

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 914 710**

51 Int. Cl.:

B60R 16/023	(2006.01) B60P 3/34	(2006.01)
B60W 30/08	(2012.01) E05B 39/04	(2006.01)
B60W 50/12	(2012.01)	
B60W 50/02	(2012.01)	
B60W 50/00	(2006.01)	
H04W 4/38	(2008.01)	
H04W 4/48	(2008.01)	
F16P 3/00	(2006.01)	
G07C 9/00	(2010.01)	
E04H 15/08	(2006.01)	

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **06.03.2020** **E 20161590 (3)**

97 Fecha y número de publicación de la concesión europea: **04.05.2022** **EP 3708435**

54 Título: **Creación de consenso entre dispositivos en red para sistemas de seguridad de vehículos recreativos**

30 Prioridad:

14.03.2019 US 201962818392 P
20.02.2020 US 202016795802

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2022

73 Titular/es:

LIPPERT COMPONENTS, INC. (100.0%)
4100 Edison Lakes Parkway, Suite 210
Mishawaka, IN 46545, US

72 Inventor/es:

MANFRED, JOHN PETER;
DIPERNA, ANTHONY J.;
HARRIS, AARON ROBERTSON y
COLLIN, MATTHEW ALLEN

74 Agente/Representante:

PONS ARIÑO, Ángel

ES 2 914 710 T3

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

DESCRIPCIÓN

Creación de consenso entre dispositivos en red para sistemas de seguridad de vehículos recreativos

5 **Campo**

Esta solicitud se refiere en general a una red de comunicaciones electrónicas usada para las comunicaciones en un sistema de bloqueo de seguridad de un vehículo recreativo.

10 **Antecedentes**

Se sabe que los vehículos recreativos incluyen controladores electrónicos (denominados también controles) diseñados para implementar circuitería que detecta y responde a condiciones de bloqueo de seguridad. Este enfoque puede ser ineficiente cuando se usan múltiples controladores electrónicos en el mismo sistema. Por ejemplo, muchos VR modernos tienen un sistema de bloqueo de seguridad que tiene controladores separados para los deslizadores, los toldos, los niveladores, las cerraduras de las puertas, etc., teniendo cada uno de tales controladores que implementar la circuitería de interbloqueo de seguridad independientemente. Un sistema de bloqueo de seguridad es un sistema que evita que se lleven a cabo ciertas operaciones electromecánicas cuando estas operaciones pueden dar como resultado una reducción de la seguridad, y el término "bloqueo" se refiere en general a la prevención o inhibición de esta funcionalidad. Otra desventaja del estado de la técnica es que diferentes controladores pueden detectar la condición de bloqueo de manera diferente, lo que puede conducir a un comportamiento inconsistente entre los controladores.

Sumario

De acuerdo con una realización, se proporciona un método para controlar una operación electromecánica de un dispositivo electromecánico basándose en una condición de bloqueo de seguridad determinada usando un sistema de bloqueo de seguridad distribuido, comprendiendo el sistema de bloqueo de seguridad distribuido una pluralidad de dispositivos en red comunicativamente acoplados mediante una red de comunicaciones, incluyendo la pluralidad de dispositivos en red uno o más controladores electrónicos y una pluralidad de dispositivos de detección de condición de bloqueo de seguridad. El método puede incluir: en uno o más de la pluralidad de dispositivos en red: (i) recibir un estado de bloqueo de seguridad de otro dispositivo en red mediante la red de comunicaciones; (ii) comparar un estado de bloqueo de seguridad local con el estado de bloqueo de seguridad recibido; (iii) determinar si actualizar el estado de bloqueo de seguridad local basándose en los resultados de la comparación del estado de bloqueo de seguridad local al estado de bloqueo de seguridad recibido y, cuando se determina actualizar el estado de bloqueo de seguridad local, a continuación, actualizar el estado de bloqueo de seguridad local al estado de bloqueo de seguridad recibido; y (iv) difundir el estado de bloqueo de seguridad local a través de la red de comunicaciones. El método puede incluir adicionalmente, en uno o más de la pluralidad de dispositivos de detección de condición de bloqueo de seguridad: (i) determinar un estado de bloqueo de seguridad propuesto basándose en datos de sensor obtenidos por el dispositivo de detección de condición de bloqueo de seguridad; (ii) comparar el estado de bloqueo de seguridad propuesto con el estado de bloqueo de seguridad local y/o un estado de bloqueo de seguridad recibido que se recibe desde otro dispositivo en red a través de la red de comunicaciones; y (iii) determinar que un estado de bloqueo de seguridad local actualizado es el estado de bloqueo de seguridad local basándose en la comparación del estado de bloqueo de seguridad propuesto con el estado de bloqueo de seguridad local y/o el estado de bloqueo de seguridad recibido. El método puede incluir adicionalmente, en cualquiera del uno o más controladores electrónicos, controlar una operación electromecánica de un dispositivo electromecánico basándose en el estado de bloqueo de seguridad local.

Opcionalmente, el sistema de bloqueo de seguridad distribuido está instalado en un vehículo recreativo.

Opcionalmente, el sistema de bloqueo de seguridad distribuido incluye una pluralidad de controladores electrónicos que incluye el uno o más controladores electrónicos y una pluralidad de dispositivos electromecánicos que incluye el dispositivo o dispositivos electromecánicos, y en donde cada uno de la pluralidad de dispositivos electromecánicos se controla por uno diferente de la pluralidad de controladores electrónicos.

Opcionalmente, un primer controlador electrónico de la pluralidad de controladores electrónicos controla la operación electromecánica de un primer dispositivo electromecánico de la pluralidad de dispositivos electromecánicos, en donde un segundo controlador electrónico de la pluralidad de controladores electrónicos controla la operación electromecánica de un segundo dispositivo electromecánico de la pluralidad de dispositivos electromecánicos, y en donde el primer controlador electrónico opera independientemente del segundo controlador electrónico.

Opcionalmente, el primer dispositivo electromecánico es un nivelador que está instalado en el vehículo recreativo, y en donde el segundo dispositivo electromecánico es un deslizador que está instalado en el vehículo recreativo.

Opcionalmente, la pluralidad de dispositivos de detección de condición de bloqueo de seguridad incluye un primer dispositivo de detección de condición de bloqueo de seguridad y un segundo dispositivo de detección de condición

de bloqueo de seguridad, en donde el primer dispositivo de detección de condición de bloqueo de seguridad está configurado para detectar una primera condición de bloqueo de seguridad, en donde el segundo dispositivo de detección de condición de bloqueo de seguridad está configurado para detectar una segunda condición de bloqueo de seguridad que es diferente de la primera condición de bloqueo de seguridad.

5 Opcionalmente, cada una de la primera condición de bloqueo de seguridad y la segunda condición de bloqueo de seguridad está basada en al menos uno de lo siguiente: señales del sistema de satélite de navegación global (GNSS) recibidas en un receptor de GNSS, un estado del freno de estacionamiento, un estado del freno del remolque, un estado del freno del vehículo remolcador, el estado de la luz de freno del vehículo remolcador, o una
10 orientación o movimiento detectado por un sensor de movimiento/orientación, y en donde la primera condición de bloqueo de seguridad es diferente de la segunda condición de bloqueo de seguridad.

Opcionalmente, la red de comunicaciones es un bus de red de área de controlador (CAN) alámbrica o una red de interconexión local alámbrica que está instalada en el vehículo recreativo.

15 Opcionalmente, la red de comunicaciones es una red de comunicaciones inalámbricas que se lleva a cabo usando una red de comunicación de corto alcance (DSRC) especializada que se proporciona en el vehículo recreativo.

Opcionalmente, la red de comunicaciones incluye una red de comunicaciones inalámbricas usada por uno primero de los dispositivos en red y una red de comunicaciones alámbrica usada por uno segundo de los dispositivos en red.

Opcionalmente, uno o más de los dispositivos en red operan de acuerdo con un protocolo de consenso que incluye un modo de duplicación de red y un modo de contención de red, en donde, cuando está en el modo de contención de red, uno o más de los dispositivos en red votan establecer un consenso en cuanto a si se reducirá el estado de
25 bloqueo de seguridad local de cada uno de los dispositivos en red.

Opcionalmente, en respuesta a emitir uno primero de los dispositivos en red una solicitud de borrado cuando cada uno de los dispositivos en red está operando en el modo de duplicación de red, cada uno de los dispositivos en red pasa para operar en el modo de contención de red para establecer el consenso.

30 De acuerdo con una realización, se proporciona un sistema de bloqueo de seguridad distribuido para un vehículo recreativo, en donde el sistema puede incluir una pluralidad de dispositivos en red instalados en un sistema electromecánico, y en donde la pluralidad de dispositivos en red pueden estar comunicativamente acoplados mediante una red de comunicaciones. La pluralidad de dispositivos en red puede incluir: (i) uno o más controladores electrónicos, cada uno de los cuales está configurado para controlar un dispositivo electromecánico del vehículo recreativo basándose en un estado de bloqueo de seguridad local; y (ii) una pluralidad de dispositivos de detección de condición de bloqueo de seguridad, cada uno de los cuales está configurado para detectar un estado de bloqueo de seguridad basándose en información de sensor obtenida por circuitería de detección de bloqueo. Además, uno o más de la pluralidad de dispositivos en red puede estar configurado para alternar entre un modo de duplicación de red y un modo de contención de red y, cuando opera en el modo de duplicación de red, para determinar un estado de bloqueo de seguridad local actualizado basándose en una comparación del estado de bloqueo de seguridad local con un estado de seguridad de bloqueo recibido, recibiendo el estado de seguridad de bloqueo recibido a través de la red de comunicaciones desde otro de los dispositivos en red; y cuando opera en el modo de contención de red, cada dispositivo de la pluralidad de dispositivos de detección de condición de bloqueo de seguridad puede estar
45 configurado para obtener el estado de bloqueo de seguridad detectado basándose en la información de sensor, para comparar el estado de bloqueo de seguridad detectado con el estado de bloqueo de seguridad local y/o un estado de bloqueo de seguridad propuesto recibido, para establecer el estado de bloqueo de seguridad local basándose en la comparación, y para difundir el estado de bloqueo de seguridad local a través de la red de comunicaciones.

50 Opcionalmente, el sistema de bloqueo de seguridad distribuido incluye una pluralidad de controladores electrónicos que incluye el uno o más controladores electrónicos y una pluralidad de dispositivos electromecánicos que incluye el dispositivo o dispositivos electromecánicos, y en donde cada uno de la pluralidad de dispositivos electromecánicos se controla por uno diferente de la pluralidad de controladores electrónicos.

55 Opcionalmente, un primer controlador electrónico de la pluralidad de controladores electrónicos controla la operación electromecánica de un primer dispositivo electromecánico de la pluralidad de dispositivos electromecánicos, en donde un segundo controlador electrónico de la pluralidad de controladores electrónicos controla la operación electromecánica de un segundo dispositivo electromecánico de la pluralidad de dispositivos electromecánicos, y en donde el primer controlador electrónico opera independientemente del segundo controlador electrónico.

60 Opcionalmente, el primer dispositivo electromecánico es un nivelador que está instalado en el vehículo recreativo, y en donde el segundo dispositivo electromecánico es un deslizador que está instalado en el vehículo recreativo.

Opcionalmente, la pluralidad de dispositivos de detección de condición de bloqueo de seguridad incluye un primer dispositivo de detección de condición de bloqueo de seguridad y un segundo dispositivo de detección de condición de bloqueo de seguridad, en donde el primer dispositivo de detección de condición de bloqueo de seguridad está
65

configurado para detectar una primera condición de bloqueo de seguridad, en donde el segundo dispositivo de detección de condición de bloqueo de seguridad está configurado para detectar una segunda condición de bloqueo de seguridad que es diferente de la primera condición de bloqueo de seguridad.

Opcionalmente, cada una de la primera condición de bloqueo de seguridad y la segunda condición de bloqueo de seguridad está basada en al menos uno de lo siguiente: señales del sistema de satélite de navegación global (GNSS) recibidas en un receptor de GNSS, un estado del freno de estacionamiento, un estado del freno del remolque, un estado del freno del vehículo remolcador, el estado de la luz de freno del vehículo remolcador, o una orientación o movimiento detectado por un sensor de movimiento/orientación, y en donde la primera condición de bloqueo de seguridad es diferente de la segunda condición de bloqueo de seguridad.

