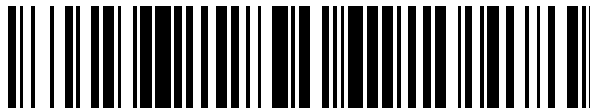


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 779 598**

51 Int. Cl.:

**H04L 12/40** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **18.11.2016** **E 16199505 (5)**

97 Fecha y número de publicación de la concesión europea: **01.01.2020** **EP 3324578**

54 Título: **Interfaz de red segura**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**18.08.2020**

73 Titular/es:  
**MERCURY MISSION SYSTEMS INTERNATIONAL  
S.A. (100.0%)  
Avenue Eugène-Lance 38  
1212 Lancy, CH**

72 Inventor/es:  
**RICCO, PHILIPPE;  
MATHYS, YVES y  
BETTAÏEB, KHALED**

74 Agente/Representante:  
**CURELL SUÑOL, S.L.P.**

**ES 2 779 598 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

Interfaz de red segura

5 **Campo de la invención**

La presente invención trata sobre una interfaz de red, y, en particular, una interfaz para comunicaciones críticas entre sistemas digitales. En particular, aunque no de forma exclusiva, la presente invención se refiere a una interfaz de red que proporciona comunicaciones críticas de seguridad entre subsistemas conectados en red. La invención resulta particularmente adecuada para aplicaciones de aviónica, aunque su dominio abarca todas las situaciones que requieren una estructuración en red de ancho de banda amplio y altamente fiable.

**Descripción de las anterioridades**

15 Con el crecimiento de los “aviones digitales” se ha producido un impulso para mejorar la integración de los accionadores, sensores y subsistemas informáticos en las aeronaves por medio de redes digitales. Aunque la introducción de redes de datos en aeronaves ha aportado una multitud de posibilidades ventajosas, existe la preocupación de que las interfaces y protocolos de red convencionales no satisfagan los exigentes requisitos de seguridad de las aplicaciones de aviónica.

20 La red Ethernet es la referencia en el campo de las redes de comunicación por cable. La implementación de dúplex completo conmutado descrita, por ejemplo, en la norma abierta IEEE 802.3, se usa frecuentemente en la industria, y los componentes de *hardware* y *software* necesarios están disponibles de manera extensa y sencilla. Sin embargo, este anuncio no puede proporcionar la fiabilidad y el determinismo que se requieren en las aplicaciones de aviónica.

25 Se han desarrollado buses y protocolos de datos específicos para aeronaves. No obstante, estas soluciones hechas a medida no proporcionan siempre el alto ancho de banda requerido en las aeronaves modernas pilotadas por cable (*fly-by-wire*), y, cuando lo hacen, el aumento del rendimiento viene acompañado de unos incrementos sustanciales de los costes.

Algunos proveedores, por ejemplo, Airbus con su tecnología AFDX®, proponen una red basada en Ethernet que puede proporcionar la fiabilidad requerida, compartiendo el ancho de banda disponible entre “enlaces virtuales” de una manera determinista. Esta tecnología se describe, entre otras, en las publicaciones EP1309131 y US6925088.

35 Los documentos US2010195634 y US6760782 divulgan también redes de Ethernet ideadas especialmente para aplicaciones de aviónica o alta fiabilidad. El documento US7065095 describe una red en anillo basada en Ethernet, y el documento US2008212504 divulga una interfaz de red inalámbrica con Calidad de Servicio.

40 El objetivo de la presente invención es proporcionar una interfaz de comunicación determinista entre subsistemas en una aeronave que tiene mecanismos para garantizar el determinismo de la comunicación por lo que respecta a latencia, fluctuaciones y ancho de banda, así como la integridad de datos, y usa protocolos y *hardware* compatibles con Ethernet.

45 **Breve resumen de la invención**

Según la invención, estos objetivos se alcanzan por medio del objeto de las reivindicaciones adjuntas. En particular, la invención propone con este fin, una interfaz de red determinista, configurada para su conexión con un sistema anfitrión y dos medios físicos de Ethernet, de tal manera que la interfaz sea conectable con dos interfaces de red vecinas, comprendiendo la interfaz una capa de Control de Acceso a los Medios, dispuesta operativamente para recibir y transmitir datos desde y hacia dichas dos interfaces de red vecinas, y para recibir y transmitir datos desde y hacia el sistema anfitrión, comprendiendo la interfaz de red determinista una zona de configuración programable y está dispuesta funcionalmente para insertar y/o reconocer direcciones IP y/o MAC en los paquetes de Ethernet sobre la base de una tabla de direcciones almacenada en la zona de configuración, siendo las direcciones IP y/o MAC de los nodos estáticamente determinadas, almacenando las zonas de configuración de las interfaces de red una tabla de las direcciones IP y MAC de otros nodos en la red, y siendo el tránsito de datos a través de la interfaz de red determinista en el tiempo.

