

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 726 770**

51 Int. Cl.:

G05B 19/042 (2006.01)

B64D 1/04 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **14.02.2011 PCT/GB2011/050272**
- 87 Fecha y número de publicación internacional: **18.08.2011 WO11098832**
- 96 Fecha de presentación y número de la solicitud europea: **14.02.2011 E 11703729 (1)**
- 97 Fecha y número de publicación de la concesión europea: **10.04.2019 EP 2534543**

54 Título: **Control de operaciones críticas para la seguridad**

30 Prioridad:

13.02.2010 EP 10250250
13.02.2010 GB 201002495

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2019

73 Titular/es:

BAE SYSTEMS PLC (100.0%)
6 Carlton Gardens
London SW1Y 5AD, GB

72 Inventor/es:

BENNETT, SIMON, GRANT;
BELCHER, NICHOLAS, ANDREW;
PARKER, DAVID;
CHALLIS, KEVIN;
WATKINS, DAVID, CHRISTOPHER y
WATKINS, GARY, ROBERT

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 726 770 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

Control de operaciones críticas para la seguridad

5 Esta invención se refiere a sistemas configurados para efectuar operaciones críticas para la seguridad, y a su control. Por "operación crítica para la seguridad" se entiende una operación que tendría o podría tener de manera previsible unas consecuencias físicas irreversibles. Un ejemplo sin carácter limitante es la liberación de una carga (p. ej., una bomba, un misil o un depósito auxiliar de combustible) desde una aeronave.

10 Aunque la invención es particularmente relevante para un sistema en un vehículo (mediante lo cual se entiende cualquier plataforma móvil, sobre el terreno o subterránea, sobre el agua o subacuática, en el aire o en el espacio) también puede encontrar aplicación en aparatos estacionarios, por ejemplo, un lanzador de misiles terrestre, una puerta de seguridad u otro aparato de control del acceso (siendo el cambio irreversible en este caso la violación de la seguridad implícita que permite el acceso), una planta de procesamiento, una planta de generación de potencia o la señalización ferroviaria.

La solicitud de patente de EE. UU. US 2008/0121097 expone un sistema de activación digital remota.

15 En general, en los sistemas conocidos, únicamente se lleva a cabo una operación crítica para la seguridad si se recibe una orden verificada, y en ausencia de una orden verificada no se lleva a cabo la operación crítica para la seguridad. Dichos sistemas no requieren autocorrección de las señales de mando debido a que se requiere que el sistema mantenga su condición por defecto de "no operación" a menos que se reciba una orden verificada. Esto se contraponen a los "sistemas basados en la disponibilidad" donde no se permite una condición de "no operación". Estos sistemas emplean de manera habitual una autocorrección de datos para garantizar la continuación de una operación cuando se requiera.

De manera convencional, los sistemas críticos para la seguridad alcanzan una integridad o disponibilidad elevadas duplicando (y a veces triplicando o incluso cuadruplicando) elementos de hardware y las vías de comunicación entre dichos elementos, y siendo necesario que las señales ejecutivas se suministren por medio de vías diferentes y concuerden entre sí, o al menos que la mayoría de dichas señales concuerden entre sí.

25 La presente invención proporciona un sistema que comprende: una sección operativa para llevar a cabo una operación crítica para la seguridad en respuesta a una orden de control recibida a través de un medio de transmisión desde una sección de mando alejada de la sección operativa, siendo la sección de mando para controlar la ejecución de la operación crítica para la seguridad, donde la orden de control comprende una pluralidad de claves de descryptación o palabras claves generadas en una parte de generación de órdenes de control de integridad elevada de la sección de mando, que se suministran únicamente en respuesta a una orden de corrección de un operario, y donde la sección operativa comprende una pluralidad de conmutadores de seguridad por clave de integridad elevada que tienen por función comparar las palabras clave respectivas recibidas desde la sección de mando, o generadas por la sección operativa tras la recepción de las claves de descryptación a través del medio de transmisión, efectuándose la ejecución de la operación crítica para la seguridad únicamente en el caso de una comparación correcta, mediante los conmutadores de seguridad por clave, de sus palabras clave respectivas.

35 Esta invención se basa en el reconocimiento de que, hasta ahora en lo que se refiere a dichas señales, no importa mediante cuantas vías se suministran las señales. Lo que es importante es que la señal ejecutiva se recibe y verifica de manera correcta. En la presente invención esto se puede hacer a través de una única vía de transmisión.

40 Por tanto, en un primer aspecto, la invención proporciona un sistema configurado de modo que efectúe el control de una operación crítica para la seguridad mediante el envío de una pluralidad de claves de descryptación o palabras clave a través de un medio de transmisión. El medio de transmisión puede comprender un medio de transmisión de integridad baja.

45 En particular, el medio de transmisión de integridad baja puede incluir una vía de transmisión individual o común. De ese modo, se puede reducir el número de canales de transmisión en el sistema (normalmente 2, 3 o 4) a uno para la mayor parte o toda su longitud. Esto puede hacer posible una reducción significativa en la complejidad y coste del sistema.

El sistema puede comprender una pluralidad de conmutadores, donde cada uno de ellos responde de manera selectiva a dichas palabras clave, requiriéndose el funcionamiento de al menos una mayoría de los conmutadores para efectuar dicho control.

50 Los conmutadores se pueden disponer en serie, por ejemplo, con respecto a un suministro de alimentación eléctrica u otra señal ejecutiva para el funcionamiento de dicho sistema.

Puede haber medios para hacer que los conmutadores funcionen en una secuencia predeterminada. Por ejemplo, se puede suministrar una de dichas palabras clave a uno de dichos conmutadores a través de una puerta lógica a la cual se suministra una salida desde otro de dichos conmutadores.

Se puede enviar una palabra clave a uno de dichos conmutadores a través de un bus de datos serie. Se puede utilizar el mismo bus de datos para todas las palabras clave.

El sistema se puede configurar de modo que proporcione una alimentación eléctrica local a uno de dichos conmutadores como parte de una señal de datos que contiene la palabra clave.