Opcionalmente, la red de comunicaciones es un bus de red de área de controlador (CAN) alámbrica o una red de interconexión local alámbrica que está instalada en el vehículo recreativo;

Opcionalmente, la red de comunicaciones es una red de comunicaciones inalámbricas que se lleva a cabo usando una red de comunicación de corto alcance (DSRC) especializada que se proporciona en el vehículo recreativo.

Opcionalmente, la red de comunicaciones incluye una red de comunicaciones inalámbricas usada por uno primero de los dispositivos en red y una red de comunicaciones alámbrica usada por uno segundo de los dispositivos en red.

Opcionalmente, cada uno de los dispositivos en red opera de acuerdo con un protocolo de consenso que incluye el modo de duplicación de red y el modo de contención de red, en donde, cuando está en el modo de contención de red, cada uno de los dispositivos en red vota establecer un consenso en cuanto a si se reducirá el estado de bloqueo de seguridad local de cada uno de los dispositivos en red.

Breve descripción de los dibujos

Se describirá en lo sucesivo una o más realizaciones en conjunto con los dibujos adjuntos, en donde designaciones similares indican elementos similares, y en donde:

La Figura 1 es un diagrama de bloques que representa una realización de un sistema de bloqueo de seguridad distribuido para un vehículo recreativo (VR) que puede llevar a cabo el método desvelado en el presente documento;

La Figura 2 es un diagrama de máquina de estado para el sistema de bloqueo de seguridad distribuido que ilustra dos modos de operación del protocolo de consenso que se llevan a cabo por cada uno de los dispositivos en red de acuerdo con una realización;

Las Figuras 3A-3B ilustran un diagrama de flujo de una realización de un proceso para llevar a cabo el modo de duplicación de red en un dispositivo en red que puede usarse como una parte de un método para controlar una operación electromecánica de un dispositivo electromecánico basándose en una condición de bloqueo de seguridad determinada usando un sistema de bloqueo de seguridad distribuido para un vehículo recreativo; y

Las Figuras 4A-4B ilustran un diagrama de flujo de una realización de un proceso para llevar a cabo el modo de contención de red en un dispositivo en red que puede usarse como una parte de un método para controlar una operación electromecánica de un dispositivo electromecánico basándose en una condición de bloqueo de seguridad determinada usando un sistema de bloqueo de seguridad distribuido para un vehículo recreativo.

Descripción detallada

Se proporciona un sistema de bloqueo de seguridad distribuido para un vehículo recreativo (VR) que tiene una pluralidad de dispositivos en red que están comunicativamente acoplados entre sí mediante una red de comunicaciones local, tal como un bus de comunicación instalado en el VR. También se proporciona un método de operación del sistema de bloqueo de seguridad distribuido. El sistema de bloqueo de seguridad distribuido se usa para detectar una condición de bloqueo de seguridad, tal como si el VR está viajando o está en movimiento actualmente, a través del uso de circuitería de detección de bloqueo, software y/u otra lógica configurada para ejecutarse o implementarse por la pluralidad de dispositivos en red. En al menos algunas realizaciones, la pluralidad de dispositivos en red que están distribuidos entre el VR en diferentes ubicaciones, están comunicativamente acoplados entre sí mediante una red de comunicaciones, y están configurados para operar de acuerdo con un protocolo común para establecer un consenso en cuanto al estado de bloqueo de seguridad actual. Este protocolo común se denomina en el presente documento un protocolo de consenso.

En general, la pluralidad de dispositivos en red incluye uno o más controladores electrónicos para controlar uno o más dispositivos electromecánicos del VR (por ejemplo, un deslizador, un toldo o un nivelador), y una pluralidad de dispositivos de detección de condición de bloqueo de seguridad para detectar una condición de bloqueo de seguridad. Un estado de bloqueo de seguridad es un estado que puede incorporarse en datos electrónicos y que representa un estado del sistema de bloqueo de seguridad, que puede usarse por el controlador o controladores electrónicos para determinar si se permite que se lleve a cabo una operación electromecánica. La condición de bloqueo de seguridad puede determinarse usando diferentes técnicas entre los dispositivos de detección de

- condición de bloqueo de seguridad (por ejemplo, el movimiento basado en GPS según se detecta por un primer dispositivo de detección de condición de bloqueo de seguridad, freno de estacionamiento no activado según se detecta por un segundo dispositivo de detección de condición de bloqueo de seguridad) mientras que el estado de bloqueo de seguridad es más universal en el sentido de que se usa el estado de bloqueo para indicar la gravedad o nivel de seguridad, tal como NIVEL 1, y que puede determinarse basándose en una o más condiciones de bloqueo de seguridad. Uno cualquiera o más de los dispositivos en red puede estar integrado con, estar localmente conectado a y/o incluir un controlador electrónico y/o un dispositivo de detección de condición de bloqueo de seguridad.
- Se proporciona un método para implementar una característica de "nivel de gravedad de bloqueo de seguridad" definida por red en una red de comunicaciones comprendida de una pluralidad de controles electrónicos (o controladores electrónicos) que operan independientemente entre sí. En algunas realizaciones, el bloqueo de seguridad es efectivo en una señal de "ESTOP de nivel de red" que se difunde a y duplica por todos los dispositivos en red a través de la red. En al menos algunas realizaciones, se usa un modo de duplicación de red para garantizar que se comparte el mismo estado de bloqueo de seguridad (por ejemplo, nivel ESTOP) entre todos los controladores electrónicos, y se usa la creación de consenso durante un modo de contención de red para determinar si/cuándo las condiciones son correctas para reducir el estado de bloqueo de seguridad para permitir operaciones electromecánicas. En al menos algunas realizaciones, se usa el sistema y método de bloqueo de seguridad distribuido para implementar un bloqueo de seguridad para un VR que tiene dispositivos electromecánicos (por ejemplo, deslizadores, niveladores y toldos) mientras el VR está en movimiento, lo que puede detectarse por un primer dispositivo de detección de condición de bloqueo de seguridad a través de, por ejemplo, la recepción de señales de GNSS en un receptor de GNSS.
- El sistema y método de bloqueo de seguridad distribuido están diseñados y/o configurados para sustituir diversos diseños de "circuitos de disparo de interbloqueo/bloqueo de seguridad" implementados en diversos controles electrónicos de VR. Estos circuitos esencialmente actúan como frenos inteligentes (puramente en hardware, o una combinación de hardware/software), que, cuando se disparan, potencialmente evitan la operación insegura de los sistemas electrónicos y electromecánicos. Un ejemplo de un circuito de este tipo sería el que evita la operación de sistemas deslizadores de VR cuando se está conduciendo un VR por la carretera.
- El sistema y método de bloqueo de seguridad distribuido pueden adaptarse para superar al menos algunas desventajas del estado actual de la técnica desacoplando la circuitería que detecta la condición de bloqueo de seguridad (o los dispositivos de detección de condición de bloqueo de seguridad) de los controladores electrónicos que responden a la condición de bloqueo de seguridad. Esto puede conseguirse comunicando el estado de bloqueo de seguridad a través de una red de comunicaciones compartida y local que se proporciona por el VR. Cualquiera o todos los controladores electrónicos en la red pueden estar configurados para recibir y reaccionar al estado de bloqueo de seguridad, independientemente de si el controlador electrónico incluye cualquier circuitería para detectar la condición de bloqueo de seguridad. En al menos algunas realizaciones, únicamente dispositivos en red seleccionados implementan la circuitería requerida para detectar la condición de bloqueo de seguridad y estos dispositivos en red se denominan dispositivos de detección de condición de bloqueo de seguridad. En al menos algunas realizaciones, estos dispositivos de detección de condición de bloqueo de seguridad tienen circuitería o mecanismos de bloqueo de seguridad que detectan una condición de seguridad (o determinan el estado de bloqueo de seguridad) de diferentes maneras; por ejemplo: un primer dispositivo de detección de condición de bloqueo de seguridad puede detectar una condición de bloqueo de seguridad (o determinar un estado de bloqueo de seguridad) usando un circuito de GPS para detectar el movimiento del vehículo, mientras que un segundo dispositivo de detección de condición de bloqueo de seguridad puede detectar una condición de bloqueo de seguridad (o determinar un estado de bloqueo de seguridad) usando circuitería para detectar que se ha desactivado el freno de estacionamiento del VR.
- Para evitar una confusión como resultado de que se informen diferentes estados de bloqueo de seguridad por diferentes dispositivos de detección de condición de bloqueo de seguridad, puede usarse el protocolo de consenso para crear el consenso entre los dispositivos en red de otra manera independientes. En al menos una realización, el protocolo permite que cualquier dispositivo en red en la red de comunicaciones "escale" el nivel de seguridad de bloqueo a voluntad; es decir, cualquier dispositivo de detección de condición de bloqueo de seguridad puede elevar el nivel de seguridad del estado de bloqueo de seguridad. Al menos en algunas realizaciones, este estado de bloqueo de seguridad es similar a un E-STOP electrónico que puede desencadenarse por cualquier dispositivo de detección de condición de bloqueo de seguridad en la red, y el protocolo de consenso provoca que todos los otros dispositivos en red dupliquen, informen y cumplan con el estado de bloqueo de seguridad.
- En al menos una realización, haciendo que todos los dispositivos en red cumplan con el estado de bloqueo de seguridad, el sistema y método de bloqueo de seguridad distribuido elimina o al menos reduce la posibilidad del comportamiento inconsistente entre controladores electrónicos. El sistema y método de bloqueo de seguridad distribuido puede usarse para copiar o duplicar el estado del bloqueo (o estado de bloqueo de seguridad) a todos los dispositivos en red en la red de comunicaciones, volviendo de esta manera eficazmente todos los dispositivos en red en "informadores de estado de bloqueo", independientemente de si un dispositivo en red particular implementa alguna circuitería de detección de bloqueo de seguridad. Por lo tanto, de acuerdo con al menos algunas

realizaciones, todos los dispositivos en red del sistema pueden hacerse eco/informar el estado actual del bloqueo (o el estado de bloqueo de seguridad) a otros dispositivos en red. De esta manera, persiste la condición de bloqueo de seguridad, incluso si se apaga, falla o se retira de otra manera de la red el dispositivo de detección de condición de bloqueo de seguridad que detectó la condición de bloqueo de seguridad. Para evitar el borrado erróneo del estado de bloqueo de seguridad, todos los dispositivos en red "votan" para garantizar que se alcanza el consenso antes de determinar borrar o resetear el estado de bloqueo de seguridad. Esto evita que un único dispositivo en red borre de manera errónea unilateralmente los estados de bloqueo de seguridad locales de cada uno de los dispositivos en red. Por ejemplo: si un primer dispositivo de detección de condición de bloqueo de seguridad determina que ha de resetearse el estado de bloqueo de seguridad (es decir, establecer a un valor de base), pero un segundo dispositivo de detección de condición de bloqueo de seguridad lo decide no hacerlo, entonces el segundo dispositivo de detección de condición de bloqueo de seguridad vota mantener el estado de bloqueo de seguridad en su nivel o estado actual. Por lo tanto, en al menos algunas realizaciones, esto evitará un comportamiento inconsistente o inseguro entre los dispositivos en red. Como se usa en el presente documento, un "valor de base" es el valor usado para representar que no ha habido problemas de seguridad detectados por el sistema. En algunas realizaciones, se implementa el valor de base siendo un valor cero o mínimo. El estado de bloqueo de seguridad puede elevarse del valor de base a un valor elevado cuando se detecta una condición de bloqueo de seguridad.