60 La invención propone, asimismo, una interfaz de red determinista según lo anterior, dispuesta funcionalmente para transferir mensajes recibidos de un nodo vecino al sistema anfitrión o retransmitirlos hacia el otro nodo vecino sobre la base de una decisión determinista; la invención propone también, opcionalmente, que las interfaces de red configuradas y estructuradas según lo anterior, estén dispuestas para transferir mensajes recibidos de un nodo vecino al sistema anfitrión o retransmitirlos al otro nodo vecino sobre la base de una decisión determinista; que la capa de Control de Acceso a los Medios y/o una capa IP puedan estar dispuestas funcionalmente para detectar errores en los datos recibidos, activar una bandera de error (del inglés, “flag”) para el sistema anfitrión, y/o almacenar los datos erróneos en unos medios de memoria para su tratamiento posterior; que la interfaz pueda

incluir una capa de UDP; y que la interfaz esté dispuesta funcionalmente para no transmitir un mensaje si se determina que el mismo ha sido retransmitido entre nodos vecinos más de un número determinado de saltos (del inglés, "hops").

5 La invención se refiere, asimismo, a una red determinista, o protocolo de red, en una aeronave, que comprende una pluralidad de nodos dispuestos en una topología de anillo, comprendiendo, cada nodo una interfaz de red según se ha especificado anteriormente, estando cada interfaz de red de cada nodo conectada con las interfaces de red de los dos nodos adyacentes en el anillo; la cual puede presentar un modo de comunicación, en el cual los nodos se comunican entre ellos exclusivamente mediante unos paquetes de UDP.

10

### Breve descripción de los dibujos

La invención se comprenderá mejor con la ayuda de la descripción de una forma de realización proporcionada a título de ejemplo e ilustrada con las figuras, en las que:

15

la figura 1 muestra una representación esquemática de una forma de realización de la presente invención.

La figura 2 muestra una pluralidad de interfaces de red de acuerdo con la presente invención dispuestas en una topología de anillo.

20

La figura 3 ilustra un mecanismo de integridad de extremo-a-extremo de acuerdo con un aspecto de la presente invención.

### Descripción detallada de posibles formas de realización de la invención

25

La figura 1 representa una interfaz de red de acuerdo con un aspecto de la presente invención. El sistema anfitrión 50 incluye una unidad de procesador programada para ejecutar uno o más programas de *software*, representados simbólicamente en el bloque 70, en una memoria 60 que puede ser, por ejemplo, un bloque de una memoria RAM dinámica.

30

En el marco de la invención, el sistema anfitrión 50 podría ser cualquier otro dispositivo conectado en red. En una aeronave, el sistema anfitrión podría incluir un sistema de gestión de vuelo, una unidad o subunidad de visualización de vuelo, un ordenador de datos aéreos, una unidad de navegación, un giróscopo, un accionador de superficies de vuelo, un aparato de radiocomunicaciones, una unidad de radar, aunque esta lista está lejos de ser exhaustiva.

35

El sistema anfitrión 50 está conectado a otros nodos de subsistemas o de red en la aeronave por medio de una interfaz de red de seguridad crítica que se representa con las capas 40, 30, 20, 10 de la figura 1. Los datos fluyen cruzando las capas de una manera determinista desde el procesador anfitrión 50 a los transceptores de PHY 10, y hacia las interfaces de red adyacentes a través de los medios físicos 120, 220, que podrían ser fibras o cables de cobre de Ethernet de gigabits, y en sentido opuesto.

40

La capa 40 es una capa de transporte de UDP que despacha datos entre el anfitrión 50 y otros anfitriones de la red. Tal como estipula el protocolo UDP, la capa 40 proporciona redundancia para la integridad de datos y gestiona datos en mensajes, a los que habitualmente se hace referencia como datagramas. La capa 40 no presenta ninguna estipulación en cuanto a la señalización de entrada en contacto o la comprobación de errores, y no hace ningún intento de garantizar la entrega de los mensajes, o de conservar su orden. Estas funciones se logran con el *software* con el soporte de las capas de comunicación inferiores, tal como se explicará en lo sucesivo.