- 5 Cuando la orden de control comprende una pluralidad de claves de descifrado generadas en una parte de generación de órdenes de control de integridad elevada de la sección de mando, que se suministran únicamente en respuesta a una orden correcta de un operario, la sección operativa puede comprender una unidad de almacenaje de integridad elevada para almacenar una pluralidad de palabras clave generadas únicamente tras la recepción de la claves de descifrado recibidas desde la sección de mando a través del medio de transmisión y la pluralidad de conmutadores de seguridad por clave de integridad elevada operan comparando las palabras claves generadas, efectuándose la ejecución de la operación crítica para la seguridad únicamente en el caso de una comparación correcta mediante los conmutadores de seguridad por clave.

- 15 Se puede preferir esta disposición si el ancho de banda del medio de transmisión es relativamente bajo, ya que las claves de descifrado requieren menos ancho de banda para la transmisión. No obstante, la sección operativa debe tener entonces una sección de integridad elevada más para almacenar las palabras clave y por lo tanto se puede incurrir en costes de hardware adicionales.

Cada conmutador se puede configurar de modo que responda a una de dichas palabras clave diferente.

- 20 Asimismo, la invención se puede aplicar en particular al control de operaciones críticas para la seguridad en aparatos ubicados de manera remota con respecto a una estación de control, por ejemplo, en un vehículo aéreo no tripulado (UAV) u otro vehículo. Por tanto, el sistema puede ser un sistema de gestión de cargas.

Por tanto, en otro aspecto, la invención proporciona un vehículo aéreo no tripulado que comprende: una sección operativa tal como se describe anteriormente.

- 25 En un aspecto adicional, esta proporciona un controlador para un aparato que funciona de manera remota configurado de modo que ejecute una operación crítica para la seguridad y que incluye un medio para transmitir al aparato a través de una única vía de transmisión una instrucción o autorización para dicha operación que comprende una pluralidad de palabras clave.

Ahora se describirá la invención simplemente a modo de ejemplo haciendo referencia a los dibujos anexos, donde;

la figura 1 muestra un sistema crítico para la seguridad convencional en un vehículo aéreo de combate no tripulado "(UCAV)";

- 30 la figura 2 muestra un sistema crítico para la seguridad de acuerdo con la invención en un UCAV;

la figura 3 muestra parte del sistema de la figura 2;

las figuras 4 y 5 muestran la implementación de dos realizaciones de la invención utilizando la estructura de la figura 3;

la figura 6 muestra con más detalle parte de la estructura de la figura 4; y

- 35 la figura 7 muestra una modificación de la realización de la figura 5.

- Haciendo referencia a la figura 1, un UCAV 10 convencional comprende, en lo que es pertinente a la presente, un receptor de radio 12 y un ordenador de misión 14, que hace funcionar una sección aérea 16 de un sistema de gestión de cargas (SMS). El SMS controla el funcionamiento y la liberación de una o más cargas (armas) 18 montadas en una unidad de soporte externa 20 del UCAV. En la siguiente descripción, la carga se supone que es un arma que se puede liberar, aunque podría ser de igual modo algún otro dispositivo que se puede liberar.

- 40 El UCAV está controlado por un operario en una estación de tierra 24 que incluye un transmisor 26, y en particular una sección controladora de base terrestre 28 del SMS. La liberación no ordenada de cualquier carga por parte del UCAV sería un problema serio, y por consiguiente el control del SMS se efectúa mediante un sistema crítico para la seguridad en el que cada una de las unidades secundarias 12, 14, 16 y 20 contienen elementos funcionales duplicados, y cada una está conectada a las demás mediante vías de comunicación dúplex 30, que incluyen un enlace de radio de doble canal 32 entre el transmisor 12 y el receptor 26.

- 45 Las vías de comunicación se consolidan en una vía individual únicamente en la interfaz entre el soporte 20 y la carga. En general, las aplicaciones del SMS requieren diversas salidas (algunas críticas para la seguridad) que se deben activar en una secuencia lógica para lograr una liberación del arma.

- 50 Una secuencia habitual de liberación de una carga es tal como sigue:

- Fase de selección del arma
 - El ordenador de misión solicita al SMS que seleccione un arma.
 - El SMS aéreo selecciona el arma y devuelve la selección al ordenador de misión.
 - 5 ○ El SMS conmuta la alimentación eléctrica no crítica para la seguridad a la carga (en general implementado mediante el accionamiento de un relé o conmutador de alimentación eléctrica individual en la unidad de soporte).
 - El arma lleva a cabo unas pruebas integradas.
- Fase de armado del arma
 - El operario de la estación terrestre envía una orden de “armado de arma”.
 - 10 ○ El SMS energiza los útiles de disparo (que siguen a las comprobaciones pertinentes de interbloqueo).
 - El SMS energiza la alimentación eléctrica crítica para la seguridad a la carga (salida del SMS crítica para la seguridad, implementada en general mediante dos conmutadores de alimentación eléctrica superior/inferior “en serie”).
- 15 • Fase de liberación del arma
 - El operario de la estación terrestre autoriza la liberación final y envía una orden de “liberación del arma”.
 - El SMS energiza la aprobación de liberación (salida del SMS crítica para la seguridad, implementada en general mediante dos conmutadores de alimentación eléctrica superior/inferior “en serie”).
 - 20 ○ El SMS energiza la salida de “Disparo” a los equipos de suspensión y liberación (salida del SMS crítica para la seguridad, implementada en general mediante dos conmutadores de alimentación eléctrica superior/inferior “en serie”).

25 Por tanto, durante el funcionamiento del sistema de la figura 1, se duplica una orden crítica para la seguridad y se envía a través de ambos canales 30, 32 desde el controlador del SMS 28. La orden se ejecuta si (y solo si) se reciben adecuadamente ambas órdenes en un comparador 34 dentro del soporte 20. Con esta arquitectura, todo el sistema desde las entradas del operario de tierra hasta las salidas de los soportes a la carga 18 se deben desarrollar con los estándares de integridad de hardware y software más elevados, p. ej., DEF-STAN-00-55/56 nivel de integridad de seguridad 4 o equivalente, con todo lo que implica en complejidad y coste.

