(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 415 506**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.06.2010 E 10165325 (1)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2013 EP 2395404**

(54) Título: **Sincronización de reloj segura**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.07.2013

(73) Titular/es:

ABB RESEARCH LTD. (100.0%)
Affolternstrasse 44
8050 Zürich, CH

(72) Inventor/es:

KIRRMANN, HUBERT y
TOURNIER, JEAN-CHARLES

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Sincronización de reloj segura

Campo de la invención

La invención se refiere a sistemas de automatización industrial o sistemas de control de proceso, y en particular a sistemas de automatización de subestaciones, con una red de comunicaciones basada en Ethernet.

Antecedentes de la invención

Se usan ampliamente sistemas de control de proceso o automatización industriales para proteger, controlar y supervisar procesos industriales en plantas industriales, por ejemplo, para fabricar artículos, transformar sustancias, o generar potencia, con el fin de supervisar y controlar sistemas primarios extendidos como sistemas de suministro de potencia eléctrica, agua o gas o sistemas de telecomunicaciones, incluyendo sus subestaciones respectivas. Un sistema de automatización industrial tiene por lo general gran número de controladores de proceso distribuidos en una planta industrial o en un sistema primario extendido, e interconectados con comunicación mediante un sistema de comunicación.

Las subestaciones en redes de potencia de voltaje alto y medio incluyen dispositivos primarios tales como cables eléctricos, líneas, barras bus, conmutadores, transformadores de potencia y transformadores de medida, que por lo general están dispuestos en centros y/o zonas restringidas de conmutación. Estos dispositivos primarios son operados de forma automatizada mediante un sistema de automatización de subestaciones (SA). El sistema SA incluye dispositivos secundarios, denominados Dispositivos Electrónicos Inteligentes (IED), responsables de la protección, el control y la supervisión de los dispositivos primarios. Los IEDs pueden estar asignados a niveles jerárquicos, tal como el nivel de estación, el nivel de zona restringida, y el nivel de proceso, donde el nivel de proceso está separado del nivel de zona restringida por la denominada interfaz de proceso. El nivel de estación del sistema SA incluye una estación de trabajo de operador (OWS) con una Interfaz Humano-Máquina (HMI) y una puerta de enlace a un Centro de Control de Red (NCC). Los IEDs en el nivel de zona restringida, que también se pueden denominar unidades de zona restringida, están conectados, a su vez, uno a otro así como a los IEDs en el nivel de estación mediante un bus inter-zona restringida o estación que cumple la finalidad de intercambiar órdenes e información de estado.

Un estándar de comunicación para comunicación entre los dispositivos secundarios de una subestación se ha introducido como parte del estándar IEC 61850 titulado “redes y sistemas de comunicación en subestaciones”. Para mensajes no críticos en el tiempo, IEC 61850-8-1 especifica el protocolo de Especificación de Mensajes de Fabricación (MMS, ISO/IEC 9506) basado en una pila reducida de protocolos de Interconexión de Sistemas Abiertos (OSI) con el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP) en la capa de transporte y red, respectivamente, y Ethernet como medio físico. Para mensajes basados en eventos de tiempo crítico, IEC 61850-8-1 especifica los Eventos de Subestación Orientados a Objeto Genérico (GOOSE) directamente en la capa de enlace de Ethernet de la pila de comunicación. Para señales que cambian periódicamente muy rápidamente en el nivel de proceso tal como voltajes o corrientes analógicos medidos, IEC 61850-9-2 especifica el servicio de Valor Muestreado (SV), que como GOOSE se basa directamente en la capa de enlace de Ethernet. Por lo tanto, el estándar define un formato para publicar, como mensajes multidifusión en una Ethernet industrial, mensajes basados en eventos y datos de medición digitalizados a partir de sensores de corriente o voltaje en el nivel de proceso.

Con la introducción de IEC 61850, la sincronización de tiempo exacto en redes basadas en Ethernet para dispositivos secundarios en sistemas de control de proceso o automatización de subestaciones se ha convertido en un problema. Como un sustitutivo de la clásica señal Pulso Por Segundo PPS, IEC 61850 recomienda el uso de IEEE 1588 para lograr el grado de sincronización temporal requerido para datos críticos tales como señales SV o de disparo. IEEE 1588 puede funcionar en dos modos. En un modo de reloj de un paso, un reloj maestro envía un mensaje de sincronización y al mismo tiempo marca el tiempo del mensaje e introduce el sello de tiempo en el contenido del mismo mensaje. En un modo de reloj de dos pasos, el sello de tiempo no es transportado directamente en el mensaje de sincronización, sino en un mensaje de seguimiento.

