(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 717 230**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.09.2013 E 13182696 (8)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2018 EP 2706722**

(54) Título: **Control remoto de instalaciones seguras**

(30) Prioridad:

06.09.2012 US 201213604677

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2019

(73) Titular/es:

WATERFALL SECURITY SOLUTIONS LTD. (100.0%)
14 Hamelacha Street Afek Industrial Park Gav Yam Building, 1st Floor
Rosh HaAyin 4809133, IL

(72) Inventor/es:

FRENKEL, LIOR;
GINTER, ANDREW y
MAOR, TOMER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Control remoto de instalaciones seguras

La presente invención está relacionada de manera general con comunicaciones y control digitales y en concreto con sistemas y métodos para comunicaciones seguras.

En una red informática que maneja datos sensibles, partes de la red pueden estar conectadas mediante enlaces de datos unidireccionales. El término “enlace unidireccional” se utiliza en el contexto de la presente solicitud de patente y en las reivindicaciones para hacer referencia a un enlace de comunicación que está configurado físicamente para transportar señales en una dirección y para ser incapaz de transportar señales en la dirección contraria. Se pueden implementar enlaces unidireccionales, por ejemplo, utilizando sistemas Waterfall®, los cuales son fabricados por Waterfall Security Solutions, Ltd. (Rosh HaAyin, Israel). El sistema Waterfall proporciona una conexión unidireccional física basada en comunicación por fibra óptica, utilizando un protocolo de transferencia propietario subyacente. Cuando un ordenador transmisor está conectado mediante un sistema Waterfall (u otro enlace unidireccional) a un ordenador receptor, el ordenador receptor puede recibir datos procedentes del ordenador transmisor, pero no tiene ningún medio físico de enviar ninguna comunicación de retorno al ordenador transmisor.

Los enlaces unidireccionales se pueden utilizar para impedir que entren o salgan datos de una instalación protegida. Por ejemplo, datos confidenciales a los que no se debe acceder desde sitios externos pueden estar almacenados en un ordenador que está configurado para recibir datos a través de un enlace unidireccional y no tiene ningún enlace saliente físico a través del cual se podrían transmitir datos a un sitio externo. Por otro lado, en algunas aplicaciones, el operador de la instalación protegida puede estar preparado para permitir que salgan datos de la instalación libremente a través de un enlace unidireccional, impidiendo al mismo tiempo que entren datos en la instalación a fin de detener a los piratas informáticos y a los ciberterroristas.

En esta última categoría, por ejemplo, la Patente de EE.UU. 7.649.452 describe protección de redes de control utilizando un enlace unidireccional. Como se describe en esta patente, un método para monitorizar un proceso incluye recibir una señal procedente de un sensor que es indicativa de un atributo físico asociado con el proceso y transmitir datos indicativos de la señal recibida a través de un enlace unidireccional. Los datos transmitidos recibidos desde el enlace unidireccional se utilizan en la monitorización del proceso. El método se describe en la patente concretamente en el contexto de sistemas de Control de Supervisión y Adquisición de Datos (SCADA, del inglés Supervisory Control And Data Acquisition). Un sistema SCADA recibe datos de monitorización procedentes de la instalación monitorizada a través de un enlace unidireccional. El sistema SCADA es incapaz de transmitir ningún tipo de datos de vuelta a la instalación monitorizada (aunque para este fin se puede proporcionar una conexión independiente, en bucle abierto), y por lo tanto no se puede utilizar como base para un ataque a la instalación.

El documento WO-A-2009/053990 describe un aparato de detección que incluye una cámara de red, la cual está configurada para capturar imágenes de una escena y proporcionar como salida una secuencia de paquetes de datos que contienen datos de video digitalizados en respuesta a las imágenes. Un enlace unidireccional está acoplado a la cámara de red para transmitir los paquetes de datos desde la cámara de red hasta una red de comunicación de paquetes.

Realizaciones de la presente invención que se describen más adelante en esta memoria proporcionan aparatos y métodos para controlar de forma automática entradas a un destino protegido. Por lo tanto se proporciona, en conformidad con un aspecto de la presente invención, un aparato de comunicación y un método para comunicación como se expone en las reivindicaciones independientes. Las realizaciones preferidas se establecen en las reivindicaciones dependientes.

En una realización, el aparato de comunicación incluye un relé de datos unidireccional, accionado por hardware, que incluye una primera interfaz hardware configurada para recibir una orden procedente de una red de comunicaciones y una segunda interfaz hardware configurada para transportar la orden recibida hasta un destino protegido cuando se acciona el relé. Un decodificador incluye una tercera interfaz hardware configurada para recibir una firma digital para la orden procedente de la red de comunicaciones y lógica de decodificación hardware acoplada para verificar la firma digital y para accionar el relé tras verificar la firma digital, por lo cual la orden es transportada a través de la segunda interfaz hardware hasta el destino protegido.

En una realización, el aparato incluye un enlace unidireccional, el cual es diferente e independiente del relé unidireccional y está configurado para transportar datos de salida desde el destino protegido hasta la red de comunicaciones pero es físicamente incapaz de transportar datos de entrada desde la red de comunicaciones hasta el destino protegido.

En una realización descrita, el destino protegido es una estación de control de servicio público, y la orden está configurada para controlar una configuración operativa de la estación.

En algunas realizaciones, el aparato incluye una estación de transmisión, la cual incluye lógica de codificación hardware, la cual está configurada para generar la firma digital para la orden para identificar una fuente de la orden. Un procesador de comunicaciones está configurado para transmitir la firma digital a través de la red a la tercera

interfaz hardware, y para enviar la orden a través de la red desde la fuente de la orden hasta la primera interfaz hardware. La lógica de codificación hardware puede estar contenida en una unidad de autenticación del usuario, la cual está configurada para autenticar una identidad de un usuario de la estación de transmisión antes de generar la firma digital.

En una realización descrita, el aparato incluye lógica hardware, la cual está acoplada entre las interfaces hardware primera y segunda para recibir la orden procedente de la primera interfaz, para comparar la orden recibida con un conjunto de máscaras hardware correspondientes a órdenes permitidas, y para pasar la orden recibida a la segunda interfaz sólo cuando la orden recibida coincide con una de las máscaras.

