(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 651 157**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.08.2012 PCT/EP2012/065677**

(87) Fecha y número de publicación internacional: **21.03.2013 WO13037578**

(96) Fecha de presentación y número de la solicitud europea: **10.08.2012 E 12751034 (5)**

(97) Fecha y número de publicación de la concesión europea: **27.09.2017 EP 2721803**

(54) Título: **Procedimiento y equipo para reconfigurar con seguridad un aparato de red**

(30) Prioridad:

12.09.2011 DE 102011082489

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.01.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

FALK, RAINER y
SEIFERT, MATTHIAS

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y EQUIPO PARA RECONFIGURAR CON SEGURIDAD UN APARATO DE RED

DESCRIPCIÓN

Los aparatos de red disponen de interfaces o bien interfaces de comunicación de red, mediante las cuales pueden comunicar los mismos con otros aparatos de red conectados a la red. Los aparatos de red de una instalación de automatización, en particular aparatos de campo para vigilar y controlar componentes de automatización, disponen cada vez más de interfaces de comunicación de red, que posibilitan una transmisión de datos de diagnóstico, datos de configuración, datos de servicio, datos de control, datos de vigilancia, etc. a través de redes de datos. Estas redes de datos son en parte redes de comunicación abiertas, en particular redes de datos Ethernet o redes de datos basadas en IP. Los componentes de automatización controlados y/o vigilados son por ejemplo componentes de automatización de una red de energía, de una central eléctrica o de un sistema de transporte, por ejemplo equipos de automatización, sistemas de agujas, barreras y similares. Además pueden ser los componentes de automatización controlados por ejemplo instalaciones semafóricas, oleoductos, refinerías o instalaciones fabriles. Para controlar tales componentes de automatización necesitan los aparatos de red de una instalación de automatización ajustes de la configuración, por ejemplo una dirección de red de un servidor de automatización o claves criptográficas.

En instalaciones o redes de automatización convencionales se establecen configuraciones de aparatos y/o se realiza un ajuste de la configuración la mayoría de las veces mediante un acceso directo de configuración. Este acceso directo de configuración presenta por ejemplo una interfaz serie, por ejemplo RS232 o USB, que permite una conexión con un PC de mantenimiento. El establecimiento de una configuración de aparato través de un acceso directo de configuración es desde luego complejo y arduo, en particular cuando se trata de una gran cantidad de componentes de automatización a instalar dentro de la red. Además puede dar lugar esta forma de proceder tradicional a problemas de seguridad, cuando se realiza un acceso no autorizado a la configuración. En tales aparatos de red y/o aparatos de automatización tradicionales dentro de una instalación de automatización pueden presentar los aparatos de red también una interfaz de usuario especial para realizar la configuración de los aparatos. Esta interfaz de usuario presenta por ejemplo pulsadores y/o una pantalla táctil o bien pulsadores y un display. Esto significa en una pluralidad de componentes de automatización o aparatos de red un coste técnico considerable. Además, en determinadas aplicaciones industriales, con las duras condiciones allí reinantes, tales interfaces de usuario no son realizables y/o son susceptibles de faltas. El documento US 2006236095 da a conocer un procedimiento para la modificación asegurada de una configuración de un aparato de red, permitiéndose la modificación sólo tras autentificar el aparato de red.