45

La interfaz de memoria está compuesta por una memoria tampón FIFO dual 41, 47 para los datos de transmisión, respectivamente los datos de recepción. Se transfiere datos hacia y desde la memoria de procesador 60 por medio de una interfaz de DMA 43, bajo instrucciones del *software*, aunque sin procesado por parte de la CPU del anfitrión. Opcionalmente, la interfaz de DMA está sincronizada con una partición temporal y espacial en un sistema operativo de tiempo real (RTOS) para garantizar que las transacciones son atómicas dentro de la partición. Solamente una partición 75 del sistema operativo está vinculada con la DMA.

50

La capa de UDP implementa, en particular, el encapsulamiento de los mensajes recibidos del sistema anfitrión, en datagramas UDP válidos, y la extracción del mensaje a partir de los datagramas recibidos de las capas jerárquicamente inferiores. Y lo que es más importante, estas operaciones se ejecutan de forma autónoma en la interfaz de red y son deterministas en el tiempo, en el sentido de que el paso a través de la capa de UDP, en cualquiera de las dos direcciones, no introduce ningún retardo imprevisible. La capa de UDP puede usar información almacenada en la zona de parámetros 80, por ejemplo, en la codificación y decodificación de los puertos de UDP, de una manera que se explicará de forma detallada posteriormente.

60

La sección de RX 47 de la unidad de UDP 40 puede detectar errores en el datagrama, por ejemplo, verificando la suma de comprobación de UDP, si estuviera presente, y, en este caso, activar una señal para el sistema anfitrión.

65

La interfaz de red de la invención puede gestionar el encapsulamiento de datagramas UDP en paquetes IP. La capa 30 es una capa IP, jerárquicamente por debajo de la capa de UDP 40. Puede proporcionar, por ejemplo, traducción de direcciones, encaminamiento, división y reensamblaje de mensajes, y la función asociada convencionalmente a capas de red. Igual que la capa de UDP 40, tiene un par de memorias tampón FIFO 31, 37 para los datos transmitidos, respectivamente recibidos. En particular, la capa IP implementa el encapsulamiento de datagramas UDP en tramas IP válidas, y la extracción de datagramas UPD a partir de los paquetes IP en la dirección opuesta. En cuanto a la capa de UDP, por lo menos el tránsito de datagramas UPD a través de la capa IP 30 es autónomo y determinista. La capa IP puede hacer uso de información almacenada en la zona de parámetros 80, por ejemplo, direcciones IP.

La memoria tampón de recepción 37 puede detectar errores en los paquetes recibidos y puede notificarlos al procesador anfitrión 50. En caso de error puede enviarse una bandera al procesador anfitrión, y los paquetes erróneos se copian en una memoria tampón de compartimentos (*bin buffer*), accesible por parte del procesador anfitrión 50 para un análisis posterior.

El bloque 20 representa una capa de Control de Acceso a los Medios (MAC) que es responsable de gestionar el acceso a los medios físicos 120, 220, usando la capa física 10 como interfaz. Tiene también la capacidad de detectar y posiblemente corregir errores en datos recibidos, y de notificarlos al procesador anfitrión 50. La señalización de errores puede usar el mismo mecanismo de bandera y memoria tampón de compartimentos que en el bloque 30.

La capa MAC 20 es responsable de la codificación de tramas MAC válidas, encapsulando los paquetes UDP/IP de las capas superiores, que, a su vez, contienen el mensaje original, y de la descodificación en la dirección opuesta. Estas etapas de procesado se llevan a cabo de forma autónoma y de una manera determinista en el tiempo, tal como anteriormente. Con este fin, la capa MAC usa información almacenada en la zona de configuración 80, por ejemplo, las direcciones MAC.

Y lo que es más importante, las interfaces de red 100 de la invención están conectadas a dos nodos adyacentes que tienen características similares, indicados con MAC#0 y MAC#2 en la figura 1. El lado TX de la capa MAC 20 recibe datos o bien de la capa IP 30 de encima, o bien de un nodo adyacente MAC#0 a través del medio 120, y los reenvía hacia la capa física 10. A la inversa, el lado de RX de la capa MAC 20 recibe datos de la capa física 10 y los reenvía o bien a la capa IP superior 30 o bien al siguiente nodo MAC#2. La figura 2 muestra una red de topología en anillo compuesta por nodos individuales 100 cada uno de los cuales puede presentar la estructura ilustrada en la figura 1, en una aeronave. No obstante, son posibles otras topologías.