30 La figura 2 muestra un sistema de acuerdo con la invención que de manera similar se opone a una liberación no ordenada de la carga, pero que es mucho más simple que el sistema de la figura 1. Las partes ya descritas tienen los mismos números de referencia que en la figura 1.

35 En esta realización, la sección del SMS de base terrestre 28, la estación terrestre del UCAV 26, el receptor del UCAV 12, el ordenador de misión 14 y la sección aérea del SMS 16 se configuran y disponen de modo que se comuniquen entre sí únicamente a través de una vía de comunicación de integridad baja individual 36, 38. La unidad de soporte tiene dos conmutadores de seguridad por clave (KSS) 40, 42, cada uno de los cuales cambia a un estado activo (cerrado) cuando se indica con una palabra clave única respectiva.

Las salidas de los conmutadores 40, 42 se comparan en un comparador 34 como en la figura 1, y si estas concuerdan el comparador envía una orden crítica para la seguridad a la carga 18.

40 Las palabras clave se almacenan de manera segura en una parte de integridad elevada de la sección del SMS de base terrestre 28 y se generan solo para su transmisión en respuesta a órdenes de corrección procedimentales del operario de la estación terrestre. Los elementos de almacenamiento, selección, recuperación y liberación del SMS de base terrestre 28 se configuran con estándares críticos para la seguridad (de integridad elevada o SIL4), aunque el resto de este junto con los demás elementos del sistema, con la excepción de los módulos de conmutación 40, 42, solo es necesario que tengan una integridad más baja. La parte aérea del SMS 16 se muestra como que dispone de vías de comunicación independientes 30 para cada conmutador 40, 42, aunque es posible enviar las palabras clave a los conmutadores a través de un bus serie común. Esto es especialmente conveniente si hay más de dos conmutadores de seguridad por clave en la unidad de soporte. Por ejemplo, cada arma puede tener un conmutador de armado y un conmutador de liberación, y de hecho habrá probablemente más de un soporte. Por tanto, puede haber un número significativo de conmutadores de seguridad por clave en el SMS, cada uno con su propia contraseña única que se le comunica a través de un bus común. Las palabras clave para los conmutadores o las operaciones que no son críticas para la seguridad se pueden almacenar en el SMS aéreo 16 en lugar de en el SMS

ES 2 726 770 T3

de base terrestre, lo que reduce de ese modo la cantidad de datos a enviar a través del canal de comunicaciones individual.

En esta realización, los requisitos de nivel de integridad del sistema serían los siguientes:

Elemento(s) del sistema	Nivel de integridad
1) SMS de base terrestre (solo los elementos responsables de la selección y recuperación de los códigos de los KSS)	DEF-STAN-00-55/56 SIL4 (o equivalente)
2) Módulos de los KSS	
Resto del SMS (de base terrestre & aéreo)	DEF-STAN-00-55/56 SIL2 (o equivalente)

- 5 En una realización alternativa, todas la palabras clave de las salidas del SMS críticas para la seguridad se mantienen en el SMS aéreo 16, así como también las palabras clave de las salidas no críticas para la seguridad. No obstante, las palabras clave de las salidas críticas para la seguridad se mantienen en forma encriptada. Únicamente las claves de descriptación se mantienen en el SMS de base terrestre 28. Durante el funcionamiento, las claves de descriptación de las operaciones críticas para la seguridad, tales como el armado y la liberación, se envían mediante el SMS de base terrestre 28, y las palabras clave se descriptan en el SMS aéreo 16. A continuación estas se aplican a los conmutadores 40, 42 tal como ya se ha descrito. Obviamente, las claves de descriptación se envían únicamente cuando lo ordena el operario de la estación terrestre, y por tanto hasta ese momento el SMS aéreo no tiene todos los datos necesarios para efectuar la liberación de la carga. Esta realización requiere que ciertos aspectos del SMS aéreo (p. ej., el control y la eliminación de la claves de descriptación) tengan un nivel de integridad elevado, aunque tiene la ventaja de una menor transferencia de datos desde el SMS de base terrestre 28.

En esta realización, los niveles de integridad requeridos son;

Elemento(s) del sistema	Nivel de integridad
1) SMS de base terrestre (solo los elementos responsables de la selección y recuperación de los códigos de los KSS)	DEF-STAN-00-55/56 SIL4 (o equivalente)
2) Módulos de los KSS	
3) SMS aéreo (solo los elementos asociados con la implementación de la "clave de descriptación")	
Resto del SMS (de base terrestre & aéreo)	DEF-STAN-00-55/56 SIL2 (o equivalente)

- 20 En ambas realizaciones, la reducción en el nivel de integridad de la mayoría del SMS, junto con el diseño de canal individual del sistema, puede ofrecer un ahorro de coste significativo en el diseño, desarrollo y posterior fabricación del sistema. No obstante, el concepto aún permite elaborar un procedimiento de seguridad razonado (que incluye la consideración de una "secuencia lógica" de acontecimientos para efectuar una liberación), para apoyar la eventual certificación del sistema.

- 25 La figura 3 ilustra que se puede lograr la función del comparador 34 simplemente conectando los conmutadores 40, 42 en serie con respecto a una cantidad a controlar. En la presente, esa cantidad es un suministro de alimentación eléctrica de la red 44, que cuando los conmutadores 40, 42 están cerrados se suministra en 46 (p. ej., al mecanismo

de liberación de la carga) como una salida del sistema crítica para la seguridad. También se ilustra el bus de datos serie común 48.

5 En la figura 4 se muestra una implementación de la realización de la figura 3. Las palabras clave de activación 50 enviadas por el SMS de base terrestre 28 se suministran al bus 48 y a continuación a los conmutadores 40, 42, cada una de las cuales está preprogramada (solo lectura) para responder a su palabra clave respectiva. Cada conmutador también tiene una palabra clave de desactivación preprogramada, a utilizar si se aborta la liberación del arma.