En al menos algunas realizaciones, se usa una red de comunicaciones y el protocolo de consenso que es común a todos los dispositivos en red para comunicar el estado del bloqueo entre dispositivos de detección de condición de bloqueo de seguridad u otros dispositivos en red de otra manera independientes. Debería apreciarse que, en una realización, el protocolo de consenso, según se implementa en cada uno de los dispositivos en red, pueden ser el mismo, es decir, se incorpora el protocolo de consenso en un único conjunto de instrucciones informáticas (que representan una única versión del protocolo de consenso) que se usa por cada uno de los dispositivos en red en conjunto con parámetros específicos almacenados para el dispositivo en red particular. Por ejemplo, un único programa informático está instalado en cada uno de los dispositivos en red, incluyendo los dispositivos de detección de bloqueo de seguridad, los controladores electrónicos y los dispositivos en red pasivos. A continuación, en un ejemplo de este tipo, cada uno de los dispositivos en red puede incluir otros datos específicos de dispositivos en red que están localmente almacenados en el respectivo dispositivo en red y que se usan como una parte de la realización del protocolo de consenso. Por ejemplo, ciertos tipos de dispositivos en red (por ejemplo, dispositivos de detección de condición de bloqueo de seguridad) pueden llevar a cabo diferentes etapas como una parte del protocolo de consenso, tal como determinando un estado de bloqueo de seguridad propuesto basándose en detectar una condición de bloqueo de seguridad. Por lo tanto, pueden usarse los datos específicos de dispositivo en red (por ejemplo, una bandera), como una entrada en el programa informático que, a continuación, hace que el dispositivo en red tome ciertas etapas que son particulares a ese dispositivo en red o a ese tipo de dispositivo en red.

En otra realización, diferentes tipos de dispositivos en red pueden implementar una versión diferente del protocolo de consenso según se incorpora en diferentes conjuntos de instrucciones informáticas. Por ejemplo, un dispositivo de detección de condición de bloqueo de seguridad puede incluir una primera versión del protocolo de consenso que incluye etapas para detectar una condición de bloqueo de seguridad, y otros tipos de dispositivos en red pueden incluir una segunda versión del protocolo de consenso que no incluye u omite estas etapas que se usan para detectar una condición de bloqueo de seguridad.

Al menos en algunas realizaciones, los dispositivos de detección de condición de bloqueo de seguridad escalan el nivel de seguridad del bloqueo detectado individual e independientemente en respuesta a detectar una condición de bloqueo de seguridad particular; es decir, cualquier dispositivo de detección de condición de bloqueo de seguridad puede escalar el estado de gravedad de bloqueo a voluntad. A continuación, este estado de bloqueo de seguridad escalado se difunde a través de la red de comunicaciones a los otros dispositivos de detección de condición de bloqueo de seguridad y/u otros dispositivos en red que, a continuación, responderán de la misma manera, tal como realizando un acuse de recibo y cumpliendo con el estado de bloqueo de seguridad. En al menos algunas realizaciones, todos los dispositivos de detección de condición de bloqueo de seguridad votan para alcanzar un consenso antes de reducir el nivel de seguridad (o estado de bloqueo de seguridad); en algunas realizaciones, todos los dispositivos en red votan para alcanzar un consenso antes de reducir el nivel de seguridad (o estado de bloqueo de seguridad). Esto garantiza que ningún dispositivo de detección de condición de bloqueo de seguridad único (o dispositivo en red) pueda reducir el estado de bloqueo de seguridad en solitario puesto que los otros dispositivos de detección de condición de bloqueo de seguridad en la red deben votar y estar de acuerdo. El protocolo de consenso hace que los dispositivos en red cada uno duplique y difunda el estado de bloqueo de seguridad a todos los dispositivos en red en la red. Por lo tanto, a través de este protocolo de consenso, todos los dispositivos en red observan el mismo estado de bloqueo de seguridad y, por lo tanto, la pérdida o fallo de uno cualquiera del dispositivo en red (por ejemplo, debido a un apagón o fallo) no provocará que falle el mecanismo de bloqueo, evitando de esta manera la operación insegura de sistemas electromecánicos del VR.

Como se muestra en la realización de la Figura 1, el sistema de bloqueo de seguridad distribuido 100 incluye dispositivos en red 102-110 que están instalados en un vehículo recreativo (VR), y que están acoplados de manera comunicativa mediante una red de comunicaciones 130. La pluralidad de dispositivos en red 102-110 incluye una pluralidad de dispositivos de detección de condición de bloqueo de seguridad, una pluralidad de controladores electrónicos y un dispositivo en red pasivo. En la realización ilustrada, dos de los dispositivos en red son

controladores electrónicos 102, 104 que están programados para controlar un dispositivo electromecánico del VR. Por ejemplo, uno primero de los controladores electrónicos 102 controla un deslizamiento electromecánico para el VR y uno segundo de los controladores electrónicos 104 controla un nivelador electromecánico para el VR. También, en la realización ilustrada, dos de los dispositivos en red son dispositivos de detección de condición de bloqueo de seguridad 108, 110 que pueden detectar una condición de bloqueo de seguridad usando su respectiva circuitería de detección de bloqueo 122, 124. Además, uno de los dispositivos en red es un dispositivo en red pasivo 106, que es un dispositivo en red que nunca es un dispositivo de detección de condición de bloqueo de seguridad ni un controlador electrónico. Por supuesto, de acuerdo con diversas realizaciones, puede usarse cualquier número adecuado de dispositivos de detección de condición de bloqueo de seguridad, controladores electrónicos y dispositivos pasivos.

Cada uno de los dispositivos en red 102-110 incluye uno o más procesadores y/o memoria, y puede incluir otros componentes electrónicos, tales como módems, tarjetas de interfaz de red, etc. Los procesadores pueden ser cualquier dispositivo adecuado para ejecutar instrucciones informáticas, que pueden almacenarse en memoria del dispositivo en red u otra memoria accesible al dispositivo en red. En algunas realizaciones, todos los dispositivos en la red pueden participar en el método; sin embargo, en otras realizaciones, uno o más dispositivos en la red no pueden participar. En al menos algunas realizaciones, cada uno de los dispositivos en la red que está participando incluye instrucciones informáticas incorporadas en memoria y que, cuando se ejecutan por el procesador del dispositivo en red, hacen que el dispositivo en red lleve a cabo operaciones de acuerdo con el protocolo de consenso, que incluye un modo de duplicación de red y un modo de contención de red, y/o de acuerdo con otra funcionalidad descrita en el presente documento.

Cada uno de los controladores electrónicos 102, 104 incluye instrucciones informáticas que posibilitan que el controlador electrónico controle al menos una operación electromecánica de al menos un dispositivo electromecánico 112, 114. Cada uno de los controladores electrónicos 102, 104 está acoplado a los dispositivos electromecánicos 112, 114, respectivamente, y, en al menos algunas realizaciones, cada uno de los controladores electrónicos 102, 104 se usa para controlar un dispositivo electromecánico diferente. Por ejemplo, un primer controlador electrónico controla las operaciones electromecánicas de un nivelador del VR (es decir, un ejemplo de un primer dispositivo electromecánico), tal como extendiendo y/o retrayendo uno o más gatos del nivelador, y un segundo controlador electrónico controla las operaciones electromecánicas de un deslizador del VR (es decir, un ejemplo de un segundo dispositivo electromecánico), tal como extendiendo y/o retrayendo un espacio deslizante del VR. Otros tipos de dispositivos electromecánicos que pueden usarse, como aquellos analizados en el presente documento, son simplemente ilustrativos.

Cada uno de los dispositivos de detección de condición de bloqueo de seguridad 108, 110 está acoplado a circuitería de detección de bloqueo 122, 124, que se usa por cada dispositivo 108, 110 para detectar una condición de bloqueo de seguridad, que puede usarse, a continuación, para determinar un estado de bloqueo de seguridad. En una realización, cada uno de (o al menos uno de) los dispositivos de detección de condición de bloqueo de seguridad detecta una condición de bloqueo de seguridad que es diferente de una condición de bloqueo de seguridad detectada por otro dispositivo de detección de condición de bloqueo de seguridad. En tales realizaciones, la circuitería de detección de bloqueo de un primer dispositivo de detección de condición de bloqueo de seguridad es de un carácter diferente y es independiente de la circuitería de detección de bloqueo de un segundo dispositivo de detección de condición de bloqueo de seguridad. En una realización, la circuitería de detección de bloqueo de un primer dispositivo de detección de condición de bloqueo de seguridad es un receptor de GNSS que determina si se está moviendo el vehículo, y la circuitería de detección de bloqueo de un segundo dispositivo de detección de condición de bloqueo de seguridad es circuitería que está acoplada a un freno de estacionamiento del VR y que se usa para determinar si está activado el freno de estacionamiento. Es decir, en un ejemplo de este tipo, el primer dispositivo de detección de condición de bloqueo de seguridad puede detectar una primera condición de bloqueo de seguridad basándose en recibir señales de sistema de satélite de navegación global (GNSS) en un receptor de GNSS, y el segundo dispositivo de detección de condición de bloqueo de seguridad puede detectar una segunda condición de bloqueo de seguridad basándose en un estado de un freno de estacionamiento del vehículo recreativo. Otros tipos de dispositivos de detección de condición de bloqueo de seguridad y circuitería de detección de bloqueo de los mismos que pueden usarse, como aquellos analizados en el presente documento, son simplemente ilustrativos.

La red de comunicaciones 130 es una red de datos electrónicos local y se ilustra en la Figura 1 como un bus de red de área de controlador (CAN), sin embargo, puede usarse cualquier tipo adecuado de red de comunicaciones alámbrica o inalámbrica, tal como un bus de red de interconexión local (LIN), conexión de Ethernet, otra conexión de cableado permanente, comunicaciones de corto alcance especializadas (DSRC) (por ejemplo, WiFi™, Bluetooth™), etc. Cada uno de los dispositivos en red 102-110 puede incluir el equipo adecuado para llevar a cabo comunicaciones a través de la red de comunicaciones 130, tal como un módem y/o una tarjeta de interfaz de red (NIC). En una realización donde se usan las comunicaciones inalámbricas, cada uno de los dispositivos en red puede incluir circuitería inalámbrica o un conjunto de chips inalámbrico para llevar a cabo las comunicaciones inalámbricas, que pueden ser Wi-Fi™, Bluetooth™, u otra tecnología de comunicación inalámbrica adecuada.

Con referencia a la Figura 2, se muestra un diagrama de máquina de estado para el sistema de bloqueo de

seguridad distribuido que ilustra dos modos de operación del protocolo de consenso que se llevan a cabo por cada uno de los dispositivos en red. Los dos modos de operación del protocolo de consenso son un modo de contención de red 166 y un modo de duplicación de red 164, y los dispositivos en red pueden alternar entre cada uno de estos modos de manera concertada, al menos en algunas realizaciones. Cuando se enciende el VR (por ejemplo, se pone en marcha un encendido, se inserta una llave, se coloca el VR en un estado accesorio (ACC)), puede establecerse un estado de bloqueo de seguridad local al valor de base, que se indica en 162.

Con referencia a las Figuras 3A-3B, se ilustra un proceso 200 para llevar a cabo el modo de duplicación de red 164 en un dispositivo en red. En el modo de duplicación de red 164, cada dispositivo en red 102-110 escucha un estado de bloqueo de seguridad de otro dispositivo en red mediante la red de comunicaciones 130 (etapa 208), y también difunde su estado de bloqueo de seguridad (o estado de bloqueo de seguridad local) a través de la red de comunicaciones 130 (etapa 216). El estado de bloqueo de seguridad local es un estado de bloqueo de seguridad del sistema según se determina en un dispositivo en red particular, es decir, cada dispositivo en red tiene un estado de bloqueo de seguridad local que se determina basándose en escuchar el estado o estados de bloqueo de seguridad difundidos a través de la red de comunicaciones y/o basándose en un estado de bloqueo de seguridad propuesto según se determina por el dispositivo en red en el caso de que el dispositivo en red sea un dispositivo de detección de condición de bloqueo de seguridad. El estado de bloqueo de seguridad local para un primer dispositivo en red puede actualizarse cuando el primer dispositivo en red recibe un estado de bloqueo de seguridad difundido que es más grave (por ejemplo, mayor o superior) que el estado de bloqueo de seguridad local. Por ejemplo, si el estado de bloqueo de seguridad local del primer dispositivo en red es un nivel 1 y el primer dispositivo en red recibe un estado de bloqueo de seguridad de un nivel 2, a continuación, el primer dispositivo en red puede actualizar su estado de bloqueo de seguridad local que es un nivel 2, tal como el que se ilustra en las etapas 212-214. En algunas realizaciones, en la etapa 216, cada uno o más de los dispositivos en red 102-110 difunde el estado de bloqueo de seguridad local a intervalos regulares (por ejemplo, cada 0,2 segundos).

