(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 727 674**

(51) Int. CI.:

H04L 1/00 (2006.01)
H04L 12/70 (2013.01)
H03M 13/09 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.10.2012 PCT/KR2012/008654**

(87) Fecha y número de publicación internacional: **06.09.2013 WO13129752**

(96) Fecha de presentación y número de la solicitud europea: **22.10.2012 E 12869882 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 2822204**

(54) Título: **Dispositivo de comunicación y método de comunicación**

(30) Prioridad:

02.03.2012 US 201261605768 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.10.2019

(73) Titular/es:

LSIS CO., LTD. (100.0%)
1026-6, Hogye-Dong, Dongan-Gu, Anyang
Gyeonggi-Do 431-080, KR

(72) Inventor/es:

LEE, SUNG HAN;
KWON, DAE HYUN y
OH, JOON SEOK

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Dispositivo de comunicación y método de comunicación

Campo técnico

La presente descripción se refiere a un dispositivo de comunicaciones y un método de comunicación, y más particularmente, a un dispositivo de comunicaciones seguras y un método de comunicación segura.

Antecedentes de la técnica

Actualmente se buscan soluciones para la comunicación segura en campos industriales. En particular, los sistemas de control industrial deben mantener un nivel de integridad de la información prescrita o superior transferida a través de una red con el fin de garantizar la seguridad de los trabajadores, evitar las amenazas al medioambiente y evitar la ocurrencia de problemas relacionados con la seguridad.

Para satisfacer tales requisitos de integridad, se requieren sistemas de control industrial para tratar problemas sobre la corrupción, la repetición no intencional, la secuencia incorrecta, la pérdida, el retraso inaceptable, la inserción, el enmascaramiento y el direccionamiento.

Con respecto al problema de la corrupción, los sistemas de control industriales deben ser capaces de determinar si se produce un error en los datos que se transfieren, con un nivel establecido o mayor de probabilidad.
Con respecto al problema de la repetición no intencional, los sistemas de control industriales deberían ser capaces de determinar si la repetición de datos que no es intencional por parte de una persona se produce normalmente, con un nivel establecido o mayor de probabilidad.

Con respecto al problema de la secuencia incorrecta, los sistemas de control industriales deben ser capaces de determinar si se cambia una secuencia de transmisión de datos, con un nivel de probabilidad establecido o mayor.

Con respecto al problema de la pérdida, los sistemas de control industriales deben ser capaces de determinar si una parte de los datos transmitidos se daña, con un nivel de probabilidad establecido o mayor.

Con respecto al problema de retraso inaceptable, los sistemas de control industrial deberían ser capaces de determinar si se produce un retraso inaceptable en la transmisión de datos, con un nivel establecido o mayor de probabilidad.

Con respecto al problema de la inserción, los sistemas de control industriales deberían ser capaces de determinar si los datos no deseados se insertan mientras se transmiten datos, con un nivel de probabilidad establecido o mayor.

Con respecto al problema del enmascaramiento, los sistemas de control industrial deberían ser capaces de determinar si los datos se cambian de forma maliciosa por una persona, con un nivel establecido o mayor de probabilidad.

Con respecto al problema del direccionamiento, los sistemas de control industriales deberían ser capaces de determinar si los datos se transmiten al receptor correcto, con un nivel de probabilidad establecido o mayor.
IEC 61508 representa una probabilidad de error al usar SIL como se muestra en la Tabla 1 a continuación.

[Tabla 1]

SIL4	>= 10^{-9}, < 10^{-8}
SIL3	>= 10^{-8}, < 10^{-7}
SIL2	>= 10^{-7}, < 10^{-6}
SIL1	>= 10^{-6}, < 10^{-5}

Por ejemplo, para satisfacer SIL3, la probabilidad de error debe satisfacer 10^{-9}.

Sin embargo, es difícil para las estructuras de Ethernet actuales cumplir con los requisitos de integridad de los sistemas de control industrial.

El documento WO 99/49695 A1 describe un método y un aparato para transferir información de identificación en un sistema de telecomunicaciones.

El documento US 2009/327826 A1 describe un sistema que transmite y recibe paquetes.

Divulgación del problema técnico de la invención

Las modalidades proporcionan un dispositivo de comunicaciones y un método de comunicación que cumple con los requisitos de integridad de los sistemas de control industrial.

Solución técnica

Un objetivo de la presente invención es un método de comunicación para transmitir datos, como se define en la reivindicación independiente 1.

Otro objetivo de la presente invención es un método de comunicación para recibir datos, como se define en la reivindicación independiente 6.

Efectos ventajosos

De conformidad con las modalidades de la presente descripción, pueden cumplirse los requerimientos de integridad de los sistemas de control industriales.

Además, de conformidad con las modalidades de la presente descripción, un identificador único de seguridad para establecer una conexión entre dispositivos de comunicación se genera para satisfacer los requerimientos de integridad de los sistemas de control industrial.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra un dispositivo de comunicaciones seguras de acuerdo con una modalidad.
La Figura 2 es un diagrama de escalera que ilustra un método de comunicación de conformidad con una modalidad.
La Figura 3 es un diagrama que ilustra un identificador único de acuerdo con una modalidad.
La Figura 4 es un diagrama que ilustra un proceso para generar un identificador único de seguridad de acuerdo con una modalidad.
La Figura 5 ilustra una estructura de una unidad de datos del protocolo de seguridad de acuerdo con una modalidad.
La Figura 6 ilustra una estructura de una trama Ethernet de conformidad con una modalidad.

Modo de llevar a cabo la invención

En lo sucesivo, un dispositivo de comunicaciones y un método de comunicación de conformidad con modalidades se describirán en detalle con referencia a los dibujos adjuntos. En la siguiente descripción, los términos "módulo" y "unidad" para referirse a elementos, se asignan a estos y se usan indistintamente por conveniencia, y por lo tanto, los términos por sí no necesariamente representan diferentes significados o funciones.

La Figura 1 es un diagrama de bloques que ilustra un dispositivo de comunicaciones seguras de acuerdo con una modalidad.

Como se ilustra en la Figura 1, un dispositivo de comunicaciones seguras 100 de conformidad con una modalidad incluye una unidad generadora de identificadores únicos de seguridad 101, una unidad de cálculo del código de detección de errores 103, una unidad generadora de la unidad de datos del protocolo (PDU) 105, una unidad generadora de la trama Ethernet 107, una unidad de transmisión de datos 109, una unidad de recepción de datos 111, una unidad de análisis de la trama Ethernet 113, una unidad de análisis de la unidad de datos del protocolo 115, una unidad de detección de errores 117, y una unidad de control 121.