10 Cada interruptor 40, 42 tiene un procesador para la comparación de claves, que puede ser, por ejemplo, un microprocesador específico, un dispositivo lógico programable o un dispositivo de enmascaramiento fijo. La elección de dispositivo dependerá de la aplicación particular, especialmente del intervalo de temperatura operativa y de los requisitos de alimentación eléctrica. La preprogramación de las palabras clave de activación y desactivación se puede implementar mediante conmutadores mecánicos (p. ej., DIL), enlaces cableados, dispositivos de memoria internos o externos o dentro de un registro de datos o una memoria permanente del microprocesador.

15 El bus de datos 48 (que puede ser un bus de datos serie de propósito general, tal como un RS422 o un USB) se puede disponer de modo que proporcione un suministro de alimentación eléctrica local a los conmutadores como parte de la señal de datos que contiene las palabras clave. A continuación, si no se suministra ningún dato en serie a un conmutador particular, este no se activará y permanecerá en un estado seguro.

Como una característica de seguridad más, se puede emplear el aislamiento de la señal en las entradas del bus de datos para:

- 20
- Evitar un modo de fallo externo de un bus de datos serie que da como resultado un funcionamiento fortuito del conmutador.
 - Proporcionar un grado elevado de inmunidad frente al ruido electromagnético.
 - Mantener un aislamiento eléctrico completo entre los buses de control.

25 Una ventaja de la realización de la figura 4 es que los conmutadores conectados al bus de datos común no es necesario que sean direccionables de manera individual, debido a que cada uno es accionado por una única palabra clave. No obstante, una desventaja es que los conmutadores no son intercambiables o sustituibles sin volver a programar el SMS de base terrestre 28, debido a que cada uno tiene su propio código. Esta desventaja se puede eliminar mediante la realización de la figura 5.

30 En esta realización, cada interruptor 40, 42, etc., es direccionable de manera única. Si se debe accionar un conmutador, el SMS de base terrestre envía dos (o más) cadenas de datos digitales largas 52 respectivas como palabras clave, junto con la dirección del conmutador. El conmutador direccionado recibe las palabras clave y las compara. Si la comparación es válida, se activa el conmutador. A continuación se repite el procedimiento para los demás conmutadores, según se requiera. El funcionamiento secuencial correcto de los interruptores se puede incluir como un interbloqueo de seguridad más, por ejemplo, tal como se muestra en la figura 7, suministrando la señal de datos al segundo conmutador 42 y de manera similar a los conmutadores posteriores (si los hay) a través de una puerta AND 72 respectiva, a la cual se aplica también la salida del conmutador 40 anterior; esta característica también se puede incluir en las demás realizaciones.

35

Se apreciará que en la realización de la figura 5, no es necesario programar las palabras clave de accionamiento en los conmutadores, sino únicamente sus direcciones respectivas. Esto se puede lograr mediante un modelo de direccionamiento independiente, o se puede programar cada conmutador con una dirección. Se puede emplear encriptación, tal como en la realización de la figura 4, manteniéndose las contraseñas encriptadas de cada conmutador en el SMS aéreo.

40

La figura 6 muestra uno de los conmutadores 40, 42 de la figura 4 con más detalle. En 54 se recibe una señal combinada de alimentación eléctrica y datos desde el bus 48. Preferentemente, la señal es una señal de activación diferencial, donde los datos codificados utilizan una codificación Manchester diferencial autosincronizada. Para la inicialización del conmutador, en primer lugar se proporciona la señal de reloj únicamente con datos inertes. En aplicaciones críticas para la seguridad, únicamente se habilita la señal de reloj una vez que los interbloques de seguridad pertinentes (p. ej., que el UAV está en vuelo y que está activado el suministro de disparo) se confirmen como presentes.

45

La señal del bus de datos recibida 54 se lleva a través de un transformador de aislamiento 56 a una unidad de extracción de datos y suministro de alimentación eléctrica 58, donde se extrae la componente de datos de la señal de datos codificada. La señal de datos además se rectifica y regula de modo que proporcione un suministro de alimentación eléctrica local 60 a un elemento de conmutación 62, al que se suministran los datos extraídos 64 desde la unidad de extracción de datos 58. El elemento de conmutación 62 compara la palabra clave en los datos extraídos con su palabra clave programada con anterioridad, y si coinciden, el elemento de conmutación ordena a un conmutador de alimentación eléctrica 66 (p. ej., un transistor de alimentación eléctrica o un relé de estado sólido) que se cierre y que suministre una alimentación eléctrica de entrada de CC de la red 68 a una salida de alimentación

50

55

eléctrica conmutada 70. Un enlace de información de retorno 74 confirma al elemento de conmutación 62 que se ha cerrado el conmutador de alimentación eléctrica.

5 La topología de un conmutador de seguridad por clave para su utilización en la realización de la figura 5 es similar; el elemento de conmutación en ese caso se configura de modo que sea direccionable, y de modo que reciba y compare dos o más palabras clave en lugar de que compare una palabra clave recibida con una palabra clave programada con anterioridad en este.

Asimismo, cada conmutador de seguridad por clave puede incluir características inteligentes, p. ej., un funcionamiento con período de activación programable por el usuario o de un solo disparo.

10 En tareas de conmutación no críticas para la seguridad se puede utilizar un conmutador de seguridad por clave individual, en lugar de dos o más en una disposición en cascada o de votación.

Aunque se prefiere un bus de datos común 48 por razones de simplicidad y coste, se puede emplear más de un bus para una mayor integridad y disponibilidad, donde cada uno da servicio a un conmutador individual o a un grupo de conmutadores.

15 La invención también incluye cualquier combinación de características expuestas en la presente, tanto si se reivindican o no de manera específica.