En una realización, el aparato de comunicación incluye una primera interfaz hardware configurada para recibir una orden procedente de una red de comunicaciones y una segunda interfaz hardware configurada para transportar la orden recibida hasta un destino protegido. Entre las interfaces primera y segunda está acoplada lógica hardware para recibir la orden procedente de la primera interfaz, para comparar la orden recibida con un conjunto de máscaras hardware correspondientes a órdenes permitidas, y para pasar la orden recibida a la segunda interfaz sólo cuando la señal recibida coincide con una de las máscaras.

En una realización descrita, las órdenes permitidas tienen un formato de datos predefinido de tal manera que cada orden permitida consiste en un nombre y un valor permitido asociado con el nombre. En una realización, el destino protegido es una estación de control de servicio público, y el aparato incluye un monitor, el cual está acoplado para recibir la orden recibida de la segunda interfaz y para decodificar la orden recibida a partir del formato de datos predefinido a un protocolo de comunicaciones entre centros de control para entrada a la estación de control de servicio público. El aparato puede incluir una estación de transmisión, la cual está configurada para recibir una entrada en conformidad con el protocolo de comunicaciones entre centros de control desde una fuente de órdenes y para codificar la entrada en conformidad con el formato de datos predefinido para transmisión a través de la red a la primera interfaz.

En una realización, el método para comunicación incluye acoplar un relé accionado por hardware, unidireccional, para recibir una orden procedente de una red de comunicaciones y transportar la orden recibida hasta un destino protegido cuando se acciona el relé. Se recibe una firma digital procedente de la red de comunicaciones y se verifica utilizando lógica de decodificación hardware. Tras verificar la firma digital, se acciona el relé, con lo cual la orden es transportada hasta el destino protegido.

En una realización adicional, el método para comunicación incluye recibir una orden dirigida a un destino protegido procedente de una red de comunicaciones. La orden recibida se compara con un conjunto de máscaras hardware correspondientes a ordenes permitidas. La orden recibida se pasa al destino protegido sólo cuando la orden recibida coincide con una de las máscaras hardware.

La presente invención se entenderá más totalmente a partir de la siguiente descripción detallada de las realizaciones de la misma, tomada junto con los dibujos, en los cuales:

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra de forma esquemática un sistema para monitorización y control seguros, en conformidad con una realización de la presente invención;

La Figura 2 es un diagrama de bloques que muestra de forma esquemática elementos funcionales de un sistema para control seguro de un destino protegido, en conformidad con una realización de la presente invención;

La Figura 3 es un diagrama de bloques que muestra de forma esquemática elementos funcionales de un sistema para control seguro de un destino protegido, en conformidad con otra realización de la presente invención;

La Figura 4 es un diagrama de bloques que muestra detalles de un controlador de enlace ascendente seguro, en conformidad con una realización de la presente invención; y

La Figura 5 es un diagrama de bloques que ilustra de forma esquemática un sistema de comunicación seguro basado en proxy, en conformidad con una realización de la presente invención;

Descripción detallada de realizaciones

A diferencia de los cortafuegos convencionales, los enlaces unidireccionales permiten que la información salga de una instalación protegida sin riesgo para la seguridad o disponibilidad de la red existente en la instalación debido a ataques que se originen en una red externa. En la práctica, sin embargo, existe a veces una necesidad de transmitir al menos pequeñas cantidades de información desde una red externa de vuelta al interior de la instalación protegida.

Existen varios riesgos asociados con estas comunicaciones. Un riesgo es que si de alguna manera se ha introducido software malicioso en la red protegida (posiblemente por colaboración de un infiltrado), las comunicaciones que vuelven al interior de la red protegida se podrían utilizar para desencadenar un ataque. Por ejemplo, el software malicioso podría hacer que un ordenador de dentro de la instalación reconociera una cierta cadena enviada de

vuelta al interior de la red protegida como una orden para iniciar alguna acción dañina. Otro riesgo es que un atacante podría utilizar el canal de comunicaciones hacia el interior de la instalación para provocar condiciones inseguras o poco fiables en la red protegida, por medio de un ataque de desbordamiento de búfer, por ejemplo. Un ataque de este tipo se podría utilizar entonces para introducir software malicioso de control remoto en el interior de la red protegida, y proporcionar a un atacante los medios para explorar y sabotear de manera interactiva la red protegida.

Realizaciones de la presente invención que se describen más adelante en esta memoria tratan estos riesgos permitiendo un flujo controlado de pequeñas cantidades de información hacia el interior de una red protegida. El flujo se controla automáticamente de modo que ataques basados en software sobre equipo protegido resultan difíciles o imposibles de llevar a cabo, incluso si partes de la propia orden y del propio sistema de comunicaciones resultan comprometidos. A diferencia de los cortafuegos convencionales, el control es llevado a cabo por lógica hardware, en lugar de software. Por consiguiente, los atacantes remotos son incapaces de modificar la configuración operativa de la lógica de protección o hacer que realice cualquier función diferente a las programadas inicialmente por el diseñador de la lógica. En las realizaciones descritas, la lógica hardware está configurada para controlar el formato y contenido de órdenes que se pueden enviar a un destino protegido. La lógica hardware también puede autenticar estas órdenes para garantizar que fueron producidas por un transmisor autorizado. Como resultado, comprometiendo a un transmisor autorizado, un atacante puede, en el peor de los casos, ser capaz de enviar una orden incorrecta al destino, pero no podrá obtener control sobre la instalación protegida.

Algunas realizaciones de la presente invención utilizan el concepto de un relé - hardware de datos que recibe y almacena un conjunto de órdenes de entrada digitales que son enviadas desde un conjunto de interfaces hardware de fuente y que están dirigidas a hardware informático de destino, una o más redes o una o más CPUs. Cuando se dispara el relé, las entradas son transferidas a las salidas del relé de datos y por tanto se ponen a disposición de interfaces hardware de destino del hardware informático de destino, de las una o más CPUs o de las una o más redes. Un componente hardware de autenticación opcional, tal como un decodificador de firma digital, puede estar configurado para disparar el relé de datos cuando se encuentra que la información de autenticación, tal como una firma digital, coincide con las órdenes de entrada digitales en el área de almacenamiento del relé de datos. Un componente de hardware de filtrado opcional, el cual puede ser parte del relé de datos, permite movimiento de las órdenes desde las interfaces de entrada hasta interfaces de salida si y sólo si las órdenes coinciden con una máscara hardware o lista blanca de órdenes permitidas.