La unidad generadora de identificadores únicos de seguridad 101 puede generar un identificador único de seguridad (SUID) al combinar un identificador único del dispositivo de comunicaciones seguras 100 y el identificador único de otro dispositivo de comunicaciones seguras 100.

La unidad de control 121 puede generar datos de seguridad, y puede proporcionar los datos de seguridad generados a la unidad de cálculo del código de detección de errores 103.

La unidad de cálculo del código de detección de errores 103 puede calcular un código de detección de errores de datos para el identificador único de seguridad y los datos de seguridad usando el identificador único de seguridad generado y los datos de seguridad.

La unidad generadora de la unidad de datos del protocolo 105 puede generar una unidad de datos del protocolo (PDU) que incluye el código de detección de errores de datos calculado, los datos de seguridad y un encabezado de PDU de seguridad.

La unidad generadora de la trama Ethernet 107 puede generar una trama Ethernet que incluye la unidad de datos del protocolo de seguridad generada.

La unidad de transmisión de datos 109 puede transmitir la trama Ethernet generada a otro dispositivo de comunicaciones seguras.

La unidad de recepción de datos 111 puede recibir la trama Ethernet que incluye la unidad de datos del protocolo de seguridad de otro dispositivo de comunicaciones seguras.

La unidad de análisis de la trama Ethernet 113 puede analizar la trama Ethernet recibida para obtener la unidad de datos del protocolo de seguridad.

La unidad de análisis de la unidad de datos del protocolo 115 puede analizar la unidad de datos del protocolo para obtener el código de detección de errores y los datos de seguridad.

La unidad de detección de errores 117 puede calcular un código de detección de errores de datos comparativo usando los datos de seguridad.

La unidad de detección de errores 117 puede comparar el código de detección de errores calculado con el código de detección de errores obtenido para detectar un error.

La unidad de control 121 puede controlar el funcionamiento general del dispositivo de comunicaciones seguras 100.

Cuando se determina que se ha producido un error en los datos de seguridad, la unidad de control 121 puede cambiar un estado de funcionamiento del dispositivo de comunicaciones seguras 100 en un estado seguro contra fallos contra fallos. En el estado seguro contra fallos, el dispositivo de comunicaciones seguras 100 suspende la comunicación segura hasta que se reciba la entrada del usuario para reiniciar. En particular, en el estado seguro contra fallos, el dispositivo de comunicaciones seguras 100 puede o no suspender las comunicaciones que no seas las comunicaciones relacionadas con los datos de seguridad, sino que suspende al menos la comunicación relacionada con los datos de seguridad.

Cuando se confirma que el identificador único de seguridad obtenido existe dentro del dispositivo de comunicaciones seguras 100, la unidad de control 121 puede consumir los datos de seguridad recibidos, y puede generar los datos de seguridad que se transmiten a continuación. Si los datos de seguridad recibidos se relacionan con una solicitud, la unidad de control 121 genera los datos de seguridad relacionados con una respuesta. Si los datos de seguridad recibidos se relacionan con una respuesta, la unidad de control 121 genera los datos de seguridad relacionados con una solicitud siguiente.

La Figura 2 es un diagrama de escalera que ilustra un método de comunicación de conformidad con una modalidad.

Como se ilustra en la Figura 2, se asume que un primer dispositivo de comunicaciones seguras 100A se comunica con un segundo dispositivo de comunicaciones 100B, el primer dispositivo de comunicaciones seguras 100A transmite una solicitud de unidad de datos del protocolo de seguridad al segundo dispositivo de comunicaciones seguras 100B, y el segundo dispositivo de comunicaciones seguras 100B transmite una respuesta de la unidad de datos del protocolo de seguridad al primer dispositivo de comunicaciones seguras 100A.

El método de comunicación de conformidad con una modalidad se refiere a la autenticación mutua (o interconexión) realizada antes de la transmisión/recepción de datos reales entre el primer dispositivo de comunicaciones seguras 100A y el segundo dispositivo de comunicaciones seguras 100B.

La unidad generadora de identificadores únicos de seguridad 101 del dispositivo de comunicaciones seguras 100 genera el SUID combinando el identificador único del primer dispositivo de comunicaciones seguras 100A y el identificador único del segundo dispositivo de comunicaciones seguras 100B (operación S101). Es decir, la unidad generadora de identificadores únicos de seguridad 101 del primer dispositivo de comunicaciones seguras 100A puede comprender el identificador único del segundo dispositivo de comunicaciones seguras 100B para conectarse al primer dispositivo de comunicaciones seguras 100A, y puede generar el SUID mediante el uso del identificador único del segundo dispositivo de comunicaciones seguras 100B.

Igualmente, la unidad generadora de identificadores únicos de seguridad 101 del segundo dispositivo de comunicaciones seguras 100B puede comprender el identificador único del primer dispositivo de comunicaciones seguras 100A que se conecta al segundo dispositivo de comunicaciones seguras 100B, y puede generar el SUID mediante el uso del identificador único del primer dispositivo de comunicaciones seguras 100A.

En una modalidad, la unidad generadora de identificadores únicos de seguridad 101 del primer dispositivo de comunicaciones seguras 100A puede conocer el identificador único de otro dispositivo de comunicaciones seguras diferente del segundo dispositivo de comunicaciones seguras 100B, y puede generar y contener un SUID adicional combinando el identificador único del primer dispositivo de comunicaciones seguras 100A y el identificador único del otro dispositivo de comunicaciones seguras.

Un proceso para generar el SUID de conformidad con una modalidad se describirá con referencia a las Figuras 3 y 4.

La Figura 3 es un diagrama que ilustra el identificador único de acuerdo con una modalidad, y la Figura 4 es un diagrama que ilustra el proceso de generación del SUID de conformidad con una modalidad.

Como se ilustra en la Figura 3, el identificador único de conformidad con una modalidad puede generarse mediante la combinación de un valor de usuario y una dirección de control de acceso al medio (MAC).

El valor del usuario puede ser cualquiera de un valor arbitrario predeterminado de conformidad con una configuración del usuario, un valor de un intervalo específico determinado de conformidad con la configuración del usuario, un identificador de un dispositivo de comunicaciones seguras, y una dirección del dispositivo de comunicaciones seguras.

El valor de usuario ilustrado en la Figura 3 puede ser un identificador del dispositivo. Aquí, el identificador del dispositivo puede ser el identificador del dispositivo de comunicaciones seguras.

La dirección MAC puede incluir información para acceder a una Ethernet.