También, en el caso de un dispositivo de detección de condición de bloqueo de seguridad que opera en el modo de duplicación de red (véase la etapa 202), cuando la circuitería de detección de bloqueo (por ejemplo, circuitería de detección de bloqueo 122, 124) determina un estado de bloqueo de seguridad que es mayor que el estado de bloqueo de seguridad local (etapa 204), a continuación, el estado de bloqueo de seguridad local puede establecerse al estado de bloqueo de seguridad (etapa 206) detectado (o propuesto).

El sistema/método puede conmutarse del modo de duplicación de red al modo de contención de red cuando un único dispositivo en red transmite una solicitud de borrado (SOLICITUD DE BORRADO) a través de la red de comunicaciones. En al menos una realización, la solicitud de borrado se transmite en un evento de vehículo predeterminado, tal como cuando se enciende o inicia el VR, o cuando se coloca el VR en un estado de transmisión particular (por ejemplo, un estado de estacionamiento de PRNDL, un estado inverso de PRNDL). En una realización, el evento de vehículo predeterminado puede ser cuando el dispositivo de detección de condición de bloqueo de seguridad no detecta ningún problema de seguridad (o se considera para detectar una condición representada por un valor de base) usando la circuitería de detección de bloqueo asociada. Como alternativa o adicionalmente, la solicitud de borrado puede transmitirse en una cantidad predeterminada de tiempo que pasa mientras está en el modo de duplicación de red.

Con referencia a las Figuras 4A-4B, se ilustra un proceso 300 para llevar a cabo el modo de contención de red 166 en un dispositivo en red. En al menos algunas realizaciones, cada dispositivo en red 102-110 selecciona un estado de bloqueo de seguridad propuesto, que puede ponerse por defecto a un valor predeterminado tal como el valor de base según se indica en la etapa 302. En algunas realizaciones, el dispositivo en red puede anular este estado/valor propuesto predeterminado y usar otro estado de bloqueo de seguridad como el estado de bloqueo de seguridad propuesto. También, en el caso de un dispositivo de detección de condición de bloqueo de seguridad que opera en el modo de contención de red, la circuitería de detección de bloqueo (por ejemplo, la circuitería de detección de bloqueo 122, 124) puede usarse para determinar un estado de bloqueo de seguridad propuesto en lugar de usar un estado/valor predeterminado o por defecto (etapas 304-306).

En el comienzo del modo de contención de red, el estado de bloqueo de seguridad local (o actual) para cada uno de los dispositivos en red pueden bloquearse o no cambiarse, excepto cuando se determina que se cambia en las etapas 314, 318, 324, 326 y 334. Cada uno de los dispositivos en red escucha un estado de bloqueo de seguridad propuesto de uno o más de los otros dispositivos en red (etapa 308) y, como se indica por la etapa 310, cuando se recibe un estado de bloqueo de seguridad propuesto de otro dispositivo en red, el proceso 300 continúa a la etapa 312; de otra manera, el proceso 300 continúa a la etapa 316. Cuando el estado de bloqueo de seguridad local es menor que (o no tan grave como) un estado de bloqueo de seguridad propuesto recibido a través de la red de comunicaciones, a continuación, el estado de bloqueo de seguridad local puede aumentarse para hacer coincidir con el estado de bloqueo de seguridad propuesto (o puede establecerse al estado de bloqueo de seguridad propuesto) (etapas 312-314) que se recibió a través de la red de comunicaciones y que es el más grave (o el más alto).

Cuando todos los dispositivos en red han establecido un estado de bloqueo de seguridad propuesto al valor de base (que puede representarse por un estado de cero (0) u otro valor/estado mínimo/inicial), a continuación, el estado de bloqueo de seguridad local para cada dispositivo en red se establece al valor de base (etapas 316-318). La

determinación de la etapa 316 puede tener en cuenta una primera cantidad de tiempo X predeterminada; por ejemplo, la determinación de la etapa 316 puede incluir determinar si todos los dispositivos en red han establecido un estado de bloqueo de seguridad propuesto al valor de base dentro de los últimos X segundos y, en caso afirmativo, el proceso 300 continúa a la etapa 318 donde se establece el estado de bloqueo de seguridad local al valor de base; de otra manera, el proceso 300 continúa a la etapa 320.

En la etapa 320, se determina si ha pasado una segunda cantidad de tiempo Y predeterminada desde que el dispositivo en red ha estado operando en el modo de contención de red 166 y, en caso afirmativo, el proceso 300 continúa a la etapa 322; de otra manera, el proceso 300 continúa a la etapa 328. En la etapa 322, puede realizarse una determinación en cuanto a si el estado de bloqueo de seguridad propuesto es mayor que el estado de bloqueo de seguridad más alto (o más grave) que se recibió por otro dispositivo en red a través de la red de comunicaciones 130. Por ejemplo, como se muestra en la etapa 322, puede determinarse si el estado de bloqueo de seguridad propuesto es mayor que el estado de bloqueo de seguridad más alto (o más grave) que se recibió por otro dispositivo en red a través del bus de comunicaciones en los últimos X segundos, donde X segundos puede ser una cantidad predeterminada de tiempo que es la misma o diferente de la cantidad de tiempo predeterminada Y. Cuando el estado de bloqueo de seguridad propuesto es mayor que el estado de bloqueo de seguridad más alto (o más grave) que se recibió por otro dispositivo en red, a continuación, el estado de bloqueo de seguridad local (o actual) puede establecerse al estado de bloqueo de seguridad propuesto (etapa 324); de otra manera, el estado de bloqueo de seguridad local (o actual) puede establecerse al estado de bloqueo de seguridad más alto (o más grave) que se recibió por otro dispositivo en red mientras se encontraba en el modo de contención de red (o durante los últimos X segundos) (etapa 326); por ejemplo, en una realización, el estado de bloqueo de seguridad local se establece al estado de bloqueo de seguridad más alto (o más grave) que se recibió por otro dispositivo en red dentro de los últimos X segundos (o dentro de otra cantidad de tiempo predeterminada).

Como se indica por la etapa 328, por dispositivos en red que no son dispositivos de detección de condición de bloqueo de seguridad (o que no incluyen circuitería de detección de bloqueo), el estado de bloqueo de seguridad propuesto se difunde a través de la red de comunicaciones (etapa 340). En una realización, el estado de bloqueo de seguridad propuesto puede difundirse a intervalos regulares. También, como se indica por la etapa 328, para dispositivos en red que son dispositivos de detección de condición de bloqueo de seguridad, se actualiza el estado de bloqueo de seguridad propuesto o el estado de bloqueo de seguridad local (o actual) a un nuevo valor según se determina por la circuitería de detección de bloqueo del dispositivo de detección de condición de bloqueo de seguridad. Por ejemplo, en la etapa 330, se detecta un nuevo estado de bloqueo de seguridad por la circuitería de detección de bloqueo del dispositivo de detección de condición de bloqueo de seguridad. Este nuevo estado de bloqueo de seguridad puede compararse a continuación al estado de bloqueo de seguridad local (o actual) (etapa 332) y, si el nuevo estado de bloqueo de seguridad es mayor que el estado de bloqueo de seguridad local (o actual), el estado de bloqueo de seguridad local (o actual) se establece al nuevo estado de bloqueo de seguridad (etapa 334); de otra manera, el proceso 300 continúa a la etapa 336.

En la etapa 336, se compara el nuevo estado de bloqueo de seguridad con el estado de bloqueo de seguridad propuesto y, si el nuevo estado de bloqueo de seguridad es mayor que el estado de bloqueo de seguridad propuesto, a continuación, el estado de bloqueo de seguridad propuesto se establece al nuevo estado de bloqueo de seguridad como se muestra en la etapa 338. Después de la etapa 338, el proceso 300 continúa de vuelta a la etapa 340 donde se difunde el estado de bloqueo de seguridad propuesto a través de la red de comunicaciones 130. Cada uno de los dispositivos en red puede volver al modo de contención de red cuando el dispositivo en red alcanza la etapa de "Retorno al modo de duplicación de red", como se ilustra en la Figura 4B, por ejemplo. En otras realizaciones, la transición del modo de contención de red al modo de duplicación de red puede coordinarse, tal como por uno de los dispositivos en red que envía una señal de modo de contención final (FIN_CONTENCIÓN) a través de la red de comunicaciones.

El proceso 200 y el proceso 300 incluyen ciertos bloques de decisión (202, 304, 328) que consultan si el dispositivo en red es un dispositivo de detección de condición de bloqueo de seguridad. En una realización, puede implementarse uno cualquiera o más de estos bloques de decisión por el dispositivo en red que inspecciona datos específicos de dispositivo en red (por ejemplo, una bandera almacenada en la memoria del dispositivo en red) que indica si el dispositivo en red es un dispositivo de detección de condición de bloqueo de seguridad. En otras realizaciones, uno cualquiera o más de estos bloques de decisión puede no corresponder a ninguna etapa real realizada o acción tomada por el dispositivo en red. En tales realizaciones, puede usarse una versión diferente del protocolo de consenso por dispositivos en red de diferentes tipos, tal como una primera versión del protocolo de consenso que se usa por los dispositivos de detección de condición de bloqueo de seguridad y una segunda versión del protocolo de consenso que se usa por los otros dispositivos en red.

Al menos de acuerdo con algunas realizaciones, todos los dispositivos en red operan independientemente, pero pueden comunicarse entre sí a través de la red de comunicaciones. Al menos de acuerdo con algunas realizaciones, todos los dispositivos en red difunden regularmente su copia local del nivel de seguridad de bloqueo (su estado de bloqueo de seguridad local) a todos los otros dispositivos en red en el sistema. Al menos de acuerdo con algunas realizaciones, en el arranque/reinicio, cada dispositivo en red tiene su nivel de seguridad (o estado de bloqueo de seguridad local) establecido al valor de base (por ejemplo, un valor mínimo, tal como cero). Al menos de acuerdo

con algunas realizaciones, cada dispositivo en red en la red escucha a todos los otros dispositivos en red en la red y, si observa (o detecta) un nivel de gravedad (o estado de bloqueo de seguridad) mayor que el suyo propio, el dispositivo en red elevará su propio nivel de seguridad (o estado de bloqueo de seguridad local) para coincidir con el valor/estado más alto difundido en la red. De esta manera, todos los dispositivos en red copian el nivel más alto observado en ese dispositivo en red, y acuerdan cuál nivel o estado de bloqueo de seguridad es. En al menos algunas realizaciones, esto garantiza la propagación del estado (por ejemplo, el estado de bloqueo de seguridad) a través de la red.

Al menos de acuerdo con algunas realizaciones, el primer controlador electrónico 102 (o un primer dispositivo en red) y el segundo controlador electrónico 104 (o un segundo dispositivo en red) accionan o controlan de otra manera un sistema electromecánico que es crítico para la seguridad, lo que significa entonces que la operación del dispositivo electromecánico es crítica para la seguridad del sistema o el vehículo recreativo. Por ejemplo: el primer controlador electrónico 102 acciona un deslizador de VR, mientras que el segundo controlador electrónico 104 acciona un sistema de nivelación o nivelador de VR. Al menos de acuerdo con algunas realizaciones, un tercer dispositivo en red 106 no controla ningún sistema relacionado con la seguridad (o detecta una condición de bloqueo de seguridad), sino que, sin embargo, aún participa en el tráfico de red y mantiene una copia del nivel de seguridad de bloqueo como el estado de bloqueo de seguridad local.

Al menos de acuerdo con algunas realizaciones, los dispositivos de detección de condición de bloqueo de seguridad 108, 110 son independientes entre sí, y pueden detectar independientemente una condición de bloqueo de seguridad. Por ejemplo: el primer dispositivo de detección de condición de bloqueo de seguridad 108 puede detectar una condición de bloqueo de seguridad si detecta movimiento de remolque mediante una o más señales del sistema de satélite de navegación global (GNSS) (por ejemplo, señales del sistema de posicionamiento global (GPS)) que se reciben por un receptor de GNSS, mientras que el segundo dispositivo de detección de condición de bloqueo de seguridad 110 puede detectar una condición de bloqueo de seguridad en respuesta a detectar que se ha desactivado un freno de estacionamiento de un remolque del VR. Otras condiciones de bloqueo de seguridad pueden incluir un estado del freno del remolque, un estado del freno del vehículo remolcador, el estado de la luz de freno del vehículo remolcador y una orientación o movimiento detectado por un sensor de movimiento/orientación, tal como un acelerómetro, sensor de giroscopio, sensor de inclinación o sensor de ángulo.