La figura 1 muestra un ejemplo de un aparato de red para describir la problemática que sirve de base a la invención. En el ejemplo de aplicación o Use Case que se presenta está previsto un aparato de codificación de la comunicación de campo, también denominado VPN-Box, con una interfaz de red externa Eth-ext basada en IP y una interfaz de red interna Eth-int basada en IP. El aparato de campo (VPN-BOX) está conectado con sensores y/o actuadores (S/A), por ejemplo de un sistema de cambio de vías o bien un control del sistema de cambio de vías, que se controla mediante un puesto de enclavamiento SW. Los datos de control y/o vigilancia CRTL se transmiten al realizar la transmisión a través de una red NW, a través de una llamada Virtual Private Network (red virtual privada) VPN, es decir, mediante un enlace de comunicaciones protegido frente a manipulaciones. Los datos de control y/o datos de vigilancia CTRL se transmiten para ello protegidos criptográficamente entre el aparato de campo (VPN-BOX) y un servidor VPN (VPN-S). Para ello puede utilizarse por ejemplo un protocolo IPsec, un protocolo L2TP, un protocolo PPTP o un protocolo SSL/TLS. La dirección del servidor VPN VPN-S, así como las credenciales criptográficas asociadas, como por ejemplo claves criptográficas, certificados digitales o palabras de paso, se configuran entonces durante la puesta en servicio del aparato de codificación de la comunicación de campo, por ejemplo a través de la interfaz de red interna o a través de una interfaz de mantenimiento y diagnóstico separada, no representada. Al respecto ha de evitarse que este ajuste de la configuración se pueda leer o manipular sin autorización en un aparato de campo instalado en campo mediante un ataque a la red. Además ha de posibilitarse también un reinicio y/o borrado de la configuración de aparatos de campo, en particular cuando ya no es posible ningún acceso de administración al aparato de codificación de la comunicación de campo (VPN-BOX), por ejemplo cuando se ha perdido una palabra de paso o una clave criptográfica.

Un aparato de codificación de la comunicación de campo convencional dispone la mayoría de las veces de un pulsador de reset propio para reiniciar o borrar su memoria de configuración. Un inconveniente al respecto es que un tal pulsador de reset puede ser accionado por descuido, por ejemplo debido a sacudidas y con ello provocar un funcionamiento incorrecto o bien un tal pulsador o contacto situado en el duro entorno de campo, en el que se encuentra el aparato de codificación de la comunicación de campo, puede ensuciarse y ya no poder ser accionado.

Es posible que el aparato de codificación de la comunicación de campo o la VPN-Box cargue su configuración de aparato a través de la interfaz de red externa, por ejemplo a través de una interfaz Ethernet externa Eth-ext, por ejemplo a través de un enlace de comunicación codificado con SSL o TLS mediante la red NW desde un servidor de configuración KS, tal como se representa en la figura 2. El

aparato de campo o la VPN carga entonces a través de la interfaz externa de red Eth-ext, desde un servidor de configuración de aparatos de campo KS, una información de configuración, por ejemplo un fichero de configuración en formato de texto o XML para el funcionamiento del aparato de campo. La dirección configurada del servidor de configuración de aparatos de campo lleva asociada dado el caso una Security Credential (credencial de seguridad), que puede ser una clave criptográfica, una palabra de paso o un certificado digital y que está previsto para el acceso protegido criptográficamente al servidor de configuración de aparatos de campo. Por ejemplo puede autentificarse la VPN-Box frente al servidor de configuración KS mediante una credencial de autentificación y autentificar el propio servidor de configuración KS y a continuación solicitar datos de configuración (C-Reg). A continuación se reciben los datos de configuración del servidor de configuración KS (C-Res). El ajuste de la configuración para la VPN-Box incluye por ejemplo informaciones sobre la dirección de un servidor VPN VPN-S mediante un protocolo VPN a utilizar, así como la descripción de Security Associations (asociaciones de seguridad) del túnel VPN de los parámetros de configuración para un protocolo de acuerdo de claves como por ejemplo IKE - Internet Key Exchange, intercambio de claves de Internet – o bien IKEv2. El ajuste de la configuración para la VPN-Box puede incluir Credentials, por ejemplo una clave criptográfica, una palabra de paso o un certificado digital. Además pueden incluir los ajustes de configuración regulaciones de filtros relativos a un tráfico de datos permitido.

Esto tiene la ventaja de que pueden realizarse modificaciones de la configuración durante el funcionamiento del aparato de campo o la VPN-Box, proporcionándose una información de configuración modificada mediante el servidor de configuración KS. Para que pueda realizarse el mecanismo de autoconfiguración representado en la figura 2 para cargar los datos de configuración, debe estar configurada la dirección de red del servidor de configuración KS en la VPN-Box. Además ha de configurarse para ello dado el caso un certificado Z y/o una clave criptográfica K en el aparato de codificación de la comunicación de campo o la VPN-Box.

