(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 590 265**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.03.2014 E 14162141 (7)**

(97) Fecha y número de publicación de la concesión europea: **22.06.2016 EP 2797283**

(54) Título: **Aparato de comunicación y método para comunicación**

(30) Prioridad:

22.04.2013 US 201313867145

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2016

(73) Titular/es:

WATERFALL SECURITY SOLUTIONS LTD. (100.0%)
21 Hamelacha Street
48091 Rosh HaAyin, IL

(72) Inventor/es:

FRENKEL, LIOR

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Aparato de comunicación y método para comunicación.

La presente invención se refiere a un aparato de comunicación y a un método para comunicación

En las realizaciones, la presente invención se refiere generalmente a comunicaciones y control digitales, y en particular a sistemas y métodos para asegurar las comunicaciones. En las realizaciones, la invención se refiere a la comunicación bidireccional sobre un enlace unidireccional.

En una red de ordenadores que gestiona actividades de misión críticas, parte de la red puede estar conectada por enlaces 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 físicamente es capaz de transportar señales en una dirección y es físicamente incapaz de transportar señales en la dirección opuesta. Enlaces unidireccionales se pueden implementar, por ejemplo, utilizando sistemas Waterfall®, que son fabricados por Waterfall Security Solutions, Ltd. (Rosh HaAyin, Israel). El sistema Waterfall proporciona una conexión unidireccional física basada en la comunicación de fibra óptica, que utiliza un protocolo de trasferencia privado subyacente. Cuando un ordenador de transmisión está conectado mediante un sistema Waterfall (o enlace unidireccional) a un ordenador de recepción, el ordenador de recepción puede recibir datos procedentes del ordenador de transmisión pero no hay medios físicos para enviar ninguna comunicación de retorno al ordenador de transmisión.

Los enlaces unidireccionales se pueden utilizar para evitar que los datos entren o salgan de una instalación protegida. Por ejemplo, los datos confidenciales a los que no se debe acceder desde sitios externos pueden estar almacenados en un ordenador que está configurado para recibir datos en un enlace unidireccional y no tiene enlace de salida físico sobre el que se pudieran trasmitir los datos a un sitio externo. Por otra parte, el algunas aplicaciones, el operador de la instalación protegida puede estar preparado para permitir que los datos salgan de la instalación libremente a través de un enlace unidireccional a la vez que se evita que los datos u otras comunicaciones entren en el instalación con el fin de frustrar la propagación de un malware, hackers y otros ciber-terroristas.

En esta última categoría, por ejemplo, el documento US-A-7.649.452 describe la protección de redes de control que utilizan un enlace unidireccional. Esta patente describe un método para monitorear un proceso que incluye la recepción de una señal procedente de un sensor que es indicativa de un atributo físico asociado con el proceso y transmite datos indicativos de que la señal recibida en un enlace unidireccional. Los datos transmitidos recibos desde el enlace unidireccional son utilizados para monitorear el proceso. El método está descrito en la patente, particularmente en el contexto de sistemas de Supervisión, Control y Adquisición de Datos (SCADA). Un sistema SCADA recibe datos de control procedentes de la instalación monitoreada a través de un enlace unidireccional. El sistema SCADA es incapaz de transmitir ningún tipo de dato de nuevo a la instalación monitoreada (aunque una conexión separada de bucle abierto puede estar prevista para este fin), y por tanto no se pueden utilizar como base para un ataque sobre esta instalación.

El documento WO 2008/001344 describe un método para asegurar las comunicaciones entre un ordenador de transmisión y un ordenador de recepción sobre un primer y segundo enlaces unidireccionales.

El documento US 2008/008207 describe un método y sistema de implementación de enlace de comunicación de datos unidireccional.

El documento WO 00/64099 describe un método para conectar dispositivos utilizando cables y pares de conmutadores Ethernet.

Las realizaciones de la presente invención que se describen más adelante proporcionan un aparato y métodos que se pueden utilizar para proporcionar un canal de entrada seguro a un destino protegido.

De acuerdo con un aspecto de la presente invención, se proporciona un aparato de comunicación que comprende: primera y segunda entradas, conectadas respectivamente para recibir señales de comunicación procedentes de primera y segunda estaciones; primera y segunda salidas, conectadas respectivamente para transportar las señales de comunicación recibidas a la primera y la segunda estaciones; un enlace unidireccional, que es físicamente capaz de transportar las señales de comunicación en una dirección y es incapaz de transportar las señales en la otra dirección opuesta; y un par de conmutadores que están conectados al enlace unidireccional y están configurados para ser conmutados entre al menos una primera configuración, en la que las señales de comunicación son transportadas desde la primera entrada a través del enlace unidireccional a la segunda salida, y una segunda configuración, en la que las señales de comunicación son transportadas desde la segunda entrada a través del único enlace unidireccional a la primera salida.

En una realización, un primer conmutador de doble polo, que está conectado entre la primera y la segunda entradas y un lado de transmisión del enlace unidireccional único y está configurado para seleccionar la primera entrada para la conexión al lado de transmisión del enlace unidireccional único en la primera configuración y para seleccionar la segunda entrada para la conexión al lado de transmisión del enlace unidireccional único en la segunda

configuración.

