(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 602 477**

(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/KR2012/008651**

(87) Fecha y número de publicación internacional: **06.09.2013 WO13129750**

(96) Fecha de presentación y número de la solicitud europea: **22.10.2012 E 12870208 (1)**

(97) Fecha y número de publicación de la concesión europea: **10.08.2016 EP 2822205**

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

(30) Prioridad:

02.03.2012 US 201261605764 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.02.2017

(73) Titular/es:

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

(72) Inventor/es:

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

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Dispositivo de comunicación y procedimiento de comunicación

CAMPO TÉCNICO

La presente divulgación se refiere a un dispositivo de comunicación y a un procedimiento de comunicación y, más específicamente, a un dispositivo de comunicación de seguridad y a un procedimiento de comunicación de seguridad.

ANTECEDENTES DE LA TÉCNICA

Actualmente se buscan soluciones para la comunicación de seguridad, a ser utilizadas en los campos industriales. En particular, se requieren sistemas de control industrial para mantener un nivel prescrito o superior de integridad de la información transferida a través de una red, con el fin de asegurar la seguridad de los trabajadores, evitar las amenazas para el medio ambiente y evitar la aparición de problemas relacionados con la seguridad.

Con el fin de satisfacer tales requisitos de integridad, se requieren sistemas de control industrial para tratar los problemas de corrupción, repetición involuntaria, secuencia incorrecta, pérdida, retraso inaceptable, inserción, suplantación y gestión de direcciones.

En cuanto al problema de la corrupción, los sistemas de control industrial deberían ser capaces de determinar si se produce un error en los datos transferidos, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema de la repetición involuntaria, los sistemas de control industrial deberían ser capaces de determinar si se produce o no normalmente repetición de datos que no sea realizada maliciosamente por una persona, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema de la secuencia incorrecta, los sistemas de control industrial deberían ser capaces de determinar si se cambia o no una secuencia de transmisión de datos, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema de la pérdida, los sistemas de control industrial deberían ser capaces de determinar si una parte de los datos transmitidos están dañados o no, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema del retraso inaceptable, los sistemas de control industrial deberían ser capaces de determinar si se produce o no un retraso inaceptable en la transmisión de datos, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema de la inserción, los sistemas de control industrial deberían ser capaces de determinar si se insertan o no datos no intencionados durante la transmisión de datos, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema de la suplantación, los sistemas de control industrial deberían ser capaces de determinar si alguna persona ha cambiado los datos maliciosamente o no, con un nivel prescrito, o superior, de probabilidad.

En cuanto al problema de la gestión de direcciones, los sistemas de control industrial deberían ser capaces de determinar si los datos se transmiten o no a un receptor correcto, con un nivel prescrito, o superior, de probabilidad.

El documento IEC 61508 representa una probabilidad de ocurrencia de errores utilizando SIL (Niveles de Integridad de Seguridad) como se muestra en la tabla 1 a continuación.

[Tabla 1]

SIL4	$>= 10^{-9}, < 10^{-8}$
SIL3	$>= 10^{-8}, < 10^{-7}$
SIL 2	$>= 10^{-7}, < 10^{-6}$
SIL1	$>= 10^{-6}, < 10^{-5}$

Por ejemplo, para satisfacer el SIL3, la probabilidad de ocurrencia de errores debería satisfacer $10^{-9.}$

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

DIVULGACIÓN DE LA INVENCIÓN

PROBLEMA TÉCNICO

Los modos de realización proporcionan un dispositivo de comunicación y un procedimiento de comunicación que cumplen los requisitos de integridad de los sistemas de control industrial.

SOLUCIÓN TÉCNICA

En un modo de realización, un procedimiento de comunicación para la transmisión, mediante un primer dispositivo de comunicación, de datos a un segundo dispositivo de comunicación incluye: el cálculo, mediante el primer dispositivo de comunicación, de un código de detección de errores de datos para detectar un error de datos utilizando los datos y un número de secuencia virtual; la generación, mediante el primer dispositivo de comunicación, de un paquete que incluye los datos y el código de detección de errores de datos; y la transmisión, mediante el primer dispositivo de comunicación, del paquete al segundo dispositivo de comunicación. El paquete puede no incluir un campo para la transmisión del número de secuencia virtual únicamente.

En otro modo de realización, un procedimiento de comunicación para la recepción, mediante un primer dispositivo de comunicación, de datos provenientes de un segundo dispositivo de comunicación incluye: la recepción, mediante el primer dispositivo de comunicación, de un paquete desde el segundo dispositivo de comunicación; la obtención, mediante el primer dispositivo de comunicación, de los datos y un código recibido de detección de errores de datos del paquete; el cálculo, mediante el primer dispositivo de comunicación, de un código comparativo de detección de errores de datos usando un número de secuencia virtual y los datos; y la determinación, mediante el primer dispositivo de comunicación, de si el paquete tiene o no un error basándose en el código recibido de detección de errores de datos y el código comparativo de detección de errores de datos. El paquete puede no incluir un campo para la transmisión del número de secuencia virtual únicamente.

EFECTOS VENTAJOSOS

De acuerdo a los modos de realización de la presente divulgación, pueden cumplirse los requisitos de integridad de sistemas de control industrial.

En particular, de acuerdo a los modos de realización de la presente divulgación, pueden detectarse errores tales como la repetición involuntaria, la secuencia incorrecta, la pérdida y la inserción.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La fig. 1 es un diagrama de bloques que ilustra un dispositivo de comunicación de seguridad según un modo de realización.

La fig. 2 es un diagrama escalonado que ilustra un procedimiento de comunicación según un modo de realización.

La fig. 3 ilustra una estructura de una unidad de datos de protocolo de seguridad de acuerdo a un modo de realización.

La fig. 4 ilustra una estructura de una trama de Ethernet según un modo de realización.

La fig. 5 es un diagrama escalonado que ilustra un procedimiento de comunicación relacionado con un número de secuencia virtual según un modo de realización.

La fig. 6 es un diagrama escalonado que ilustra un procedimiento de comunicación relacionado con un número de secuencia virtual según otro modo de realización.

MODO DE LLEVAR A CABO LA INVENCIÓN

En lo sucesivo, se describirá de forma detallada un terminal móvil relacionado con un modo de realización, con referencia a los dibujos adjuntos. En la siguiente descripción, los términos "módulo" y "unidad" para referirse a elementos están asignados a la misma, y se utilizan de forma intercambiable para mayor comodidad y, por lo tanto, los términos por sí mismos no necesariamente representan diferentes significados o funciones.

En lo sucesivo, se describirán un dispositivo de comunicación de seguridad y un procedimiento de comunicación de seguridad de acuerdo a los modos de realización, con referencia a los dibujos adjuntos.

La fig. 1 es un diagrama de bloques que ilustra un dispositivo de comunicación de seguridad según un modo de realización.

Como se ilustra en la fig. 1, un dispositivo de comunicación de seguridad 100 de acuerdo a un modo de realización

incluye una unidad de cálculo de códigos de detección de errores 110, una unidad de generación de unidades de datos de protocolo (PDU) 120, una unidad de generación de tramas de Ethernet 130, una unidad de transmisión de datos 140, una unidad de recepción de datos 150, una unidad de análisis de tramas de Ethernet 160, una unidad de análisis de unidades de datos de protocolo 170, una unidad de detección de errores 180 y una unidad de control 190.

La unidad de control 190 genera datos de seguridad y proporciona los datos de seguridad generados a la unidad de cálculo de códigos de detección de errores 110.