Otro aspecto prominente en automatización de subestaciones es la mayor importancia dada a la ciberseguridad. Aunque los protocolos definidos por IEC 61850, tales como 8-1 y 9-2, están cubiertos por IEC 62351-6 para definir los mecanismos de seguridad requeridos, IEEE 1588 permanece sin protección. Uno de los problemas de asegurar IEEE 1588 es la incapacidad de asegurar el protocolo al usar un acercamiento de reloj de un paso. Es trivial asegurar un reloj de dos pasos, tanto con un esquema simétrico como asimétrico, dado que el mensaje de sincronización es un mensaje no sensible que nunca se modifica. Por otra parte, un acercamiento de reloj de paso único asegurado requiere asegurar el mensaje de sincronización al vuelo (mientras es enviado), y así es de implementación casi imposible (para un esquema asimétrico) o imposible (para un esquema simétrico o para una red de 1 Gbit/s).

La solicitud de patente EP 2148473 se refiere a aplicaciones de transmisión crítica o altamente disponibles en base a

una red de comunicaciones del tipo de anillo con una pluralidad de nodos de conmutación y que opera con enlaces dúplex completos. Un nodo emisor que está conectado en un primer y segundo puerto respectivo a la red de comunicaciones transmite pares de tramas redundantes. Para que cada trama sea enviada en la red anular, se transmiten una trama fuente y otra duplicada en direcciones opuestas, retardándose ambas tramas por los otros nodos de la red anular hasta que eventualmente vuelven al nodo emisor originante. Como consecuencia, la carga de la red es aproximadamente el doble con respecto a una red anular convencional, pero el nodo de destino recibirá los datos después de un retardo de transmisión máximo que es igual al recorrido más largo posible del anillo. En el estado sin fallo, el nodo de destino recibe así dos tramas redundantes con el mismo contenido. Las tramas redundantes pueden ser identificadas según un protocolo de redundancia paralela PRP, por lo tanto solamente la trama anterior o primera de las dos tramas es enviada a los protocolos de capa superior y la trama posterior o segunda es desechada. Dado que el mensaje de sincronización y el mensaje de seguimiento de un acercamiento de reloj de dos pasos pueden tomar recorridos o direcciones diferentes en HSR, se prefiere el uso de un reloj de un paso.

El documento “Practical Application of 1588 Security”, por Albert Treytl, Bernd Hirschler, IEEE International Symposium on Precise Clock Synchronization, Septiembre 2008, Ann Harbor, Estados Unidos de América, propone una forma de implementar un reloj de un paso seguro en el que a una parte estática del mensaje de sincronización se le aplica una función hash por adelantado. Entonces se produce el sello de tiempo y se incrusta en el mensaje, después de lo que la función hash se completa rápidamente en la parte restante del mensaje, es decir, el sello de tiempo. El inconveniente de este acercamiento es que solamente permite un esquema de protección simétrico que consume menos tiempo que el asimétrico. De hecho, la operación todavía se efectúa al vuelo, es decir, la aplicación de la función hash a la parte restante así como la firma, y por lo tanto es de tiempo crítico. Otro inconveniente es la limitación de este acercamiento a una red de 100 Mbit/s, dado que para 1 Gbit/s las operaciones de aplicación de función hash restantes no se completarán a tiempo.

Descripción de la invención

Por lo tanto, un objetivo de la invención es asegurar un reloj IEEE 1588 de paso único usando un esquema de protección simétrico o asimétrico. Este objetivo se logra con un método de sincronizar relojes y un dispositivo de reloj maestro según las reivindicaciones independientes. Realizaciones preferidas son evidentes a partir de las reivindicaciones de patente dependientes, donde la dependencia indicada de las reivindicaciones no se deberá interpretar como exclusión de combinaciones de reivindicaciones significativas adicionales.