En una realización, un segundo conmutador de doble polo, que está conectado entre la primera y la segunda salidas y un lado de recepción del enlace unidireccional único y está configurado para seleccionar la segunda salida para la conexión al lado de recepción del enlace unidireccional único en la primera configuración y para seleccionar la primera salida para la conexión al lado de recepción del encale unidireccional único en la segunda configuración.

En una realización, el al menos un conmutador comprende al menos un relé eléctrico y un conmutador óptico.

En una realización, la primera estación está situada en un red protegida, y en donde el aparato comprende lógica de control, que está configurada para mantener el al menos un conmutador normalmente en la primera configuración para habilitar la transmisión de datos desde la primera estación a la segunda estación, y para conmutar el al menos un conmutador a la segunda configuración sólo en momentos deseados para habilitar la entrada de instrucciones desde la segunda estación a la primera estación.

En una realización, la red protegida es una parte de un sistema de control industrial en una instalación protegida.

En una realización, el aparato comprende lógica de control que está configurada para mantener al menos un conmutador normalmente en la primera configuración y para conmutar el al menos un conmutador a la segunda configuración en momentos fijos, predefinidos.

En una realización, el aparato comprende lógica de control, que está configurada para mantener el al menos un conmutador normalmente en la primera configuración y para conmutar el al menos un conmutador a la segunda configuración sólo como respuesta a una orden autorizada.

En una realización, la lógica de control está configurada para conmutar el al menos un conmutador a la segunda configuración durante un tiempo suficiente para transportar, a través del aparato, no más de un número presente de mensajes a la primera instalación, antes de volver a la primera configuración.

En una realización, la lógica de control está configurada para esperar durante un cierto periodo de retraso antes de conmutar el al menos un conmutador a la segunda configuración.

En una realización, el al menos un conmutador tiene una tercera configuración, en la que no son transportadas señales de comunicación ni desde la primera entrada a la segunda salida ni desde la segunda entrada a la primera salida.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un método de acuerdo con la reivindicación 11. Las realizaciones adicionales se exponen en las reivindicaciones dependientes 12 y 13.

En una realización, la transmisión de las primeras y las segundas señales de comunicación comprende controlar el enlace unidireccional de manera que cualquier tiempo dado durante el cual la primera y la segunda estaciones estén en comunicación, el enlace unidireccional transporta o bien las primeras señales de comunicación o bien las segundas señales de comunicación, pero no ambas primeras y segundas señales de comunicación.

En una realización, controlar el enlace unidireccional comprende conmutar al menos un conmutador, que está conectado al único enlace unidireccional, entre al menos una primera configuración, en la que sólo las primeras señales de comunicación son transportadas a través de un único enlace unidireccional hasta la segunda salida, y una segunda configuración, en la que solo las segundas señales de comunicación son transportadas a través de un único enlace unidireccional.

Se proporciona por tanto, de acuerdo con una realización de la presente invención, un aparato de comunicación, que incluye primera y segunda entradas, conectadas respectivamente para recibir señales de comunicación procedentes de primera y segunda estaciones, y primera y segunda salidas, conectadas respetivamente para transportar las señales de comunicación recibidas a la primera y la segunda estaciones. Un único enlace unidireccional que físicamente es capaz de transportar las señales de comunicación en una dirección e incapaz de transportar las señales en la otra dirección opuesta, está conectado a un par de conmutadores, que está configurado para ser conmutado entre al menos una primera configuración, en la que las señales de comunicación son transportadas desde la primera entrada al único enlace unidireccional a la segunda salida, y una segunda configuración, en la que las señales de comunicación son transportadas desde la segunda entrada a través del único enlace unidireccional a la primera salida.

En una realización descrita, el par de conmutadores incluye al menos un primer conmutador de doble polo, que está conectado entre la primera y la segunda entradas y un lado de transmisión del único enlace unidireccional y está configurado para seleccionar la primera entrada para la conexión al lado de transmisión del único enlace unidireccional en la primera configuración y para seleccionar la segunda conexión de entrada al lado de transición del enlace unidireccional único a la segunda configuración. El par de conmutadores también puede incluir un segundo conmutador de doble polo, que está acoplado entre la primera y la segunda salidas y un lado de recepción del único enlace unidireccional y está configurado para seleccionar la segunda salida para la conexión al lado de

recepción del único enlace unidireccional en la primera configuración y para seleccionar la primera salida para la conexión al lado de recepción del único enlace unidireccional en la segunda configuración. El par de conmutadores puede incluir un relé eléctrico o un conmutador óptico.

En una realización típica, la primera estación está situada en una red protegida, y el aparato incluye lógica de control, que está configurada para mantener el al menos un conmutador normalmente en la primera configuración para habilitar la transmisión de datos desde la primera estación a la segunda estación, y para conmutar el al menos un conmutador a la segunda configuración sólo en momentos seleccionados para habilitar la entrada de instrucciones procedentes de la segunda estación a la primera estación. La red protegida puede ser una parte de un sistema de control industrial en la instalación protegida.

En algunas realizaciones, el aparato incluye lógica de control, que está configurada para mantener el al menos un conmutador normalmente en la primera configuración y para conmutar el al menos un conmutador a la segunda configuración en momentos fijos predefinidos.