La unidad de cálculo de códigos de detección de errores 110 calcula un código de detección de errores de datos para los datos de seguridad utilizando los datos de seguridad.

La unidad de generación de unidades de datos de protocolo 120 genera una unidad de datos de protocolo de seguridad que incluye el código calculado de detección de errores de datos y los datos de seguridad generados. Aquí, la unidad de datos de protocolo de seguridad puede denominarse un paquete.

La unidad de generación de tramas de Ethernet 130 genera una trama de Ethernet que incluye la unidad generada de datos de protocolo de seguridad.

La unidad de transmisión de datos 140 transmite la trama de Ethernet generada a otro dispositivo de comunicación de seguridad. De esta manera, la unidad de transmisión de datos 140 transmite la unidad generada de datos de protocolo de seguridad al otro dispositivo de comunicación de seguridad.

La unidad de recepción de datos 150 recibe la trama de Ethernet que incluye la unidad de datos de protocolo de seguridad desde el otro dispositivo de comunicación de seguridad.

La unidad de análisis de tramas de Ethernet 160 analiza la trama de Ethernet recibida para obtener la unidad de datos de protocolo de seguridad.

La unidad de análisis de unidades de datos de protocolo 170 analiza la unidad de datos de protocolo para obtener el código de detección de errores de datos y los datos de seguridad.

La unidad de detección de errores 180 calcula el código de detección de errores de datos utilizando los datos de seguridad y, a continuación, compara el código calculado de detección de errores de datos con el código obtenido de detección de errores de datos, para detectar un error. En el caso de que el código calculado de detección de errores de datos sea igual al código obtenido de detección de errores de datos, la unidad de detección de errores 180 determina que no se ha producido un error en los datos de seguridad. Por el contrario, en el caso de que el código calculado de detección de errores de datos sea diferente al código obtenido de detección de errores de datos, la unidad de detección de errores 180 determina que se ha producido un error en los datos de seguridad.

Cuando se determina que se ha producido un error en los datos de seguridad, la unidad de control 190 cambia un estado de funcionamiento del dispositivo de comunicación de seguridad 100 a un estado a prueba de fallos. En el estado a prueba de fallos, el dispositivo de comunicación de seguridad 100 suspende la comunicación de seguridad hasta que se reciba una entrada de usuario para el reinicio. En particular, en el estado a prueba de fallos, el dispositivo de comunicación de seguridad 100 puede o no suspender la comunicación distinta a la comunicación relacionada con los datos de seguridad, pero 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 190 genera los datos de seguridad que han de transmitirse a continuación. Si los datos de seguridad recibidos están relacionados con una petición, la unidad de control 190 genera los datos de seguridad relacionados con una respuesta. Si los datos de seguridad recibidos están relacionados con una respuesta, la unidad de control 190 genera los datos de seguridad relacionados con una petición siguiente.

La fig. 2 es un diagrama escalonado que ilustra un procedimiento de comunicación según un modo de realización.

Como se ilustra en la fig. 2, se supone que un primer dispositivo de comunicación de seguridad 100A se comunica con un segundo dispositivo de comunicación 100B, el primer dispositivo de comunicación de seguridad 100A transmite una petición de una unidad de datos de protocolo de seguridad al segundo dispositivo de comunicación de seguridad 100B, y el segundo dispositivo de comunicación de seguridad 100B transmite una respuesta de una unidad de datos de protocolo de seguridad al primer dispositivo de comunicación de seguridad 100A.

La unidad de control 190 del primer dispositivo de comunicación de seguridad 100A genera los datos de seguridad para una petición (operación S101). El primer dispositivo de comunicación de seguridad 100A puede generar datos de cabecera de seguridad relacionados con los datos de seguridad de petición, junto con los datos de seguridad de petición.

Cuando se generan los datos de seguridad de petición, la unidad de cálculo de códigos de detección de errores 110 del primer dispositivo de comunicación de seguridad 100A incrementa un número de secuencia virtual en un paso (operación S102). Aquí, el paso puede ser 1 o un número natural mayor que 1. El número de secuencia virtual indica un número de secuencia de la unidad de datos de protocolo de seguridad que se generará posteriormente, y no se incluye en la unidad de datos de protocolo de seguridad. Es decir, la unidad de datos de protocolo de seguridad puede no incluir un campo para la transmisión del número de secuencia virtual únicamente. Cuando se reinicia el primer dispositivo de comunicación de seguridad 100A, la unidad de cálculo de códigos de detección de errores 110 del primer dispositivo de comunicación de seguridad 100A reinicia el número de secuencia virtual.

La unidad de cálculo de códigos de detección de errores 110 del primer dispositivo de comunicación de seguridad 100A calcula el código de detección de errores de datos para los datos de seguridad utilizando los datos de seguridad y el número de secuencia virtual (operación S103). Aquí, la unidad de cálculo de códigos de detección de errores 110 del primer dispositivo de comunicación de seguridad 100A puede calcular un código de detección de errores de cabecera para detectar un error en los datos de cabecera de seguridad utilizando los datos de seguridad y el número de secuencia virtual. El código de detección de errores puede ser un valor de comprobación de redundancia cíclica (CRC).

En particular, como se muestra en la ecuación 1 a continuación, la unidad de cálculo de códigos de detección de errores 110 del primer dispositivo de comunicación de seguridad 100A puede calcular el código de detección de errores de cabecera CRC_CABECERA utilizando un campo de cabecera, un identificador único y el número de secuencia virtual. Aquí, el identificador único puede ser un identificador único de seguridad (SUID).

Ecuación 1

CRC_CABECERA: = f (SUID, número_de_secuencia_virtual, campo_de_cabecera)

En la ecuación 1, *f* indica una función de troceo.

El identificador único de seguridad puede representar una relación de conexión entre el primer dispositivo de comunicación de seguridad 100A y el segundo dispositivo de comunicación de seguridad 100B. En particular, el identificador único de seguridad puede generarse mediante la combinación de una dirección de control de acceso a medios (MAC), un identificador de dispositivo de origen, una dirección de MAC de destino y un identificador de dispositivo de destino. Dado que el primer dispositivo de comunicación de seguridad 100A transmite los datos de seguridad y el segundo dispositivo de comunicación de seguridad 100B recibe los datos de seguridad, el primer dispositivo de comunicación de seguridad 100A es un origen y el segundo dispositivo de comunicación de seguridad 100B es un destino. En este caso, el identificador único de seguridad puede ser una combinación de una dirección de MAC del primer dispositivo de comunicación de seguridad 100A, un identificador de dispositivo del primer dispositivo de comunicación de seguridad 100A, una dirección de MAC del segundo dispositivo de comunicación de seguridad 100B y un identificador de dispositivo del segundo dispositivo de comunicación de seguridad 100B. El identificador único de seguridad solo puede utilizarse para calcular el código de detección de errores, sin estar incluido en la PDU de seguridad.

El número de secuencia virtual puede representar un número de secuencia de la PDU de seguridad. El primer dispositivo de comunicación de seguridad 100A utiliza 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 comunicación de seguridad 100B.

Como se muestra en la ecuación 2 a continuación, la unidad de cálculo de códigos de detección de errores 110 del primer dispositivo de comunicación de seguridad 100A puede calcular el código de detección de errores de datos CRC_DATOS utilizando los datos de seguridad, el identificador único y el número de secuencia virtual. Aquí, el identificador único puede ser un identificador único de seguridad (SUID).