El tamaño del identificador único de acuerdo con una modalidad puede ser 64 bits, pero no se limita a esto.

Los tamaños del identificador del dispositivo y la dirección MAC pueden ser 16 bits y 48 bits respectivamente, pero no se limitan a esto.

Como se ilustra en la Figura 4, la unidad generadora de identificadores únicos de seguridad 101 del primer dispositivo de comunicaciones seguras 100A puede generar el SUID mediante el uso de un identificador del dispositivo fuente, una dirección MAC de la fuente, un identificador del dispositivo de destino, y una dirección MAC de destino.

El SUID puede usarse para confirmar la validez de conexión entre el primer dispositivo de comunicaciones seguras 100A y otro dispositivo de comunicaciones seguras. En el caso en que el primer dispositivo de comunicaciones seguras 100A y el otro dispositivo de comunicaciones seguras tengan los SUID correspondientes entre sí, puede confirmarse la validez de conexión entre el primer dispositivo de comunicaciones seguras 100A y el otro dispositivo de comunicaciones seguras.

En detalle, como se muestra en la Ecuación 1 más abajo, la unidad generadora de identificadores únicos de seguridad 101 del primer dispositivo de comunicaciones seguras 100A puede generar el SUID mediante el uso del identificador del dispositivo fuente, la dirección MAC de la fuente, el identificador del dispositivo de destino, y la dirección MAC de destino.

[Ecuación 1]

SUID = f(dirección MAC de la fuente e ID del dispositivo, dirección MAC de destino e identificación del dispositivo)

En más detalle, la unidad generadora de identificadores únicos de seguridad 101 del primer dispositivo de comunicaciones seguras 100A puede generar un identificador del dispositivo para el SUID mediante la combinación del identificador del dispositivo fuente del identificador único del primer dispositivo de comunicaciones seguras 100A y el identificador del dispositivo de destino del identificador único del segundo dispositivo de comunicaciones seguras 100B y la dirección MAC del identificador único del segundo dispositivo de comunicaciones seguras 100B y la dirección MAC del identificador único del segundo dispositivo de comunicaciones seguras 100B, y puede generar el SUID al combinar el identificador del dispositivo generado y la dirección MAC generada.

El requisito de seguridad entre los dispositivos de comunicaciones seguras puede cumplirse con el identificador del dispositivo para el SUID generado, y el requisito de exclusividad entre los dispositivos de comunicaciones seguras puede cumplirse con la dirección MAC para el SUID generado.

Dado que el primer dispositivo de comunicaciones seguras 100A transmite los datos de seguridad y el segundo dispositivo de comunicaciones seguras 100B recibe los datos de seguridad, el primer dispositivo de comunicaciones seguras 100A es una fuente y el segundo dispositivo de comunicaciones seguras 100B es un destino. En este caso, el SUID puede ser una combinación de la dirección MAC del primer dispositivo de comunicaciones seguras 100A, el identificador del dispositivo del primer dispositivo de comunicaciones seguras 100A, la dirección MAC del segundo dispositivo de comunicaciones seguras 100B, y el identificador del dispositivo del segundo dispositivo de comunicaciones seguras 100B.

El tamaño del SUID generado puede ser 8 octetos, pero no se limita a esto. Un octeto generalmente representa 8 bits.

Los tamaños del identificador del dispositivo y la dirección MAC del SUID generado pueden ser 2 octetos y 6 octetos respectivamente, pero no se limitan a esto.

Con referencia a la Figura 2, la unidad de control 121 del primer dispositivo de comunicaciones seguras 100A genera

los datos de seguridad para una solicitud (operación S103). La unidad de control 121 del primer dispositivo de comunicaciones seguras 100A puede generar datos del encabezado de seguridad relacionados con los datos de seguridad de la solicitud junto con los datos de seguridad solicitados.

Con referencia de nuevo a la Figura 2, la unidad de cálculo del código de detección de errores 103 del primer dispositivo de comunicaciones seguras 100A calcula un código de detección de errores de datos para el SUID y los datos de seguridad mediante el uso del SUID generado y los datos de seguridad (operación S105). Aquí, la unidad de cálculo del código de detección de errores 103 del primer dispositivo de comunicaciones seguras 100A puede calcular un código de detección de errores de encabezado para los datos del encabezado de seguridad mediante el uso de los datos del encabezado de seguridad. El código de detección de errores puede calcularse mediante el uso de una función resumen, en donde la verificación de redundancia cíclica (CRC) puede usarse como la función resumen. El código de detección de errores puede ser un valor CRC.

En particular, como se muestra en la Ecuación 2 a continuación, la unidad de cálculo del código de detección de errores 103 del primer dispositivo de comunicaciones seguras 100A puede calcular el código de detección de errores del encabezado HEADER_CRC usando un campo de encabezado, el SUID y un número de secuencia.

[Ecuación 2]

$$HEADER\_CRC := f(SUID, Sequence\_Number, header\_field)$$

En la Ecuación 1, f denota una función resumen.

El SUID puede usarse solamente para calcular el código de detección de errores, sin incluirse en la PDU de seguridad.

El número de secuencia puede representar un número de secuencias de la PDU de seguridad. El número de secuencia usado para calcular el código de detección de errores puede ser un número de secuencia virtual que no se incluye en la PDU de seguridad. Es decir, el primer dispositivo de comunicaciones seguras 100A usa el número de secuencia virtual para calcular el código de detección de errores, pero no transmite el número de secuencia virtual al segundo dispositivo de comunicaciones seguras 100B.

Como se muestra en la Ecuación 3 más abajo, la unidad de cálculo del código de detección de errores 103 del primer dispositivo de comunicaciones seguras 100A puede calcular el código de detección de errores de DATA_CRC mediante el uso de los datos de seguridad, el SUID y el número de secuencia.

[Ecuación 3]

$$DATA\_\_CRC := f\ (SUID, Sequence\_Number, Safety\_Data)$$

En la Ecuación 3, f denota una función resumen.

La Figura 2 se describirá nuevamente.

La unidad generadora de la unidad de datos del protocolo 105 del primer dispositivo de comunicaciones seguras 100A genera la PDU de seguridad que incluye los datos de seguridad y el código de detección de errores de datos calculado (operación S107). Aquí, la PDU de seguridad puede incluir además los datos del encabezado de seguridad y el código de detección de errores del encabezado calculado. Una estructura de la PDU de seguridad de conformidad con una modalidad se describirá con referencia a la Figura 5.

La Figura 5 ilustra la estructura de la PDU de seguridad de conformidad con una modalidad.