Adicionalmente o alternativamente, la lógica de control puede estar configurada para conmutar el al menos un conmutador a la segunda configuración sólo como respuesta a una orden autorizada. La lógica de control puede estar configurada para conmutar el al memos un conmutador a la segunda configuración durante un tiempo suficiente, a través del aparato, no más de un número presente de mensajes a la instalación, antes de volver a la primera configuración. Adicionalmente o alternativamente, la lógica de control puede estar configurada para esperar durante un cierto periodo de retraso antes de conmutar el al menos un conmutador a la segunda configuración.

En una realización, el al menos un conmutador tiene una tercera configuración, en la que no son transportadas señales de comunicación ni desde la primera entrada a la segunda salida ni desde la segunda entrada a la primera salida.

También se proporciona, de acuerdo con una realización de la presente invención, un método para la comunicación, que incluye transmitir primeras señales de comunicación, desde una primera estación a una segunda estación, y segundas señales de comunicación, desde la segunda estación a la primera estación, a través de un único enlace unidireccional, que físicamente es capaz de llevar la señales de comunicación en una dirección e incapaz de transportar las señales de comunicación en la dirección opuesta.

En las realizaciones descritas, la transmisión de la primera y segunda señales de comunicación incluye controlar el enlace unidireccional de manera que en cualquier tiempo durante el cual la primera y la segunda estaciones estén en comunicación, el enlace unidireccional transporte o bien las primeras señales de comunicación o bien las segundas señales de comunicación, pero no ambas primeras y segundas señales de comunicación.

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

la Fig. 1 es un diagrama de bloques que ilustra esquemáticamente un sistema para la monitorización y control seguros, de acuerdo con una realización de la presente invención; y

la Fig. 2 es un diagrama de bloques que muestra esquemáticamente los detalles de un contralor de comunicación bidireccional basado en un único enlace unidireccional, de acuerdo con una realización de la presente invención.

A diferencia de los cortafuegos convencionales, los enlaces unidireccionales permiten que la información salga de una instalación protegida sin riesgo para la seguridad ni para la disponibilidad de la red en la instalación debido a ataques que se originan en una red externa, dado que el enlace unidireccional no ofrece un canal físico a través del cual tal ataque se pudiera realizar. En la práctica, sin embargo, a veces existe la necesidad de transmitir al menos pequeñas cantidades de información desde una red externa a la instalación protegida, particularmente, por ejemplo, cuando una instalación está en una situación remota y está desatendida. En algunas instalaciones, un canal de comunicaciones separado (que puede comprender un enlace unidireccional desde la red externa a la instalación protegida) está dispuesto para este fin.

Hay un cierto número de riesgos asociados con este último tipo de comunicaciones. Por ejemplo, un atacante podría utilizar el canal de comunicaciones a la instalación para producir condiciones no seguras o no fiables en la red protegida, por medio de un ataque por desbordamiento de búfer, por ejemplo. Tal ataque podría entonces ser utilizado para introducir malware de control remoto en la red protegida, y proporcionar al atacante los medios para explorar de forma interactiva y para sabotear la red protegida.

Para realizar un ataque de este tipo generalmente requiere que el atacante mantenga una conexión bidireccional interactiva con un ordenador en la instalación durante el menos una cantidad mínima de tiempo, con el fin de poder acceder a la respuesta del ordenador a los mensajes enviados desde el exterior de la instalación. Un atacante sofisticado puede utilizar enlaces unidireccional hacia dentro y hacia fuera de la instalación simultáneamente para proporcionar el canal de comunicación bidireccional virtual deseado, como una plataforma para el inicio de un ataque. Una vez que el canal de comunicación bidireccional se ha establecido, un ciberataque utiliza herramientas y técnicas estándar. El presente inventor se ha dado cuenta sin embargo, que si se establece un único enlace

unidireccional de manera que en cualquier momento, el enlace unidireccional transporte o bien las señales de comunicación de salida procedentes de la instalación o bien las señales de comunicación de entrada a la instalación, pero no ambas (ya que es físicamente imposible), los intentos del atacante para establecer comunicación bidireccional simultánea con la instalación quedarán frustrados.

Las realizaciones de la presente invención que se describen más adelante se basan en esta idea para proporcionar métodos y aparatos para la comunicación en los que las señales son transportadas tanto desde una primera estación a una segunda estación y desde la segunda estación a la primera estación a través del mismo, único enlace unidireccional en diferentes momentos. Uno o más conmutadores están típicamente dispuestos conectados a un enlace unidireccional y conmutan el enlace entre dos configuraciones distintas: una en la que las señales de comunicación fluyen a través del enlace unidireccional sólo desde la primera estación a la segunda, y la otra en la que las señales fluyen desde la segunda estación a la primera. La “primera estación” puede ser, por ejemplo, un ordenador en una instalación protegida, que transmite datos con fines de monitorización, en donde la “segunda estación” es un terminal de monitorización y control fuera de la instalación; pero los principios de la presente invención se pueden aplicar de manera similar a los ordenadores de protección y redes de otros tipos.