Ecuación 2

CRC_DATOS: = f (SUID, número_de_secuencia_virtual, datos_de_seguridad)

En la ecuación 2, *f* indica una función de troceo.

La unidad de generación de unidades de datos de protocolo 120 del primer dispositivo de comunicación de seguridad 100A genera la unidad de datos de protocolo de seguridad incluyendo los datos de seguridad y el código calculado de detección de errores de datos. Aquí, la unidad de datos de protocolo de seguridad puede incluir además los datos de cabecera de seguridad y el código calculado de detección de errores de cabecera. Se describirá una estructura de la unidad de datos del protocolo de seguridad de acuerdo a un modo de realización, con referencia a la fig. 3.

La fig. 3 ilustra la estructura de la unidad de datos de protocolo de seguridad de acuerdo a un modo de realización.

Como se ilustra en la fig. 3, la unidad de datos de protocolo de seguridad incluye de forma secuencial una cabecera de PDU de seguridad y una carga útil de PDU de seguridad. La cabecera de PDU de seguridad incluye de forma secuencial un campo de cabecera de seguridad y el código de detección de errores de cabecera. La carga útil de PDU de seguridad incluye de forma secuencial los datos de seguridad y el código de detección de errores de datos. En particular, la cabecera de PDU de seguridad puede estar dispuesta en una primera línea de la unidad de datos de protocolo de seguridad. La cabecera de PDU de seguridad incluye de forma secuencial un campo de comando y un campo reservado. Los datos de seguridad pueden estar relacionados con la cabecera de PDU de seguridad. En particular, los datos de seguridad pueden estar relacionados con el campo de comando. En particular, en el modo de realización de la fig. 3, el campo de cabecera 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 cabecera 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 los mismos. Un octeto representa generalmente 8 bits.

La tabla 2 muestra ejemplos de valores del campo de comando de acuerdo a un modo de realización.

[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 parámetros. Si el valor del campo de comando es 0x04, los datos de seguridad pueden representar un comando de transmisión de datos.

En particular, el modo de realización de la fig. 2 puede corresponder a un procedimiento 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 comunicación de seguridad 100A puede corresponder a un iniciador, y el segundo dispositivo de comunicación de seguridad 100B puede corresponder a un respondedor. El iniciador está en una modalidad en la que los datos de seguridad de petición se transmiten al respondedor pero los datos de seguridad de respuesta no se transmiten. El respondedor está en una modalidad en la que los datos de seguridad de respuesta se transmiten al iniciador pero los datos de seguridad de petición no se transmiten.

El campo reservado puede utilizarse más adelante para otros propósitos.

Como se ilustra en la fig. 3, la unidad de datos de protocolo de seguridad puede no incluir el número de secuencia virtual. Es decir, la unidad de datos de protocolo de seguridad puede no incluir un campo para la transmisión del número de secuencia virtual únicamente.

La fig. 2 se describirá de nuevo.

La unidad de generación de tramas de Ethernet 130 del primer dispositivo de comunicación de seguridad 100A genera una trama de Ethernet que incluye los datos de seguridad de petición (operación S107). Aquí, la trama de Ethernet puede incluir la unidad generada de datos de protocolo de seguridad. Se describirá una estructura de la trama de Ethernet de acuerdo a un modo de realización, con referencia a la figura 4.

La fig. 4 ilustra la estructura de la trama de Ethernet de acuerdo a un modo de realización.

Como se ilustra en la fig. 4, la trama de Ethernet incluye de forma secuencial una cabecera de Ethernet, una carga útil de Ethernet y una secuencia de verificación de trama (FCS). La trama de Ethernet incluye la PDU de seguridad como la carga útil. La cabecera de la trama de Ethernet incluye un campo de preámbulo, un campo de dirección de destino, un campo de dirección de origen y un campo de tipo. El campo de dirección de destino contiene una dirección de un dispositivo de comunicación de seguridad correspondiente a un destino, y el campo de dirección de origen contiene una dirección de un dispositivo de comunicación de seguridad correspondiente a un origen. La secuencia de verificación de trama puede generarse utilizando datos dentro de la cabecera de Ethernet y datos dentro de la carga útil.

La fig. 2 se describirá de nuevo.

La unidad de transmisión de datos 140 del primer dispositivo de comunicación de seguridad 100A transmite la trama de Ethernet que incluye los datos de seguridad de petición al segundo dispositivo de comunicación de seguridad 100B (operación S109). De esta manera, la unidad de transmisión de datos 140 puede transmitir la unidad generada de datos de protocolo de seguridad al segundo dispositivo de comunicación de seguridad 100B.

La unidad de recepción de datos 150 del segundo dispositivo de comunicación de seguridad 100B recibe, desde el primer dispositivo de comunicación de seguridad 100A, la trama de Ethernet que incluye la unidad de datos de protocolo de seguridad relacionada con una petición (operación S111). Aquí, la trama de Ethernet puede tener la estructura que se ilustra en la fig. 4.

La unidad de análisis de tramas de Ethernet 160 del segundo dispositivo de comunicación de seguridad 100B analiza la trama de Ethernet recibida para obtener la unidad de datos de protocolo de seguridad (operación S113). Aquí, la unidad de datos de protocolo de seguridad puede tener la estructura que se ilustra en la fig. 3.

La unidad de análisis de unidades de datos de protocolo 170 del segundo dispositivo de comunicación de seguridad 100B analiza la unidad de datos de protocolo para obtener los datos de cabecera de seguridad, un código recibido de detección de errores de cabecera, los datos de seguridad de petición y un código recibido de detección de errores de datos (operación S115).

Cuando se recibe la unidad de protocolo de seguridad y se obtienen los datos de seguridad de petición, la unidad de detección de errores 180 del segundo dispositivo de comunicación de seguridad 100B incrementa el número de secuencia virtual administrado de esta manera en un paso (operación S116). Como se ha mencionado anteriormente, el paso puede ser 1 o un número natural mayor que 1.

La unidad de detección de errores 180 del segundo dispositivo de comunicación de seguridad 100B calcula un código comparativo de detección de errores de datos utilizando los datos de seguridad de petición y el número de secuencia virtual incrementado (operación S117). Además, la unidad de detección de errores 180 del segundo dispositivo de comunicación de seguridad 100B puede calcular un código comparativo de detección de errores de cabecera utilizando los datos de cabecera de seguridad y el número de secuencia virtual incrementado.

En particular, la unidad de detección de errores 180 del segundo dispositivo de comunicación de seguridad 100B puede calcular el código comparativo de detección de errores de cabecera utilizando la Ecuación 1.

Además, la unidad de detección de errores 180 del segundo dispositivo de comunicación de seguridad 100B puede calcular el código comparativo de detección de errores de datos utilizando la Ecuación 2.

La unidad de detección de errores 180 del segundo dispositivo de comunicación de seguridad 100B compara un código calculado de detección de errores y un código obtenido de detección de errores para detectar un error (operación S119). En el caso en que el código comparativo de detección de errores de datos sea igual al código recibido de detección de errores de datos y el código comparativo de detección de errores de cabecera sea igual al código recibido de detección de errores de cabecera, la unidad de detección de errores 180 puede determinar que no se ha producido un error en los datos de seguridad. Por el contrario, en el caso en que el código comparativo de detección de errores de datos sea diferente al código recibido de detección de errores de datos, o el código comparativo de detección de errores de cabecera sea diferente al código recibido de detección de errores de cabecera, la unidad de detección de errores 180 podrá determinar que se ha producido un error en los datos de seguridad.