REIVINDICACIONES

1. Un sistema que comprende: una sección operativa para llevar a cabo una operación crítica para la seguridad en respuesta a una orden de control recibida a través de un medio de transmisión desde una sección de control (24) alejada de la sección operativa (18), teniéndose la sección de control (24) para controlar la ejecución de la operación crítica para la seguridad,
- 5
- caracterizado por que
- la orden de control comprende una pluralidad de claves de descifrado o palabras clave (52) generadas en una parte de generación de órdenes de control de integridad elevada (28) de la sección de mando (24), que se suministran únicamente en respuesta a una orden correcta de un operario, y la sección operativa (18) comprende una pluralidad de conmutadores de seguridad por clave de integridad elevada (40, 42) que operan de modo que comparen las palabras clave respectivas recibidas desde la sección de mando, o generadas por la sección operativa tras la recepción de las claves de descifrado, a través del medio de transmisión (36, 38), efectuándose la ejecución de la operación crítica para la seguridad únicamente en el caso de una comparación correcta mediante los conmutadores de seguridad por clave (40, 42) de sus palabras clave respectivas.
- 10
- 15
2. El sistema de la reivindicación 1, que comprende además el medio de transmisión (36, 38), donde el medio de transmisión comprende una vía de transmisión común para las claves de descifrado o palabras clave.
3. El sistema de la reivindicación 1 o la reivindicación 2, que comprende una pluralidad de conmutadores (40, 42), donde cada uno responde de manera selectiva a dichas palabras clave recibidas o generadas, requiriéndose el funcionamiento de al menos una mayoría de los conmutadores para efectuar dicho control.
- 20
4. El sistema de la reivindicación 3, donde los conmutadores se disponen en serie con respecto a un suministro de alimentación eléctrica (44) u otra señal ejecutiva para el funcionamiento de dicho sistema.
5. El sistema de la reivindicación 4, que comprende un medio (72) para hacer que los conmutadores funcionen en una secuencia predeterminada.
- 25
6. El sistema de cualquiera de las reivindicaciones 3, 4 o 5, donde una de dichas palabras clave se envía a uno de dichos conmutadores a través de un bus de datos serie (48).
7. El sistema de cualquiera de las reivindicaciones anteriores, configurado para proporcionar una alimentación eléctrica local al conmutador (40, 42) desde una señal de datos que contiene la palabra clave.
8. El sistema de la reivindicación 3 o de cualquier reivindicación que dependa de esta, donde cada conmutador (40, 42) se configura de modo que responda a una de dichas palabras clave (52) diferente.
- 30
9. El sistema de la reivindicación 8, donde cada uno de dichos conmutadores (40, 42) es direccionable de manera individual.
10. El sistema de cualquier reivindicación anterior, donde la orden de control comprende una pluralidad de claves de descifrado, y la sección operativa comprende una unidad de almacenamiento de integridad elevada para almacenar una pluralidad de palabras clave (52), generadas únicamente tras la recepción de las claves de descifrado recibidas desde la sección de mando (24) a través del medio de transmisión (36, 38), y la pluralidad de conmutadores de seguridad por clave de integridad elevada (40, 42) operan de modo que comparen las palabras clave generadas.
- 35
11. El sistema de la reivindicación 10, donde la sección operativa (18) comprende un medio para descifrar las palabras clave y suministrarlas a los conmutadores (40, 42).
- 40
12. El sistema de cualquier reivindicación anterior, que se configura de modo que se incorpore, al menos parcialmente, en un vehículo aéreo no tripulado o en otro vehículo.
13. El sistema de la reivindicación 12, que es un sistema de gestión de cargas.
14. El sistema de cualquier reivindicación anterior, donde el medio de transmisión (36, 38) comprende un medio de transmisión de integridad baja.
- 45
15. El sistema de cualquier reivindicación anterior, donde la orden de control comprende una pluralidad de claves de descifrado.
16. Un vehículo aéreo no tripulado que comprende el sistema de cualquier reivindicación anterior.

Fig.1.