Como se ha indicado anteriormente, los relés de datos de este tipo pueden ser particularmente útiles en conjunto con enlaces unidireccionales, por ejemplo en situaciones en las que se permite que fluya libremente información fuera de una instalación a través de un enlace unidireccional, mientras que el flujo de órdenes hacia el interior de la instalación está estrictamente controlado. Sin embargo, Los principios de tales relés de datos y proxies de comunicación segura que se describen en esta memoria, no están limitados de ninguna manera a este tipo de entorno operativo y se pueden utilizar con o sin un enlace unidireccional, dependiendo de requisitos del sistema y de la aplicación.

La Figura 1 es un diagrama de bloques que ilustra de forma esquemática un sistema 20 para monitorización y control seguros en conformidad con una realización de la presente invención. En este ejemplo, se utiliza un sistema 20 para monitorizar y controlar un sistema de control industrial en una estación 22 de control de servicio público, tal como por ejemplo una estación de transmisión y conmutación de una instalación de energía eléctrica. Aunque para mayor simplicidad, en la Figura 1 sólo se muestra una única estación 22, en la práctica los servicios públicos generalmente operan muchas estaciones de este tipo. La estación 22 comprende típicamente elementos operacionales, tales como interruptores 24, los cuales cierran y abren conexiones de alimentación. En muchos sistemas reales, las estaciones 22 son no atendidas, y los interruptores 24 son controlados de manera remota por estaciones de transmisión de órdenes, tales como un terminal 32 de control, por ejemplo.

Aunque el ejemplo representado está relacionado, a modo de ilustración, con una instalación de energía eléctrica, los principios de la presente invención no están limitados a este contexto operativo concreto. En lugar de esto, el aparato y los métodos que se describen más adelante se pueden aplicar a instalaciones de otros tipos (tales como instalaciones de gas o de agua, por ejemplo), así como en entornos industriales y substancialmente cualquier otra aplicación en la cual se deba ejercer un control estrecho sobre órdenes que se pueden proporcionar como entrada a un destino protegido. La estación 22 es sólo un ejemplo de un destino de este tipo, el cual se presenta aquí para mayor claridad de explicación. Algunas realizaciones de la presente invención se describen más adelante en esta memoria, para mayor claridad y sin limitación, con respecto a los elementos del sistema 20, pero los principios de estas realizaciones y las técnicas que ellas incorporan se pueden aplicar de manera similar en otros entornos operativos en los cuales se debe proteger un destino frente a entrada de datos no deseados y acceso no autorizado.

La estación 22 está diseñada típicamente como una instalación cerrada, segura, protegida físicamente contra entradas no autorizadas. Un monitor 26 en la estación 22 proporciona como entradas órdenes a los interruptores 24 y monitoriza el funcionamiento de los interruptores y otros componentes de la estación.

Típicamente, el monitor 26 comprende múltiples sensores y actuadores, los cuales están distribuidos por toda la estación 22 y reportan a través de una red interna segura a un controlador (no mostrado), como se describe, por

ejemplo, en la Patente de EE.UU. 7.649.452 mencionada anteriormente. El monitor 26 proporciona como salida datos recogidos de los sensores y actuadores a través de un enlace unidireccional 28 a una red 30, la cual transporta los datos hasta terminales 32. La red 30 puede comprender cualquier red conectada por cables o inalámbrica apropiada, o una combinación de redes de estos tipos, incluidas redes públicas, tales como la Internet.

El enlace unidireccional 28 transporta datos de salida desde la estación 22 hasta la red 30 pero es físicamente incapaz de transportar datos de entrada desde la red hasta la estación. Para este último propósito, la estación 22 comprende un controlador 34 de enlace ascendente, el cual típicamente tiene una interfaz acoplada a la red 30 y otra interfaz acoplada a los elementos protegidos de la estación. En este ejemplo, el controlador 34 proporciona como entrada órdenes al monitor 26, el cual a continuación acciona interruptores 24 para llevar a cabo las órdenes, El controlador 34 de enlace ascendente comprende lógica hardware, la cual autentica las órdenes que se proporcionan como entrada al monitor 26 y limita los tiempos, las cantidades, y/o el contenido de estas órdenes, como se describe con mayor detalle más adelante en esta memoria. El monitor 26 no recibe ninguna entrada procedente de la red 30 aparte de a través del controlador 34 de enlace ascendente, el cual está típicamente contenido en la estación 22 y por lo tanto está él mismo protegido frente a manipulación física y eléctrica.

Órdenes iniciadas por un operador del terminal 32 (o posiblemente iniciadas de manera autónoma por el propio terminal) son formateadas por un procesador 36, el cual típicamente comprende un procesador informático de propósito general que ejecuta software estándar. Las órdenes se pueden formular en conformidad con un protocolo estándar, tal como el protocolo de comunicaciones entre centros de control (ICCP), como es conocido en la técnica. Un codificador 38 seguro opera en conjunto con el procesador 36 para transmitir entradas al controlador 34 de enlace ascendente en la forma correcta, autenticada. Típicamente (aunque no necesariamente), el codificador 38 también comprende lógica hardware, para impedir que un atacante imite u obtenga control sobre las funciones de codificación. Sin embargo, incluso si un atacante obtiene control sobre el codificador 38, el daño que él o ella será capaz de hacer a la estación 22 estará generalmente limitado a la introducción de órdenes incorrectas (como por ejemplo configuraciones incorrectas de interruptores 24), ya que otras órdenes son bloqueadas por la lógica de protección en el controlador 34 de enlace ascendente.

La Figura 2 es un diagrama de bloques que muestra de forma esquemática elementos funcionales del sistema 20, en conformidad con una realización de la presente invención. En esta realización, el terminal 32 comprende una fuente 40 de órdenes, típicamente en forma de software que se ejecuta en el procesador 36, la cual genera una entrada de orden en un formato convencional (tal como ICCP) o cualquier formato propietario apropiado. Un codificador 42 hardware, el cual puede estar implementado en el codificador 38, codifica la entrada de orden en conformidad con un formato de datos predefinido que es soportado por el controlador 34 de enlace ascendente. Este formato define una sintaxis de órdenes permitidas, y puede especificar, por ejemplo, que cada orden permitida consiste en un nombre de parámetro y un valor asociado con el nombre. Los nombres y valores se seleccionan de listas limitadas, predefinidas, de nombres y valores permitidos. Entradas de orden procedentes de la fuente 40 que se pueden expresar de esta manera son aceptadas y codificadas por el codificador 42, mientras que órdenes que intentan invocar a otras funciones dentro de la estación 22, incluso si están compuestas legalmente en el formato de órdenes convencional, pueden ser rechazadas. Típicamente, el codificador 42 hardware está implementado en lógica conectada por cables o programable y no incluye ningún componente accionado por software, tal como una unidad central de proceso (CPU). El codificador hardware puede codificar las órdenes utilizando técnicas de encriptado fuerte y autenticación criptográfica, de modo que el controlador 34 de enlace ascendente puede distinguir órdenes procedentes de una fuente auténtica de otras órdenes y ataques.