En la capa MAC, se toma una decisión sobre si encaminar los datos al siguiente nodo (MAC#2, 101) o a las capas superiores, basándose, por ejemplo, en la comparación de direcciones o cualquier otro criterio adecuado. Se añade un módulo lógico para garantizar que los paquetes tienen un tiempo de vida finito y no inundan la red circulando de forma indefinida. En una posible implementación, un contador de HOP se decrementa en cada pasada comenzando desde un valor inicial, y el paquete no se retransmite cuando el contador llega a cero.

La memoria tampón de TX 21 acepta datos de la capa IP 30 ó del MAC#0 emparejado (99). Un algoritmo de arbitraje determinista regula el tráfico entre estas dos fuentes. Y lo que es más importante, este arbitraje, en combinación con la topología en anillo, evita en su totalidad colisiones de paquetes, garantizando un comportamiento determinista de la red.

Y lo que es más importante, cada una de las interfaces de red de la invención se puede conectar con dos interfaces de red vecinas de tal manera que forman una red compuesta totalmente por conexiones de punto-a-punto. Entre cada par de nodos vecinos se usa una Ethernet dúplex completo; y la red queda en su totalidad libre de colisiones.

Puesto que la comunicación en la red realizada mediante las interfaces de red se basa totalmente en paquetes no conectados, por ejemplo, paquetes UDP, no se ven implicados acuses de recibo o señalización alguna, con lo cual se evita un posible motivo de contienda de recursos que podría introducir retardos imprevisibles en la propagación de los paquetes.

Por otra parte, las interfaces de red incluyen una unidad de resolución de direcciones que evita cualquier retardo no determinista en la entrega de los paquetes, tal como se describirá en lo sucesivo.

Cada interfaz de red incluye una zona de configuración 80 programable que almacena, entre otros, una tabla de direcciones que registra las direcciones de nivel 2 (MAC) y nivel 3 (IP) de todos los nodos de la red con los que necesita comunicarse la interfaz. Y lo que es más importante, la asignación de direcciones MAC e IP en la red es estática, y el sistema no se basa en los protocolos convencionales de configuración y resolución de direcciones como ARP, DNS, DHCP y similares.

La tabla de direcciones en la zona de configuración 80 programable puede estar preprogramada, puede estar fijada por la CPU del sistema anfitrión, se puede rellenar dinámicamente o se puede proporcionar de cualquier otra manera.

5 Y lo que es más importante, no es necesario que el sistema anfitrión conozca la dirección IP o MAC de un dispositivo con el cual se comunica para identificarlo. Los dispositivos en la red se pueden identificar mediante un índice localizándolos en una tabla de configuración de direcciones almacenada en la zona de configuración 80 de la interfaz de red. La zona de configuración 80 también puede contener información de direccionamiento suplementaria, por ejemplo, los números de puerto UDP de servicio remotos o locales dados en la red. No obstante, el sistema anfitrión puede tener la capacidad de realizar lecturas y/o escrituras en la tabla de configuración de direcciones 80.

10 Cuando se envía un mensaje a otro nodo en la red, la interfaz de red recibe del sistema anfitrión el mensaje que se debe enviar, y un identificador de alto nivel del destinatario designado. La interfaz de red selecciona direcciones IP y MAC de la tabla de configuración de direcciones 80 basándose en el identificador recibido. Este último puede ser un índice, un puntero o cualquier información que permita seleccionar una entrada en la tabla de configuración de direcciones. La interfaz de red está dispuesta funcionalmente para construir un paquete de Ethernet encapsulando el mensaje deseado, sin la asistencia del sistema anfitrión. La resolución de direcciones se puede implementar mediante una FPGA programada adecuadamente, en un ASIC, mediante una CPU programada, o mediante cualquier otra unidad lógica adecuada. De la misma manera, en la trama de Ethernet también se pueden incluir números de puerto UDP apropiados.