En una instalación convencional contiene el aparato de codificación de la comunicación de campo o la VPN-Box una interfaz local de configuración, por ejemplo en forma de una interfaz serie según RS232, que implica un coste adicional en técnica de circuitos. Existe también en la configuración tradicional representada en la figura 2 la necesidad de configurar protegidos los datos de configuración necesarios para el acceso al servidor de configuración de aparatos de campo KS, en particular su dirección de red, al aparato de campo de la red, en particular la VPN-Box representada en la figura 2 y/o bien borrar o modificar de forma protegida la configuración del aparato de campo compatible con la red, sin tener que prever para ello una interfaz de configuración propia adicional.

Resumen de la invención

Un objetivo de la presente invención consiste en proporcionar un procedimiento y un equipo con cuya ayuda puede modificarse de forma protegida un ajuste de configuración de un aparato de red, sin que para ello tenga que preverse en el aparato de red una interfaz de configuración adicional.

Este objetivo se logra según la invención mediante un procedimiento con las características indicadas en la reivindicación 1.

La invención logra según ello un procedimiento para modificar de manera asegurada un ajuste de configuración de un aparato de red que mediante al menos una interfaz puede conectarse a otro aparato de red, en el que puede modificarse el ajuste de la configuración del aparato de red, siempre que exista un estado de conexión física captado de al menos una interfaz del aparato de red, que durante un funcionamiento regular del aparato de red no se presenta.

En una forma de realización posible del procedimiento de acuerdo con la invención, se comprueba el estado de conexión física captado de al menos una interfaz del aparato de red en base a criterios de prueba predeterminados en el sentido de si el estado de conexión física puede presentarse o no puede presentarse durante el funcionamiento regular o funcionamiento normal del aparato de red.

En una forma de realización posible del procedimiento de acuerdo con la invención, se permite una modificación del ajuste de la configuración del aparato de red incluso sin una autentificación de quien accede, por ejemplo un servidor de configuración de la red o un PC de mantenimiento, en el caso de que el estado de conexión física determinado no se presente durante un funcionamiento regular del aparato de red.

En una forma de realización posible del procedimiento de acuerdo con la invención, se permite una modificación del ajuste de la configuración del aparato de red en el caso de que el estado de conexión física determinado pueda presentarse en un funcionamiento regular del aparato de red, siempre que se haya realizado con éxito una autentificación de quien quiere acceder, por ejemplo un servidor de configuración o un PC de mantenimiento.

En una forma de realización posible del procedimiento de acuerdo con la invención presenta el ajuste de configuración del aparato de red una dirección de red de un servidor de configuración.

En otra forma de realización posible del procedimiento de acuerdo con la invención se borran en una modificación de la dirección de red del servidor de configuración los datos de configuración del aparato de red proporcionados por el servidor de configuración que actuaba hasta ahora.

En una forma de realización posible del procedimiento de acuerdo con la invención, se señaliza una posibilidad de modificación del ajuste de la configuración del aparato de red a al menos otro aparato de red correspondiente a la red o a un aparato de configuración, a continuación de lo cual se transmiten los datos de configuración previstos para la reconfiguración automáticamente al aparato de red.

En una forma de realización posible del procedimiento de acuerdo con la invención, se memorizan localmente los datos de configuración transmitidos para modificar el ajuste de la configuración del aparato de red en una memoria de datos de configuración del aparato de red.

En una forma de realización posible del procedimiento de acuerdo con la invención se conecta la interfaz del aparato de red, de las que al menos hay una, con un aparato de configuración, que origina un estado de conexión física del aparato de red que en un funcionamiento regular del aparato de red no se presenta o no puede presentarse, para permitir o liberar una modificación del ajuste de la configuración del aparato de red.

En una forma de realización posible del aparato de red de acuerdo con la invención, el aparato de red es un aparato de automatización de una instalación de automatización, en particular un aparato de campo.

La invención logra además un aparato de red con las características indicadas en la reivindicación 11.

La invención logra en consecuencia además un aparato de red que puede conectarse a través de al menos una interfaz a otro aparato de red, en el que sólo puede modificarse un ajuste de la configuración del aparato de red cuando exista un estado de conexión física captado de al menos una interfaz del aparato de red que no se presenta durante un funcionamiento regular del aparato de red.