Arquitectura tradicional del SMS

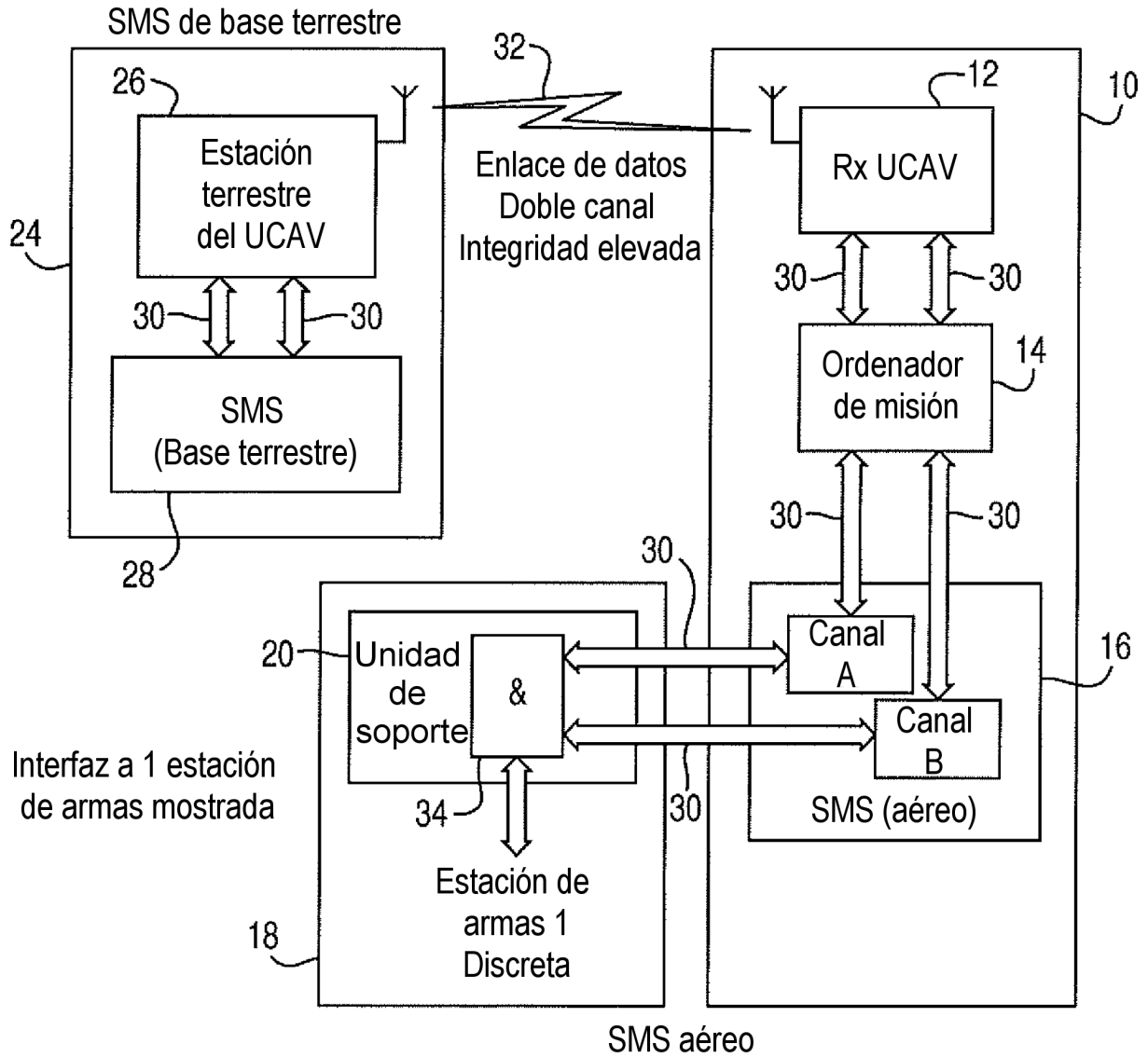


Fig.2.

Arquitectura del SMS de conceptos ITD/KSS

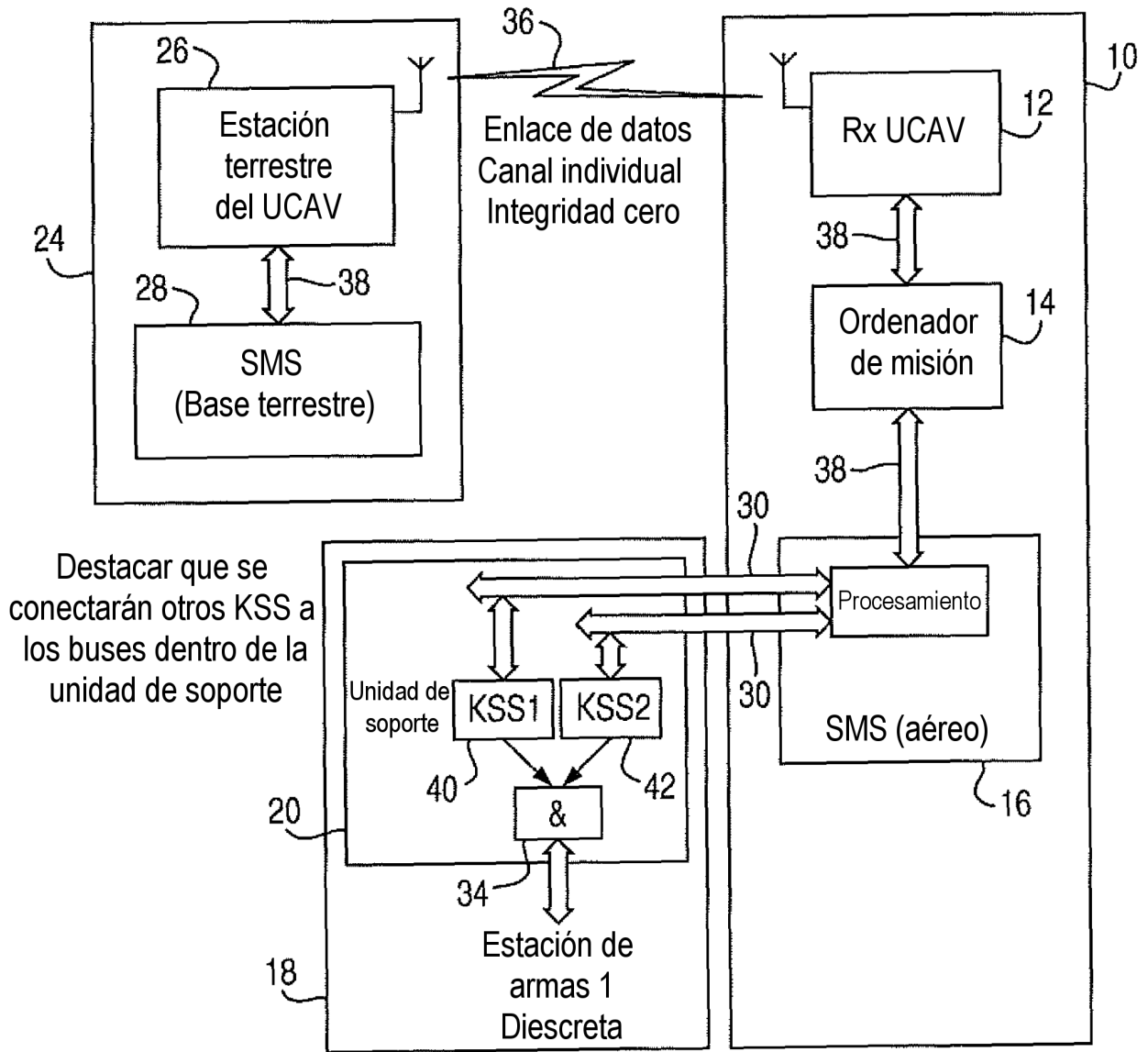


Fig.3.