20 A la inversa, cuando se recibe un paquete de Ethernet de otro nodo, la interfaz de red de la invención encuentra la entrada en la tabla de configuración 80 que se corresponde con las direcciones MAC e IP del mensaje, y proporciona al sistema anfitrión la carga útil de la trama, es decir el mensaje que se envió originalmente; y una información que identifica el emisor en la tabla de configuración 80, por ejemplo, un índice. Como para el caso de la transmisión, la interfaz de red de la invención es capaz de llevar a cabo estas operaciones de forma autónoma de una manera determinista en el tiempo, sin asistencia del sistema anfitrión.

30 En la descripción de esta invención, las capas de la pila de la interfaz se han representado y descrito como entidades independientes, por motivos de simplificación. No obstante, esto no es una característica esencial de la invención que podría incluir, también, una variante en la que algunas de las capas anteriores se combinan entre sí, comparten algún elemento de *hardware*, o se materializan en su totalidad o parcialmente en *software*.

35 La figura 3 ilustra otro aspecto importante de la invención: una integridad de extremo-a-extremo. En esta forma de realización, la interfaz de red de la invención se comunica con el sistema anfitrión, representado por una CPU 55 y una memoria 60, a través de una interfaz de anfitrión 145, una interfaz puente 150 y un enlace de alta velocidad 170. Entre la interfaz de red y el enlace de alta velocidad se interpone una memoria tampón 160. En este tipo de estructuras, que están ampliamente extendidas en los sistemas modernos de aviónica, los datos deben viajar cruzando diversos buses y medios de almacenamiento temporal, pudiendo los mismos verse alterados por el ruido, las interferencias o la radiación de gran altitud. Por lo tanto, existe una necesidad de un mecanismo de control de la integridad.

40 Los protocolos de Ethernet, y otros protocolos de la misma familia, protegen los datos en el medio físico por medio de un código de detección de errores, indicado habitualmente como FCS, o Secuencia de Comprobación de Trama. La figura 3 muestra una trama de Ethernet ilustrativa que está compuesta por un encabezamiento, el cual contiene direcciones físicas de destino y de origen, un mensaje o carga útil 14 y una FCS 18 que es un código de CRC obtenido a partir de la secuencia de encabezamiento+mensaje y añadido en forma de una cola. Cuando la trama es recibida por el nodo deseado, el CRC se vuelve a calcular y se verifica con respecto a la FSC recibida con el fin de detectar alteraciones o errores en el mensaje.

50 De acuerdo con un aspecto de la invención, cuando el mensaje 14 que se va a transmitir se compone en la memoria 60 del anfitrión, se calcula un código de detección de errores 15 y el mismo se asocia al mensaje. El código de detección de errores puede ser, por ejemplo, un CRC, o el resultado de cualquier función adecuada de corrección de errores. A continuación, el mensaje se envía hacia la interfaz de red a través de la totalidad de los diversos enlaces y memorias tampón, y baja por la pila de protocolos hacia la capa MAC 20. Cuando el mensaje es recibido en la interfaz de red, se verifica el código de detección de errores 15 y el mismo se extrae del mensaje. En la figura, la verificación se dibuja en el nivel MAC, aunque también podría ocurrir en una de las capas superiores.

60 Si la verificación del código de CRC 15 falla, el mensaje 14 ha sido modificado en el recorrido desde el sistema anfitrión a la interfaz de red, y la interfaz de red se puede programar para llevar a cabo acciones correctoras o paliativas. Se puede generar un código de error 25 para permitir que el emisor corrija la situación. El mensaje se puede conservar, o se puede enviar de cualquier manera al destinatario deseado, pero se combina con una secuencia de FSC no válida, de tal manera que el destinatario detecte el error y reaccione como si el error hubiese aparecido en la capa de Ethernet física. Ventajosamente, esta manera de lidiar con errores no requiere la gestión de condiciones de error nuevas en *software*.