En una forma de realización posible del aparato de red de acuerdo con la invención, la interfaz, de las que al menos hay una, es una interfaz ligada a línea física.

Además puede ser la interfaz también una interfaz de comunicación inalámbrica.

En una forma de realización posible del aparato de red de acuerdo con la invención, presenta el aparato de red un dispositivo detector integrado para detectar el estado de conexión física de la interfaz, de las que al menos hay una.

La interfaz, de las que al menos hay una, es una interfaz que está prevista para el funcionamiento normal o funcionamiento regular del aparato de red y no una interfaz de comunicación del aparato de red prevista expresamente para la configuración. El aparato de red no presenta con preferencia ninguna interfaz de configuración autónoma.

La invención logra además una red con las características indicadas en la reivindicación 15.

La invención logra en consecuencia una red, en particular una red de una instalación de automatización, que presenta aparatos de red, pudiendo conectarse los aparatos de red mediante respectivas interfaces a otros aparatos de red incluidos en la red, pudiendo modificarse un ajuste de la configuración de un aparato de red sólo cuando existe un estado de conexión física captado de la interfaz, de las que al menos hay una, que no se presenta durante un funcionamiento regular del aparato de red dentro de la red.

La invención logra además un aparato de configuración o aparato para configurar con las características indicadas en la reivindicación 16.

La invención logra en consecuencia un aparato de configuración para un aparato de red de una red, en el que puede conectarse el aparato de configuración a al menos una interfaz del aparato de red y genera un estado de conexión física en el aparato de red que no se presenta durante un funcionamiento regular del aparato de red, con lo que se permite una modificación del ajuste de la configuración del aparato de red.

En lo que sigue se describirán más en detalle formas de realización posibles del procedimiento de acuerdo con la invención y del equipo de acuerdo con la invención para la modificación asegurada de un ajuste de configuración de un aparato de red con referencia a las figuras adjuntas.

Se muestra en:

figura 1 un ejemplo de realización para describir la problemática que sirve de base a la invención;
figura 2 otro diagrama para describir la problemática que sirve de base a la invención;

figura 3 un diagrama de conexión de bloques para representar un ejemplo de realización de un aparato de red acuerdo con la invención, en el que puede ejecutarse el procedimiento de acuerdo con la invención para la modificación asegurada de un ajuste de configuración;

figura 4 un diagrama secuencial de un ejemplo de realización del procedimiento de acuerdo con la invención para la modificación asegurada de un ajuste de configuración de un aparato de red y

figura 5 otro diagrama secuencial para representar un ejemplo de realización del procedimiento de acuerdo con la invención para la modificación asegurada de un ajuste de configuración de un aparato de red.