Al menos de acuerdo con algunas realizaciones, cuando el primer o segundo dispositivos de detección de condición de bloqueo de seguridad 108, 110 detecta una condición de bloqueo de seguridad, entonces el dispositivo de bloqueo de seguridad: (1) eleva su propio nivel de gravedad (o estado de bloqueo de seguridad local) a un valor que indica la gravedad de la condición detectada (aumentar el valor indica aumentar la gravedad); y (2) a continuación difunde el nivel de seguridad (o estado de bloqueo de seguridad) a todos los otros dispositivos en red en la red de comunicaciones. En al menos algunos de tales casos, todos los dispositivos en red en la red de comunicaciones reciben la señal y aumentan su propia copia del nivel de seguridad para hacerla coincidir con la señal recibida. Cuando un dispositivo en red tiene un nivel de gravedad mayor que la señal recibida, el nivel del dispositivo en red permanece sin cambiar.

Al menos de acuerdo con algunas realizaciones, los controladores electrónicos 102, 104, en respuesta a observar un estado de bloqueo de seguridad elevado, limitan o evitan la operación de cualquier sistema o dispositivo electromecánico adjunto o asociado. En una realización, cuando el estado de bloqueo de seguridad se encuentra por encima un valor umbral predeterminado o se establece a un estado umbral predeterminado, el controlador electrónico puede determinar detener todas las operaciones electromecánicas juntas, o puede determinar detener aquellas operaciones electromecánicas asociadas con el valor o estado umbral predeterminado.

Al menos de acuerdo con algunas realizaciones, el dispositivo en red pasivo 106 recibe el estado de bloqueo de seguridad y lo registra localmente como un estado de bloqueo de seguridad local. Incluso aunque el dispositivo en red pasivo 106 pueda no tener un sistema de control adjunto, sin embargo, aún participa en las comunicaciones y es una fuente de buenos datos en la red, tal como datos indicativos de un estado de bloqueo de seguridad preciso.

Con respecto a la realización ilustrada de la Figura 1, considérese un escenario en el que están desactivados los dispositivos de detección de condición de bloqueo de seguridad 108, 110 (por ejemplo, apagados) o han fallado: incluso aunque los dispositivos de detección de condición de bloqueo de seguridad desactivados o fallidos 108, 110 ya no puedan detectar una condición de bloqueo de seguridad, la red por medio de los otros dispositivos en red, tal como el dispositivo en red pasivo 106, mantiene una copia del estado de bloqueo de seguridad previamente detectado. De esta manera, incluso si falla o se desconecta alguno o muchos dispositivos en red, se conserva el estado del nivel de gravedad de interbloqueo de seguridad (o el estado de bloqueo de seguridad). Se conserva el nivel o estado de bloqueo de seguridad siempre que al menos un dispositivo en red permanezca activo.

Con respecto a la realización ilustrada de la Figura 1, considérese un escenario en el que el dispositivo en red pasivo 106 emite un comando de borrado para borrar el estado de bloqueo de seguridad (es decir, resetear el estado de bloqueo de seguridad al valor de base): el dispositivo en red pasivo 106 emite el comando de borrado, lo que provoca que comience un periodo de elección o voto en la red en el que todos los otros dispositivos en red pueden votar. En este caso, los controladores electrónicos 102, 104 votan y acuerdan borrar el estado de bloqueo de

seguridad. El primer dispositivo de detección de condición de bloqueo de seguridad 108 también vota borrar el estado de bloqueo de seguridad con la condición de que el primer dispositivo de detección de condición de bloqueo de seguridad 108 no detecte una condición de bloqueo de seguridad. Sin embargo, el segundo dispositivo de detección de condición de bloqueo de seguridad 110, detecta que aún existe una condición de bloqueo de seguridad, y vota el comando de borrado en la red (o vota contra el borrado del estado de bloqueo de seguridad). En este ejemplo, ya que todos los dispositivos en red no han establecido un consenso, se vota el comando de borrado emitido por el dispositivo en red pasivo 106, y la red permanece en la condición de nivel de gravedad de bloqueo elevada o en el estado de bloqueo de seguridad elevado.

Al menos de acuerdo con algunas realizaciones, se usa el concepto de un NIVEL_GRAVEDAD_BLOQUEO (que puede representarse por un estado de bloqueo de seguridad) y se comunica entre los dispositivos en red, de acuerdo con la siguiente descripción: los valores inferiores indican menos gravedad (el valor de base puede ser cero o algún otro valor por defecto que indica que el VR es seguro para llevar a cabo ciertas operaciones (por ejemplo, poner una marcha)); valores superiores indican un nivel creciente de gravedad; cada dispositivo en red en la red tiene su propia copia LOCAL de NIVEL DE GRAVEDAD DE BLOQUEO, que puede denominarse también el estado de bloqueo de seguridad local; y en el arranque/reseteo, la copia LOCAL del NIVEL_GRAVEDAD_BLOQUEO se establece a valor de base.

Al menos de acuerdo con algunas realizaciones, en el modo de duplicación de red: el NIVEL_GRAVEDAD_BLOQUEO (o el estado de bloqueo de seguridad) se duplica a través de todos los dispositivos en red en la red para garantizar que todos los dispositivos en red están en el mismo estado de protección contra fallos (o al menos tienen conocimiento del mismo estado de bloqueo de seguridad); todos los dispositivos en red en la red difundirán regularmente su NIVEL_GRAVEDAD_BLOQUEO (o el estado de bloqueo de seguridad) a todos los otros dispositivos en red en la red; esta difusión puede tener lugar a una tasa de datos predeterminada (por ejemplo, los datos se transmiten una vez por segundo), y/o puede transmitirse en un cambio de estado o en respuesta a un evento predeterminado; cualquier dispositivo en red puede escalar (o aumentar) el estado de bloqueo de seguridad y, después de hacer eso, el nuevo estado de bloqueo de seguridad se difunde inmediatamente a todos los otros dispositivos en red en la red para reducir la latencia; y/o todos los dispositivos en red escuchan la red y reciben un NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) difundido desde los otros dispositivos en red, y: si algún dispositivo en red recibe un NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) que es mayor que su valor local (o estado de bloqueo de seguridad local), entonces el valor local del dispositivo en red (o estado de bloqueo de seguridad local) se establecerá para que coincida con el valor recibido, o si el valor local (o estado de bloqueo de seguridad) es mayor, el valor local (o estado de bloqueo de seguridad local) queda sin cambiar (y se retransmite en el siguiente intervalo planificado).

Al menos de acuerdo con algunas realizaciones, en el modo de duplicación de red: puede usarse uno cualquiera o más dispositivos de detección de condición de bloqueo de seguridad para elevar el estado de bloqueo de seguridad local cuando sea apropiado. De acuerdo con al menos una realización, múltiples dispositivos en red pueden ser un dispositivo de detección de condición de bloqueo de seguridad, y pueden detectar al menos una condición de bloqueo de seguridad. En algunas realizaciones, cada dispositivo de detección de condición de bloqueo de seguridad puede detectar una condición de bloqueo de seguridad diferente que otro dispositivo de detección de condición de bloqueo de seguridad, lo que puede dar como resultado que los dispositivos de detección de condición de bloqueo de seguridad determinen diferentes estados de bloqueo de seguridad; es decir, los estados de bloqueo de seguridad propuestos, según se determina por cada uno de los dispositivos de detección de condición de bloqueo de seguridad, no necesitan estar de acuerdo entre sí. En algunas realizaciones, estos dispositivos de detección de condición de bloqueo de seguridad son las fuentes de los bloqueos en la red puesto que son los dispositivos que inicialmente aumentan el estado de bloqueo de seguridad.

Al menos de acuerdo con algunas realizaciones, en el modo de duplicación de red: cuando dos dispositivos en red indican diferentes valores para NIVEL_GRAVEDAD_BLOQUEO (o el estado de bloqueo de seguridad), el dispositivo en red con el estado de bloqueo de seguridad local menos grave aumentará su estado de bloqueo de seguridad local para coincidir con el estado de bloqueo de seguridad local del otro dispositivo en red. De esta manera, todos los dispositivos en red eventualmente se hacen eco del valor más alto (o estado de bloqueo de seguridad más grave) observado y todos los dispositivos en red en la red duplican el NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) a través de la red, y acuerdan entre sí como resultado del modo de contención de red.

Al menos de acuerdo con algunas realizaciones, la única manera de borrar o reducir de otra manera el NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) es a través de difundir en primer lugar una solicitud de borrado (SOLICITUD DE BORRADO) a través de la red de comunicaciones. En una realización, cualquier dispositivo en la red puede emitir una SOLICITUD DE BORRADO (incluso dispositivos en red que no tengan circuitería de detección de condición de bloqueo). En al menos algunas realizaciones, después de (o en respuesta a) la transmisión de la solicitud de borrado, se inicia un periodo o modo de contención de red, tal como el modo de contención de red 166 (y/o el proceso 300), para permitir que el cambio solicitado se propague a través de la red.

Al menos de acuerdo con algunas realizaciones, en el modo de contención de red: se congela (es decir, se fija,

bloquea) el valor actual de NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) y el dispositivo en red continuará comportándose como si el NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) no hubiera cambiado durante la duración del modo de contención de red. Este valor se denominará el valor ACTUAL o estado de bloqueo de seguridad local. En una realización, el dispositivo en red elegirá un NIVEL_GRAVEDAD_BLOQUEO apropiado o propuesto (o estado de bloqueo de seguridad) en respuesta a la solicitud de borrado, que se denominará el valor PROPUESTO o estado de bloqueo de seguridad propuesto. Al menos en algunas realizaciones, el valor PROPUESTO se pone por defecto al valor de base, que puede usarse para permitir un borrado completo de NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad), o puede determinarse el estado de bloqueo de seguridad propuesto basándose en detectar (o determinar la presencia de) una condición de bloqueo de seguridad en el momento de recibir la solicitud de borrado. En algunas realizaciones, el estado de bloqueo de seguridad propuesto por defecto puede establecerse a otro NIVEL_GRAVEDAD_BLOQUEO reducido (o estado de bloqueo de seguridad), que es menos grave que el estado de bloqueo de seguridad local, pero que no es el valor de base.

Al menos de acuerdo con algunas realizaciones, en el modo de contención de red: los dispositivos en red detienen la difusión de su NIVEL_GRAVEDAD_BLOQUEO ACTUAL (o estado de bloqueo de seguridad local) a través de la red de comunicaciones y, en su lugar, comienzan a difundir su valor PROPUESTO (o estado de bloqueo de seguridad propuesto), que puede incluir difundir el estado de bloqueo de seguridad propuesto de acuerdo con un intervalo de transmisión fijo, por ejemplo. Al menos de acuerdo con algunas realizaciones, en el modo de contención de red: los dispositivos en red continúan escuchando la red para mensajes desde otros dispositivos en red en el bus para determinar si los otros dispositivos en red han realizado acuse de recibo de la solicitud de borrado. En una realización, cuando un dispositivo en red en la red difunde un NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad) que es mayor que el NIVEL_GRAVEDAD_BLOQUEO ACTUAL (o estado de bloqueo de seguridad local), entonces: el NIVEL_GRAVEDAD_BLOQUEO (o estado de bloqueo de seguridad local) se aumenta al valor observado en el bus; y el modo de contención de red finaliza y se reanuda la operación normal (o el modo de duplicación de red).

Al menos de acuerdo con algunas realizaciones, en el modo de contención de red: si todos los dispositivos en red en la red difunden un estado de bloqueo de seguridad que se establece al valor de base (por ejemplo, el NIVEL_GRAVEDAD_BLOQUEO es cero) durante un periodo de tiempo fijo (o una cantidad predeterminada, que puede representarse como X segundos) (por ejemplo, 2,2 segundos) con ninguna interrupción (por ejemplo, con ningún dispositivo en red que difunda un estado de bloqueo de seguridad que no es el valor de base), entonces: se reduce el estado de bloqueo de seguridad al valor de estado de bloqueo de seguridad propuesto, que es el valor de base; y el modo de contención de red finaliza y se reanuda la operación normal (o el modo de duplicación de red).