Según la invención, los relojes de dispositivos de transmisión crítica o altamente disponibles en sistemas de automatización industrial conectados a una red de comunicaciones son sincronizados enviando, por un reloj maestro, un mensaje de sincronización, en particular un solo mensaje del reloj del tipo de un paso según IEEE 1588, incluyendo un sello de tiempo, y recibiendo y evaluando, por un reloj esclavo, el mensaje de sincronización. Un componente o módulo de sincronización del reloj maestro prepara, o compone, antes de un tiempo de envío previsto t_{send}, un mensaje de sincronización incluyendo un sello de tiempo del tiempo de envío previsto, y asegura el mensaje de sincronización con anterioridad al tiempo de envío previsto. Asegurar el mensaje de sincronización tiene lugar por medios criptográficos adecuados que permiten al menos la autenticación del sello de tiempo en un reloj esclavo receptor, por ejemplo calculando y firmando una suma de verificación o hash del mensaje de sincronización. El mensaje de sincronización asegurado se transmite en el tiempo de envío previsto.

En una realización ventajosa de la invención, el mensaje de sincronización asegurado se almacena en un componente de espera dedicado de un transmisor del dispositivo de reloj maestro antes de ser enviado en t_{send}.

En otra realización ventajosa de la invención, una cola de prioridad baja (LPQ) del transmisor es bloqueada y el envío de mensajes de no sincronización procedentes de la LPQ es inhabilitado durante un intervalo de bloqueo anterior a t_{send}. Un intervalo de bloqueo conservador correspondiente al mensaje más largo esperado en la LPQ asegura que no haya ningún mensaje en el proceso de ser transmitido en t_{send}. En una variante más sofisticada, la longitud de un mensaje procedente de la LPQ es verificada antes del envío con el fin de conocer la terminación de su transmisión antes de t_{send}. Por lo tanto, los mensajes de sincronización siempre serán transmitidos sin retardo o inestabilidad adicionales debidos a la transmisión en curso de mensajes de prioridad baja.

Preferiblemente, los dispositivos de reloj están dispuestos como nodos de conmutación en una red de comunicaciones del tipo de anillo que opera con enlaces dúplex completos, donde un nodo emisor que está conectado en un primer y un segundo puerto respectivo a la red de comunicaciones transmite pares de tramas redundantes. Para cada mensaje de sincronización a enviar en la red anular, se transmite un mensaje fuente y un mensaje de sincronización duplicado en direcciones opuestas, siendo retardados ambos mensajes por los otros nodos de la red anular hasta que eventualmente vuelven al nodo emisor originante. Dicha topología de red de comunicaciones redundante se emplea ventajosamente en sistemas de automatización industrial o sistemas de control de proceso, en particular en sistemas de automatización de subestaciones para subestaciones en redes de potencia eléctrica de voltaje alto y medio.

Breve descripción de los dibujos

La materia de la invención se explicará con más detalle en el texto siguiente con referencia a realizaciones ejemplares preferidas que se ilustran en los dibujos adjuntos, en los que:

La figura 1 ilustra una secuencia de operaciones para una implementación de un reloj de un paso seguro fuera del alcance de la presente invención.

La figura 2 ilustra una secuencia de operaciones modificada para un reloj de un paso seguro.

Y las figuras 3 y 4 ilustran arquitecturas de sistema correspondientes.

Descripción detallada de realizaciones preferidas

La figura 1 ilustra una secuencia de operaciones ejemplar, pero más bien inviable, requerida para una implementación directa de un reloj IEEE 1588 de un paso seguro. El problema principal asociado es la incapacidad de calcular todas las operaciones requeridas al vuelo. En particular, dicho reloj tendría que empezar a enviar el primer byte del mensaje de sincronización SINC, luego marcar el sello de tiempo de la operación, insertar el sello de tiempo en el mensaje, y finalmente aplicar la función hash y firmar el mensaje con el retardo de tiempo más corto posible.