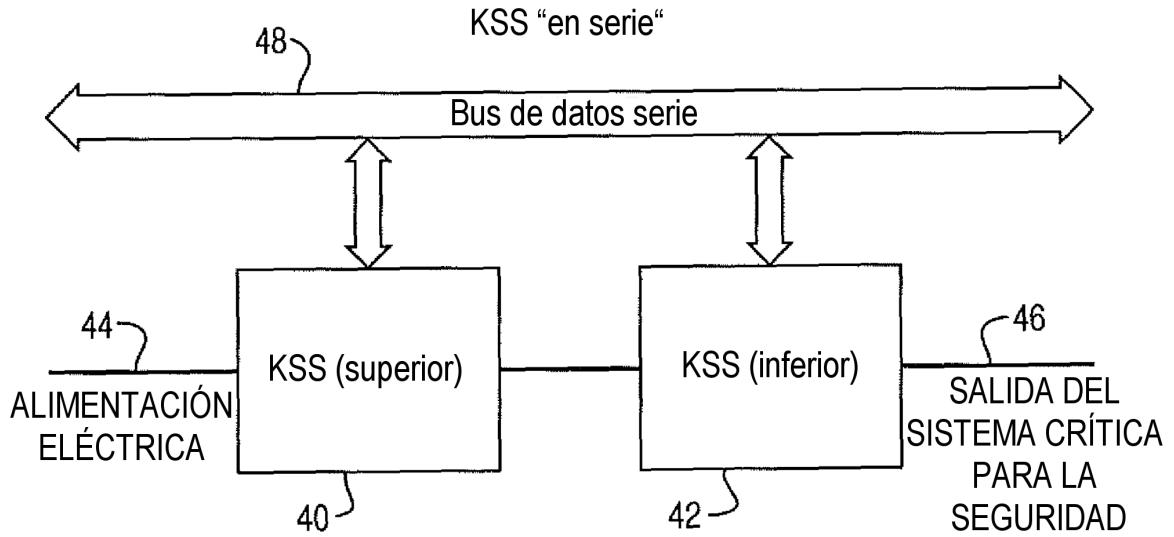


Fig.6.

Diagrama de bloques típico del KSS

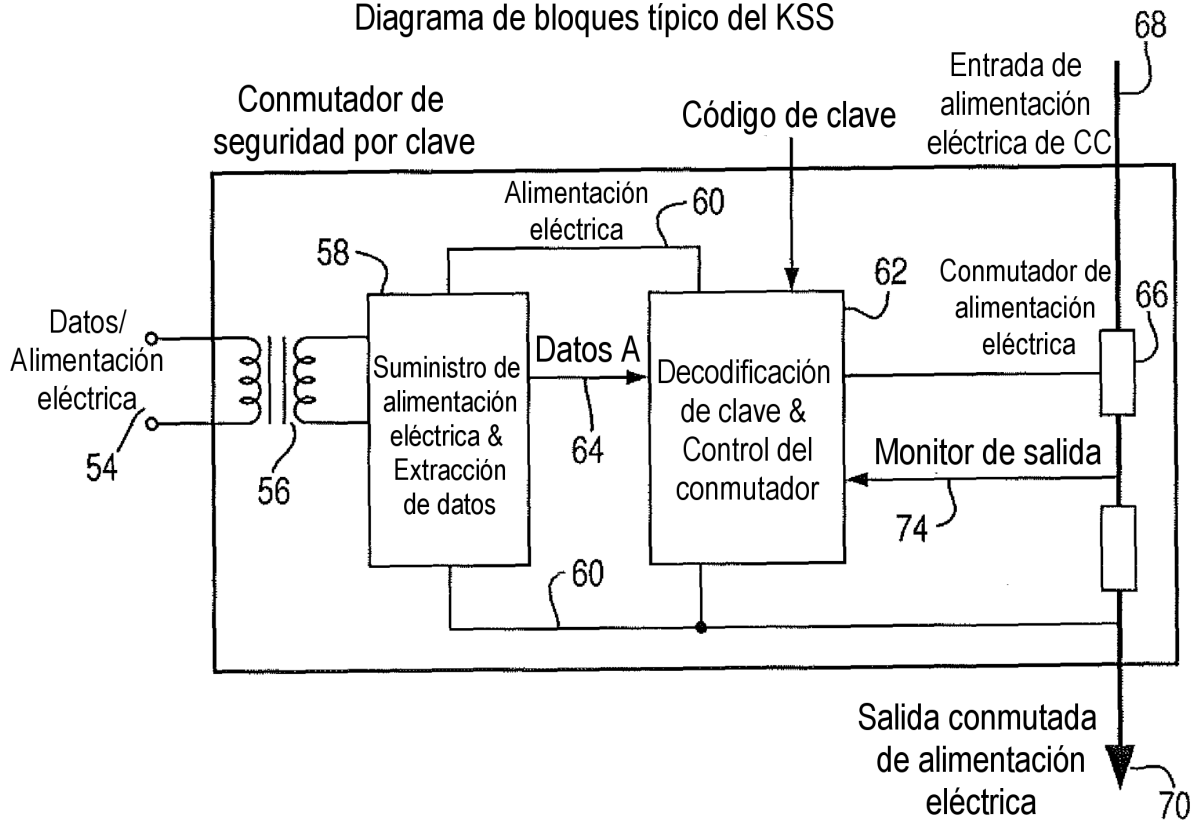


Fig.4.