Cuando se determina que se ha producido un error en los datos de seguridad, la unidad de control 190 del segundo dispositivo de comunicación de seguridad 100B cambia el estado de funcionamiento del dispositivo de comunicación de seguridad 100 al estado a prueba de fallos (operación S121). En el estado a prueba de fallos, el dispositivo de comunicación de seguridad 100 suspende la comunicación de seguridad hasta que se reciba la entrada del usuario para el reinicio. En particular, en el estado a prueba de fallos, el dispositivo de comunicación de seguridad 100 puede o no suspender la comunicación distinta a la comunicación relacionada con los datos de seguridad, pero 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 190 del segundo dispositivo de comunicación de seguridad 100B consume los datos de seguridad de la petición recibida (operación S123) y genera los datos de seguridad de respuesta que deben transmitirse a continuación (operación S125).

La unidad de cálculo de códigos de detección de errores 110, la unidad de generación de unidades de datos de protocolo 120, la unidad de generación de tramas de Ethernet 130 y la unidad de transmisión de datos 140 del segundo dispositivo de comunicación de seguridad 100B generan la trama de Ethernet que incluye la PDU de seguridad de respuesta que incluye los datos de seguridad de respuesta, como se ha descrito anteriormente con respecto a las operaciones S101 a S109 y, a continuación, transmiten la trama de Ethernet al primer dispositivo de comunicación de seguridad 100A (operación S127). En un modo de realización, el número de secuencia virtual

puede incrementarse cuando se transmiten los datos de seguridad de petición, y el número de secuencia virtual puede incrementarse cuando se transmiten los datos de seguridad de respuesta. En otro modo de realización, el número de secuencia virtual puede incrementarse cuando se transmiten los datos de seguridad de petición, pero el número de secuencia virtual puede no cambiar cuando se transmiten los datos de seguridad de respuesta.

La unidad de recepción de datos 150, la unidad de análisis de tramas de Ethernet 160, la unidad de análisis de unidades de datos de protocolo 170, la unidad de detección de errores 180 y la unidad de control 190 del primer dispositivo de comunicación de seguridad 100A reciben la trama de Ethernet que incluye la PDU de seguridad de respuesta, realizan la detección de errores y consumen los datos de seguridad de respuesta, como se ha descrito anteriormente con respecto a las operaciones S111 a S123. En un modo de realización, el número de secuencia virtual puede incrementarse cuando se reciben los datos de seguridad de petición, y el número de secuencia virtual puede incrementarse cuando se reciben los datos de seguridad de respuesta. En otro modo de realización, el número de secuencia virtual puede incrementarse cuando se reciben los datos de seguridad de petición, pero el número de secuencia virtual puede no cambiar cuando se reciben los datos de seguridad de respuesta.

La fig. 5 es un diagrama escalonado que ilustra un procedimiento de comunicación relacionado con el número de secuencia virtual según un modo de realización.

En primer lugar, se supone que los números de secuencia virtuales administrados por los dispositivos primero y segundo de comunicación de seguridad 100A y 100B tienen un valor de N.

Cuando se generan los datos de seguridad de petición, el primer dispositivo de comunicación de seguridad 100A incrementa el número de secuencia virtual N en 1 con el fin de transmitir un paquete que incluya los datos de seguridad de petición (operación S201).

El primer dispositivo de comunicación de seguridad 100A genera el valor de CRC utilizando el número de secuencia virtual incrementado N+1, y transmite un paquete de seguridad de petición que incluye el CRC generado y los datos de seguridad de petición al segundo dispositivo de comunicación de seguridad 100B (operación S203). Es decir, el número de secuencia virtual para este paquete de seguridad de petición es N+1.

Tras recibir el paquete de seguridad de petición que incluye los datos de seguridad de petición, el segundo dispositivo de comunicación de seguridad 100B incrementa el número de secuencia virtual N en 1 (operación S205).

El segundo dispositivo de comunicación de seguridad 100B verifica si el paquete de seguridad de petición tiene o no un error utilizando el número de secuencia virtual incrementado N+1 (operación S207).

A continuación, cuando se generan los datos de seguridad de respuesta, el segundo dispositivo de comunicación de seguridad 100B incrementa el número de secuencia virtual N+1 en 1 con el fin de transmitir un paquete de seguridad de respuesta que incluya los datos de seguridad de respuesta (operación S209).

El segundo dispositivo de comunicación de seguridad 100B genera el valor de CRC utilizando el número de secuencia virtual incrementado N+2, y transmite un paquete de respuesta que incluye el CRC generado y los datos de seguridad de respuesta al primer dispositivo de comunicación de seguridad 100A (operación S211). Es decir, el número de secuencia virtual para este paquete de seguridad de respuesta es N+2.

Tras recibir el paquete de seguridad de respuesta, el primer dispositivo de comunicación de seguridad 100A incrementa el número de secuencia virtual N+1 en 1 (operación S213).

El primer dispositivo de comunicación de seguridad 100A verifica si el paquete de seguridad de respuesta tiene o no un error utilizando el número de secuencia virtual incrementado N+2 (operación S215).

Las operaciones S217 a S231 son repeticiones de las operaciones S201 a S215.

La fig. 6 es un diagrama escalonado que ilustra un procedimiento de comunicación relacionado con el número de secuencia virtual según otro modo de realización.

En primer lugar, se supone que los números de secuencia virtuales administrados por los dispositivos primero y segundo de comunicación de seguridad 100A y 100B tienen un valor de N.

Cuando se generan los datos de seguridad de petición, el primer dispositivo de comunicación de seguridad 100A incrementa el número de secuencia virtual N en 1 con el fin de transmitir un paquete que incluya los datos de seguridad de petición (operación S301).

El primer dispositivo de comunicación de seguridad 100A genera el valor de CRC utilizando el número de secuencia virtual incrementado N+1, y transmite el paquete de seguridad de petición que incluye el CRC generado y los datos de seguridad de petición al segundo dispositivo de comunicación de seguridad 100B (operación S303). Es decir, el

número de secuencia virtual para este paquete de seguridad de petición es N+1.

Tras recibir el paquete de seguridad de petición que incluye los datos de seguridad de petición, el segundo dispositivo de comunicación de seguridad 100B incrementa el número de secuencia virtual N en 1 (operación S305).

El segundo dispositivo de comunicación de seguridad 100B verifica si el paquete de seguridad de petición tiene o no un error utilizando el número de secuencia virtual incrementado N+1 (operación S307).

A continuación, incluso aunque se generen los datos de seguridad de respuesta, el segundo dispositivo de comunicación de seguridad 100B mantiene el número de secuencia virtual N+1 administrado con el fin de transmitir el paquete de seguridad de respuesta que incluye los datos de seguridad de respuesta.

El segundo dispositivo de comunicación de seguridad 100B genera el valor de CRC utilizando el número de secuencia virtual actual N+1, y transmite el paquete de respuesta que incluye el CRC generado y los datos de seguridad de respuesta al primer dispositivo de comunicación de seguridad 100A (operación S311). Es decir, el número de secuencia virtual para este paquete de seguridad de respuesta es N+1. Tras recibir el paquete de seguridad de respuesta, el primer dispositivo de comunicación de seguridad 100A mantiene el número de secuencia virtual N+1.

El primer dispositivo de comunicación de seguridad 100A verifica si el paquete de seguridad de respuesta tiene o no un error utilizando el número de secuencia virtual actual N+1 (operación S315).

Las operaciones S317 a S331 son repeticiones de las operaciones S301 a S315.