Como se ilustra en la Figura 5, la PDU de seguridad incluye secuencialmente un encabezado de PDU de seguridad y una carga útil de PDU de seguridad. El encabezado de seguridad de PDU incluye secuencialmente un campo de encabezado de seguridad y el código de detección de errores de encabezado. En particular, el encabezado de PDU de seguridad puede disponerse a delante de la PDU de seguridad. El encabezado de seguridad de PDU incluye secuencialmente un campo de comando y un campo reservado. Los datos de seguridad pueden relacionarse con la PDU de seguridad. En particular, los datos de seguridad pueden relacionarse con el campo de comando. Particularmente, en la modalidad de la Figura 5, el campo de encabezado de seguridad tiene un tamaño de 4 octetos, el campo de comando tiene un tamaño de 2 octetos, el campo reservado tiene un tamaño de 2 octetos, el código de detección de errores de encabezado tiene un tamaño de 4 octetos, y el código de detección de errores de datos tiene un tamaño de 4 octetos.; sin embargo, los tamaños de los campos no se limitan necesariamente a estos. Un octeto generalmente representa 8 bits.

La Tabla 2 muestra ejemplos de valores del campo de comando de conformidad con una modalidad.

[Tabla 2]

Comando	Descripción
0x01	Reinicio
0x02	Conexión
0x03	Parámetro
0x04	Datos

Como se muestra en la Tabla 2, si el valor del campo de comando es 0x01, los datos de seguridad pueden representar un comando de reinicio. Si el valor del campo de comando es 0x02, los datos de seguridad pueden representar un comando de conexión. Si el valor del campo de comando es 0x03, los datos de seguridad pueden representar un comando de transmisión de parámetro. Si el valor del campo de comando es 0x04, los datos de seguridad pueden representar un comando de transmisión de datos.

En particular, la modalidad de la Figura 2 puede corresponder a un método de comunicación en un estado de conexión en el que el campo de comando tiene el valor correspondiente al comando de conexión. En el estado de conexión, el primer dispositivo de comunicaciones seguras 100A puede corresponder a un iniciador, y el segundo dispositivo de comunicaciones seguras 100B puede corresponder a un respondedor. El iniciador puede transmitir los datos de seguridad de solicitud al respondedor, sin transmitir los datos de seguridad de la respuesta a los mismos. El respondedor puede transmitir los datos de seguridad de la respuesta correspondientes a los datos de seguridad de la solicitud al iniciador, sin transmitir los datos de seguridad de la solicitud a los mismos.

El campo reservado puede usarse más tarde para otros propósitos. La Figura 2 se describirá nuevamente.

La unidad generadora de la trama Ethernet 107 del primer dispositivo de comunicaciones seguras 100A genera una trama Ethernet que incluye los datos de seguridad solicitados (operación S109). Aquí, la trama Ethernet relacionado con una solicitud puede incluir la PDU de seguridad generada. Una estructura de la trama Ethernet de conformidad con una modalidad se describirá con referencia a la Figura 6.

La Figura 6 ilustra la estructura de la trama Ethernet de conformidad con una modalidad.

Como se ilustra en la Figura 6, la trama Ethernet incluye secuencialmente un encabezado Ethernet, una carga útil de Ethernet, y una secuencia de verificación de la trama (FCS). La trama Ethernet incluye la PDU de seguridad como la carga útil. El encabezado de la trama Ethernet incluye un campo preámbulo, un campo de dirección de destino, un campo de dirección de fuente y un campo de tipo. El campo de dirección de destino contiene una dirección de un dispositivo de comunicaciones seguras que corresponde a un destino, y el campo de dirección de fuente contiene una dirección de un dispositivo de comunicaciones seguras que corresponde a una fuente. La secuencia de verificación de la trama puede generarse usando datos dentro del encabezado Ethernet y datos dentro de la carga útil. La Figura 2 se describirá nuevamente.

La unidad de transmisión de datos 109 del primer dispositivo de comunicaciones seguras 100A transmite la trama Ethernet incluyendo los datos de seguridad de solicitud al segundo dispositivo de comunicaciones seguras 100B (operación S111). De esta manera, la unidad de transmisión de datos 109 puede transmitir la PDU de seguridad generada al segundo dispositivo de comunicaciones seguras 100B.

Aquí, la trama Ethernet transmitido al segundo dispositivo de comunicaciones seguras 100B no incluye el SUID generado.

La unidad de recepción de datos 111 del segundo dispositivo de comunicaciones seguras 100B recibe, desde el primer dispositivo de comunicaciones seguras 100A, la trama Ethernet incluye la PDU de seguridad que incluye los datos de seguridad solicitados (operación S113). Aquí, la trama Ethernet puede tener la estructura como se ilustra en la Figura 6.

La unidad de análisis de la trama Ethernet 113 del segundo dispositivo de comunicaciones seguras 100B analiza la trama Ethernet recibida para obtener la PDU de seguridad (operación S115). Aquí, la PDU de seguridad puede tener la estructura como se ilustra en la Figura 5.

La unidad de análisis de la unidad de datos del protocolo 115 del segundo dispositivo de comunicaciones seguras 100B analiza la unidad de datos del protocolo para obtener los datos del encabezado de seguridad, un código de detección de errores del encabezado recibido, los datos de seguridad de solicitud, y un código de detección de errores de datos recibido (operación S117). La unidad de detección de errores 117 del segundo dispositivo de comunicaciones seguras 100B calcula un código de detección de errores de datos comparativo usando los datos de seguridad de solicitud (operación S119). Adicionalmente, la unidad de detección de errores 180 del segundo dispositivo de comunicaciones seguras 100B puede calcular un código de detección de errores de encabezado comparativo usando

los datos del encabezado de seguridad. Como se describió anteriormente, la unidad de detección de errores 117 del segundo dispositivo de comunicaciones seguras 100B puede calcular el código de detección de errores del encabezado comparativo para detectar un error del campo de datos del encabezado usando los datos del encabezado.

En particular, la unidad de detección de errores 117 del segundo dispositivo de comunicaciones seguras 100B puede calcular el código de detección de errores del encabezado comparativo usando la Ecuación 2.

Además, la unidad de detección de errores 117 del segundo dispositivo de comunicaciones seguras 100B puede calcular el código de detección de errores de datos comparativo usando la Ecuación 3.

