, virtualmente y en tiempo real en el procesador de ordenador.

13. Método según la reivindicación 12, que comprende además comparar verificaciones de integridad de mensaje de entrada de tareas primera y segunda respectivas antes de generar datos de sistemas críticos de seguridad de salida respectivos.

14. Método según la reivindicación 13, que comprende además comparar datos de sistemas críticos de seguridad de salida respectivos de tareas primera y segunda, en particular antes de la generación del código de seguridad de salida.

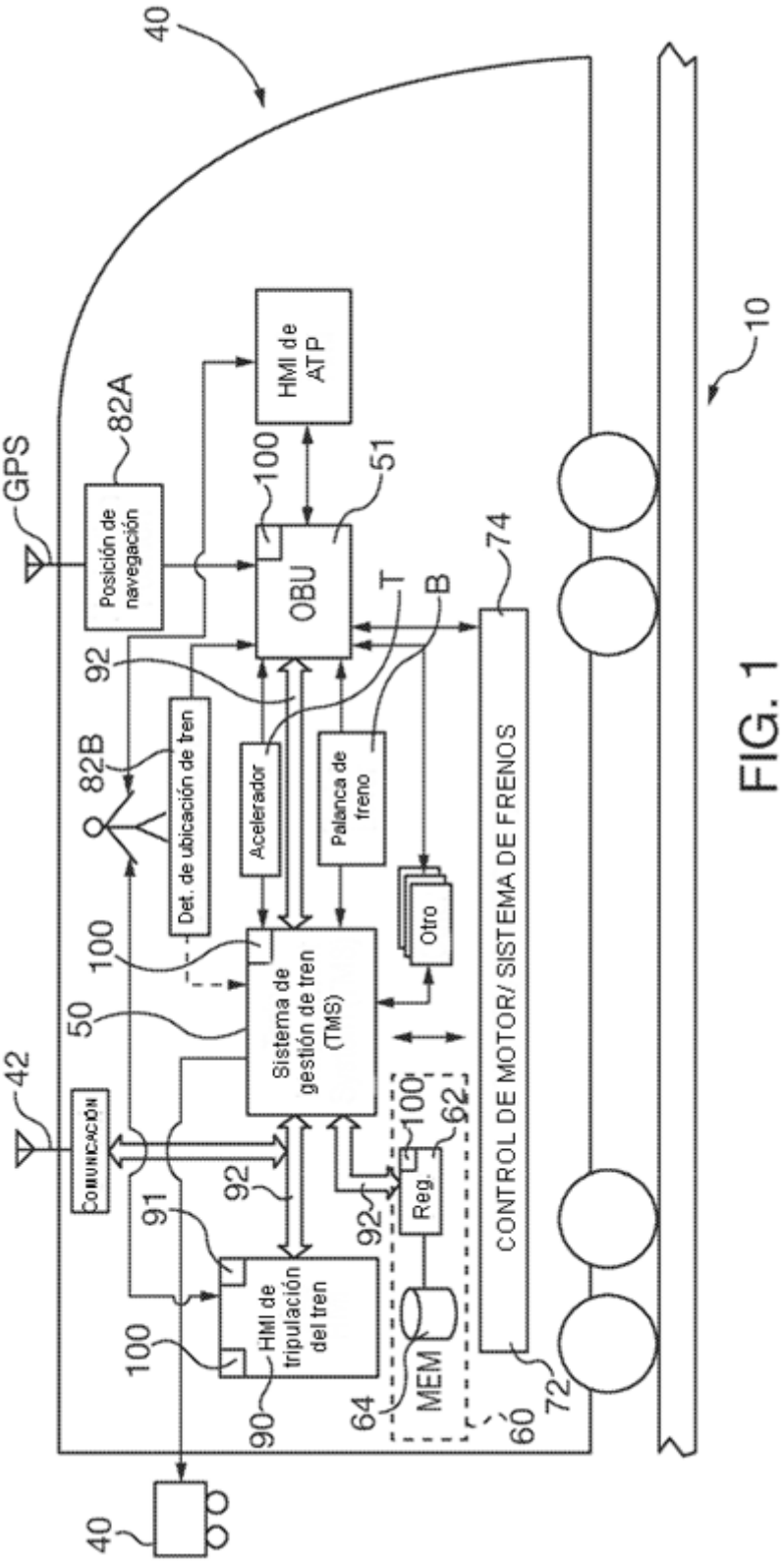
40
GPS
82A
Posición de navegación
HMI de ATP
100
51
OBU
T
B
74
92
82B
Det. de ubicación de tren
Acelerador
Palanca de freno
Otro
100
50
Sistema de gestión de tren (TMS)
42
COMUNICACIÓN
100
62
Reg.
92
91
92
HMI de tripulación del tren
100
MEM
64
60
72
CONTROL DE MOTOR/ SISTEMA DE FRENOS
90
40
10