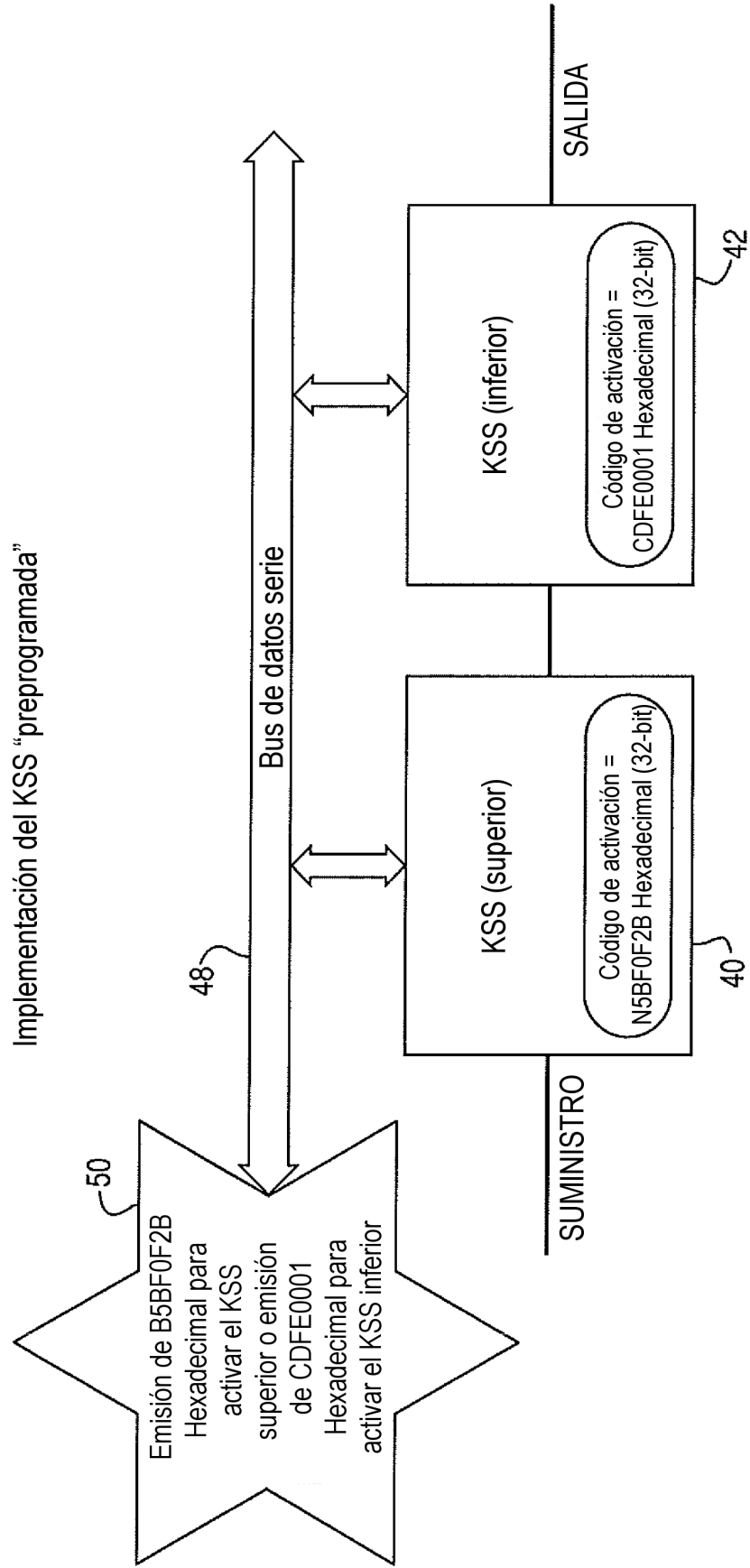


Fig.5.

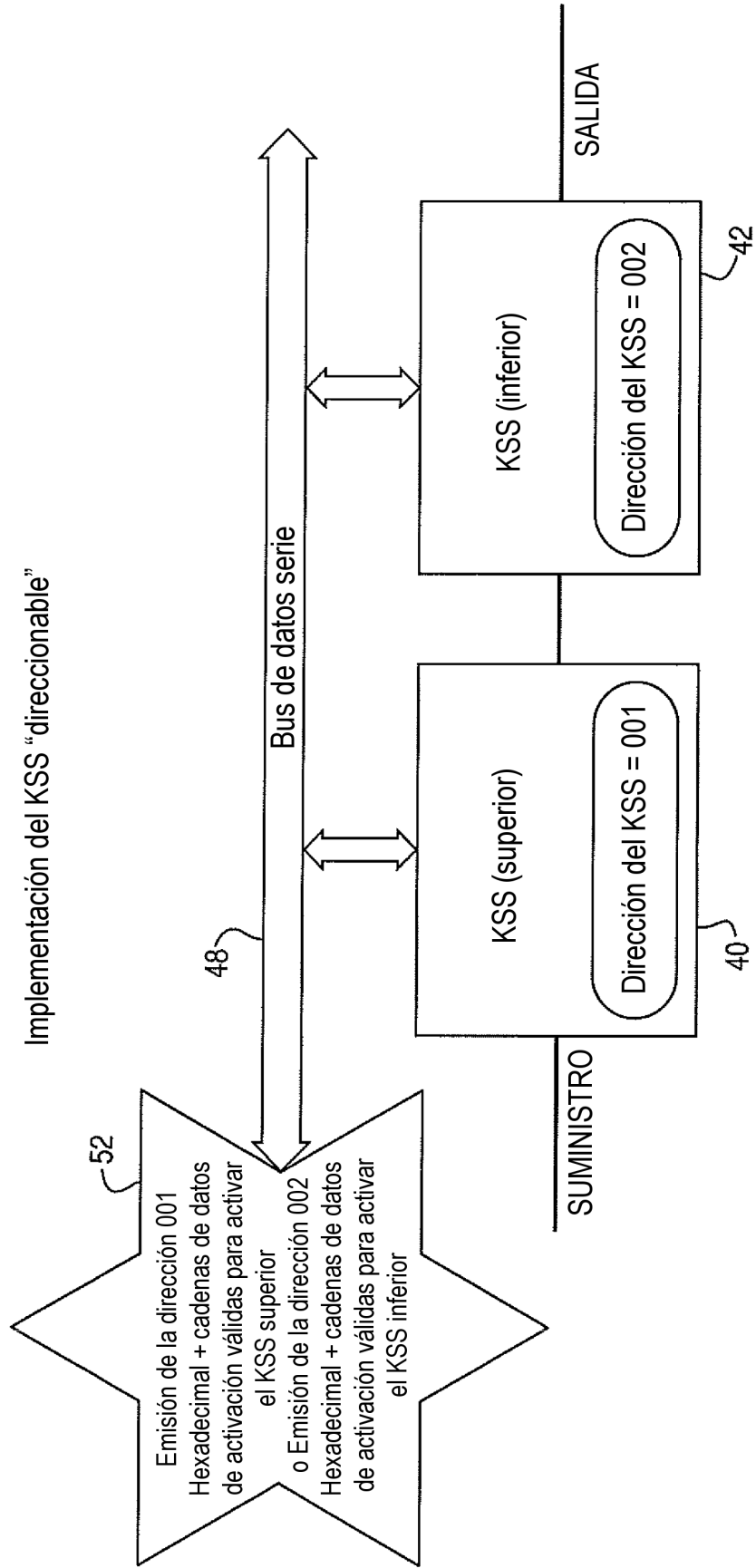


Fig.7.