La figura 2 ilustra una secuencia de operaciones ejemplar de un reloj de paso único IEEE 1588 seguro que prepara mensajes de sincronización con anterioridad. Esta invención propone preparar el mensaje de sincronización SINC para un sello de tiempo futuro, es decir, producir y embeber el sello de tiempo para un tiempo futuro $t_{send} = t_{prep} + \Delta t$, donde el tiempo t_{prep} designa el tiempo en el que empieza la preparación del mensaje de sincronización y se determina su sello de tiempo avanzado. Eligiendo con cuidado el intervalo de preparación o el retardo de avance Δt, se dispone de tiempo suficiente para realizar todas las operaciones necesarias antes de enviar la sincronización asegurada en el tiempo de envío previsto t_{send}.

La figura 3 representa la arquitectura de sistema correspondiente de una implementación típica de reloj de paso único. La responsabilidad última de la pila IEEE 1588 de nivel bajo es asegurar que el mensaje de sincronización sea enviado a tiempo, y la mejora propuesta se implementa en hardware para lograr la precisión de tiempo requerida. El nivel de hardware, o pila de nivel bajo, incluye un chip de circuito integrado (IC) dedicado o matriz de puertas programable in situ (FPGA), preferiblemente como parte de la tarjeta de interfaz de red (NIC) 10 del dispositivo, y ejecuta todos los aspectos de tiempo crítico del procedimiento de sincronización, es decir, aplicando el sello de tiempo en los mensajes IEEE 1588 SINC cuando son recibidos y enviados. Las puertas lógicas de la unidad de sello de tiempo (TSU) 11 son codificadas por medio de un lenguaje de programación bajo tal como VHDL. En un nivel de abstracción más alto, todos los aspectos de tiempo no crítico son implementados dentro de la pila IEEE 1588 regular 14, en el mismo chip dedicado o en la CPU 13 del dispositivo, estando éste último conectado a la TSU mediante un bus de comunicaciones ejemplar (por ejemplo PCI) 12. En este caso, la pila IEEE 1588 se ejecuta en la CPU como una implementación de software, mientras que solamente la operación de sello de tiempo se logra a nivel de hardware. La invención propuesta no implica ninguna modificación en la pila de software, sino solamente en la implementación lógica de la secuencia de pasos según la figura 2, es decir, al enviar un mensaje de sincronización.

La figura 4 ilustra finalmente la arquitectura detallada de una pila de nivel bajo que soporta el reloj IEEE 1588 de un paso asegurado formado con anterioridad. Los varios componentes se deberán entender desde un punto de vista de la arquitectura (es decir, en términos de ingeniería de software) como entidades que realizan una función y que tienen entradas y salidas. Como se ha mencionado anteriormente, desde un punto de vista de la implementación, un componente puede ser implementado como un componente VHDL (es decir, puertas dedicadas con alguna memoria) si se implementa en FPGA, pero también una función C u objeto Java si se implementa en software.

La lógica receptora ilustrada en la figura 4 no se modifica en comparación con una implementación normal de IEEE 1588 con soporte de hardware. Su finalidad es descodificar los mensajes recibidos de la red, y detectar la llegada de un mensaje de sincronización pidiendo que la TSU realice una operación de sello de tiempo. Igualmente, la lógica de transmisión detecta la presencia de un mensaje de sincronización exterior, que se origina, por ejemplo, en la CPU del dispositivo, y que pide igualmente una operación de sello de tiempo. La secuencia de operaciones representada en la figura 2 se implementa en los componentes SINC 20 y la espera 21. El primero es responsable de preparar, incluyendo recibir el sello de tiempo de la TSU, el mensaje de sincronización completamente asegurado, mientras que la última retiene el envío del mensaje hasta el tiempo de envío previsto t_{send}. El puerto de transmisión TX contiene dos colas, una cola de prioridad alta (HPQ) 21 dedicada a mensajes de sincronización seguros IEEE 1588 y una cola de prioridad baja (LPQ) 22 para mensajes de no sincronización. La HPQ 21 tiene la prioridad más alta, lo que significa que siempre que se ponga un mensaje en la cola, el mensaje será transmitido sin más retardo. No obstante, en el caso de que el transmisor acabe de empezar a enviar un mensaje de la LPQ 22, el envío del mensaje de sincronización se retarda [(sizeof(max_length_ethernet_packet) + interframe_gap) / network_speed). Esto da lugar a un retardo máximo de (1526x8+12x8)1(100Mbits/s)= 12,6 µs para una trama 802.3 MAC en una red de 100 M bit/s. Para evitar esta inestabilidad adicional no controlada, el componente de espera 21 tiene que bloquear o inhabilitar el envío de cualquier trama desde la LPQ en un intervalo de bloqueo Δ_{block} de 12 µs antes de t_{send}.