De acuerdo a un modo de realización, los procedimientos mencionados anteriormente pueden implementarse con códigos legibles por procesador en un medio grabado por programa. Un medio de grabación legible por procesador incluye, por ejemplo, una ROM, una RAM, un CD-ROM, una cinta magnética, un disco flexible y un dispositivo de almacenamiento de datos ópticos, y también puede implementarse en forma de una onda portadora (por ejemplo, transmisión por Internet).

Los terminales móviles mencionados anteriormente no se limitan a la configuración y a los procedimientos de los modos de realización mencionados anteriormente.

REIVINDICACIONES

1. Un procedimiento de comunicación para la transmisión, mediante un primer dispositivo de comunicación, de datos a un segundo dispositivo de comunicación, comprendiendo el procedimiento de comunicación:

el cálculo, por el primer dispositivo de comunicación, de un código de detección de errores de datos (CRC_Datos) para detectar un error de los datos utilizando los datos, y un número de secuencia virtual y un identificador único;

la generación, mediante el primer dispositivo de comunicación, de un paquete que comprende los datos y el código de detección de errores de datos; y

la transmisión, mediante el primer dispositivo de comunicación, del paquete al segundo dispositivo de comunicación.

2. El procedimiento de comunicación de acuerdo a la reivindicación 1, en el que el paquete comprende la pluralidad de los campos excepto un campo para transmitir el número de secuencia virtual.

3. El procedimiento de comunicación de acuerdo a la reivindicación 2, que comprende, en el caso en que los datos sean datos de petición, el incremento del número de secuencia virtual, en el que el cálculo del código de detección de errores de datos comprende el cálculo del código de detección de errores de datos usando los datos y el número de secuencia virtual incrementado.

4. El procedimiento de comunicación de acuerdo a la reivindicación 3, en el que, en el caso en que los datos sean datos de respuesta, no se cambia el número de secuencia virtual.

5. El procedimiento de comunicación de acuerdo a la reivindicación 3, que comprende, en el caso en que los datos sean datos de respuesta, el incremento del número de secuencia virtual, en el que el cálculo del código de detección de errores de datos comprende el cálculo del código de detección de errores de datos usando los datos y el número de secuencia virtual incrementado.

6. El procedimiento de comunicación de acuerdo a la reivindicación 3, que comprende:

el cálculo, mediante el primer dispositivo de comunicación, de un código de detección de errores de cabecera para detectar un error de los datos de cabecera utilizando los datos de cabecera y el número de secuencia virtual, en el que
la generación del paquete comprende la generación del paquete que comprende los datos de cabecera, el código de detección de errores de cabecera, los datos y el código de detección de errores de datos.

7. El procedimiento de comunicación de acuerdo a la reivindicación 6, en el que el cálculo del código de detección de errores de cabecera comprende el cálculo del código de detección de errores de cabecera utilizando adicionalmente el identificador único, en el que el identificador único representa una relación de conexión entre el primer dispositivo de comunicación y el segundo dispositivo de comunicación.

8. Un procedimiento de comunicación para la recepción, por un primer dispositivo de comunicación, de datos provenientes de un segundo dispositivo de comunicación, comprendiendo el procedimiento de comunicación:

la recepción, por el primer dispositivo de comunicación, de un paquete proveniente del segundo dispositivo de comunicación;

la obtención, por el primer dispositivo de comunicación, de los datos y un código recibido de detección de errores de datos del paquete;

el cálculo, por el primer dispositivo de comunicación, de un código comparativo de detección de errores de datos (CRC_Datos) utilizando un número de secuencia virtual, y un identificador único y los datos; y
la determinación, por el primer dispositivo de comunicación, de si el paquete tiene o no un error basándose en el código recibido de detección de errores de datos y el código comparativo de detección de errores de datos.

9. El procedimiento de comunicación de acuerdo a la reivindicación 8, en el que el paquete comprende la pluralidad de los campos, excepto un campo para transmitir el número de secuencia virtual.

10. El procedimiento de comunicación de acuerdo a la reivindicación 9, que comprende, en el caso en que los datos sean datos de petición, el incremento del número de secuencia virtual, en el que el cálculo del código comparativo de detección de errores de datos comprende el cálculo del código comparativo de detección de errores de datos usando los datos de petición y el número de secuencia virtual incrementado.

11. El procedimiento de comunicación de acuerdo a la reivindicación 10, en el que, en el caso en que los datos sean datos de respuesta, no se cambia el número de secuencia virtual.

12. El procedimiento de comunicación de acuerdo a la reivindicación 10, que comprende, en el caso en que los datos sean datos de respuesta, el incremento del número de secuencia virtual, en el que el cálculo del código comparativo de detección de errores de datos comprende el cálculo del código comparativo de detección de errores de datos usando los datos de respuesta y el número de secuencia virtual incrementado.

13. El procedimiento de comunicación de acuerdo a la reivindicación 9, en el que la determinación de si el paquete tiene el error comprende:

la comparación del código comparativo de detección de errores de datos con el código recibido de detección de errores de datos; la determinación de que no se ha producido un error en el paquete si el código comparativo de detección de errores de datos es igual al código recibido de detección de errores de datos; y
la determinación de que se ha producido un error en el paquete si el código comparativo de detección de errores de datos es diferente al código recibido de detección de errores de datos.

14. El procedimiento de comunicación de acuerdo a una cualquiera de las reivindicaciones 8 a 11, en el que, en el caso en que se determine que el paquete tiene un error, se cambia un estado de funcionamiento a un estado en el que se suspende la comunicación hasta que se reciba una entrada de usuario para el reinicio.

15. El procedimiento de comunicación de acuerdo a la reivindicación 9, en el que la obtención de los datos y el código recibido de detección de errores de datos comprende la obtención de los datos de cabecera, un código recibido de detección de errores de cabecera, los datos y el código recibido de detección de errores de datos, a partir del paquete, comprendiendo el procedimiento de comunicación:

el cálculo de un código comparativo de detección de errores de cabecera para detectar un error de los datos de cabecera utilizando los datos de cabecera y el número de secuencia virtual, en el que
la determinación de si el paquete tiene un error comprende la determinación de si el paquete tiene un error basándose en el código recibido de detección de errores de cabecera, el código comparativo de detección de errores de cabecera, el código recibido de detección de errores de datos y el código comparativo de detección de errores de datos.

16. El procedimiento de comunicación de acuerdo a la reivindicación 11, en el que
el cálculo del código comparativo de detección de errores de cabecera comprende el cálculo del código comparativo de detección de errores de cabecera utilizando adicionalmente el identificador único, en el que el identificador único representa una relación de conexión entre el primer dispositivo de comunicación y el segundo dispositivo de comunicación.