FIG. 1

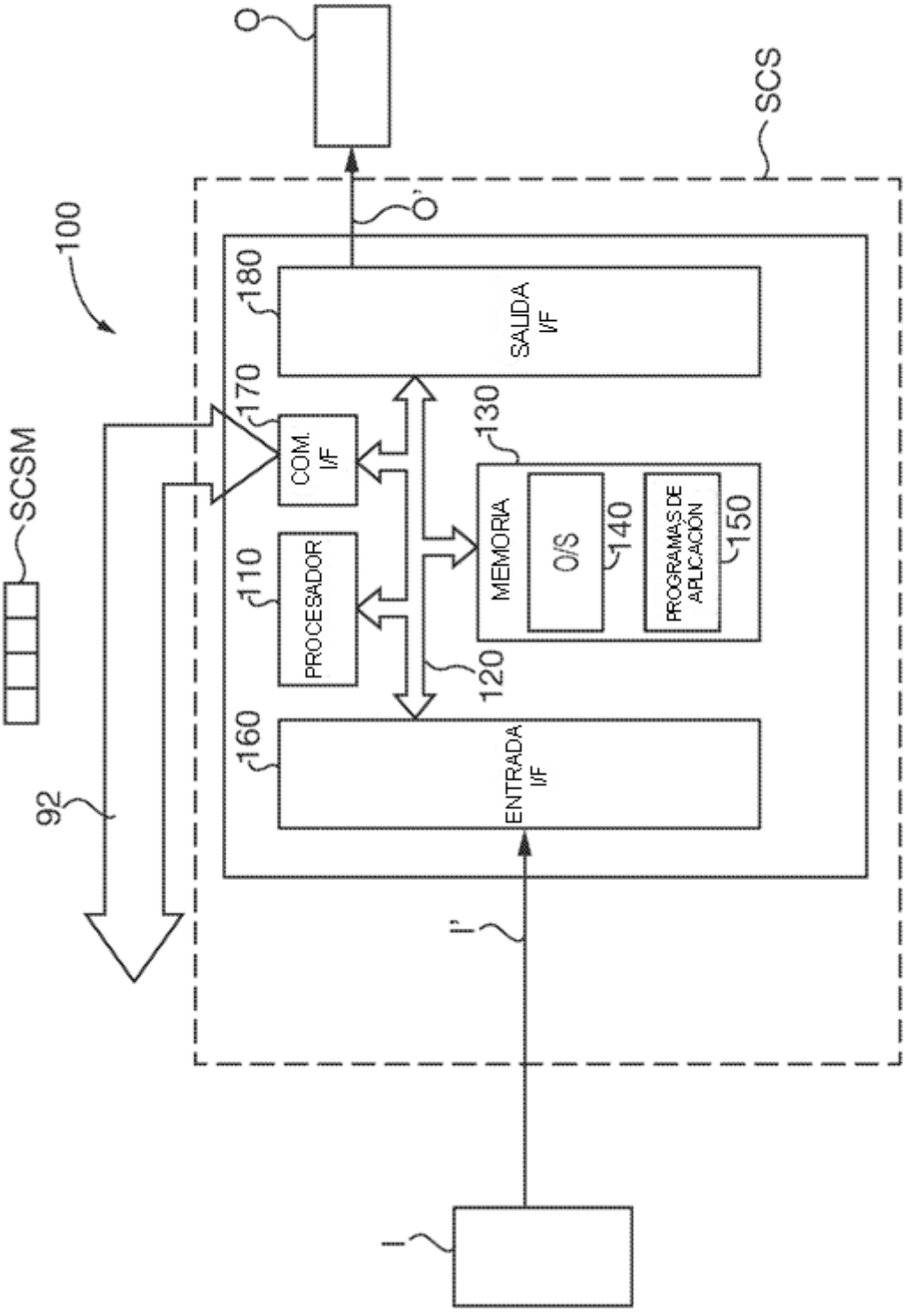
O
SCS
O'
100
180
SALIDA I/F
170
COM. I/F
130
MEMORIA
O/S
140
PROGRAMAS DE APLICACIÓN
150
SCSM
110
PROCESADOR
120
160
ENTRADA I/F
92
I'
I