La opción del intervalo de preparación Δt depende de muchos parámetros tales como el hardware usado, el esquema de seguridad, la velocidad de la red, etc. Por ejemplo, la implementación VHDL de una función hash específica conocida como AES (estándar de encriptado avanzado) requiere entre 50 (alto rendimiento) y 106 (bajo rendimiento) ciclos de 20 ns (50 MHz) para aplicación de función hash de 6 bytes, dando lugar a un retardo de aproximadamente 33 µs o 70 µs para una trama de sincronización típica de 200 bytes de largo. En este caso, Δt debe ser al menos 33 µs o 70 µs más el retardo requerido para insertar el sello de tiempo en el mensaje de sincronización.

REIVINDICACIONES

1. Un método de sincronizar relojes conectados a una red de comunicaciones, incluyendo enviar, por un reloj maestro, un mensaje de sincronización incluyendo un sello de tiempo, y recibir el mensaje de sincronización por un reloj esclavo, incluyendo además

- preparar, antes de un tiempo de envío previsto t_{send}, un mensaje de sincronización incluyendo un sello de tiempo del tiempo de envío previsto t_{send},

- asegurar el mensaje de sincronización, y

- enviar, en el tiempo de envío previsto t_{send}, el mensaje de sincronización asegurado.

2. El método según la reivindicación 1, incluyendo

- almacenar, en un componente de espera (21), el mensaje de sincronización asegurado antes del envío en el tiempo de envío previsto t_{send}.

3. El método según la reivindicación 1, incluyendo

- inhabilitar, durante un intervalo de bloqueo A_{block} anterior al tiempo de envío previsto t_{send}, el envío de mensajes de no sincronización con una longitud que supera la longitud del intervalo de bloqueo A_{block}.

4. El método según la reivindicación 1, incluyendo

- iniciar la preparación del mensaje de sincronización asegurado en un tiempo t_{prep} precedente al tiempo de envío previsto t_{send} en Δt, donde Δt es un retardo de preparación en base a una capacidad de procesado de un hardware de procesado que genera el mensaje de sincronización.

5. El método según una de las reivindicaciones 1 a 4, donde la red de comunicaciones tiene una topología de aro y donde el reloj maestro pertenece a un dispositivo de reloj maestro con un primer y un segundo puerto de comunicación conectados respectivamente a un primer y un segundo nodo contiguo de la red de comunicaciones, incluyendo, por el dispositivo de reloj maestro,

- generar un mensaje de sincronización duplicado del mensaje de sincronización asegurado, y

- transmitir, de forma esencialmente simultánea mediante el primer y el segundo puerto, respectivamente, el mensaje de sincronización y el mensaje de sincronización duplicado al primer y segundo nodo contiguo.

6. El método según la reivindicación 5, donde los relojes esclavos pertenecen a Dispositivos Electrónicos Inteligentes IEDs de un sistema de control de proceso o automatización de subestaciones.

7. Un dispositivo de reloj maestro para sincronizar relojes esclavos conectados a una red de comunicaciones, configurado para preparar y enviar mensajes de sincronización incluyendo un sello de tiempo, **caracterizado** porque el dispositivo incluye

- un componente de sincronización (20) adaptado para preparar un mensaje de sincronización incluyendo un sello de tiempo de un tiempo de envío previsto t_{send} y para asegurar el mensaje de sincronización, y

- un componente de espera (21) adaptado para almacenar temporalmente el mensaje de sincronización asegurado hasta el tiempo de envío previsto t_{send}.

8. El dispositivo de reloj maestro según la reivindicación 7, **caracterizado** porque incluye un puerto de transmisión TX con una cola de prioridad baja LPQ (23), configurado de tal manera que, durante un intervalo de bloqueo A_{block} anterior al tiempo de envío previsto t_{send}, se inhabilite el envío de mensajes de no sincronización desde la LPQ con una longitud superior a la longitud del intervalo de bloqueo A_{block}.