65 En la otra dirección, cuando la unidad de MAC 20 recibe una trama de red, la misma verifica la FSC, la extrae del mensaje, y calcula un CRC 15 que se corresponde con el mensaje recibido. El CRC 15 se transmite con el mensaje

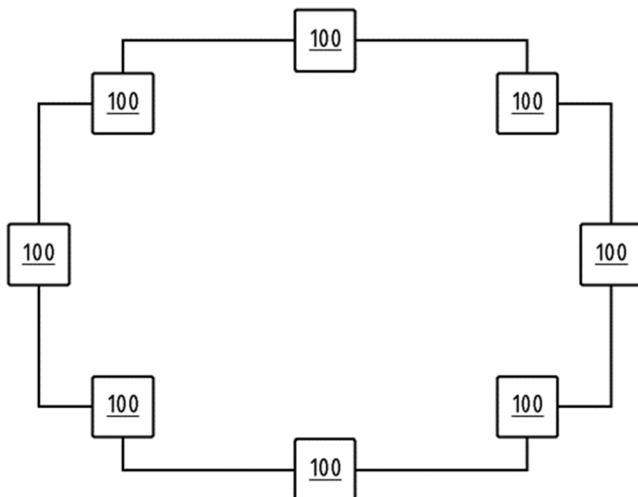
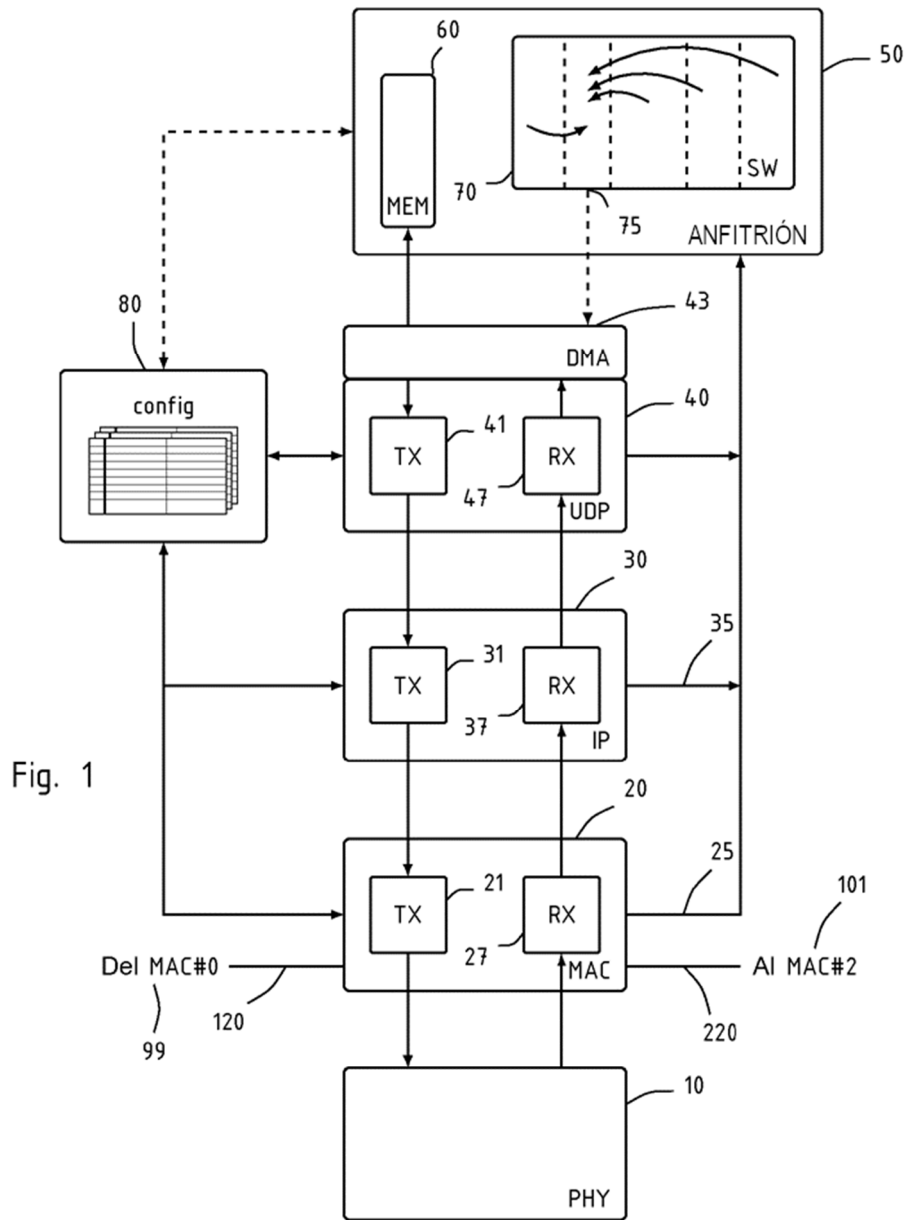
14 al sistema anfitrión donde, una vez es recibido, se verifica de nuevo. A continuación, el anfitrión puede tener la confirmación de que el mensaje no ha sido alterado o, en caso contrario, pueda adoptar medidas adecuadas.