Al menos de acuerdo con algunas realizaciones, si se agota el periodo de contención de la red (que puede definirse como una segunda cantidad de tiempo predeterminada (por ejemplo, 5 segundos) tomada del tiempo cuando se envía la solicitud de borrado, por ejemplo) sin acuerdo entre los dispositivos en red, entonces: (i) el estado de bloqueo de seguridad se establece a cualquiera de los siguientes valores que sea mayor o más grave: (a) el valor más grande o más grave observado en la red durante los últimos X segundos (por ejemplo, 2,2 segundos) de actividad de red, o (b) el valor PROPUESTO del dispositivo en red local; y (ii) el modo de contención de red finaliza y se reanuda la operación normal (o el modo de duplicación de red).

Al menos de acuerdo con algunas realizaciones, si un dispositivo de detección de condición de bloqueo de seguridad determina aumentar el estado de bloqueo de seguridad local a un nuevo estado o valor (por ejemplo, el NIVEL_GRAVEDAD_BLOQUEO a un NUEVO NIVEL), que puede aumentarse basándose en detectar una condición de bloqueo de seguridad usando circuitería de detección de bloqueo de seguridad, entonces: (i) si el nuevo estado o valor es mayor que el estado de bloqueo de seguridad actual o local (por ejemplo, el NUEVO_NIVEL > ACTUAL), entonces: (a) el estado de bloqueo de seguridad local se aumenta al nuevo estado o valor, y (b) el modo de contención de red finaliza y se reanuda la operación normal (o el modo de duplicación de red); (ii) si el nuevo estado o valor es menor o igual que el estado de bloqueo de seguridad actual o local y el nuevo estado o valor es mayor que el estado de bloqueo de seguridad propuesto (por ejemplo, ACTUAL >= NUEVO_NIVEL > PROPUESTO), entonces: (a) el estado de bloqueo de seguridad propuesto se establece al nuevo estado o valor, y (b) el modo de contención de red continúa; y (iii) si el nuevo estado o valor es menor que el estado de bloqueo de seguridad propuesto (por ejemplo, NUEVO_NIVEL < PROPUESTO), entonces: no se realiza ninguna acción. En al menos algunas realizaciones, después de que finaliza el modo de contención de red, se transmite el estado de bloqueo de seguridad (o NIVEL_GRAVEDAD_BLOQUEO) en la red de acuerdo con una operación normal o de acuerdo con el modo de duplicación de red.

En al menos algunas realizaciones, todos los dispositivos en red participan en el modo de duplicación de red, incluso si el dispositivo en red no usa de lo contrario la información, tal como para determinar si controlar un dispositivo electromecánico. De esta manera, al menos de acuerdo con algunas realizaciones, este método/sistema maximiza (o al menos mejora) la capacidad de la red para mantener el estado de bloqueo de seguridad correcto (o NIVEL_GRAVEDAD_BLOQUEO), incluso si se apaga o se desactiva de lo contrario o fallan la mayoría de los dispositivos en red en la red. Por ejemplo: cuando un primer dispositivo en red detecta y establece un NIVEL_GRAVEDAD_BLOQUEO elevado, otros dispositivos en red mantienen y retienen una copia del estado de

bloqueo de seguridad incluso si se apaga el primer dispositivo en red.

En al menos algunas realizaciones, todos los dispositivos en red en la red deben acordar antes de que se reduzca o borre (es decir, se establezca al valor de base) el estado de bloqueo de seguridad (o NIVEL_GRAVEDAD_BLOQUEO). Esencialmente, en algunas realizaciones, todos los dispositivos en red deben votar para determinar si es apropiado establecer el estado de bloqueo de seguridad al valor de base u otro valor reducido. Por ejemplo, si un dispositivo en red está en desacuerdo con la solicitud de borrado (SOLICITUD DE BORRADO), entonces el dispositivo en red puede evitar que se establezca el estado de bloqueo de seguridad de los otros dispositivos en red al valor de base.

En al menos algunas realizaciones, el método/sistema permite que más de un dispositivo en red implemente circuitería de detección de condición de bloqueo, y estos dispositivos en red pueden implementar esta circuitería de detección de bloqueo de diferentes maneras. Los dispositivos en red no necesitan estar de acuerdo cuando tiene lugar una condición de bloqueo, únicamente necesitan estar de acuerdo en lo que respecta a cuál es el estado de bloqueo de seguridad y qué hacer a continuación. El sistema está diseñado para capturar y duplicar el estado de bloqueo de seguridad más alto (o NIVEL_GRAVEDAD_BLOQUEO) observado en la red. Por ejemplo, si dos o más dispositivos de detección de condición de bloqueo de seguridad detectan una condición de bloqueo de seguridad en o aproximadamente al mismo tiempo, entonces el estado de bloqueo de seguridad usado por la red es el estado de bloqueo de seguridad más alto (o más grave). Por lo tanto, en tales realizaciones, la condición más seria detectada en la red (o el estado de bloqueo de seguridad más grave) se le da prioridad.

Esta descripción, en lugar de describir limitaciones de una invención, únicamente ilustra realizaciones de la invención indicadas en las reivindicaciones. Por lo tanto, el lenguaje de esta descripción es exclusivamente descriptivo y no limitante.

De manera evidente, es posible modificar esta invención de lo que enseña la descripción. Dentro del alcance de las reivindicaciones, puede ponerse en práctica la invención de manera distinta de como se ha descrito anteriormente.

REIVINDICACIONES

1. Un método para controlar una operación electromecánica de un dispositivo electromecánico basándose en una condición de bloqueo de seguridad determinada usando un sistema de bloqueo de seguridad distribuido (100), comprendiendo el sistema de bloqueo de seguridad distribuido una pluralidad de dispositivos en red (102-110) comunicativamente acoplados mediante una red de comunicaciones (130), incluyendo la pluralidad de dispositivos en red uno o más controladores electrónicos (102, 104) y una pluralidad de dispositivos de detección de condición de bloqueo de seguridad (108, 110); comprendiendo el método:
 - en uno o más de la pluralidad de dispositivos en red (102-110):
 - recibir (210) un estado de bloqueo de seguridad de otro dispositivo en red mediante la red de comunicaciones (130);
 - comparar (212) un estado de bloqueo de seguridad local al estado de bloqueo de seguridad recibido;
 - determinar si actualizar el estado de bloqueo de seguridad local basándose en los resultados de la comparación (212) del estado de bloqueo de seguridad local al estado de bloqueo de seguridad recibido y, cuando se determina actualizar el estado de bloqueo de seguridad local, a continuación, actualizar (214) el estado de bloqueo de seguridad local al estado de bloqueo de seguridad recibido; y
 - difundir (216) el estado de bloqueo de seguridad local a través de la red de comunicaciones (130);
 - en uno o más de la pluralidad de dispositivos de detección de condición de bloqueo de seguridad (108, 110):
 - determinar un estado de bloqueo de seguridad propuesto basándose en datos de sensor obtenidos por el dispositivo de detección de condición de bloqueo de seguridad (108, 110);
 - comparar (204) el estado de bloqueo de seguridad propuesto con el estado de bloqueo de seguridad local y/o un estado de bloqueo de seguridad recibido que se recibió desde otro dispositivo en red a través de la red de comunicaciones (130); y
 - determinar (206) que un estado de bloqueo de seguridad local actualizado es el estado de bloqueo de seguridad local basándose en la comparación (204) del estado de bloqueo de seguridad propuesto con el estado de bloqueo de seguridad local y/o el estado de bloqueo de seguridad recibido; y
 - en cualquiera del uno o más controladores electrónicos (102, 104), controlar una operación electromecánica de un dispositivo electromecánico basándose en el estado de bloqueo de seguridad local.
2. El método de la reivindicación 1, en donde el sistema de bloqueo de seguridad distribuido (100) está instalado en un vehículo recreativo.
3. El método de la reivindicación 1 o la reivindicación 2, en donde el sistema de bloqueo de seguridad distribuido (100) incluye una pluralidad de controladores electrónicos (102, 104) que incluye el uno o más controladores electrónicos y una pluralidad de dispositivos electromecánicos (112, 114) que incluye el dispositivo o dispositivos electromecánicos, y en donde cada uno de la pluralidad de dispositivos electromecánicos (112, 114) se controla por uno diferente de la pluralidad de controladores electrónicos (102, 104);
 - opcionalmente, en donde un primer controlador electrónico (104) de la pluralidad de controladores electrónicos (102, 104) controla la operación electromecánica de un primer dispositivo electromecánico (114) de la pluralidad de dispositivos electromecánicos (112, 114), en donde un segundo controlador electrónico (102) de la pluralidad de controladores electrónicos (102, 104) controla la operación electromecánica de un segundo dispositivo electromecánico (112) de la pluralidad de dispositivos electromecánicos (112, 114), y en donde el primer controlador electrónico (104) opera independientemente del segundo controlador electrónico (102);
 - opcionalmente, en donde el primer dispositivo electromecánico es un nivelador (114) que está instalado en el vehículo recreativo, y en donde el segundo dispositivo electromecánico es un deslizador (112) que está instalado en el vehículo recreativo.
4. El método de una cualquiera de las reivindicaciones 1 a 3, en donde la pluralidad de dispositivos de detección de condición de bloqueo de seguridad (108, 110) incluye un primer dispositivo de detección de condición de bloqueo de seguridad y un segundo dispositivo de detección de condición de bloqueo de seguridad, en donde el primer dispositivo de detección de condición de bloqueo de seguridad está configurado para detectar una primera condición de bloqueo de seguridad, en donde el segundo dispositivo de detección de condición de bloqueo de seguridad está configurado para detectar una segunda condición de bloqueo de seguridad que es diferente de la primera condición de bloqueo de seguridad;
 - opcionalmente, en donde cada una de la primera condición de bloqueo de seguridad y la segunda condición de bloqueo de seguridad está basada en al menos uno de lo siguiente: señales del sistema de satélite de navegación global (GNSS) recibidas en un receptor de GNSS, un estado del freno de estacionamiento, un estado del freno del remolque, un estado del freno del vehículo remolcador, el estado de la luz de freno del vehículo remolcador, o una orientación o movimiento detectado por un sensor de movimiento/orientación, y en donde la primera condición de bloqueo de seguridad es diferente de la segunda condición de bloqueo de seguridad.

5. El método de una cualquiera de las reivindicaciones 1 a 4, en donde la red de comunicaciones (130) es un bus de red de área de controlador (CAN) alámbrica o una red de interconexión local alámbrica que está instalada en el vehículo recreativo.

5 6. El método de una cualquiera de las reivindicaciones 1 a 5, en donde la red de comunicaciones (130) es una red de comunicaciones inalámbricas que se lleva a cabo usando una red de comunicación de corto alcance (DSRC) especializada que se proporciona en el vehículo recreativo.

10 7. El método de una cualquiera de las reivindicaciones 1 a 6, en donde la red de comunicaciones (130) incluye una red de comunicaciones inalámbricas usada por uno primero de los dispositivos en red y una red de comunicaciones alámbrica usada por uno segundo de los dispositivos en red.

15 8. El método de una cualquiera de las reivindicaciones 1 a 7, en donde uno o más de los dispositivos en red (102-110) operan de acuerdo con un protocolo de consenso (160) que incluye un modo de duplicación de red (164) y un modo de contención de red (166), en donde, cuando está en el modo de contención de red (166), uno o más de los dispositivos en red (102-110) votan establecer un consenso en cuanto a si se reducirá el estado de bloqueo de seguridad local de cada uno de los dispositivos en red (102-110); opcionalmente, en donde, en respuesta a emitir uno primero de los dispositivos en red una solicitud de borrado cuando cada uno de los dispositivos en red (102-110) está operando en el modo de duplicación de red (164), cada uno de los dispositivos en red (102-110) pasa para operar en el modo de contención de red (166) para establecer el consenso.