Fig. 1

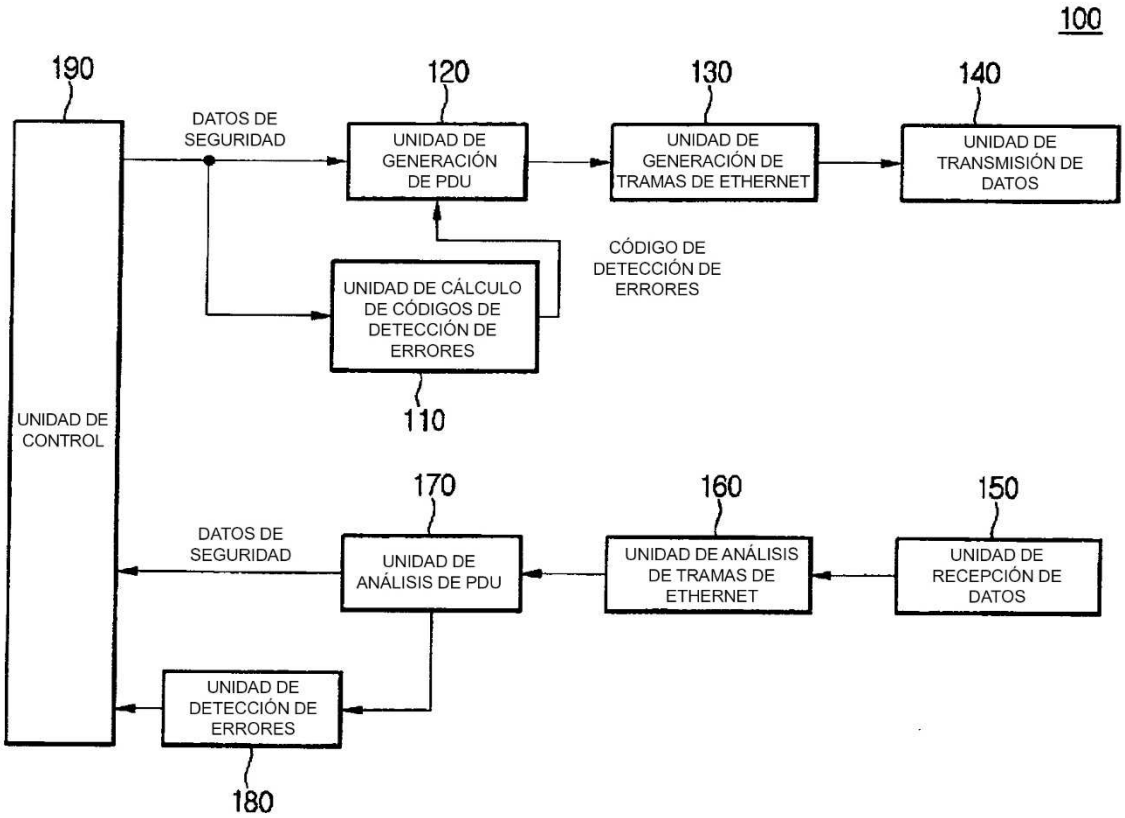

100
190
120
130
140
DATOS DE SEGURIDAD
UNIDAD DE GENERACIÓN DE PDU
UNIDAD DE GENERACIÓN DE TRAMAS DE ETHERNET
UNIDAD DE TRANSMISIÓN DE DATOS
CÓDIGO DE DETECCIÓN DE ERRORES
UNIDAD DE CÁLCULO DE CÓDIGOS DE DETECCIÓN DE ERRORES
110
UNIDAD DE CONTROL
170
160
150
DATOS DE SEGURIDAD
UNIDAD DE ANÁLISIS DE PDU
UNIDAD DE ANÁLISIS DE TRAMAS DE ETHERNET
UNIDAD DE RECEPCIÓN DE DATOS
UNIDAD DE DETECCIÓN DE ERRORES
180

Fig. 2

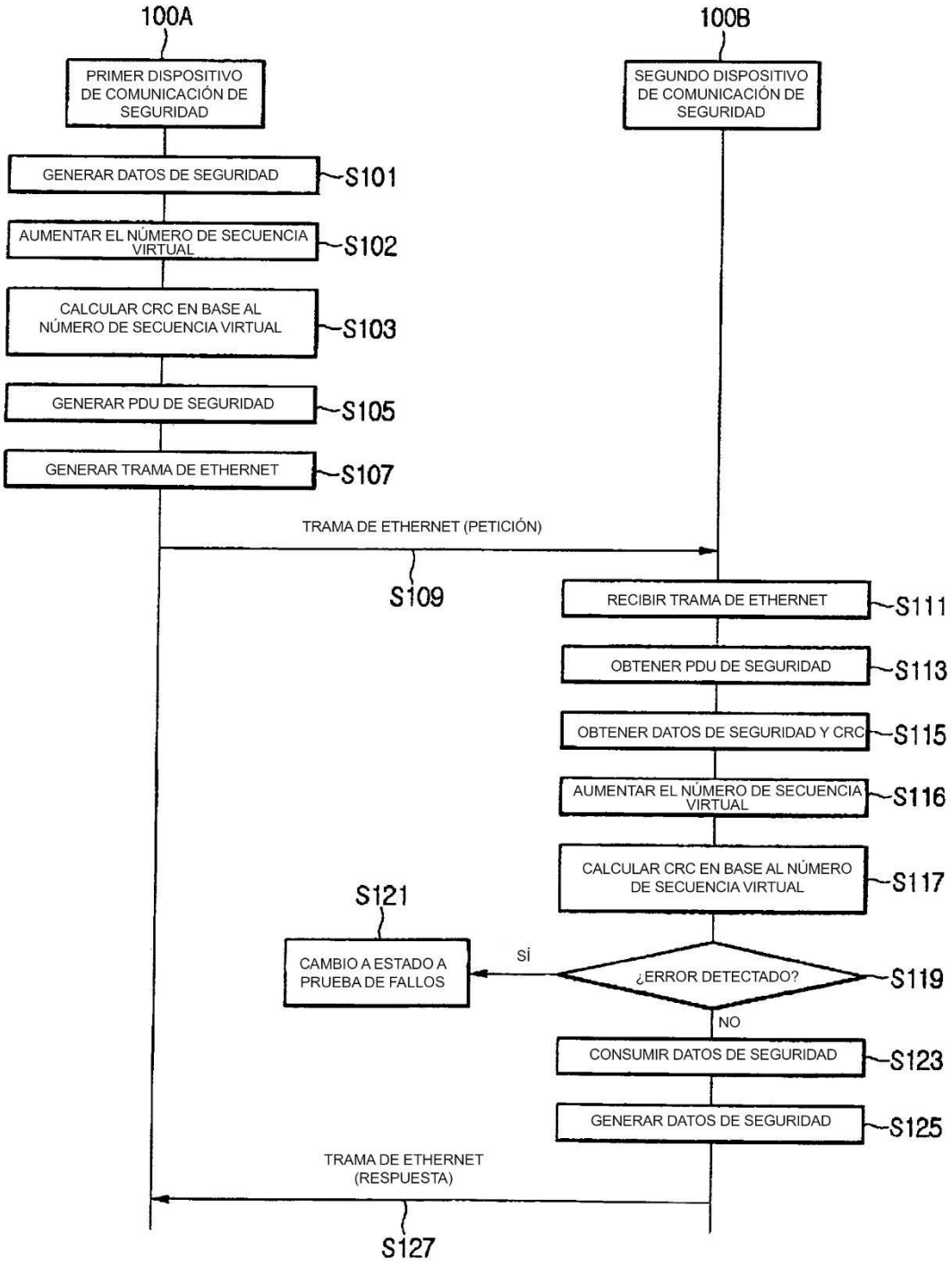

100A
PRIMER DISPOSITIVO DE COMUNICACIÓN DE SEGURIDAD
GENERAR DATOS DE SEGURIDAD
S101
AUMENTAR EL NÚMERO DE SECUENCIA VIRTUAL
S102
CALCULAR CRC EN BASE AL NÚMERO DE SECUENCIA VIRTUAL
S103
GENERAR PDU DE SEGURIDAD
S105
GENERAR TRAMA DE ETHERNET
S107
TRAMA DE ETHERNET (PETICIÓN)
S109
100B
SEGUNDO DISPOSITIVO DE COMUNICACIÓN DE SEGURIDAD
RECIBIR TRAMA DE ETHERNET
S111
OBTENER PDU DE SEGURIDAD
S113
OBTENER DATOS DE SEGURIDAD Y CRC
S115
AUMENTAR EL NÚMERO DE SECUENCIA VIRTUAL
S116
CALCULAR CRC EN BASE AL NÚMERO DE SECUENCIA VIRTUAL
S117
¿ERROR DETECTADO?
S119
SÍ
S121
CAMBIO A ESTADO A PRUEBA DE FALLOS
NO
CONSUMIR DATOS DE SEGURIDAD
S123
GENERAR DATOS DE SEGURIDAD
S125
TRAMA DE ETHERNET (RESPUESTA)
S127