Una interfaz 44 de comunicación del terminal 32 genera una corriente de comunicación que contiene la orden codificada para su transmisión a través de la red 30 hasta la estación. La interfaz 44 puede, por ejemplo, establecer una conexión segura (tal como una conexión encriptada de Seguridad de la Capa de Transporte [TLS, del inglés Transport Layer Security], como es conocida en la técnica) con una interfaz 46 de comunicación correspondiente de controlador 34 de enlace ascendente. Este tipo de medida de seguridad de datos convencionales añade una capa de protección adicional al funcionamiento de la lógica hardware dedicada.

La interfaz 46 de comunicación pasa órdenes que recibe a la lógica 48 de decodificación de hardware, la cual como el codificador 42 típicamente no contiene ninguna CPU u otros componentes accionados por software. Como el codificador 42, el decodificador 48 puede ser parte de una unidad 49 decodificadora hardware/software. La lógica 48 puede autenticar órdenes recibidas, y aceptar sólo órdenes auténticas. La lógica 48 decodifica órdenes aceptadas y compara cada una de estas órdenes con un conjunto de máscaras hardware predefinidas correspondientes a órdenes permitidas (tales como parejas permitidas de nombres y valores, como se ha descrito anteriormente). Las órdenes que coinciden con una de las máscaras se hacen pasar a través de un destino 50 de órdenes, tal como el monitor 26. Asumiendo que el monitor 26 comprende componentes estándar, la unidad 49 decodificadora puede decodificar estas órdenes devolviéndolas a un formato convencional, tal como ICCP, al cual están programados para responder estos componentes. El decodificador 48 rechaza órdenes que no coinciden con ninguna de las máscaras hardware predefinidas. Como resultado, sólo órdenes que invocan ciertas acciones permitidas, predefinidas, en la estación 22 alcanzarán el monitor 26, mientras que órdenes mal formadas o peligrosas que pudieran ser utilizadas para montar un ataque son bloqueadas. La Figura 3 es un diagrama de bloques que muestra de forma esquemática elementos funcionales del sistema 20, en conformidad con otra realización de la presente invención. Esta realización se puede utilizar junto con la realización de la Figura 2 o con independencia de ella, dependiendo de las

necesidades de seguridad. En esta realización, el terminal 32 comprende una unidad 52 de autenticación hardware, la cual puede estar comprendida (funcionalmente y/o físicamente) en el codificador 38. La unidad 52 comprende lógica de codificación hardware, la cual genera una firma digital para identificar la fuente de las órdenes. La firma digital se puede generar, por ejemplo, utilizando métodos de encriptado asimétrico que son conocidos en la técnica, o utilizando cualquier otra técnica apropiada. El procesador 36 genera órdenes para la estación 22, y la interfaz 44 de comunicación transmite estas órdenes junto con la firma digital a través de la red 30 hasta la estación 22.

La unidad 52 de autenticación puede comprender una unidad enchufable de autenticación de usuario, la cual genera la firma digital sólo después de autenticar la identidad del operador del terminal 32 que está introduciendo las órdenes. Para este fin, la unidad 52 puede comprender, por ejemplo, una memoria segura con una clave secreta y circuitos de encriptado para generar la firma digital, como es conocido en la técnica. Para mayor seguridad, la unidad 52 puede comprender un teclado para introducción de una contraseña por parte del usuario y/o un dispositivo de identificación biométrico, tal como un lector de huellas dactilares. De forma adicional o alternativa, la unidad 52 puede incluir una marca temporal y/o un número de secuencia en las firmas que genera para desbaratar ataques repetitivos.

El controlador 34 de enlace ascendente tiene dos interfaces con la red 30: una interfaz 46 de comunicación, la cual recibe las firmas digitales generadas por la unidad 52 de autenticación, y una interfaz de entrada con un relé 56 accionado por hardware, unidireccional, que recibe las órdenes generadas por el procesador 36. Las dos interfaces pueden ser interfaces físicas diferentes o simplemente puertos diferentes en una única interfaz física. La interfaz 46 pasa las firmas digitales a un decodificador 54, que comprende lógica de decodificación hardware, el cual verifica la firma digital. Tras verificar que la firma es correcta y auténtica, el decodificador 54 acciona el relé 56, de modo que la orden enviada por el procesador 36 es transportada a través del relé hasta el monitor 26.

De esta manera, la orden proporcionada como entrada al monitor 26 está abierta sólo durante periodos de tiempo cortos, controlados. Todas las transmisiones fuera de estos periodos (procedentes del terminal 32 o de otras fuentes) son bloqueadas. Debido a que el decodificador 54 y el relé 56 están implementados en hardware, el cual está situado dentro del entorno protegido de la estación 22, es esencialmente imposible puentear su funcionalidad de bloqueo por medio de un ataque software. Los periodos de tiempo durante los cuales se acciona el relé 56 pueden ser cortos (típicamente menores de 10 segundos, y posiblemente menores de 1 segundo, por ejemplo), y la cantidad de datos que se permite que pasen cada vez que el relé se abre puede estar restringida a un cierto número de bytes. Por consiguiente, incluso si un atacante es capaz de obtener control de la unidad 52 de autenticación, su capacidad para interactuar a través del controlador 34 de enlace ascendente con otros elementos de la estación 22 seguirá siendo muy limitada. Las funciones de conmutación del decodificador 54 y del relé 56 se pueden combinar con la función de enmascaramiento de la realización de la Figura 2 para una seguridad todavía mayor.