El uso de un único enlace unidireccional de este modo para soportar las comunicaciones bidireccionales es ventajoso para reducir los costes de hardware y requisitos de estación, con relación a los sistemas convencionales que utilizan enlaces unidireccionales separados para el acceso y para la salida desde la instalación protegida. Además, la configuración del único enlace unidireccional es las realizaciones descritas impone, en hardware, un modelo de comunicación de semi-dúplex, haciendo imposible que el atacante lleve a cabo una sesión de comunicación bidireccional simultánea con un ordenador en una instalación protegida. La posibilidad de ataque se puede inhibir más manteniendo el enlace unidireccional normalmente en la configuración en la que los datos son extraídos desde la instalación protegida, y limitando estrictamente los tiempos en los que el enlace está conmutado para permitir la trasmisión a la instalación protegida. La duración de tal transmisión se puede limitar también.

La Fig. 1 es un diagrama de bloques que ilustra esquemáticamente el sistema 20 para la monitorización y el control seguros, de acuerdo con una realización de la presente invención. En este ejemplo, el sistema 20 se utiliza para monitorizar y controlar un sistema de control industrial en una estación de control de empresas 22, tal como una subestación de transmisión y conmutación de una empresa de energía eléctrica. Aunque para una mayor simplicidad, sólo se muestra una única estación 22 en la Fig. 1, en la práctica las empresas generalmente operan muchas de tales estaciones. La estación 22 típicamente comprende elementos operacionales, tales como conmutadores 24, que establecen y rompen conexiones. En muchos sistemas reales, las estaciones de control 22 no tienen personal, y los conmutadores 24 son controlados remotamente monitorizando y controlando las estaciones, tal como un terminal de control 32, por ejemplo.

Aunque el ejemplo representado se refiere, a modo de ilustración, a una empresa de energía eléctrica, los principios de la presente invención no se limitan a este contexto de funcionamiento particular. En lugar de ello, el aparato y los métodos que se describen más adelante se pueden aplicar a empresas de otros tipos (tales como empresas de agua, por ejemplo), así como a ambientes industriales y sustancialmente a cualquier otra aplicación en la que vaya a ser ejercido un estricto control sobre las entradas a una instalación protegida. La estación 22 es sólo un ejemplo de tal instalación, que se presenta aquí con el fin de una mayor claridad de explicación. Ciertas realizaciones de la presente invención están descritas más adelante, con el fin de una mayor claridad y sin fisuración, con respecto a los elementos del sistema 20, los principios de estos elementos y todas las técnicas que incorporan puede de manera similar ser aplicados a otros ambientes de funcionamiento y configuraciones de sistema en los que la finalidad sea proteger de entradas de datos no deseadas y accesos no autorizados.

La estación 22 está típicamente diseñada como una instalación cerrada, segura, protegida físicamente contra la entrada no autorizada. Un monitor 26 en la instalación 22 introduce comandos a los conmutadores 24 y monitoriza el funcionamiento de los conmutadores y otros componentes de la estación. Típicamente, el monitor 26 comprende múltiple sensores y actuadores, que están distribuidos a través de toda la estación 22 e informan a través de una red interna segura a un controlador (no mostrado), como se ha descrito, por ejemplo, en la Patente de Estados Unidos 7.649.452 mencionada anteriormente. El monitor 26 envía los datos recogidos desde los sensores ya actuadores a través de un controlador de acceso/salida 34 a una red 30, que transporta los datos a un termina 32. La red 30 puede comprender cualquier red de cable o inalámbrica adecuada, o una combinación de tales redes, incluyendo redes públicas, tales como Internet.

El controlador de acceso/salida 34 transporta los datos de salida desde la estación 22 a la red 30 y recibe instrucciones desde la red 30 para introducir en la estación 22. En este ejemplo, el controlador 34 introduce comandos en el monitor 26, que entonces acciona los conmutadores 24 para ejecutar los comandos. Como se muestra en la Fig. 2, el controlador 34 comprende un enlace unidireccional y lógica de control asociada, que permite que un enlace unidireccional transporte comandos (y/u otros datos) a la estación 22 sólo en unos ciertos momentos bien definidos, que pueden estar prestablecidos o pueden seguir a un desencadenamiento, o ser controlados por cualquier mecanismo de programación o de desencadenamiento adecuado. Durante estos momentos, el controlador 34 físicamente es incapaz de enviar datos desde la estación 22 a la red 30. El monitor 26 se comunica con la red 30 sólo a través del controlador 34 (que puede estar el mismo contenido en la estación 22 para una protección de una alteración física o eléctrica).

La Fig. 2 es un bloque de diagramas que muestra esquemáticamente los detalles del controlador de acceso/salida 34 de acuerdo con una realización de la presente invención. El controlador 34 comprende un enlace unidireccional 40, que físicamente es capaz de transportar señales sólo en una dirección: desde un transmisor de enlace 42 a un receptor de enlace 44 a través de una medio de comunicación 46. El enlace 40 puede ser, por ejemplo, un enlace Waterfall del tipo descrito anteriormente en la sección de Antecedentes, en el que el medio 46 es una fibra óptica, con un transmisor óptico en un extremo y un receptor óptico en el otro, pero se puede utilizar alternativamente cualquier otro tipo de hardware de trasmisión unidireccional adecuado. Una circuitería auxiliar, que incluye conmutadores, y lógica de control en la presente realización, está conectada al enlace unidireccional de manera que proporcionan la funcionalidad de comunicación bidireccional que se describe aquí.