Tal como puede verse en la figura 3, presenta un aparato de red 1 en el ejemplo de realización representado dos interfaces de comunicación. El aparato de red 1 representado en la figura 3 es por ejemplo una VPN-Box para la transmisión asegurada criptográficamente de datos de control y vigilancia de un aparato de automatización conectado. El aparato de red 1 dispone de dos interfaces 2, 3, que por ejemplo son interfaces Ethernet. Mediante la interfaz de Ethernet interna 2 puede conectarse el aparato de red por ejemplo con un sensor o actuador S/A, por ejemplo con un sistema ferroviario de cambio de vía o bien una barrera de paso a nivel del ferrocarril o bien un aparato de control del sistema ferroviario de cambio de vía o de la barrera de paso a nivel del ferrocarril. Mediante la interfaz de Ethernet externa 3 está conectado el aparato de red 1 por ejemplo a través de una red NW con un servidor VPN VPN-S y/o un servidor de configuración KS. Ambas interfaces 2, 3 del aparato de red 1 están conectadas con una unidad de control 4 integrada a través de una interfaz de comunicación 5, 6. Además está conectada la unidad de control o CPU con una memoria de configuración 7, que memoriza localmente datos de configuración y/o ajustes de configuración del aparato de red 1. La unidad de control 4 codifica los datos recibidos a través de la interfaz 2 y envía los datos codificados a través de la interfaz 3 a los aparatos unidos con la misma. Además decodifica la unidad de control 4 los datos recibidos de la interfaz de Ethernet externa 3 y envía los datos decodificados a través de la interfaz de Ethernet interna 2. En la memoria de configuración 7 pueden estar archivados datos de configuración, en particular datos de información de direcciones, así como claves criptográficas. El aparato de red 1 representado en la figura 3 no dispone de ningún pulsador de reset, por ejemplo para reiniciar o borrar la memoria de configuración 7. Además no dispone el aparato de red 1 de ninguna interfaz de mantenimiento o interfaz de configuración local. Puesto que el aparato de red 1 puede conectarse mediante ambas interfaces 2, 3 a otros aparatos de red, pueden modificarse sus ajustes de configuración memorizados en la memoria de configuración local 7 cuando un estado de conexión física captado de la interfaz 2, 3 del aparato de red, de las que al menos hay una, no se presenta y/o no puede presentarse durante un funcionamiento regular o normal del aparato de red. El aparato de red 1 dispone con preferencia de un dispositivo detector 8 integrado, para detectar un estado de conexión física de una o de ambas interfaces 2, 3. Alternativamente puede realizarse la detección del estado de conexión también mediante el equipo de control 4. Entonces se comprueba el estado de conexión física captado de las interfaces 2, 3 del aparato de red 1 en una forma de realización posible en base a criterios de prueba predeterminados en cuanto a si el estado de conexión puede presentarse o no puede presentarse durante el funcionamiento regular o normal del aparato de red. Tales criterios de prueba en cuanto a un cableado o conexión correctos incluyen por ejemplo la comprobación de si la interfaz de red interna 2 sólo está conectada con un aparato y a la interfaz de red externa 3 no está conectado ningún aparato y/o ningún cable de conexión. Esto puede detectarse por ejemplo mediante detección de medios en una interfaz de Ethernet o bien previendo el correspondiente sensor. Un sensor puede captar por ejemplo si está enchufado un conector o bien captar la resistencia y/o capacidad y/o impedancia entre contactos de la o de las interfaces de red 2, 3. Además puede comprobarse el proceso de enchufe. Otro criterio de prueba adicional es si existe o se presenta un cortocircuito entre contactos de un conector o entre contactos de distintos conectores. En el caso de que el aparato de red 1 disponga por ejemplo de una interfaz de sensor, un valor de medida inválido, que por ejemplo indica un estado de conexión física que se encuentra fuera de una gama de valores admisible, es un estado que no se presenta durante el funcionamiento normal del aparato de red 1. Cuando por ejemplo en una interfaz analógica con una gama de valores de 4 – 20 mA el valor de medida válido para el flujo de corriente se encuentra en esta gama de 4 mA – 20 mA, indica un flujo de corriente de por ejemplo 50 mA o 1 mA un valor inválido y representa un estado de conexión física que no puede presentarse durante un funcionamiento normal del aparato de red 1. Otros criterios de prueba posibles son una resistencia, capacidad o una impedancia prescritas de contactos del conector o entre contactos de distintos conectores. Además puede comprobarse en cuanto a la interfaz de red externa 3 si no existe ninguna conectividad de la red o si por ejemplo no puede lograrse una determinada dirección de la red, que por ejemplo puede estar prescrita como dirección de IP o como URL. También puede comprobarse mediante un protocolo Router-Discovery (de descubrimiento de enrutador), como el “ICMP Internet Router Discovery Protocol” (IRDP) que no existe ningún enrutador de IP. Además puede comprobarse el estado de conexión en cuanto a si se utiliza otra ocupación de los conectores. Además es posible comprobar la alcanzabilidad de otros componentes de red o aparatos de red. Por ejemplo no deben ser alcanzables durante un funcionamiento regular normal determinados componentes de red. Además pueden comprobarse otros criterios adicionales. Por ejemplo sólo es posible una dirección de un servidor de autoconfiguración durante un espacio de tiempo fijado tras aplicar una fuente de alimentación externa, cuando por ejemplo un sensor de posición o sensor de montaje indica que el aparato de campo o aparato de red no está montado, por ejemplo no está encajado en una barra de sombrerete. El aparato de red o aparato de campo compatible con la red 1 representado en la figura 3 dispone de interfaces eléctricas, por ejemplo las interfaces de red Ethernet 2, 3. Además puede dispone el aparato de red también de