La Figura 4 es un diagrama de bloques que muestra de forma esquemática detalles del controlador 34 de enlace ascendente, en conformidad con una realización de la presente invención. En esta implementación, el controlador de enlace ascendente comprende una parte 60 abierta y una parte 62 a prueba de manipulaciones, segura. La interfaz 46 de comunicación, la cual comprende un componente hardware apropiado tal como una interfaz Ethernet, recibe y pasa paquetes de datos entrantes procedentes de la red 30 a un microcontrolador 64 externo (no seguro), tal como una unidad de procesamiento ARM9 con una memoria 66 para su procesamiento inicial. El microcontrolador 64 pasa las firmas digitales a través de un enlace unidireccional a la lógica 54 de decodificación hardware. La lógica 54 puede comprender una matriz de puertas o chip ASIC, la cual está programada para decodificar y verificar las firmas digitales utilizando claves y otros datos secretos almacenados en una memoria 70 segura. Tras verificar con éxito una firma digital entrante, la lógica 54 envía una señal un microcontrolador 72 interno, seguro, el cual de manera similar puede comprender una unidad de procesamiento ARM9 con una memoria 74. El microcontrolador 72 da instrucciones a la lógica 56 de control del relé para que abra un relé de datos unidireccional desde una interfaz 76 de entrada, la cual está conectada a la red 30, hasta una interfaz 78 de salida, la cual está conectada al monitor 26. Como la interfaz 46, las interfaces 76 y 78 comprenden componentes hardware apropiadas, tales como interfaces Ethernet, aunque de forma similar también pueden estar soportados otros estándares de comunicación.

La Figura 5 es un diagrama de bloques que ilustra de forma esquemática un sistema 80 de comunicación seguro basado en proxy, en conformidad con otra realización de la presente invención. En este ejemplo, proxies 86 y 88 ICCP seguros soportan una sesión de comunicaciones seguras, punto a punto ("*peer-to-peer*"), entre un Sistema de Gestión de Energía (EMS, del inglés Energy Management System) 82 dentro de un centro de control y un Sistema de Control Distribuido (DCS, del inglés Distributed Control System) 84, el cual controla un generador eléctrico. Una conexión convencional entre el EMS 82 y el DCS 84 utilizaría ICCP a través de una red de comunicaciones dedicada, de confianza, o a través de una Red Privada Virtual (VPN, del inglés Virtual Private Network) que atraviesa una red no de confianza. La configuración ilustrada permite que tanto el EMS como el DCS mantengan este modelo de comunicación ICCP convencional. Los proxies 86 y 88 ICCP seguros convierten estas comunicaciones convencionales en un par de canales de órdenes seguros de una manera que es transparente al EMS y al DCS. Los proxies 86 y 88 transmiten información a través de la red 30 no de confianza, por ejemplo la Internet pública, sin riesgo de que un ataque procedente de la red comprometa al EMS o el DCS, o sin riesgo de que un ataque procedente de un EMS o un DCS comprometido que se propaga a través de la conexión ICCP ponga en compromiso el punto DCS o EMS.

En la realización de la Figura 5, cada proxy 86, 88 ICCP seguro es tanto una fuente como un destino de un canal de órdenes seguro. En el proxy 86 ICCP seguro, por ejemplo, un procesador 90 de proxy ICCP recibe órdenes enviadas por el EMS 82, y las convierte en el tipo seguro de sintaxis nombre:valor descrito anteriormente. Un codificador 92 de fuente codifica las órdenes convertidas, típicamente utilizando lógica de codificación implementada en hardware como se ha descrito anteriormente, y un procesador 94 de comunicaciones envía de esta forma las órdenes de manera segura a través de la red 30 hasta el procesador de comunicaciones del proxy 88. Un decodificador 96 de destino existente en el proxy 88 decodifica las órdenes, típicamente utilizando lógica de decodificación implementada en hardware, y el procesador 90 de proxy ICCP del proxy 88 las convierte de vuelta al formato ICCP estándar para envío al DCS 84, como si el EMS las hubiera comunicado directamente al DCS.

De forma similar, el proxy 88 ICCP seguro recibe informes de datos ICCP procedentes del DCS 84 y convierte y codifica los informes para su transmisión al proxy 86. El proxy 86 decodifica y convierte los datos de vuelta al formato ICCP y pasa los datos al EMS 82, como si el DCS hubiera comunicado los informes directamente al EMS utilizando ICCP.

La configuración mostrada en la Figura 5 se puede adaptar de forma similar para su uso en otros escenarios de comunicación y con otros protocolos. Por ejemplo, este mismo tipo de configuración puede proteger comunicaciones EMS-a-subestación utilizando el Protocolo de Red Distribuida DNP3, substituyendo DNP3 por ICCP en la descripción anterior y sustituyendo una unidad terminal remota (RTU, del inglés Remote Terminal Unit) de la subestación por el DCS. Otras aplicaciones resultarán evidentes para las personas con experiencia en la técnica y se considera que están dentro del alcance de las reivindicaciones adjuntas.

De esta manera se apreciará que las realizaciones descritas anteriormente se citan a modo de ejemplo, y que la presente invención no está limitada a lo que se ha mostrado y descrito particularmente anteriormente en esta memoria. Más bien, el alcance de las reivindicaciones adjuntas incluye tanto combinaciones como subcombinaciones de los diferentes rasgos descritos anteriormente en esta memoria, así como variaciones y modificaciones de los mismos que se le ocurrirían a personas con experiencia en la técnica tras la lectura de la descripción anterior y que no se describen en la técnica anterior. El alcance de la invención está definido sólo por las reivindicaciones adjuntas. Las realizaciones que no caen dentro del alcance de las reivindicaciones se deben considerar ejemplos.

REIVINDICACIONES

1. Aparato de comunicación, que comprende:

una estación (32) de transmisión que comprende:

un procesador (36) que ejecuta software que genera órdenes en un formato de orden predeterminado, en respuesta a entrada procedente de un usuario;

lógica (38) de codificación hardware configurada para recibir órdenes en el formato de orden predeterminado procedentes del software que se ejecuta en el procesador (36), para convertir las órdenes recibidas en un formato de datos convertidos predefinido de órdenes permitidas que incluye sólo un subconjunto limitado de las órdenes en el formato de orden predeterminado; y

un procesador (36) de comunicaciones configurado para transmitir las órdenes convertidas a través de una red (30) de comunicaciones; y

un controlador (34) de enlace ascendente, que comprende:

una primera interfaz (46) hardware configurada para recibir órdenes procedentes de la estación (32) de transmisión a través de la red (30) de comunicaciones;

una segunda interfaz hardware configurada para transportar las órdenes recibidas hasta un destino (50) protegido; y

lógica (48) hardware, la cual está acoplada entre las interfaces primera y segunda para recibir órdenes procedentes de la primera interfaz, para comparar las órdenes recibidas con un conjunto de máscaras hardware correspondientes a órdenes permitidas para comprobar que las órdenes están en el formato de datos predefinido, y para pasar a la segunda interfaz sólo órdenes recibidas que coinciden con una de las máscaras.