Uno o más conmutadores están conectados a un enlace unidireccional 40 con el fin de controlar si las señales que son transportadas a través del enlace desde un transmisor 56 en el monitor 26 hasta un receptor 58 en el termina 32 (como normalmente es el caso), o alternativamente, en otros momentos, desde un transmisor 54 en el terminal 32 a un receptor 60 en el monitor 26. (Aunque se muestran el transmisor 54 y el receptor 58, para una mayor claridad en la explicación, como bloques funcionales separados, en la práctica típicamente están implementados como partes de una misma interfaz o terminal de comunicación 32; y de manera similar, el transmisor 56 y el receptor 60 pueden estar implementados como partes de la misma interfaz de comunicación del monitor 26.) En la realización representada, estos conmutadores adoptan la forma de dos conmutadores de doble polo 48 y 50, pero otras configuraciones con equivalente funcionalidad, que utilizan solo un único conmutador (tal como un conmutador de doble tiro y de doble polo) o múltiples conmutadores, serán evidentes para los expertos en la técnica y son considerados dentro del campo de la presente invención. Los conmutadores 48 y 50 pueden comprender relés eléctricos o conmutadores ópticos, por ejemplo, o cualquier otro tipo de conmutadores conocidos en la técnica.

El conmutador 48 está conectado entre los transmisores 54 y 56 al lado de transmisión (transmisión 42) de un enlace unidireccional 40, mientras que el conmutador 50 está conectado entre el lado de recepción (receptor 44) del enlace unidireccional y los receptores 58 y 60. Los polos 62 y 64 del conmutador 48 sirven como entradas para el controlador de acceso/salida 34, mientras que los polos 66 y 68 sirven como salidas. La lógica de control 52 controla el funcionamiento de los conmutadores 48 y 50. Aunque la lógica de control se muestra en las figuras como un bloque funcional unificado, puede adoptar una gran variedad de formas físicas diferentes. Por ejemplo, la lógica de control 52 puede comprender un procesador programable y/o circuitos lógicos de hardware. Alternativamente o adicionalmente, la lógica de control puede simplemente comprender uno o más temporizadores conectados a los conmutadores 48 y 50, posiblemente en forma de un temporizador separado para cada conmutador. Además, alternativamente o adicionalmente, la lógica de control 52 puede comprender un desencadenante externo para operar los conmutadores en caso de emergencia, y/o un botón pulsador físico u otro control para la actuación por un operario humano.

Típicamente, la lógica de control 52 conmuta los conmutadores 48 y 50 conjuntamente de manera que en la configuración normal, en la que los datos son transmitidos desde la estación 22 a la red 30, el conmutador 48 selecciona el polo 64 para la conexión al lado de transmisión de un enlace unidireccional 40, mientras que el conmutador 50 selecciona el polo 66 para la conexión al lado de recepción. Por otra parte, durante los periodos (típicamente limitados) durante los cuales la estación 22 está para recibir entradas desde la red 30, la lógica de control cambia la configuración de ambos conmutadores 48 y 50, de manera que el polo 62 está conectado al lado de transmisión del enlace unidireccional, mientras que el polo 68 está conectado al lado de recepción. De esta manera, el controlador 34 emula el funcionamiento de un enlace de semi-dúplex bidireccional, utilizando un único enlace unidireccional 40, sin embargo, para transportar el tráfico de comunicaciones en ambas direcciones.

El controlador de acceso/salida 34 también puede soportar otras configuraciones de conmutadores 48 y 50. Por ejemplo, en una configuración de loopback, los conmutadores pueden seleccionar repetidamente los polos 64 y 68 al mismo tiempo, o los polos 62 y 66 al mismo tiempo, en cuyo caso no hay conexión de datos en absoluto entre el terminal 32 y la estación 22. Opcionalmente, uno o ambos de los conmutadores pueden tener una posición adicional, en la que ambos polos están desconectados. Este tipo de configuración de loopback o desconectada puede ser la configuración de fallo del controlador 34 al inicio. En cualquier caso, no hay configuración de los conmutadores que permita comunicaciones bidireccionales simultáneas entre el terminal y la estación. Por lo tanto, la seguridad de la estación 22 se mantiene incluso si los conmutadores 48 y 50 no están mutuamente sincronizados.

Como se ha observado anteriormente, la lógica de control 52 mantiene los conmutadores 48 y 50 normalmente en la primera configuración descrita anteriormente, que hace posible la transmisión de datos desde el monitor 26 en la estación 22 al terminal 32, y conmuta los conmutadores a la segunda configuración sólo el momentos seleccionados para habilitar la entrada de instrucciones desde el terminal 32 a la estación 22. Típicamente, la conmutación tiene lugar sólo como respuesta a una orden autorizada. Tal orden podría ser realizada manualmente accionando un control adecuado, típicamente situado dentro de la estación 22. Alternativamente o adicionalmente, los conmutadores 48 y 50 pueden ser conmutados sobre un comando automático desde la lógica de control 52 en momentos fijos, predefinidos, por ejemplo cada pocas horas.