**Números de referencia**

5	10 capa PHY
	13 encabezamiento MAC
	14 mensaje
	15 código de corrección de errores
10	18 secuencia de comprobación de trama
	20 capa MAC
	21 memoria tampón de TX MAC
	25 señalización de errores
	27 memoria tampón de RX MAC
15	30 capa IP
	31 memoria tampón de TX IP
	35 señalización de errores
	37 memoria tampón de RX IP
	40 capa de UDP
20	41 capa de TX UDP
	43 interfaz de DMA
	47 memoria tampón de RX UDP
	50 sistema anfitrión
	55 unidad de procesado
25	60 memoria
	70 <i>software</i>
	75 partición
	80 tablas de configuración
	99 nodo previo
30	100 nodo de red
	101 siguiente nodo
	120 medios físicos
	145 interfaz de anfitrión
	150 interfaz puente
35	160 memoria tampón de mensajes
	170 enlace de alta velocidad
	220 medios físicos

**REIVINDICACIONES**

- 5 1. Interfaz de red determinista (100), configurada para su conexión con un sistema anfitrión (50) y dos medios físicos de Ethernet (120, 220), de tal manera que la interfaz sea conectable con dos interfaces de red vecinas (99, 101), comprendiendo la interfaz una capa de Control de Acceso a los Medios (10), dispuesta funcionalmente para recibir y transmitir datos desde y hacia dichas dos interfaces de red vecinas, y para recibir y transmitir datos desde y hacia el sistema anfitrión, comprendiendo la interfaz de red determinista una zona de configuración programable (80) y estando dispuesta funcionalmente para insertar y/o reconocer direcciones IP y/o MAC en los paquetes de Ethernet sobre la base de una tabla de direcciones almacenada en la zona de configuración (80), siendo las direcciones IP y/o MAC de los nodos estáticamente determinadas, almacenando las zonas de configuración de las interfaces de red una tabla de las direcciones IP y/o MAC de otros nodos en la red, y siendo el tránsito de datos a través de la interfaz de red determinista en el tiempo.
- 15 2. Interfaz de red determinista según cualquiera de las reivindicaciones anteriores, dispuesta funcionalmente para transferir mensajes recibidos de un nodo vecino (99) al sistema anfitrión (50) o retransmitirlos al otro nodo vecino (101) sobre la base de una decisión determinista.
- 20 3. Interfaz de red determinista según la reivindicación anterior, en la que la capa de Control de Acceso a los Medios (10) está dispuesta funcionalmente para detectar errores en los datos recibidos, activar una bandera de error para el sistema anfitrión (50), y/o almacenar los datos erróneos en unos medios de memoria para su tratamiento posterior en el sistema anfitrión (50).
- 25 4. Interfaz de red determinista según cualquiera de las reivindicaciones anteriores, que comprende asimismo una capa IP (20) entre la capa de Control de Acceso a los Medios y el sistema anfitrión (50), dispuesta funcionalmente para detectar errores en los datos recibidos de dicha Capa de Control de Acceso a los Medios (10), activar una bandera de error para el sistema anfitrión (50), y/o almacenar los datos erróneos en unos medios de memoria para su tratamiento posterior en el sistema anfitrión (50).
- 30 5. Interfaz de red determinista según cualquiera de las reivindicaciones anteriores, que comprende asimismo una capa de UDP (40) con una interfaz de DMA dispuesta funcionalmente para transferir de forma autónoma datos entre una memoria (60) del sistema anfitrión (50) y un par de memorias tampón FIFO (41, 47).
- 35 6. Interfaz de red determinista según la reivindicación anterior, dispuesta funcionalmente para no transmitir un mensaje si se determina que el mismo ha sido retransmitido entre nodos vecinos más de un número determinado de saltos.
- 40 7. Red determinista, en una aeronave, que comprende una pluralidad de nodos dispuestos en una topología de anillo, comprendiendo cada nodo una interfaz de red según una de las reivindicaciones anteriores, estando cada interfaz de red de cada nodo conectada con las interfaces de red de los dos nodos adyacentes en el anillo.
- 45 8. Red determinista según las reivindicaciones anteriores, que tiene un modo de comunicación, en el que los nodos se comunican entre ellos exclusivamente mediante unos paquetes UDP.
9. Red determinista según la reivindicación anterior, en la que cada interfaz está dispuesta funcionalmente para transferir unos mensajes recibidos de un nodo vecino (99) al sistema anfitrión (50) o retransmitirlos al otro nodo vecino (101) sobre la base de una decisión determinista.