La unidad de detección de errores 117 del segundo dispositivo de comunicaciones seguras 100B compara un código de detección de errores calculado con un código de detección de errores obtenido para detectar un error (operación S121). En el caso donde el código de detección de errores de datos comparativo es igual al código de detección de errores de datos recibido y el código de detección de errores de encabezado comparativo es igual al código de detección de errores del encabezado recibido, la unidad de detección de errores 117 puede determinar que no se ha producido un error en los datos de seguridad. Por el contrario, en el caso donde el código de detección de errores de datos comparativo es diferente del código de detección de errores de datos recibido o el código de detección de errores de encabezado comparativo es diferente del código de detección de errores del encabezado recibido, la unidad de detección de errores 117 puede determinar que se ha producido un error en los datos de seguridad.

En detalle, en el caso donde el código de detección de errores de datos comparativo es igual al código de detección de errores de datos recibido y el código de detección de errores de encabezado comparativo es igual al código de detección de errores de encabezado recibido, la unidad de detección de errores 117 puede determinar que el SUID del primer dispositivo de comunicaciones seguras 100A coincida con el del segundo dispositivo de comunicaciones seguras 100B.

Por el contrario, en el caso donde el código de detección de errores comparativo es diferente del código de detección de errores de datos recibido o el código de detección de errores de encabezado comparativo es diferente del código de detección de errores de encabezado recibido, la unidad de detección de errores 117 puede determinar que el SUID del primer dispositivo de comunicaciones seguras 100A no coincide con el del segundo dispositivo de comunicaciones seguras 100B. Cuando se determina que se ha producido un error en los datos de seguridad, la unidad de control 121 del segundo dispositivo de comunicaciones seguras 100B cambia el estado de funcionamiento del dispositivo de comunicaciones seguras 100 en el estado seguro contra fallos (operación S123). En el estado seguro contra fallos, el dispositivo de comunicaciones seguras 100 suspende la comunicación segura hasta que se reciba la entrada del usuario para reiniciar. En particular, en el estado seguro contra fallos, el dispositivo de comunicaciones seguras 100 puede o no suspender las comunicaciones que no seas las comunicaciones relacionadas con los datos de seguridad, sino que suspende al menos la comunicación relacionada con los datos de seguridad. Cuando se determina que no se ha producido un error en los datos de seguridad, la unidad de control 121 del segundo dispositivo de comunicaciones seguras 100B consume los datos de seguridad de solicitud recibidos (operación S125), y genera los datos de seguridad de la respuesta a transmitir a continuación (operación S127).

La unidad de cálculo del código de detección de errores 101, la unidad generadora de la unidad de datos del protocolo 105, la unidad generadora de la trama Ethernet 107, y la unidad de transmisión de datos 109 del segundo dispositivo de comunicaciones seguras 100B generan la trama Ethernet que incluye la PDU de seguridad de la respuesta incluyendo los datos de seguridad de la respuesta, como se describe anteriormente con respecto a las operaciones S101 a S109, y después transmite la trama Ethernet al dispositivo de comunicaciones seguras 100A (operación S129).

De conformidad con una modalidad, los métodos mencionados anteriormente pueden implementarse con códigos legibles por un procesador en un medio de almacenamiento de programas. Un medio de registro legible por un procesador incluye, por ejemplo, una ROM, una RAM, un CD-ROM, una cinta magnética, un disquete, y un dispositivo de almacenamiento óptico de datos, y puede implementarse además en forma de una onda portadora (por ejemplo, transmisión a través de Internet).

El dispositivo de comunicaciones mencionado anteriormente no se limita a las configuraciones y métodos de las modalidades mencionadas anteriormente. La totalidad o una parte de cada modalidad puede combinarse selectivamente entre sí para realizar varias modificaciones.

REIVINDICACIONES

1. Un método de comunicación para transmitir, mediante un primer dispositivo de comunicaciones (100A), datos a un segundo dispositivo de comunicaciones (100B), el método de comunicación comprende:
generar, mediante el primer dispositivo de comunicaciones (100A), un identificador único de seguridad para confirmar la validez de la conexión entre el primer dispositivo de comunicaciones (100A) y el segundo dispositivo de comunicaciones (100B) mediante el uso de un identificador único del primer dispositivo de comunicaciones (100A) y un identificador único del segundo dispositivo de comunicaciones (100B);
calcular, mediante el primer dispositivo de comunicaciones (100A), un código de detección de errores de datos para detectar un error usando el identificador único de seguridad y los datos de seguridad;
generar, mediante el primer dispositivo de comunicaciones (100A), un paquete que comprende los datos de seguridad y el código de detección de errores de datos; y
transmitir, por el primer dispositivo de comunicaciones (100A), el paquete al segundo dispositivo de comunicaciones (100B), en donde en el caso donde el primer dispositivo de comunicaciones (100A) y el segundo dispositivo de comunicaciones (100B) tienen los identificadores únicos de seguridad correspondientes entre sí, la validez de la conexión entre el primer dispositivo de comunicaciones (100A) y el segundo dispositivo de comunicaciones (100B) puede confirmarse,
caracterizado porque los datos de seguridad se relacionan con un campo de comando,
si un valor del campo de comando es un primer valor, los datos de seguridad representan un comando de reinicio,
si el valor del campo de comando es un segundo valor, los datos de seguridad representan un comando de conexión,
si el valor del campo de comando es un tercer valor, los datos de seguridad representan un comando de transmisión de parámetro, y
si el valor del campo de comando es un cuarto valor, los datos de seguridad representan un comando de transmisión de datos.

2. El método de comunicación de conformidad con la reivindicación 1, en donde el paquete comprende una pluralidad de campos excepto un campo para transmitir el identificador único de seguridad.

3. El método de comunicación de conformidad con la reivindicación 1, en donde el identificador único del primer dispositivo de comunicaciones (100A) comprende un identificador del dispositivo fuente y una dirección MAC de la fuente, y el identificador único del segundo dispositivo de comunicaciones (100B) comprende un identificador del dispositivo de destino y una dirección MAC de destino.

4. El método de comunicación de conformidad con la reivindicación 3, en donde generar el identificador único de seguridad comprende:
generar un identificador del dispositivo para el identificador único de seguridad combinando el identificador del dispositivo fuente y el identificador del dispositivo de destino;
generar una dirección MAC para el identificador único de seguridad combinando la dirección MAC de la fuente y la dirección MAC de destino; y
generar el identificador único de seguridad combinando el identificador del dispositivo y la dirección MAC.

5. El método de comunicación de conformidad con la reivindicación 1, que comprende:
calcular, mediante el primer dispositivo de comunicaciones (100A), un código de detección de errores de encabezado para detectar un error de datos de encabezado usando los datos de encabezado, el identificador único de seguridad y un número de secuencia, en donde la generación del paquete comprende generar el paquete que comprende los datos del encabezado, el código de detección de errores de encabezado, los datos de seguridad y el código de detección de errores de datos.