Como una alternativa más, la lógica de control 52 puede conmutar los conmutadores 48 y 50 bajo solicitud (presentada o bien desde dentro o bien desde fuera de la estación 22), pero solo después de esterar durante un cierto periodo de retraso. La duración del retraso puede ser fija o aleatoria y puede estar acompañada por una alerta

a un administrador del sistema, que puede entonces intervenir si es necesario antes de que se produzca cualquier daño por un atacante que gestiona de alguna manera para aprobar la solicitud de conmutación.

De manera más adicional o alternativa, para aumentar la seguridad, la lógica de control 52 controla los conmutadores 48 y 50 de manera que ellos conmutan a la segunda configuración solo durante un periodo de tiempo corto. La temporización de este periodo se puede establecer de manera que sea suficiente para transportar sólo un cierto número de mensajes prestablecido (posiblemente sólo un único mensaje) desde el terminal 32 a la estación 22, antes de volver a la primera configuración. En este caso, también después de que los conmutadores hayan conmutado a la primera configuración, la lógica 52 puede esperar durante un cierto periodo de retraso antes de aceptar otra solicitud de conmutación.

Aunque la descripción anterior incide sobre los elementos y el funcionamiento del controlador de acceso/salida 34, en las aplicaciones prácticas, tal controlador puede ser sólo una parte de una solución total de comunicaciones segura. Otros métodos y aparatos para comunicaciones seguras en el tipo de contexto que se ejemplifica mediante el sistema 20 están descritos, por ejemplo en las Patentes de Estados Unidos anteriormente mencionadas 7.649.452, así como en la Solicitud de Patente de Estados Unidos 13/604.677, presentada el 6 de Septiembre de 2012, concedida al cesionario de la presente solicitud. Las realizaciones de la presente invención que se describen aquí pueden especialmente ser mejoradas mediante la integración con otros métodos o aparatos.

De este modo, se apreciará que las realizaciones descritas anteriormente se citan a modo de ejemplo, y que la presente invención no se limita a las que han sido particularmente mostradas y descritas anteriormente. En su lugar, el campo de la presente invención incluye tanto combinaciones como subcombinaciones de las diversas características descritas aquí.

REIVINDICACIONES

1. Aparato de comunicación (34) que comprende:

primera y segunda entradas (62, 64), conectadas respectivamente para recibir señales de comunicación procedentes de una primera y segunda estaciones (22, 32); y

primera y segunda salidas (66, 68), conectadas respectivamente para transportar las señales de comunicación recibidas a la primera y la segunda estaciones;

un único enlace unidireccional (40), que es físicamente capaz de transportar las señales de comunicación en una dirección e incapaz de trasportar las señales en la otra dirección opuesta; y

un par de conmutadores (48, 50), que están conectados al enlace unidireccional y están configurados para ser conmutados entre al menos una primera configuración, en la que las señales de comunicación son transportadas desde la primera entrada (62) a través del único enlace unidireccional (40) a la segunda salida (68), y una segunda configuración, en la que las señales de comunicación son transportadas desde la segunda entrada (64) a través del único enlace unidireccional (40) a la primera salida (66),

caracterizado por que el par de conmutadores (48, 50) comprende:

un primer conmutador de doble polo, que está conectado entre la primera y la segunda entradas (62, 64) y un lado de transmisión del único enlace unidireccional y está configurado para seleccionar la primera entrada (62) para la conexión al lado de transmisión del único enlace unidireccional en la primera configuración y para seleccionar la segunda entrada (64) para la conexión al lado de transmisión del único enlace unidireccional (40) en la segunda configuración, y

un segundo conmutador de doble polo, que está conectado entre la primera y la segunda salidas (66, 68) y un lado de recepción del único enlace unidireccional (40) y está configurado para seleccionar la segunda salida (68) para la conexión al lado de recepción del primer enlace unidireccional en la primera configuración y para seleccionar la primera salida (66) para la conexión al lado de recepción del único enlace unidireccional en la segunda configuración.

2. El aparato de acuerdo con la reivindicación 1, en el que el par de conmutadores (48, 50) comprende relés eléctricos.

3. El aparato de acuerdo con la reivindicación 1, en el que el par de conmutadores (48, 50) comprende conmutadores ópticos.

4. El aparato de acuerdo con cualquiera de las la reivindicaciones 1-3, en el que la primera estación está situada en una red protegida, y en el que el aparato comprende lógica de control (52), que está configurada para mantener el al menos un conmutador normalmente en la primera configuración para hacer posible la transmisión de datos desde la primera estación a la segunda estación, y para conmutar el par de conmutadores (48, 50) a la segunda configuración solo en momentos seleccionados para hacer posible la entrada de instrucciones desde la segunda estación a la primera estación.

5. El aparato de acuerdo con la reivindicación 4, en el que la red protegida es una parte de un sistema de control industrial en una instalación protegida.

6. El aparato de acuerdo con cualquiera de las la reivindicaciones 1-5, y que comprende lógica de control (52), que está configurado para mantener el al menos un conmutador normalmente en la primera configuración y para conmutar el par de conmutadores (48, 50) a la segunda configuración en momentos fijos, predeterminados.