FIG. 2

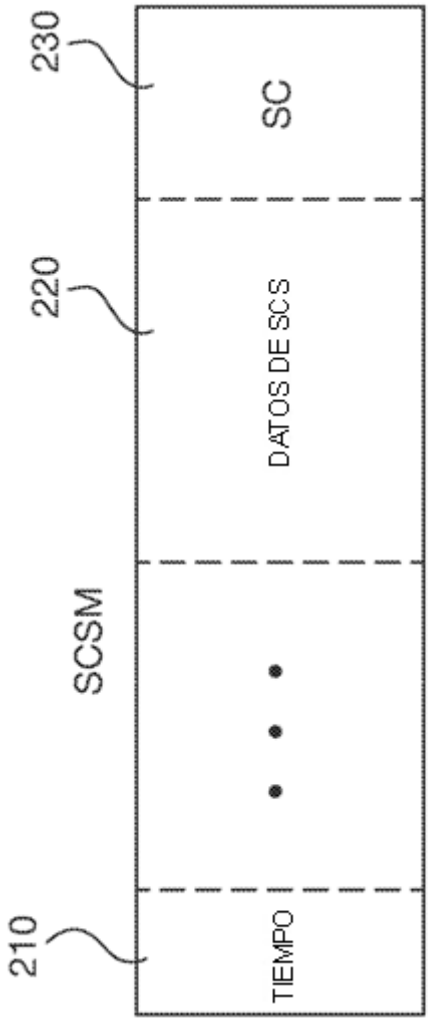

FIG. 3

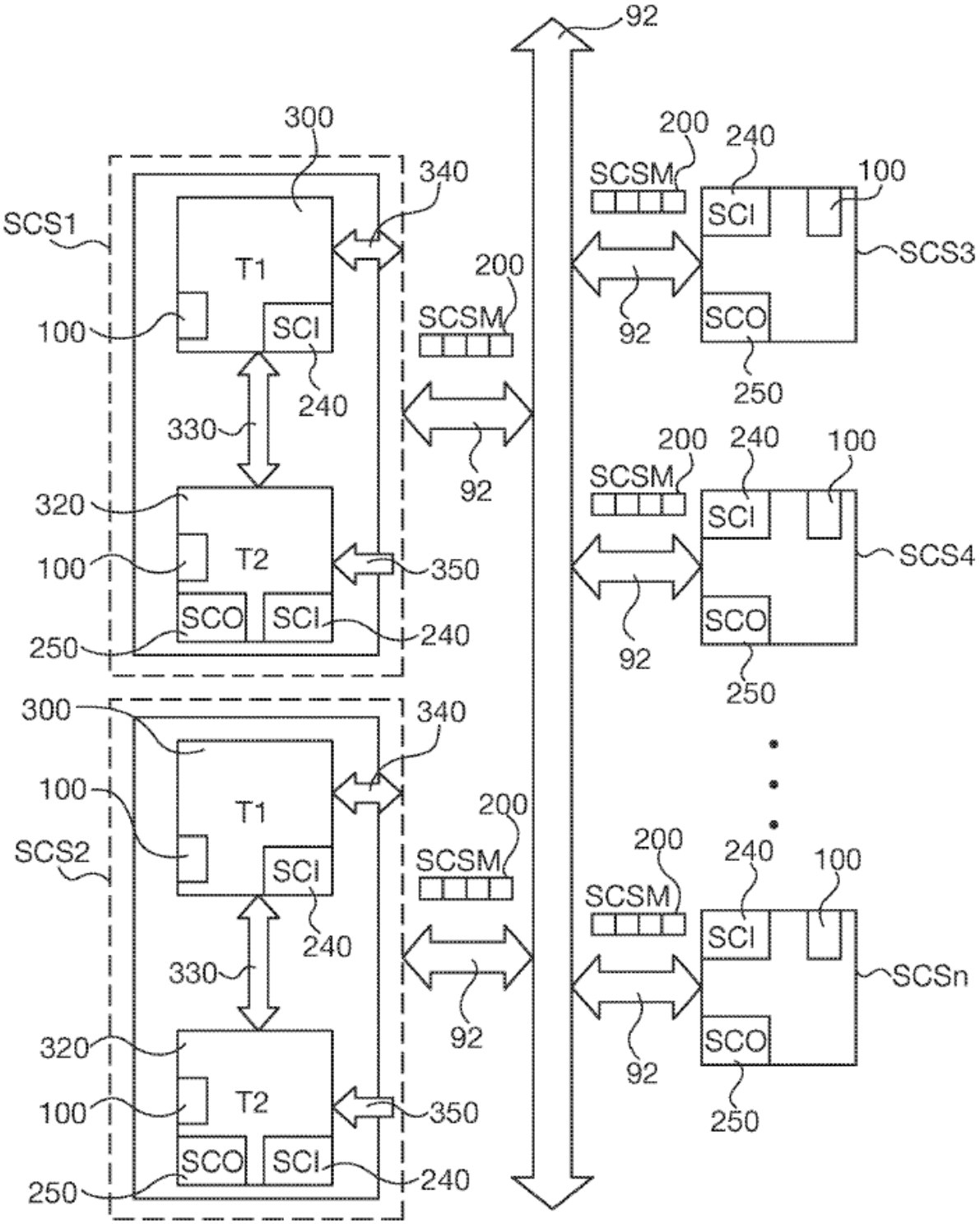
92
300
340
SCS1
T1
100
SCI
240
330
320
T2
100
SCO
SCI
250
240
350
200
SCSM
92
200
240
100
SCSM
SCI
SCS3
SCO
92
250
200
240
100
SCSM
SCI
SCS4
SCO
92
250
300
340
100
T1
SCS2
SCI
240
330
320
T2
100
SCO
SCI
250
240
350
200
SCSM
92
200
240
100
SCSM
SCI
SCSn
SCO
92
250