Fig. 3

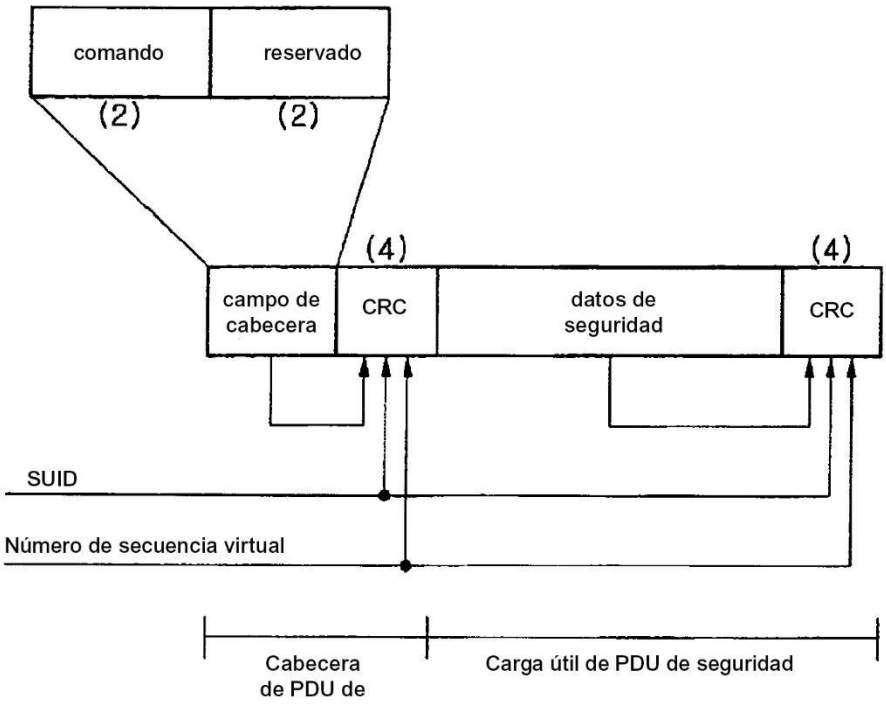

comando
reservado
(2)
(2)
(4)
(4)
campo de cabecera
CRC
datos de seguridad
CRC
SUID
Número de secuencia virtual
Cabecera de PDU de
Carga útil de PDU de seguridad

Fig. 4

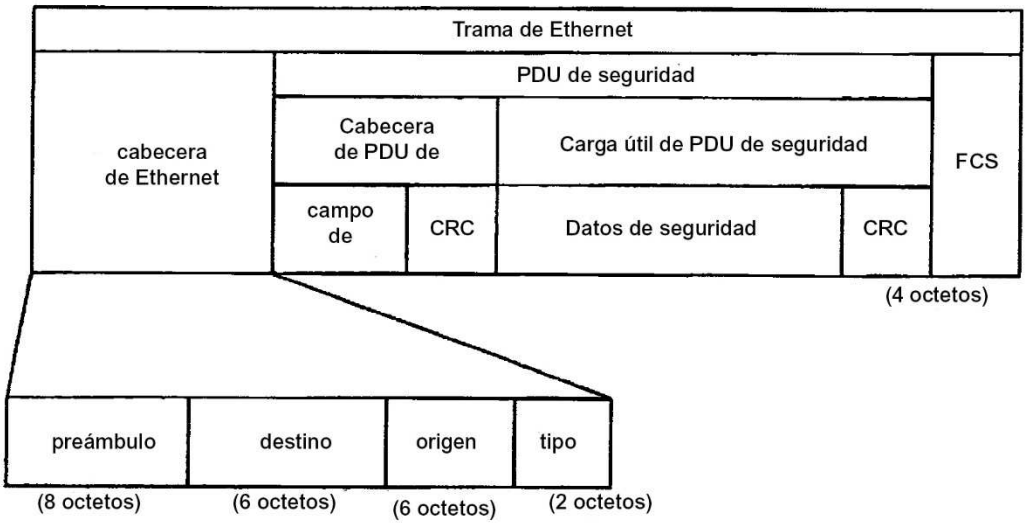

Trama de Ethernet
cabecera de Ethernet
PDU de seguridad
Cabecera de PDU de
Carga útil de PDU de seguridad
FCS
campo de
CRC
Datos de seguridad
CRC
(4 octetos)
preámbulo
destino
origen
tipo
(8 octetos)
(6 octetos)
(6 octetos)
(2 octetos)