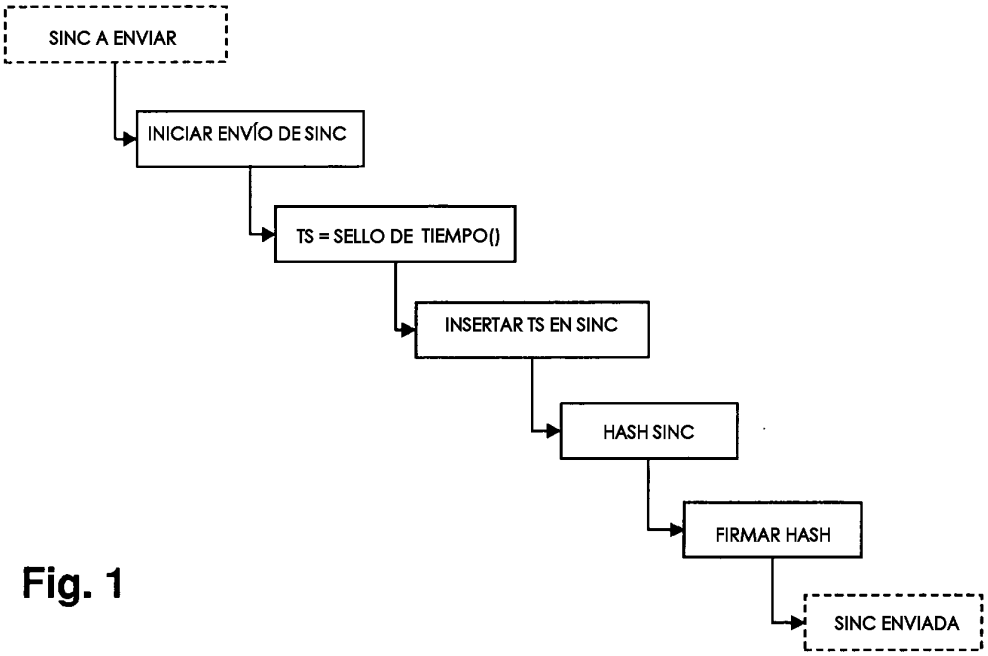

SINC A ENVIAR
INICIAR ENVÍO DE SINC
TS = SELLO DE TIEMPO()
INSERTAR TS EN SINC
HASH SINC
FIRMAR HASH
SINC ENVIADA

Fig. 1

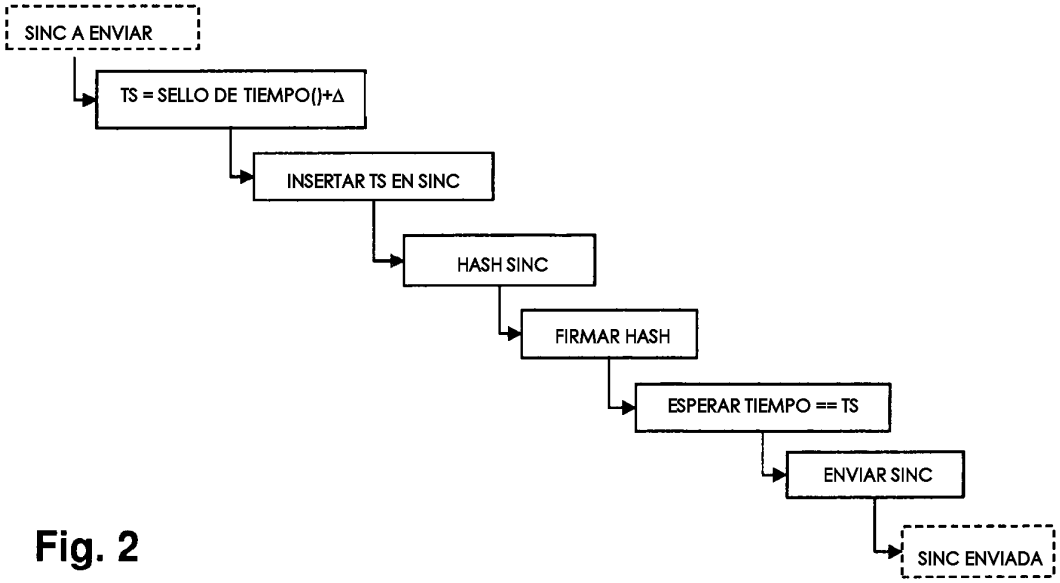

SINC A ENVIAR
TS = SELLO DE TIEMPO()+Δ
INSERTAR TS EN SINC
HASH SINC
FIRMAR HASH
ESPERAR TIEMPO == TS
ENVIAR SINC
SINC ENVIADA