9. Un sistema de bloqueo de seguridad distribuido (100) para un vehículo recreativo, que comprende:

25 una pluralidad de dispositivos en red (102-110) instalados en un sistema electromecánico, estando la pluralidad de dispositivos en red (102-110) comunicativamente acoplados mediante una red de comunicaciones (130), e incluyendo la pluralidad de dispositivos en red (102-110):

30 uno o más controladores electrónicos (102, 104), cada uno configurado para controlar un dispositivo electromecánico (112, 114) del vehículo recreativo basándose en un estado de bloqueo de seguridad local; y una pluralidad de dispositivos de detección de condición de bloqueo de seguridad (108, 110), cada dispositivo de detección de condición de bloqueo de seguridad (108, 110) configurado para detectar un estado de bloqueo de seguridad basándose en información de sensor obtenida por circuitería de detección de bloqueo (122, 124);

35 en donde uno o más de la pluralidad de dispositivos en red (102-110) están configurados para alternar entre un modo de duplicación de red (164) y un modo de contención de red (166) y, cuando operan en el modo de duplicación de red (164), para determinar un estado de bloqueo de seguridad local actualizado basándose en una comparación (212) del estado de bloqueo de seguridad local con un estado de seguridad de bloqueo recibido, recibándose el estado de seguridad de bloqueo recibido a través de la red de comunicaciones (130) de otro de los dispositivos en red (102-110), y para difundir (216) el estado de bloqueo de seguridad local a través de la red de comunicación (130); y
40 cuando operan en el modo de contención de red (166), cada dispositivo de la pluralidad de dispositivos de detección de condición de bloqueo de seguridad (108, 110) está configurado para obtener (330) el estado de bloqueo de seguridad detectado basándose en la información de sensor, para comparar (332, 336) el estado de bloqueo de seguridad detectado con el estado de bloqueo de seguridad local y/o un estado de bloqueo de seguridad propuesto recibido, para establecer (334, 338) el estado de bloqueo de seguridad local basándose en la comparación, y para difundir (340) el estado de bloqueo de seguridad local a través de la red de comunicaciones (130).

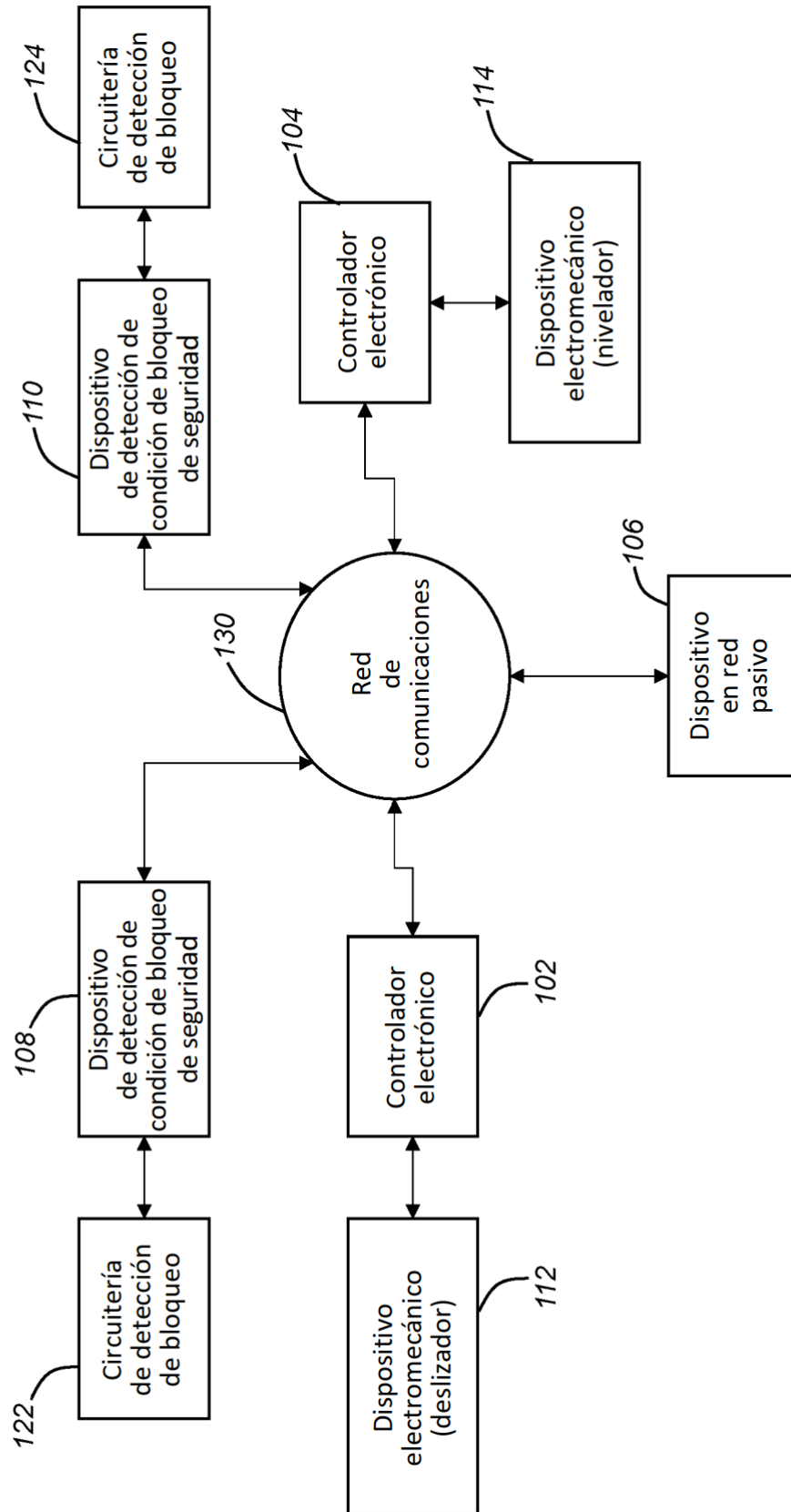
50 10. El sistema de bloqueo de seguridad distribuido (100) de la reivindicación 9, en donde el sistema de bloqueo de seguridad distribuido (100) incluye una pluralidad de controladores electrónicos (102, 104) que incluye el uno o más controladores electrónicos y una pluralidad de dispositivos electromecánicos (112, 114) que incluye el dispositivo o dispositivos electromecánicos, y en donde cada uno de la pluralidad de dispositivos electromecánicos (112, 114) se controla por uno diferente de la pluralidad de controladores electrónicos (102, 104).

60 11. El sistema de bloqueo de seguridad distribuido (100) de la reivindicación 10, en donde un primer controlador electrónico de la pluralidad de controladores electrónicos (102, 104) controla la operación electromecánica de un primer dispositivo electromecánico de la pluralidad de dispositivos electromecánicos (112, 114), en donde un segundo controlador electrónico de la pluralidad de controladores electrónicos (102, 104) controla la operación electromecánica de un segundo dispositivo electromecánico de la pluralidad de dispositivos electromecánicos (112, 114), y en donde el primer controlador electrónico opera independientemente del segundo controlador electrónico; opcionalmente, en donde el primer dispositivo electromecánico es un nivelador (114) que está instalado en el vehículo recreativo, y en donde el segundo dispositivo electromecánico es un deslizador (112) que está instalado en el vehículo recreativo.

12. El sistema de bloqueo de seguridad distribuido (100) de una cualquiera de las reivindicaciones 9 a 11, en donde la pluralidad de dispositivos de detección de condición de bloqueo de seguridad (108, 110) incluye un primer dispositivo de detección de condición de bloqueo de seguridad y un segundo dispositivo de detección de condición de bloqueo de seguridad, en donde el primer dispositivo de detección de condición de bloqueo de seguridad está
- 5 configurado para detectar una primera condición de bloqueo de seguridad, en donde el segundo dispositivo de detección de condición de bloqueo de seguridad está configurado para detectar una segunda condición de bloqueo de seguridad que es diferente de la primera condición de bloqueo de seguridad;
- 10 opcionalmente, en donde cada una de la primera condición de bloqueo de seguridad y la segunda condición de bloqueo de seguridad está basada en al menos uno de lo siguiente: señales del sistema de satélite de navegación global (GNSS) recibidas en un receptor de GNSS, un estado del freno de estacionamiento, un estado del freno del remolque, un estado del freno del vehículo remolcador, el estado de la luz de freno del vehículo remolcador, o una orientación o movimiento detectado por un sensor de movimiento/orientación, y en donde la primera condición de bloqueo de seguridad es diferente de la segunda condición de bloqueo de seguridad.
- 15 13. El sistema de bloqueo de seguridad distribuido (100) de una cualquiera de las reivindicaciones 9 a 12, en donde la red de comunicaciones (130) es un bus de red de área de controlador (CAN) alámbrica o una red de interconexión local alámbrica que está instalada en el vehículo recreativo.
- 20 14. El sistema de bloqueo de seguridad distribuido (100) de una cualquiera de las reivindicaciones 9 a 13, en donde la red de comunicaciones (130) incluye:
- (a) una red de comunicaciones inalámbricas que se lleva a cabo usando una red de comunicación de corto alcance (DSRC) especializada que se proporciona en el vehículo recreativo; y/o
- 25 (b) una red de comunicaciones inalámbricas usada por uno primero de los dispositivos en red y una red de comunicaciones alámbrica usada por uno segundo de los dispositivos en red.
15. El sistema de bloqueo de seguridad distribuido (100) de una cualquiera de las reivindicaciones 9 a 14, en donde cada uno de los dispositivos en red (102-110) opera de acuerdo con un protocolo de consenso (160) que incluye el modo de duplicación de red (164) y el modo de contención de red (166), en donde, cuando está en el modo de
- 30 contención de red (166), cada uno de los dispositivos en red (102-110) vota establecer un consenso en cuanto a si se reducirá el estado de bloqueo de seguridad local de cada uno de los dispositivos en red (102-110).