Fig. 5

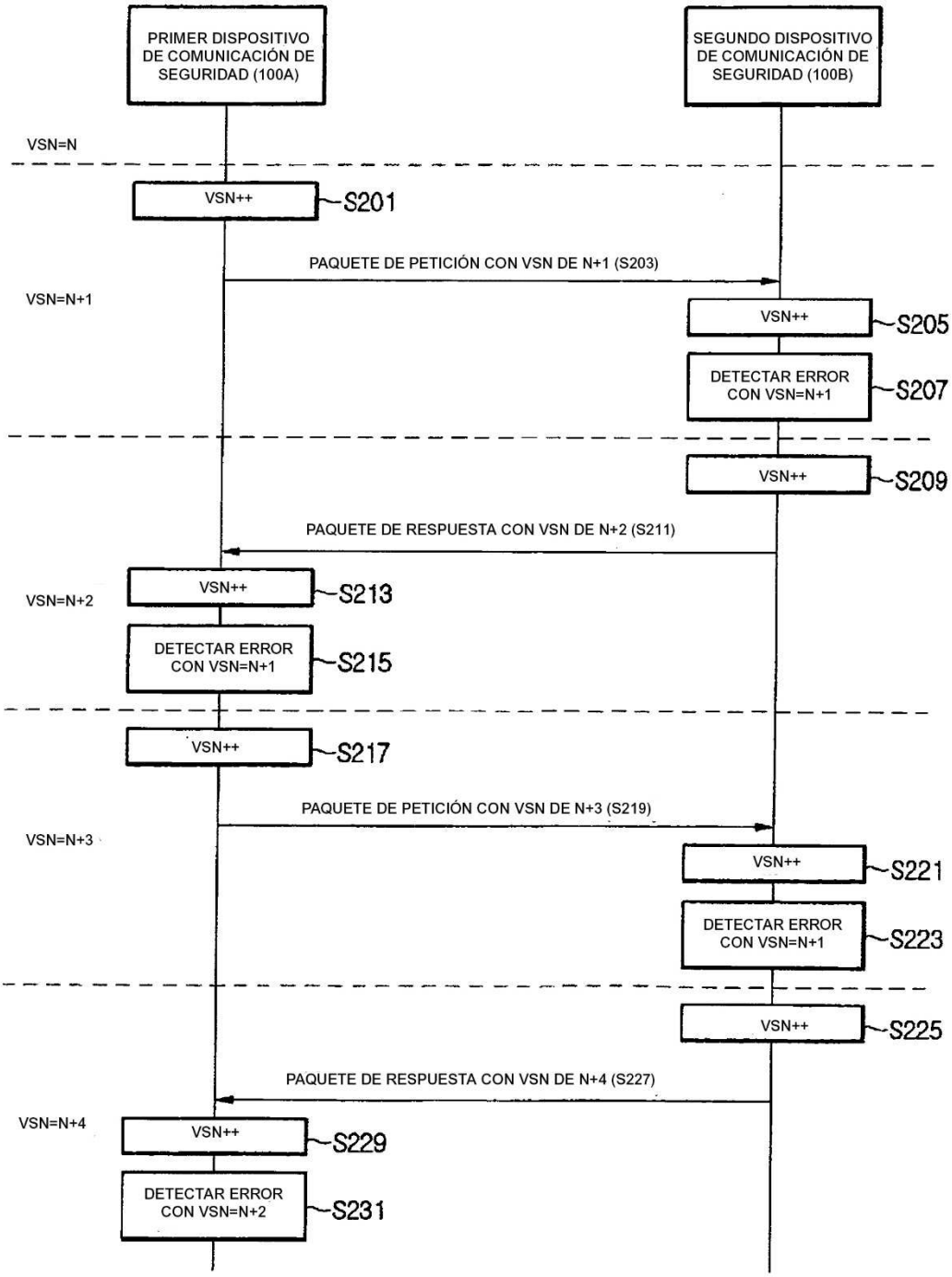
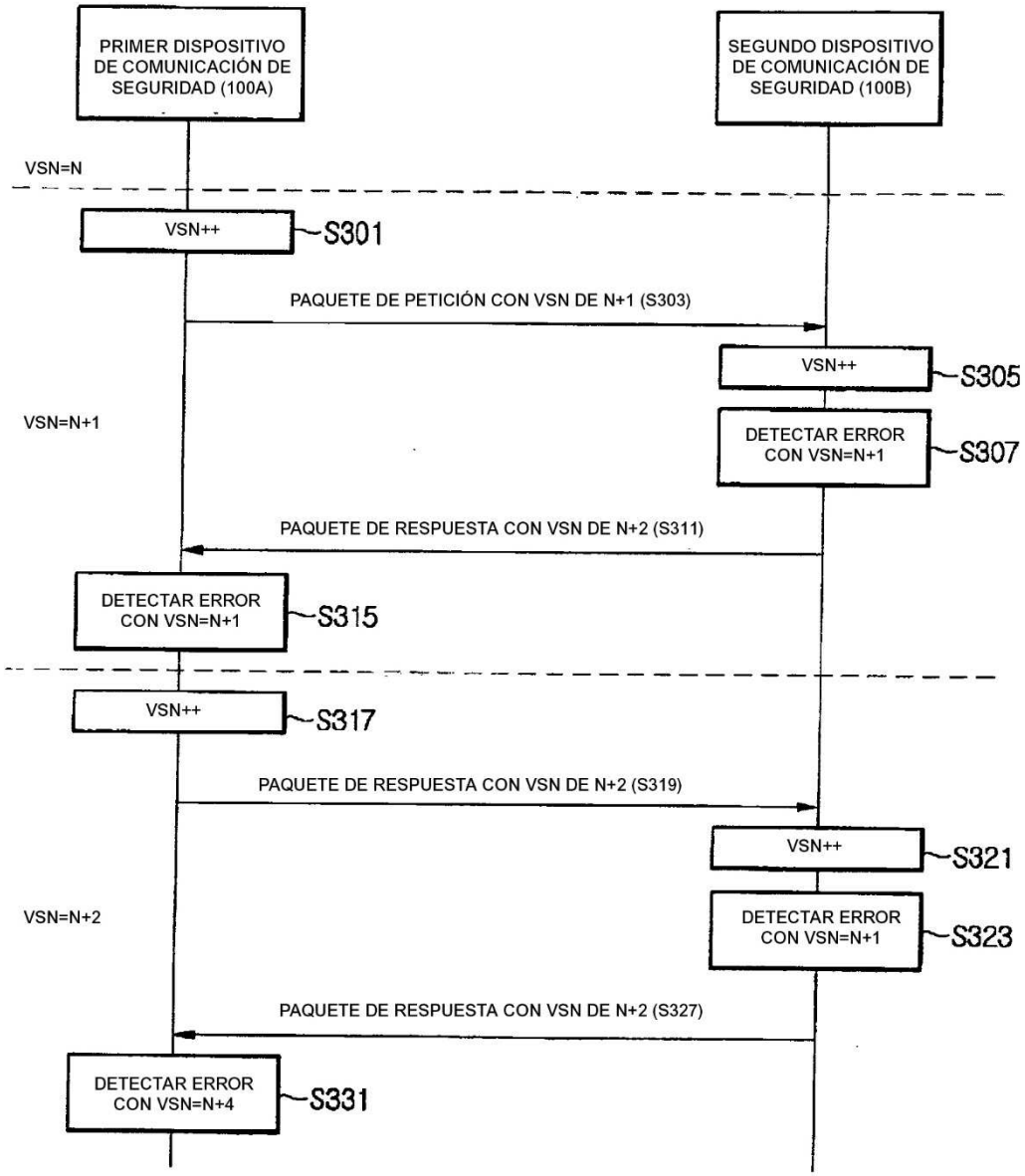

PRIMER DISPOSITIVO DE COMUNICACIÓN DE SEGURIDAD (100A)
SEGUNDO DISPOSITIVO DE COMUNICACIÓN DE SEGURIDAD (100B)
VSN=N
VSN++
S201
PAQUETE DE PETICIÓN CON VSN DE N+1 (S203)
VSN=N+1
VSN++
S205
DETECTAR ERROR CON VSN=N+1
S207
VSN++
S209
PAQUETE DE RESPUESTA CON VSN DE N+2 (S211)
VSN=N+2
VSN++
S213
DETECTAR ERROR CON VSN=N+1
S215
VSN++
S217
PAQUETE DE PETICIÓN CON VSN DE N+3 (S219)
VSN=N+3
VSN++
S221
DETECTAR ERROR CON VSN=N+1
S223
VSN++
S225
PAQUETE DE RESPUESTA CON VSN DE N+4 (S227)
VSN=N+4
VSN++
S229
DETECTAR ERROR CON VSN=N+2
S231

Fig. 6


PRIMER DISPOSITIVO DE COMUNICACIÓN DE SEGURIDAD (100A)
SEGUNDO DISPOSITIVO DE COMUNICACIÓN DE SEGURIDAD (100B)
VSN=N
VSN++
S301
PAQUETE DE PETICIÓN CON VSN DE N+1 (S303)
VSN++
S305
VSN=N+1
DETECTAR ERROR CON VSN=N+1
S307
PAQUETE DE RESPUESTA CON VSN DE N+2 (S311)
DETECTAR ERROR CON VSN=N+1
S315
VSN++
S317
PAQUETE DE RESPUESTA CON VSN DE N+2 (S319)
VSN++
S321
VSN=N+2
DETECTAR ERROR CON VSN=N+1
S323
PAQUETE DE RESPUESTA CON VSN DE N+2 (S327)
DETECTAR ERROR CON VSN=N+4
S331