6. Un método de comunicación para recibir, mediante un primer dispositivo de comunicaciones (100A), datos de un segundo dispositivo de comunicaciones (100B), el método de comunicación comprende:
recibir, por el primer dispositivo de comunicaciones (100A), un paquete desde el segundo dispositivo de comunicaciones (100B); obtener, por el primer dispositivo de comunicaciones (100A), los datos de seguridad y un identificador único de seguridad y un código de detección de errores de datos recibidos del paquete;
calcular, mediante el primer dispositivo de comunicaciones (100A), un código de detección de errores de datos comparativo mediante el uso de los datos de seguridad; y
determinar, por el primer dispositivo de comunicaciones (100A), si el paquete tiene un error en base al código de detección de errores de datos recibido y al código de detección de errores de datos comparativo,
en donde en el caso donde el primer dispositivo de comunicaciones (100A) y el segundo dispositivo de comunicaciones (100B) tienen los identificadores únicos de seguridad correspondientes entre sí, puede confirmarse la validez de conexión entre el primer dispositivo de comunicaciones (100A) y el segundo dispositivo de comunicaciones (100B),
caracterizado porque los datos de seguridad se relacionan con un campo de comando,
si un valor del campo de comando es un primer valor, los datos de seguridad representan un comando de reinicio,

si el valor del campo de comando es un segundo valor, los datos de seguridad representan un comando de conexión,
si el valor del campo de comando es un tercer valor, los datos de seguridad representan un comando de transmisión de parámetro,
y
si el valor del campo de comando es un cuarto valor, los datos de seguridad representan un comando de transmisión de datos.

7. El método de comunicación de conformidad con la reivindicación 6, en donde el paquete comprende una pluralidad de campos excepto el identificador único de seguridad.

8. El método de comunicación de conformidad con la reivindicación 6, en donde determinar si el paquete tiene el error comprende:
comparar el código de detección de errores de datos comparativo con el código de detección de errores de datos recibidos;
determinar que el error no ha ocurrido en el paquete si el código de detección de errores de datos comparativo es igual
al código de detección de errores recibidos; y
determinar que el error se ha producido en el paquete si el código de detección de errores de datos comparativo es diferente del código de detección de errores de datos recibido.

9. El método de comunicación de conformidad con la reivindicación 7, en donde el identificador único de seguridad comprende una combinación de un identificador único del primer dispositivo de comunicaciones (100A) y un identificador único del segundo dispositivo de comunicaciones (100B).

10. El método de comunicación de conformidad con la reivindicación 9, en donde el identificador único del primer dispositivo de comunicaciones (100A) comprende un identificador del dispositivo de destino y una dirección MAC de destino, y el identificador único del segundo dispositivo de comunicaciones (100B) comprende un identificador del dispositivo fuente y una dirección MAC de la fuente.

11. El método de comunicación de conformidad con la reivindicación 10, en donde el identificador único de seguridad se genera combinando un identificador del dispositivo generado mediante la combinación del identificador del dispositivo fuente y el identificador del dispositivo de destino y una dirección MAC generada mediante la combinación de la dirección MAC de la fuente y la dirección MAC de destino.

12. El método de comunicación de conformidad con cualquiera de las reivindicaciones 6 y 8, que comprende: cambiar un estado de funcionamiento a un estado en el cual se suspende la comunicación hasta que se reciba una entrada del usuario para reiniciar, en el caso en que se determine el paquete como que tiene el error.