FIG. 4

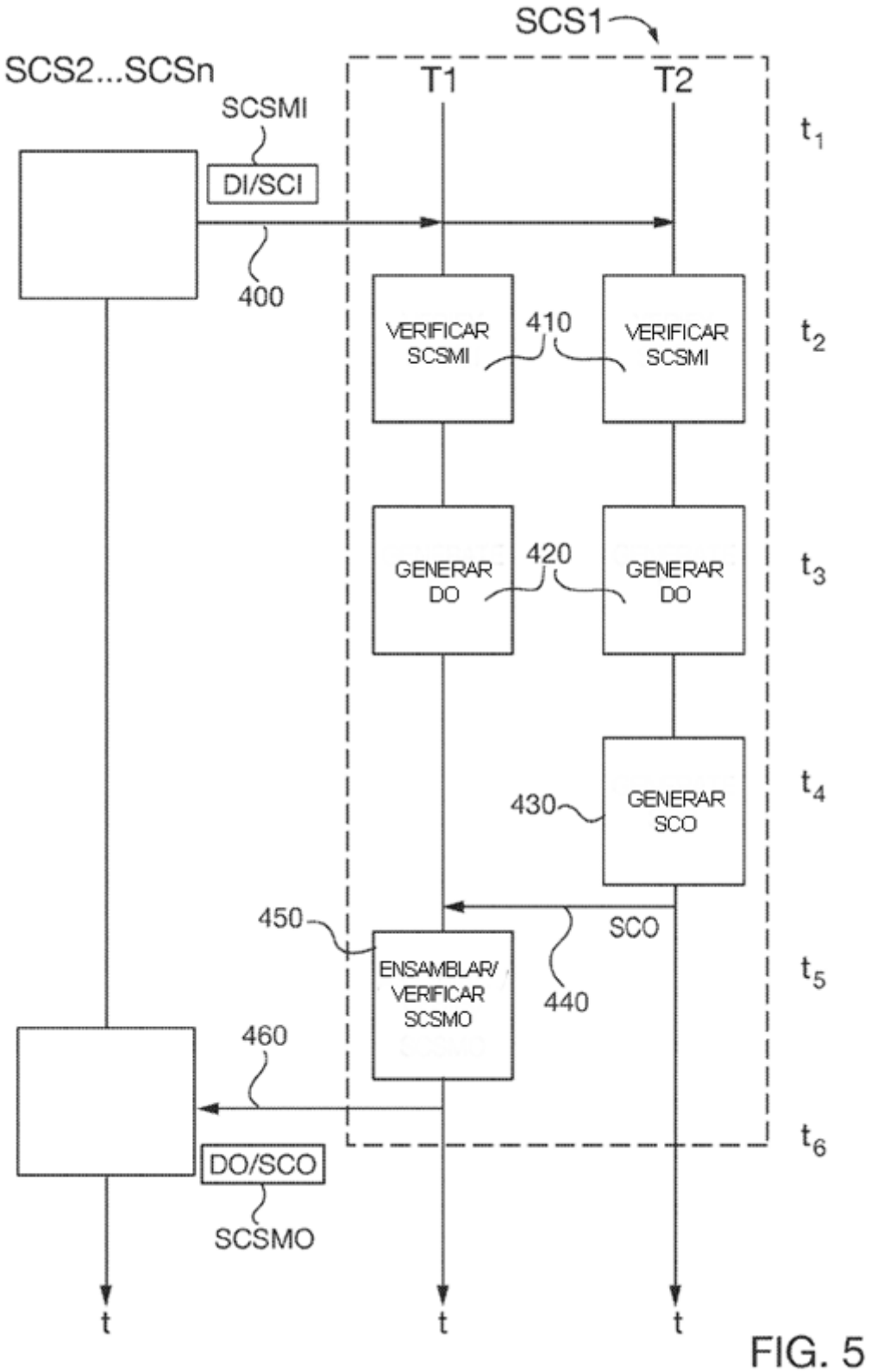
SCS1
SCS2...SCSn
T1
T2
SCSMI
DI/SCI
400
VERIFICAR SCSMI
410
VERIFICAR SCSMI
GENERAR DO
420
GENERAR DO
430
GENERAR SCO
SCO
450
ENSAMBLAR/ VERIFICAR SCSMO
440
460
DO/SCO
SCSMO
t1
t2
t3
t4
t5
t6
t
t
t