FIG. 1

100



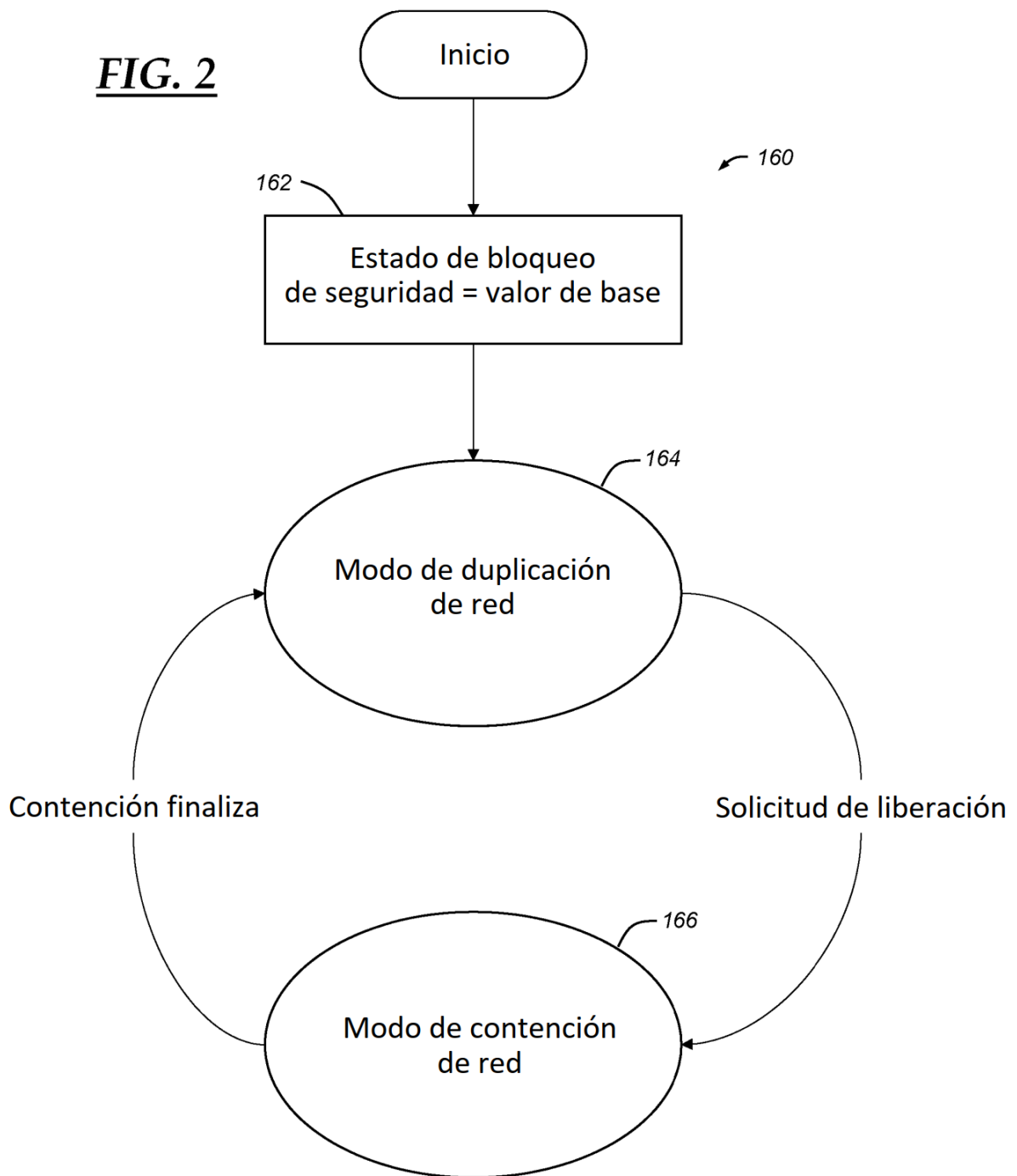


FIG. 3A

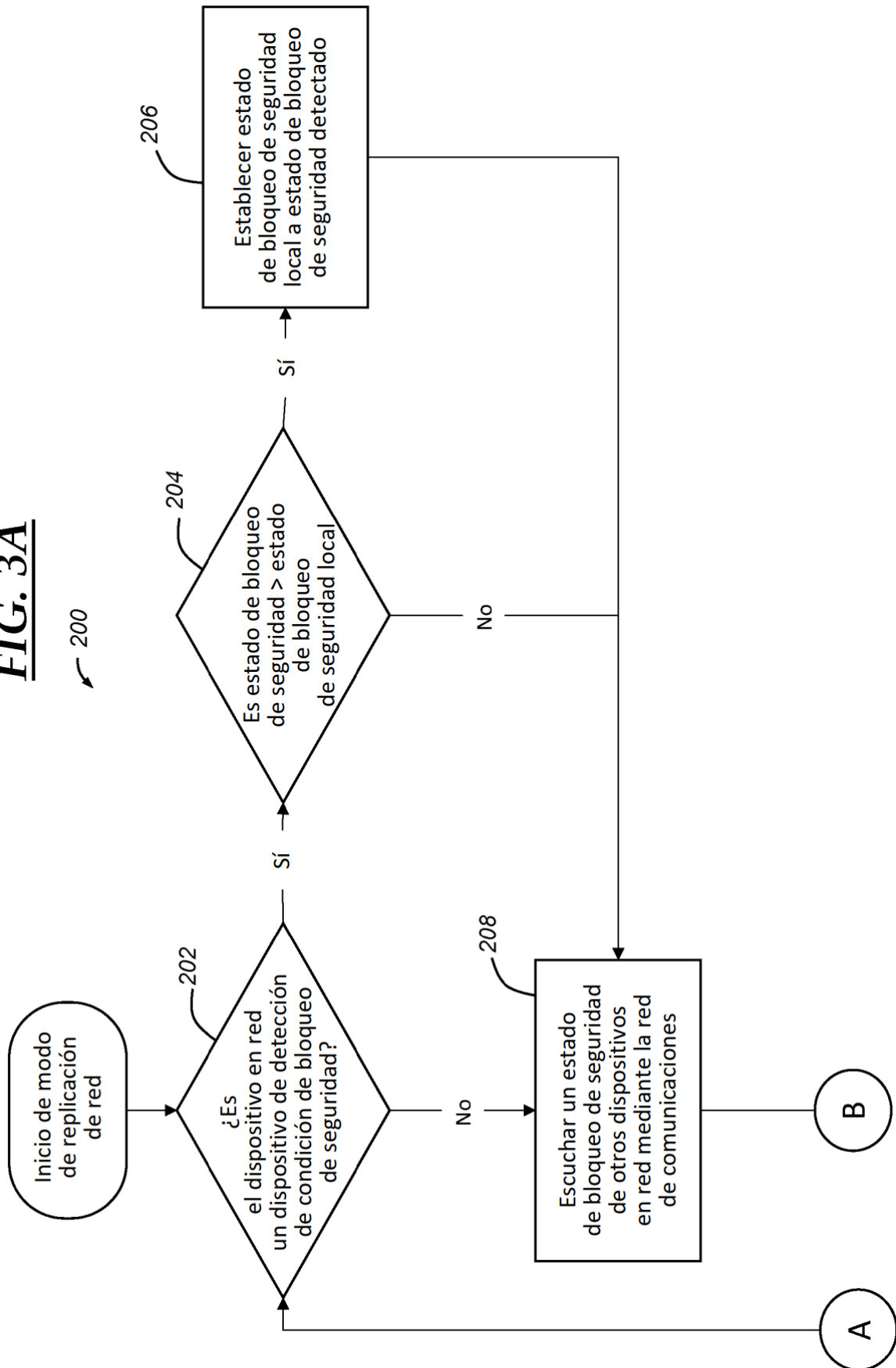


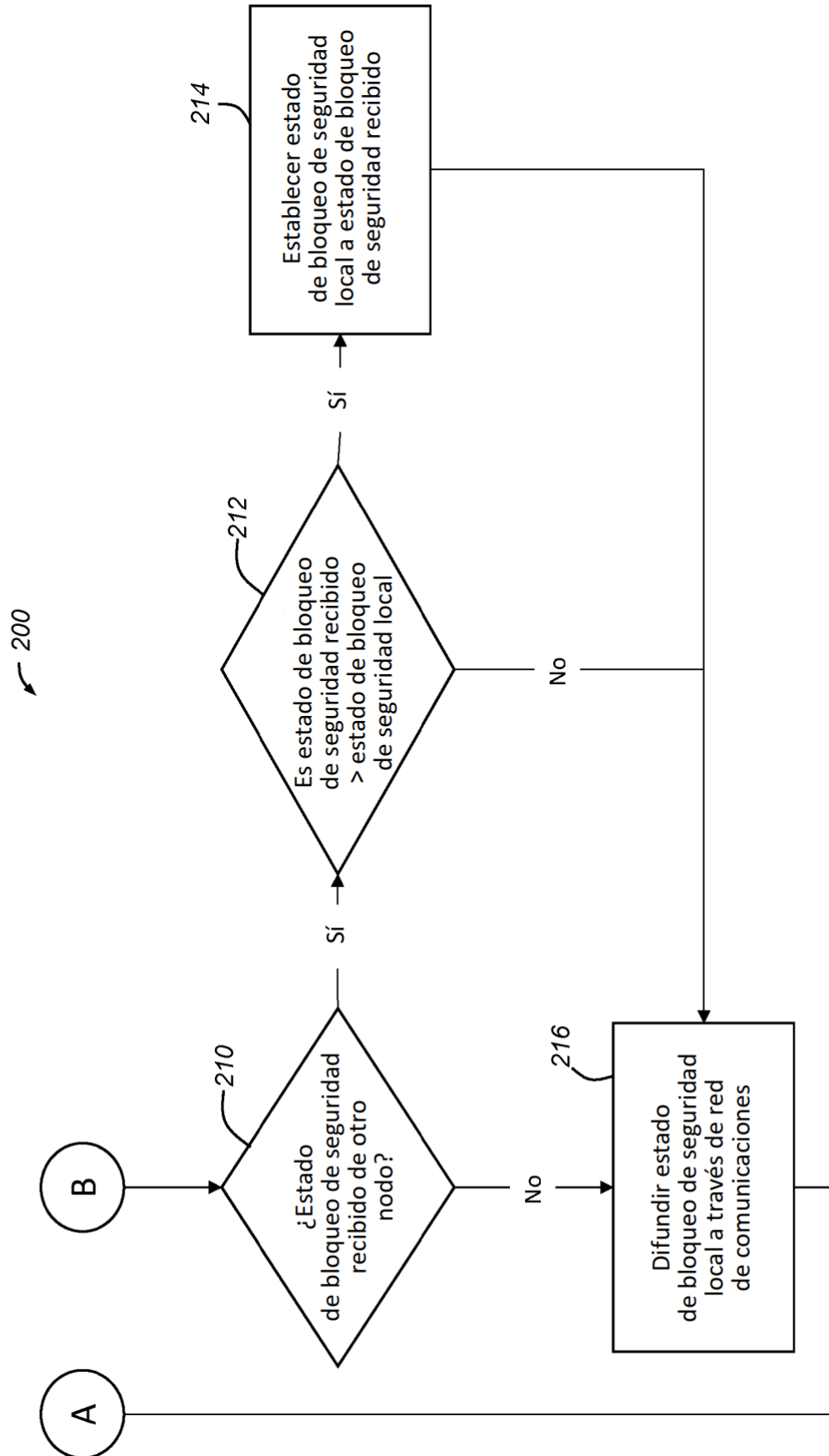
FIG. 3B

FIG. 4A

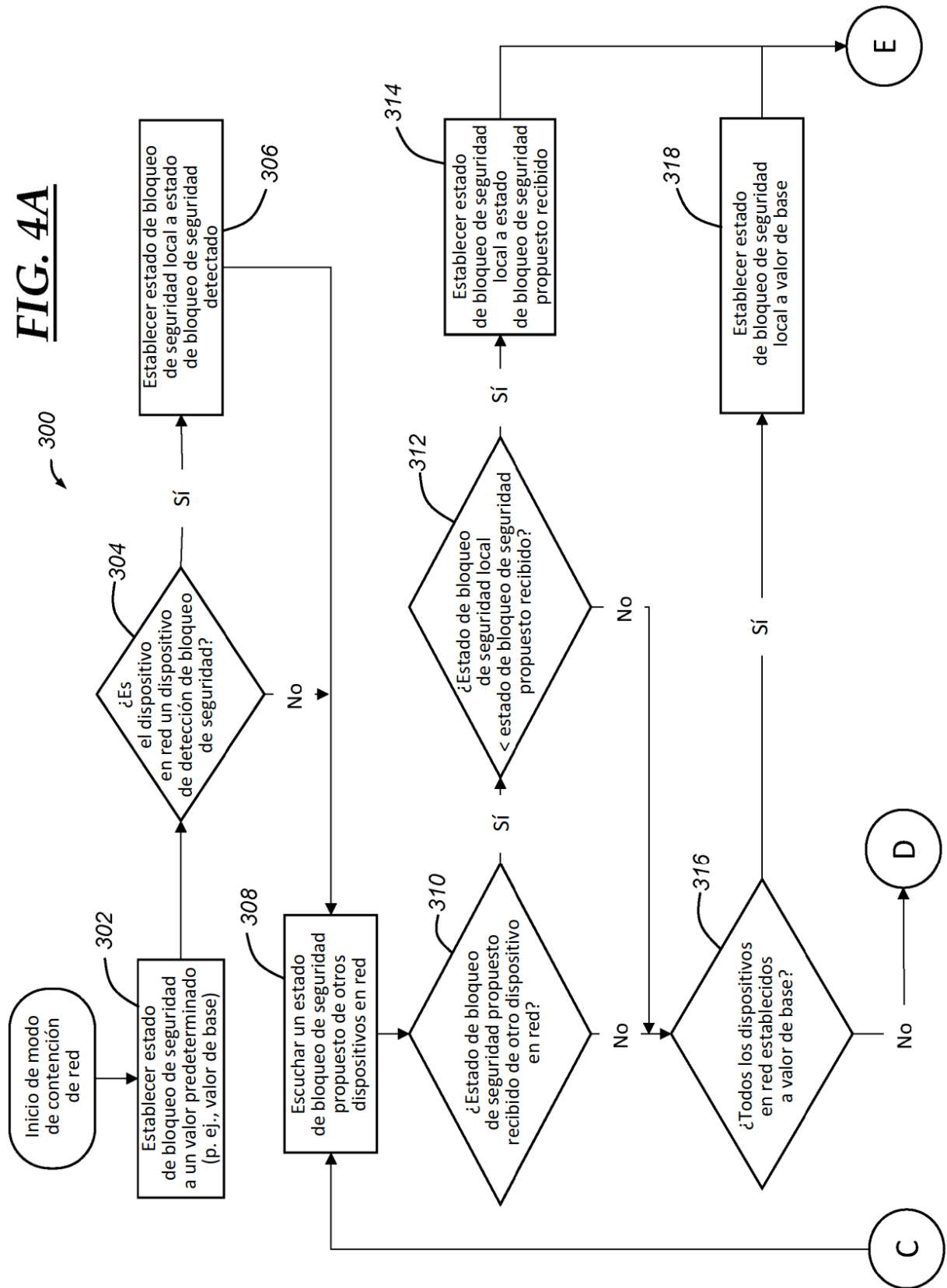


FIG. 4B