7. El aparato de acuerdo con cualquiera de las la reivindicaciones 1-5, y que comprende lógica de control (52), que está configurado para mantener el par de conmutadores (48, 50) normalmente en la primera configuración y para conmutar el par de conmutadores a la segunda configuración solo como respuesta a una orden autorizada.

8. El aparato de acuerdo con la reivindicación 7, en el que la lógica de control (52) está configurada para conmutar el par de conmutadores (48, 50) a la segunda configuración durante un tiempo suficiente para transportar, a través del aparato, no más de un cierto número de mensajes presentes, a la primera estación, antes de volver a la primera configuración.

9. El aparato de acuerdo con la reivindicación 7, en el que la lógica de control (52) está configurada para esperar durante un cierto periodo de retraso antes de conmutar el par de conmutadores (48, 50) a la segunda configuración.

10. El aparato de acuerdo con cualquiera de las la reivindicaciones 1-9, en el que el par de conmutadores (48, 50) tiene una tercera configuración, en la que no son transportadas señales de comunicación ni desde la primera entrada (62) a la segunda salida (68) ni desde la segunda entrada (64) a la primera salida (66).

11. Método para comunicación, que comprende transmitir primeras señales de comunicación, desde una primera estación (22) a una segunda estación (32), a través de un par de conmutadores (48, 50) y un enlace único unidireccional (40), que físicamente es capaz de transportar señales de comunicación en una dirección y es incapaz de transportar señales de comunicación en la dirección opuesta,

estando el método caracterizado también por que incluye:

transmitir segundas señales de comunicación, desde la segunda estación (32) a la primera estación (22) a través del par de conmutadores (48, 50) y el único enlace unidireccional (40),

en el que en par de conmutadores (48, 50) comprende:

un primer conmutador de doble polo, que está conectado entre la primera y segunda entradas (62, 64), conectado respectivamente para recibir señales de comunicación procedentes de la primera y la segunda estaciones (22, 32), y un lado de transmisión del único enlace unidireccional (40), y está configurado para seleccionar la primera entrada (62) para la conexión al lado de transmisión del único enlace unidireccional en una primera configuración y para seleccionar la segunda entrada (64) para la conexión al lado de transmisión del único enlace unidireccional en una segunda configuración, y

un segundo conmutador de doble polo, que está conectado entre la primera y la segunda salidas (66, 68) conectado respectivamente para transportar las señales de comunicación recibidas a la primera y la segunda estaciones, y un lado de recepción del único enlace unidireccional, y está configurado para seleccionar la segunda salida (68) para la conexión al lado de recepción del único enlace unidireccional (40) en la primera configuración y para seleccionar la primera salida (66) para la conexión a lado de recepción del único enlace unidireccional en la segunda configuración.

12. El método de acuerdo con la reivindicación 11, en el que la transmisión de las primeras y segundas señales de comunicación comprende controlar el enlace unidireccional (40) de manera que en cualquier momento dado durante el cual la primera y la segunda estaciones (22, 32) están en comunicación, el enlace unidireccional (40) transporta o bien las primeras señales de comunicación o bien las segundas señales de comunicación, peo no ambas primeras y segundas señales de comunicación.

13. El método de acuerdo con la reivindicación 12, en el que controlar el enlace unidireccional comprende conmutar el par de conmutadores (48, 50) entre al menos una primera configuración, en la que sólo las primeras señales de comunicación son transportadas a través del único enlace unidireccional (40) a la segunda salida (68), y una segunda configuración en la que sólo las segundas señales de comunicación son transportadas a través del único enlace unidireccional (40).