2. El aparato de acuerdo con la reivindicación 1, y que comprende un enlace unidireccional configurado para transportar datos de salida desde el destino protegido hasta la red de comunicaciones pero es físicamente incapaz de transportar datos de entrada desde la red de comunicaciones hasta el destino protegido.

3. El aparato de acuerdo con la reivindicación 1 ó 2, en el cual el destino protegido es un sistema de control industrial, y en el cual las órdenes permitidas están configuradas para controlar una configuración operativa del sistema de control industrial.

4. El aparato de acuerdo con cualquiera de las reivindicaciones 1-3, en el cual la lógica de codificación hardware de la estación de transmisión está configurada para encriptar las órdenes que recibe y la lógica hardware del controlador de enlace ascendente está configurada para desencriptar las órdenes recibidas.

5. El aparato de acuerdo con la reivindicación 1, en el cual la lógica de codificación hardware está contenida en una unidad de autenticación de usuario, la cual está configurada para autenticar una identidad de un usuario de la estación de transmisión antes de generar la firma digital.

6. El aparato de la reivindicación 1, en el cual la lógica (38) de codificación hardware está configurada para generar una firma digital para órdenes permitidas, y en el cual la lógica hardware del controlador de enlace ascendente está configurada además para recibir la firma digital con órdenes recibidas y para transportar órdenes permitidas a través de la segunda interfaz hardware sólo tras verificar la firma digital.

7. El aparato de acuerdo con la reivindicación 1, en el cual la lógica de codificación hardware de la estación de transmisión y la lógica hardware del controlador de enlace ascendente comprenden lógica hardware no accionada por software.

8. El aparato de acuerdo con la reivindicación 1, en el cual el conjunto de máscaras hardware indica órdenes permitidas indicando un nombre de la orden y valores permitidos asociados con el nombre.

9. El aparato de acuerdo con la reivindicación 1 u 8, en el cual las órdenes permitidas tienen un formato de datos predefinido, y en el cual el destino protegido es una estación de control de servicio público, y en el cual el aparato comprende un monitor, el cual está acoplado para recibir la orden recibida procedente de la segunda interfaz y para decodificar la orden recibida desde el formato de datos predefinido a un protocolo de comunicaciones entre centros de control para entrada a la estación de control de servicio público.

10. El aparato de acuerdo con la reivindicación 9, en el cual la estación de transmisión está configurada para recibir una entrada en conformidad con el protocolo de comunicaciones entre centros de control desde una fuente de órdenes y para codificar la entrada en conformidad con el formato de datos predefinido para transmisión a través de la red a la primera interfaz.

11. Un método para comunicación, que comprende:

recepción, por parte de una estación (32) de transmisión, de una entrada que indica una orden que debe ser dirigida a un destino (50) protegido desde un usuario;

generación de una orden en un formato de orden predeterminado, por parte de un procesador (36) que ejecuta software, en respuesta a la entrada del usuario;

conversión de la orden generada a un formato de datos convertidos predefinido de órdenes permitidas que incluye sólo un subconjunto limitado de las órdenes en el formato de orden predeterminado, mediante lógica (38) de codificación hardware;

transmisión, por parte de un procesador (36) de comunicaciones, de la orden convertida a través de una red (30) de comunicaciones a un controlador de enlace ascendente;

comparación de la orden recibida con un conjunto de máscaras hardware correspondientes a órdenes permitidas, mediante lógica hardware del controlador (48) de enlace ascendente; y

pasar la orden recibida al destino (50) protegido sólo cuando la orden recibida coincide con una de las máscaras hardware.

12. El método de acuerdo con la reivindicación 11, y que comprende transportar datos de salida desde el destino protegido hasta la red (30) de comunicaciones a través de un enlace unidireccional, el cual es diferente e independiente de las máscaras hardware y que es físicamente incapaz de transportar datos de entrada desde la red de comunicaciones hasta el destino protegido.

13. El método de acuerdo con la reivindicación 11, en el cual la comparación de la orden recibida con un conjunto de máscaras hardware correspondientes a órdenes permitidas comprende comparar la orden recibida con un conjunto de máscaras que tienen un formato de datos predefinido tal que cada orden permitida dentro del conjunto está definida por nombre de la orden y valores permitidos asociados con el nombre.

14. El método de acuerdo con la reivindicación 11, en el cual la conversión de la orden generada a un formato de datos convertidos predefinido, mediante la lógica de codificación hardware comprende encriptar las órdenes.

15. El método de la reivindicación 11, y que comprende la generación de una firma digital para órdenes permitidas mediante la lógica (38) de codificación hardware y la recepción, por el controlador de enlace ascendente, de la firma digital con las órdenes recibidas y el transporte de órdenes permitidas hasta el destino protegido sólo tras verificar la firma digital.