Figura 1

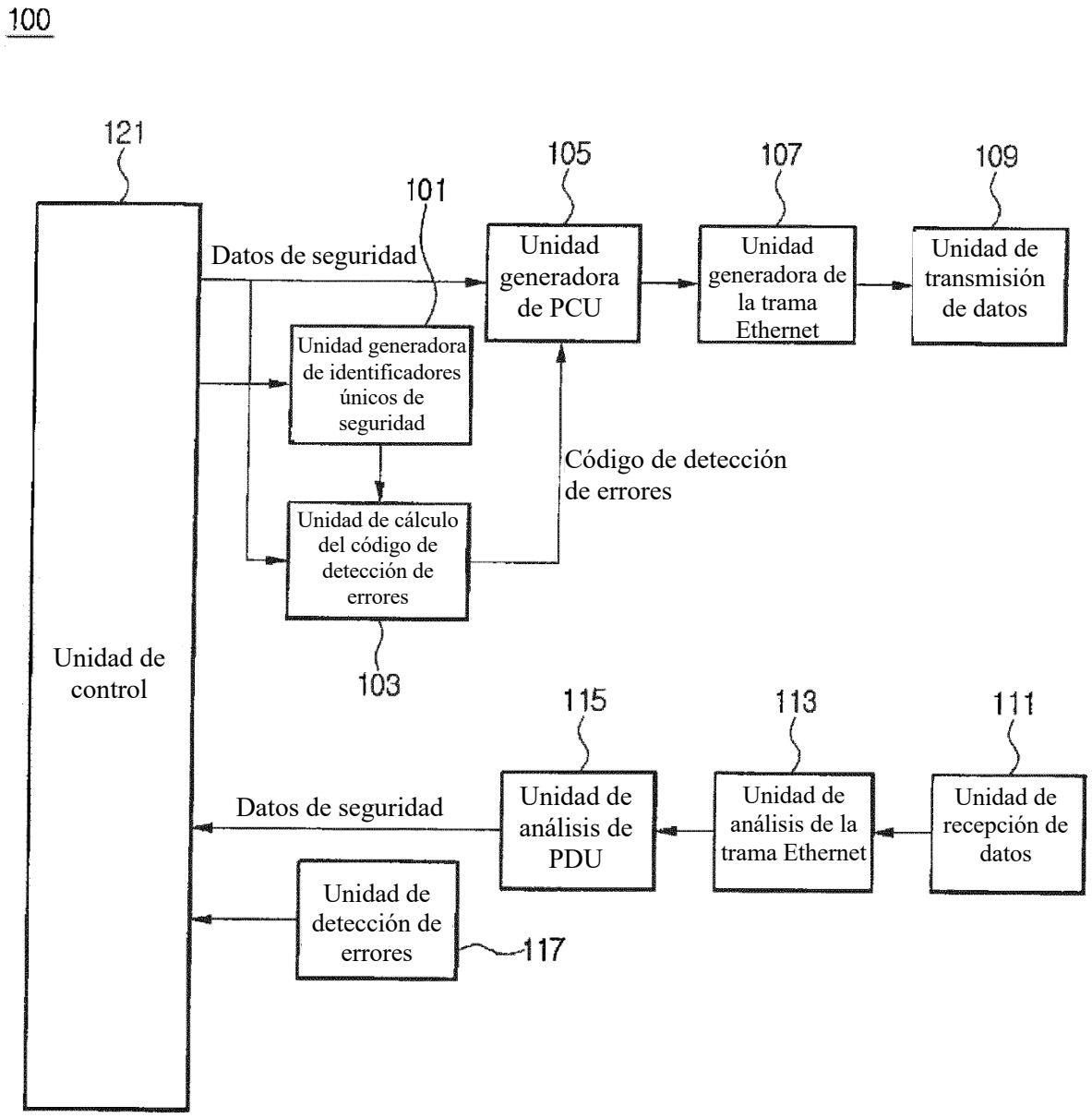

100
121
101
105
107
109
Datos de seguridad
Unidad generadora de PCU
Unidad generadora de la trama Ethernet
Unidad de transmisión de datos
Unidad generadora de identificadores únicos de seguridad
Código de detección de errores
Unidad de cálculo del código de detección de errores
Unidad de control
103
115
113
111
Datos de seguridad
Unidad de análisis de PDU
Unidad de análisis de la trama Ethernet
Unidad de recepción de datos
Unidad de detección de errores
117

Figura 2

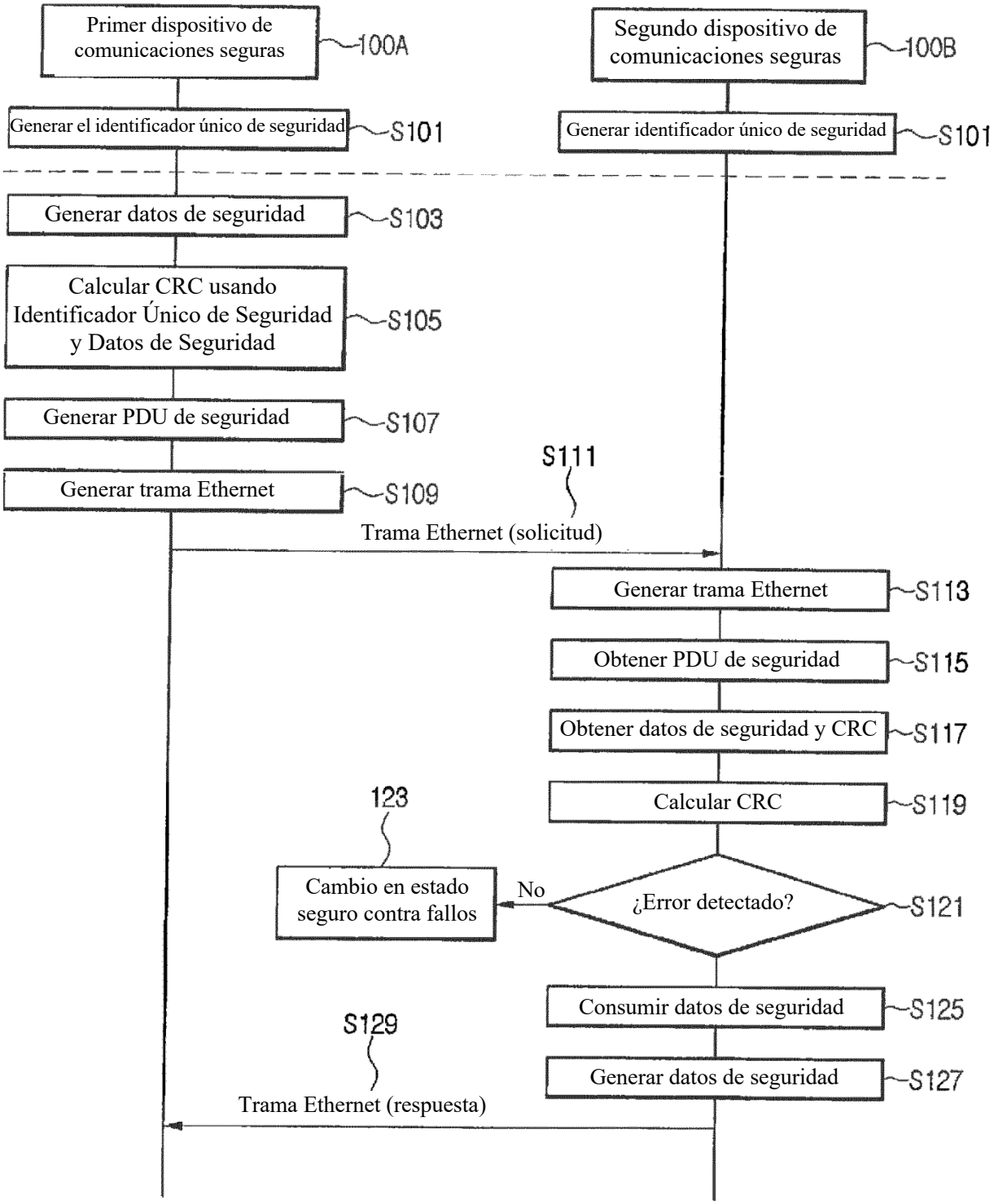

Primer dispositivo de comunicaciones seguras
100A
Segundo dispositivo de comunicaciones seguras
100B
Generar el identificador único de seguridad
S101
Generar identificador único de seguridad
S101
Generar datos de seguridad
S103
Calcular CRC usando Identificador Único de Seguridad y Datos de Seguridad
S105
Generar PDU de seguridad
S107
Generar trama Ethernet
S109
S111
Trama Ethernet (solicitud)
Generar trama Ethernet
S113
Obtener PDU de seguridad
S115
Obtener datos de seguridad y CRC
S117
Calcular CRC
S119
123
Cambio en estado seguro contra fallos
No
¿Error detectado?
S121
Consumir datos de seguridad
S125
S129
Generar datos de seguridad
S127
Trama Ethernet (respuesta)