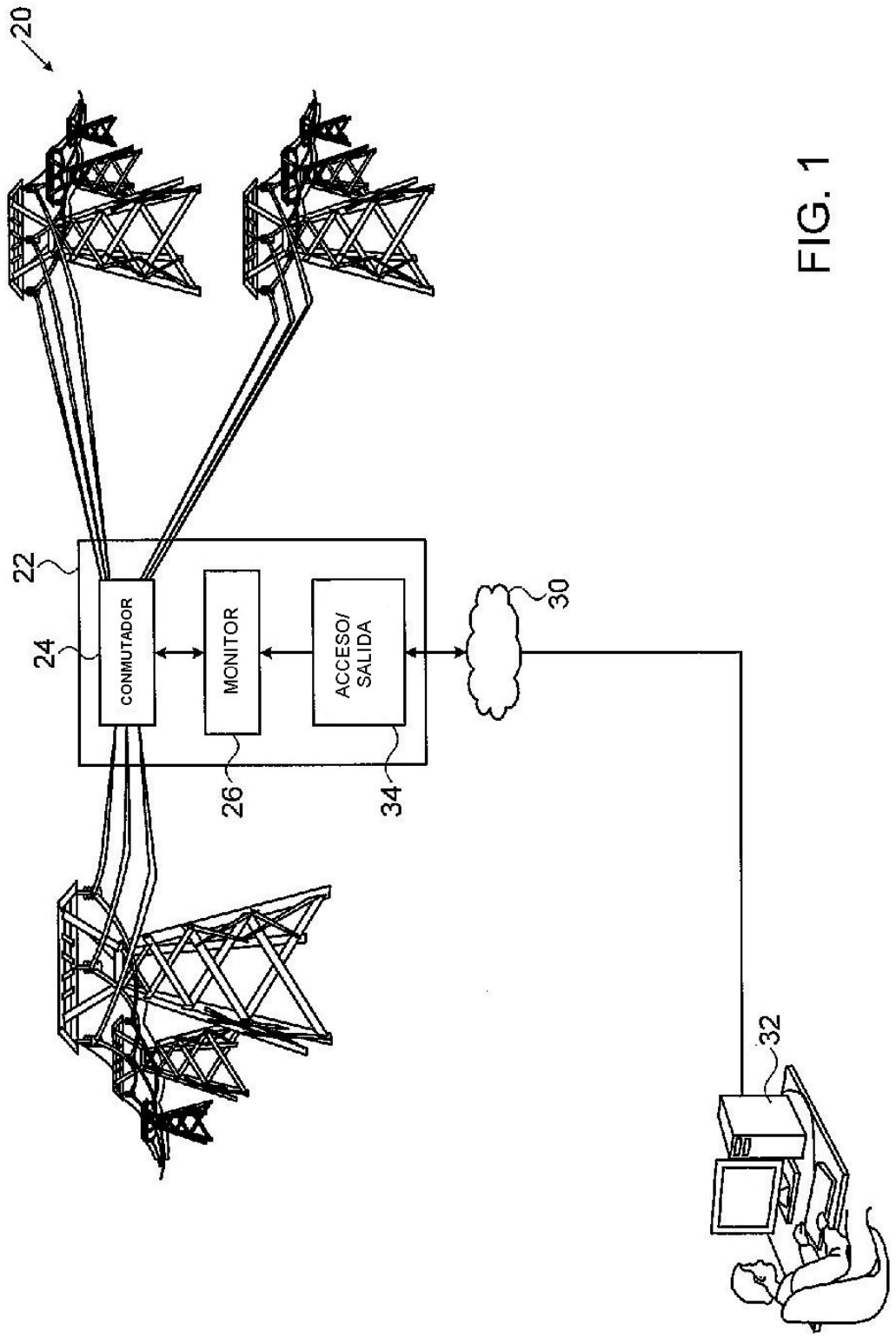

FIG. 1

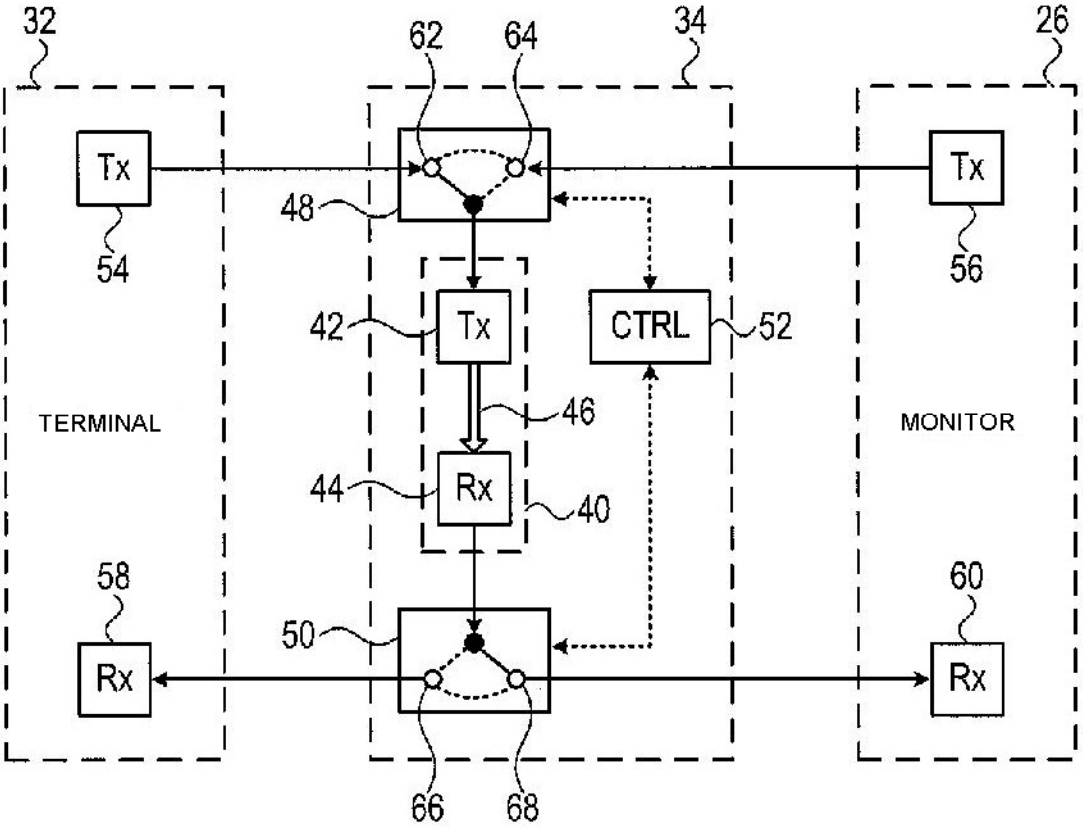
32
62
64
34
26
Tx
48
Tx
54
56
42
Tx
CTRL
52
TERMINAL
46
MONITOR
44
Rx
40
58
60
50
Rx
Rx
66
68

FIG. 2