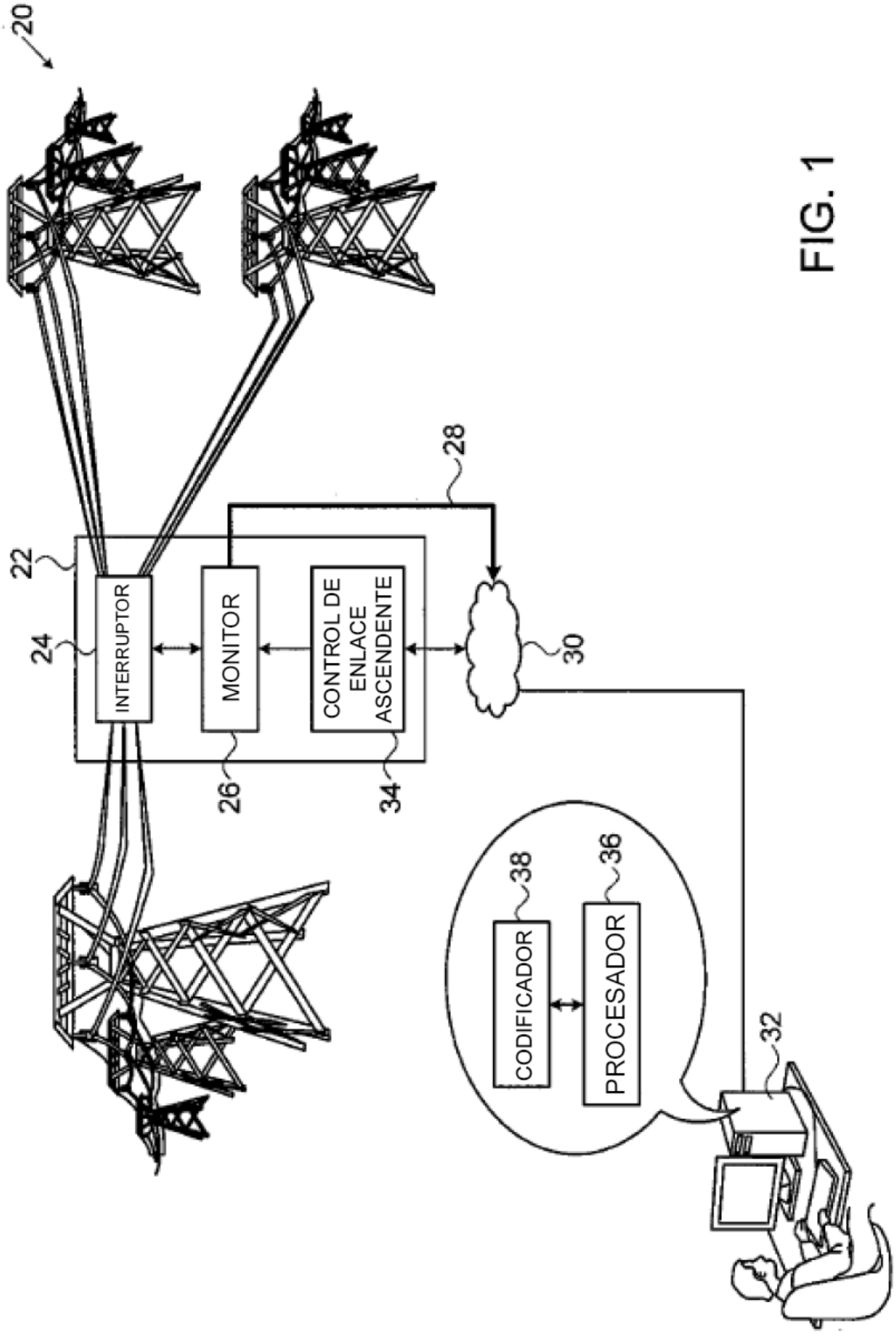
20
22
24
INTERRUPTOR
MONITOR
CONTROL DE ENLACE ASCENDENTE
26
28
30
34
32
36
PROCESADOR
38
CODIFICADOR

FIG. 1

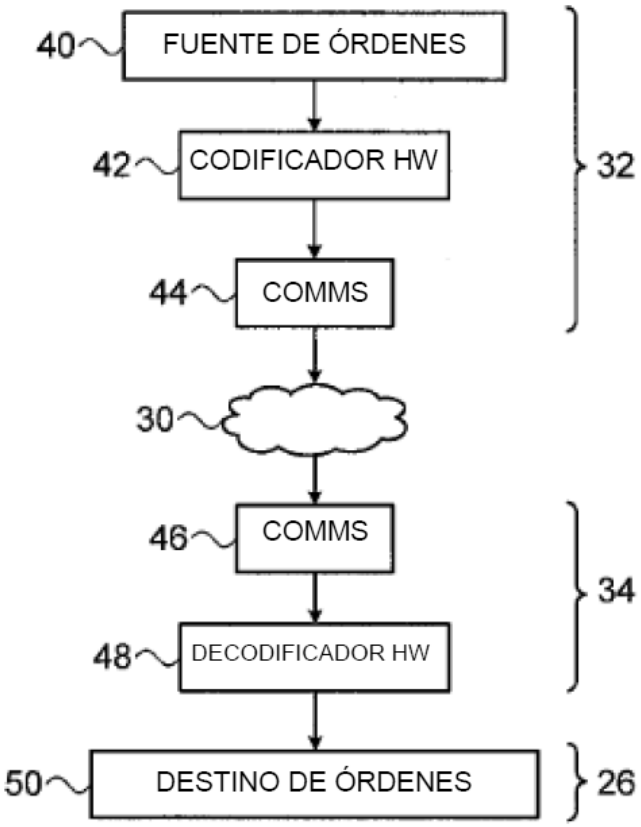
40
FUENTE DE ÓRDENES
42
CODIFICADOR HW
44
COMMS
32
30
46
COMMS
48
DECODIFICADOR HW
34
50
DESTINO DE ÓRDENES
26

FIG. 2

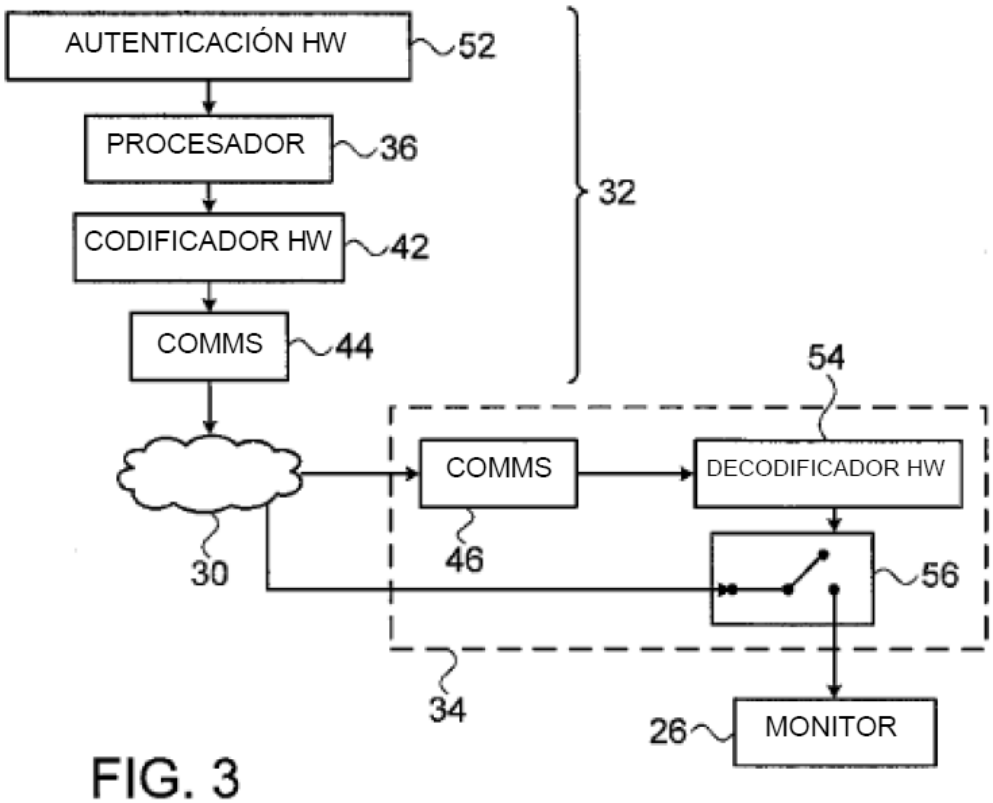
AUTENTICACIÓN HW
52
PROCESADOR
36
CODIFICADOR HW
42
COMMS
44
32
54
COMMS
DECODIFICADOR HW
30
46
56
34
26
MONITOR