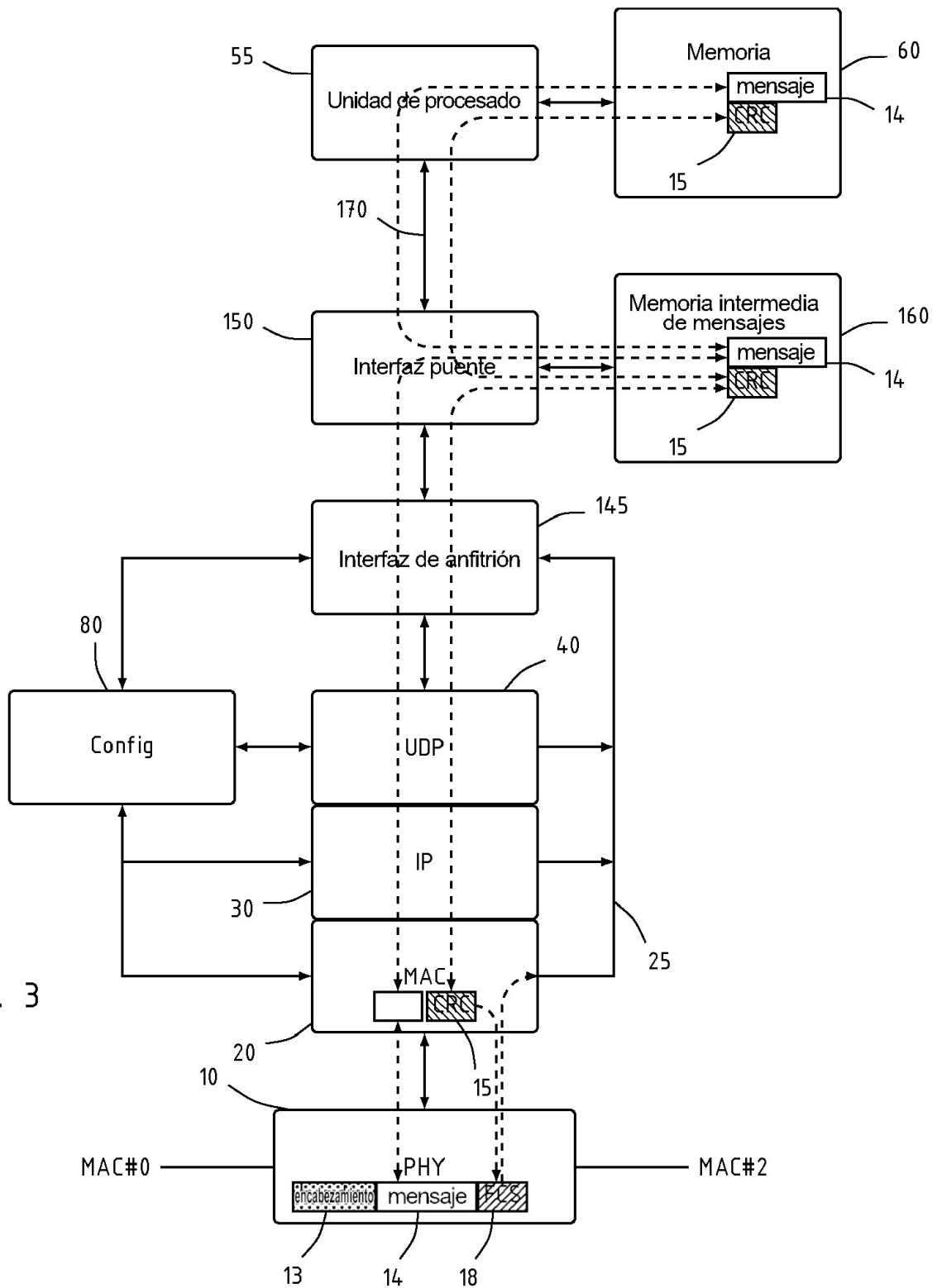


Fig. 3