Figura 3

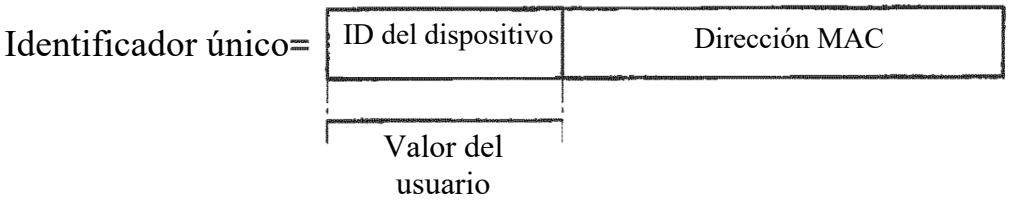


Figura 4

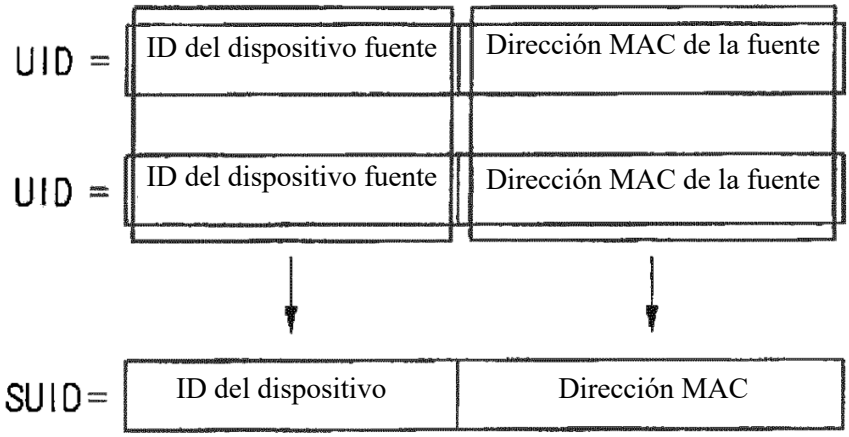


Figura 5

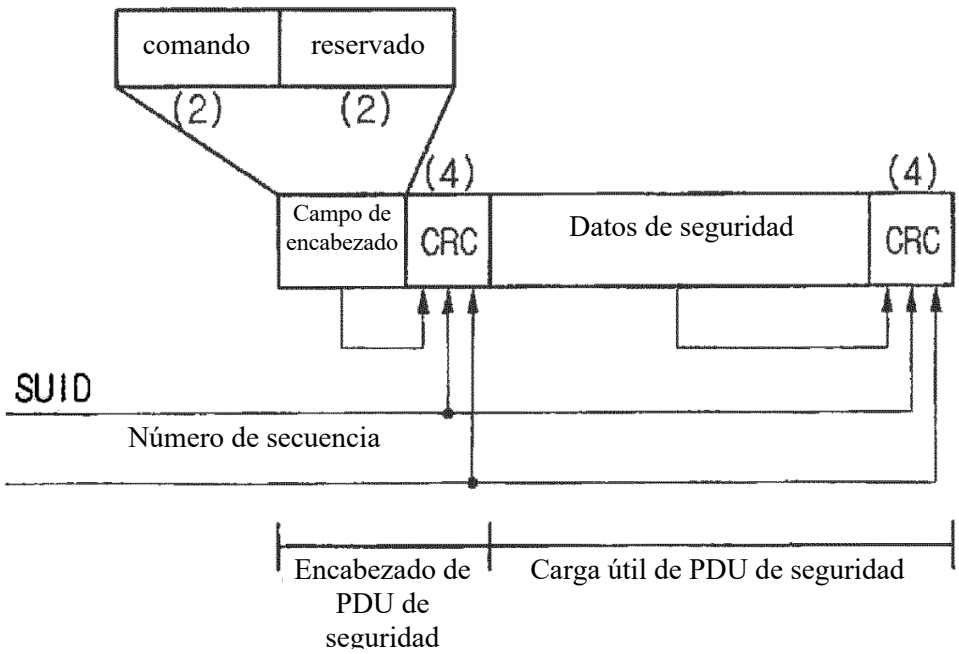
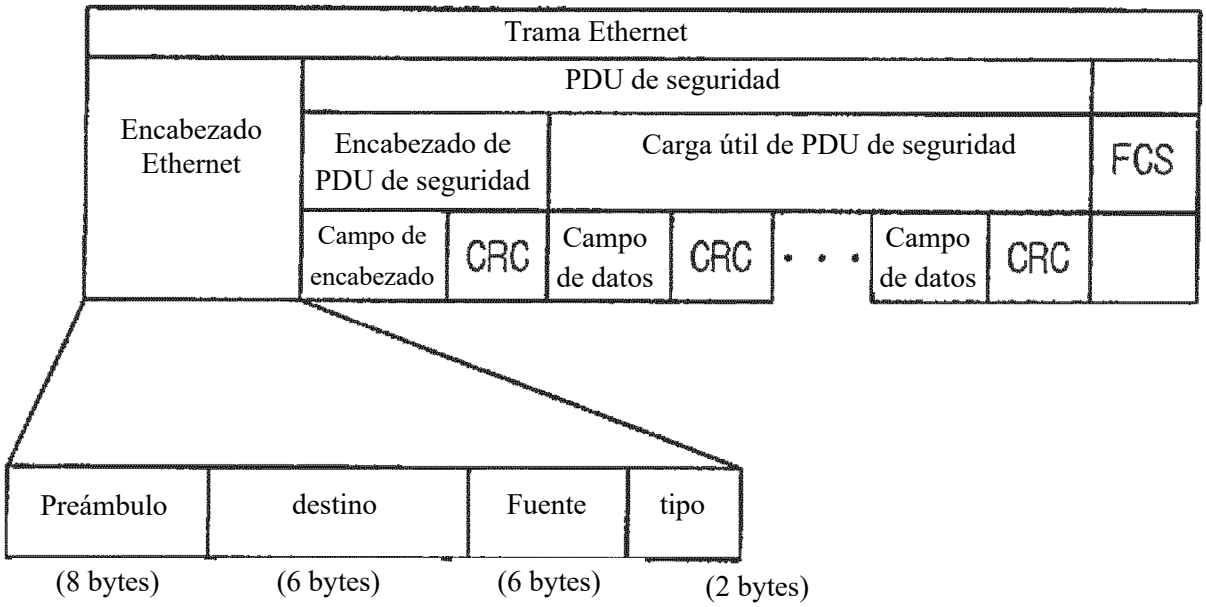


Figura 6


Trama Ethernet
Encabezado Ethernet
PDU de seguridad
Encabezado de PDU de seguridad
Carga útil de PDU de seguridad
FCS
Campo de encabezado
CRC
Campo de datos
CRC
Campo de datos
CRC
Preámbulo
destino
Fuente
tipo
(8 bytes)
(6 bytes)
(6 bytes)
(2 bytes)