FIG. 3

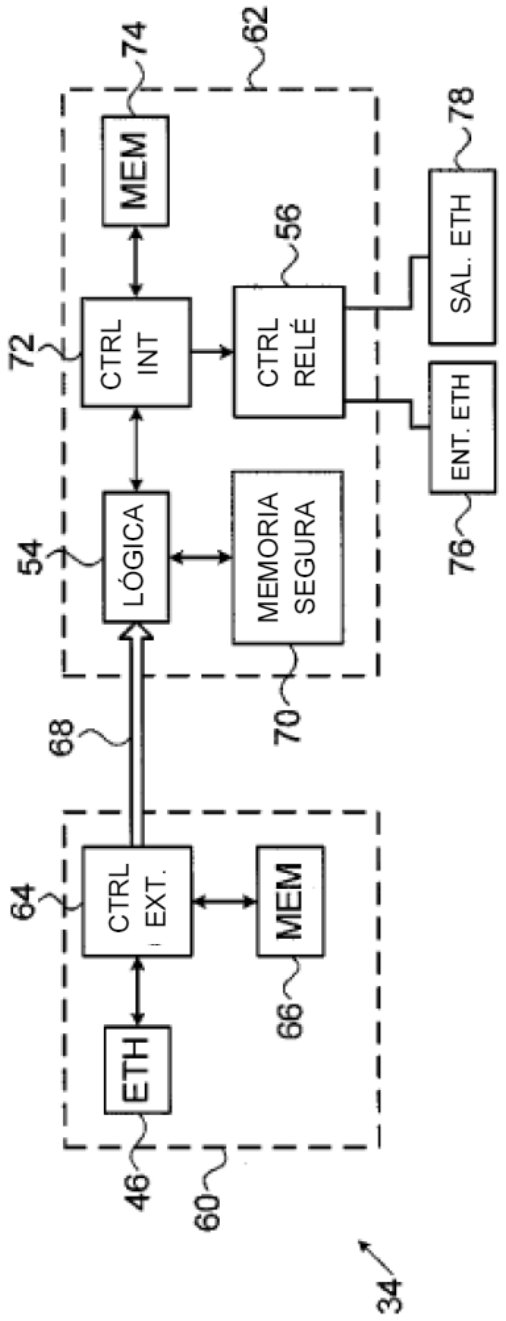
34
60
46
ETH
64
CTRL EXT.
MEM
66
68
70
62
74
MEM
72
CTRL INT
54
LÓGICA
MEMORIA SEGURA
56
CTRL RELÉ
78
SAL. ETH
ENT. ETH
76

FIG. 4

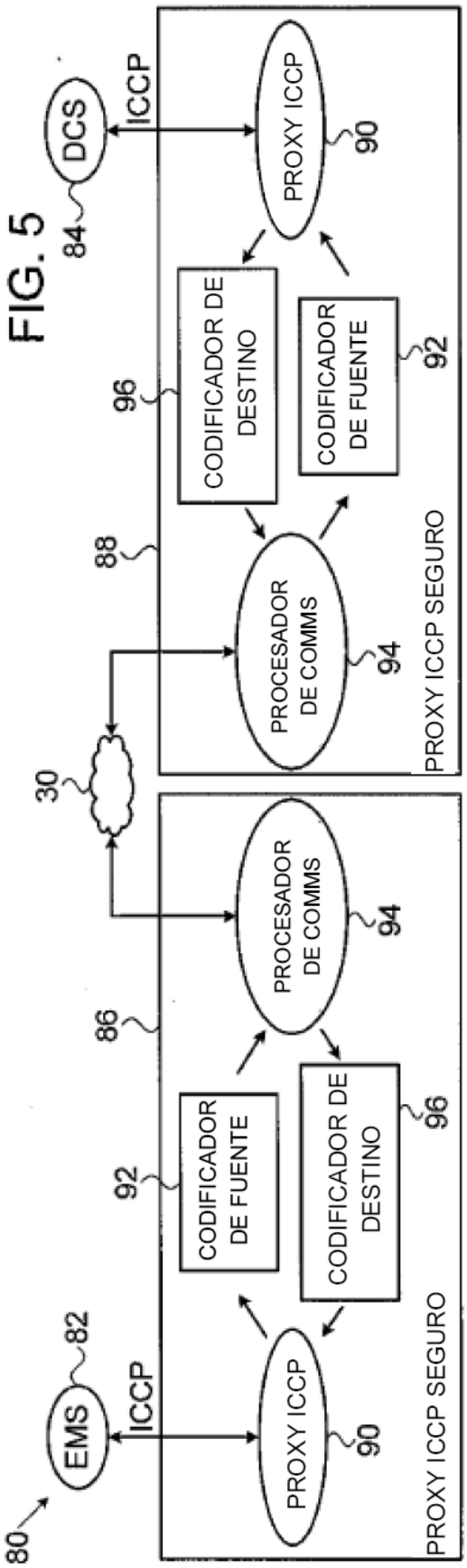
80
EMS
82
ICCP
PROXY ICCP
90
CODIFICADOR DE FUENTE
92
CODIFICADOR DE DESTINO
96
PROCESADOR DE COMMS
94
86
PROXY ICCP SEGURO
30
88
PROCESADOR DE COMMS
94
CODIFICADOR DE DESTINO
96
CODIFICADOR DE FUENTE
92
PROXY ICCP
90
ICCP
DCS
84
PROXY ICCP SEGURO

FIG. 5