FIG. 5

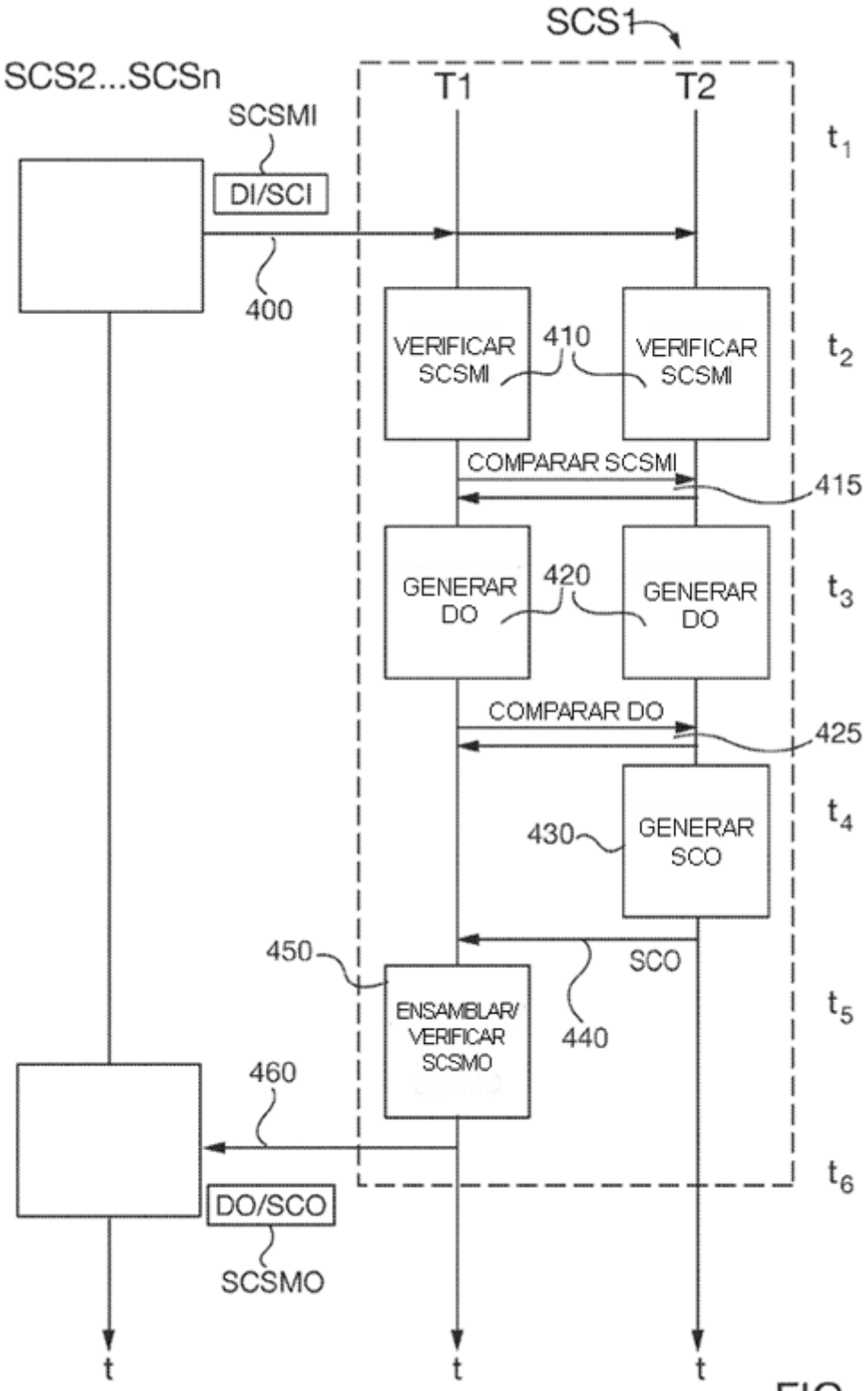
SCS1
SCS2...SCSn
T1
T2
SCSMI
DI/SCI
400
VERIFICAR SCSMI
410
VERIFICAR SCSMI
COMPARAR SCSMI
415
GENERAR DO
420
GENERAR DO
COMPARAR DO
425
430
GENERAR SCO
SCO
450
ENSAMBLAR/ VERIFICAR SCSMO
440
460
DO/SCO
SCSMO
t1
t2
t3
t4
t5
t6
t
t
t

FIG. 6