Fig. 2

Fig. 3

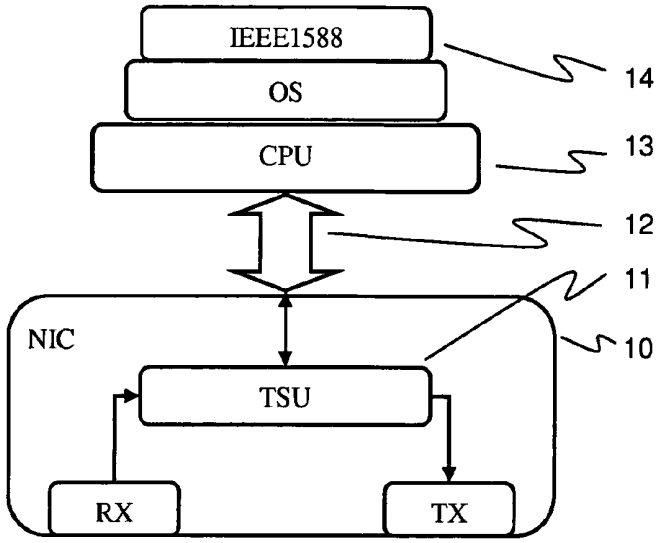
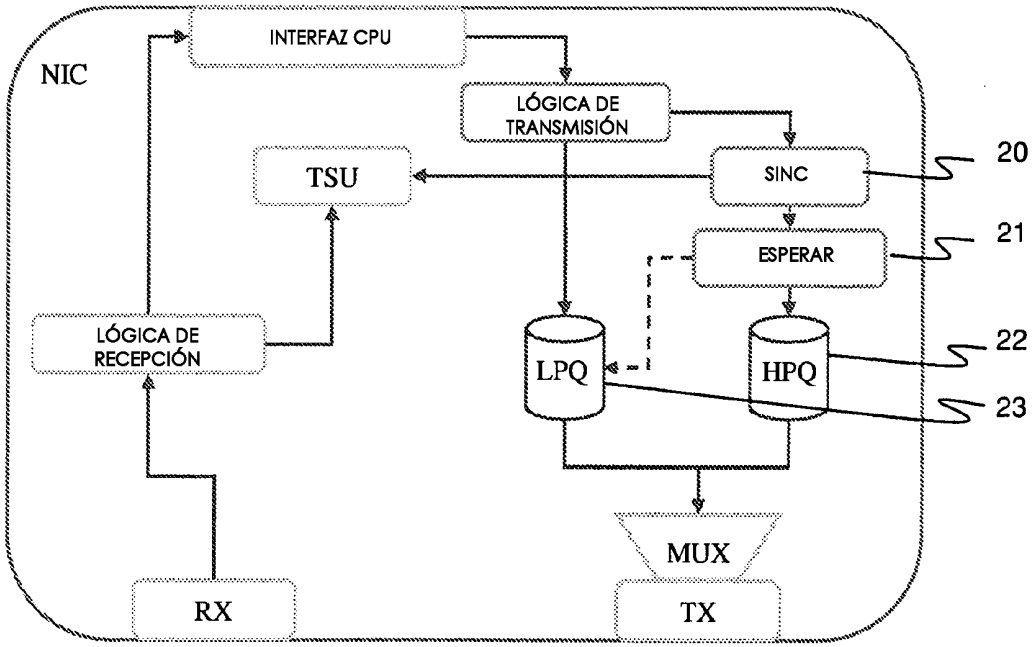

IEEE1588
OS
CPU
NIC
TSU
RX
TX
14
13
12
11
10

Fig. 4


NIC
INTERFAZ CPU
LÓGICA DE TRANSMISIÓN
TSU
SINC
ESPERAR
LÓGICA DE RECEPCIÓN
LPQ
HPQ
MUX
RX
TX
20
21
22
23