otras interfaces, por ejemplo una interfaz de entrada/salida, a la que pueden conectarse sensores y/o actuadores S/A, por ejemplo a través de un bus de campo, como por ejemplo un bus CAN, un bus M o un Profibus o a través de una interfaz analógica o interfaz digital. Para que el aparato de red 1 pueda cumplir la función a la que está destinado, debe estar conectado y/o cableado correctamente. Bajo cableado se entiende aquí la conexión de las interfaces físicas. Un criterio de prueba puede referirse a características físicas de una interfaz y dado el caso también a características lógicas de la interfaz.

El aparato de red 1 de acuerdo con la invención dispone de una funcionalidad para determinar una información que depende del cableado existente en ese momento o bien del estado de conexión física actual del aparato de campo o bien aparato de red 1. El equipo de detección 8 comprueba al respecto si existe una conexión física correcta. Si éste no es el caso, es decir, si el cableado o bien la conexión del aparato de red 1 es defectuoso/a o bien “absurdo/a”, entonces puede modificarse un ajuste de configuración memorizado, por ejemplo datos de configuración memorizados en la memoria de configuración 7. La modificación de los datos de configuración sólo puede realizarse cuando existe una conexión carente de sentido o no admisible durante el funcionamiento regular o normal del aparato de red 1. Entonces es posible comprobar la existencia de cualquier conexión o cableado defectuoso o la existencia de un determinado cableado defectuoso prescrito. En una variante no se acepta cualquier conexión o cableado defectuoso para liberar la modificación del ajuste de la configuración, sino sólo uno o varios cableados o conexiones defectuosos determinados prescritos/as.

Puesto que se comprueba un cableado o conexión especial, que no se presenta durante el funcionamiento regular del aparato de red 1, se garantiza además con fiabilidad que en un aparato de red 1 instalado para el funcionamiento regular, no puede bajarse esta funcionalidad. En particular no puede realizar un atacante esta funcionalidad para modificar el ajuste de la configuración mediante una comunicación de datos, a través de una interfaz de red, por ejemplo las interfaces de red 2, 3 representadas en la figura 3. De esta manera se impide con fiabilidad que desde otro aparato de red pueda activarse un Factory-Reset (retorno a la configuración de fábrica) y/o reinicio de los ajustes de la configuración mediante la transmisión de paquetes de datos adecuados. De esta manera se logra una protección claramente mayor frente a abusos que la que se tenía en aparatos de red tradicionales. Siempre que el aparato de red esté correctamente conectado y/o cableado, sus ajustes de configuración están debido a ello enclavados (en inglés “configuration lock”) y por lo tanto no pueden modificarse.

En una forma de realización posible, es factible la modificación de la configuración al detectarse un cableado y/o conexión incorrectos incluso sin una autentificación del acceso al mantenimiento, es decir, sin que previamente tenga que introducirse por ejemplo una palabra de paso de administración o bien sin que tenga que realizarse una autentificación del acceso al mantenimiento utilizando una clave criptográfica. Por el contrario sólo puede modificarse la configuración cuando se detecta un cableado y/o conexión correctos, en una variante de realización posible, tras una comprobación de autentificación con éxito del aparato de red.

Cuando se tenga un cableado y/o conexión del aparato de red 1 que usualmente se considera defectuoso, puede modificarse o modificarse de una determinada manera un determinado ajuste de la configuración del aparato de red 1. Una tal modificación del ajuste de la configuración no puede realizarse en consecuencia cuando el aparato de red 1 esté correctamente instalado, es decir, cuando se encuentra en un funcionamiento regular o funcionamiento normal operativo.

En una forma de realización posible presenta el ajuste de la configuración protegido de acuerdo con la invención una dirección de red de un servidor de configuración de aparatos de campo KS. La activación de esta dirección de red puede realizarse en particular a través de una primera interfaz de red, en particular la interfaz de red interna 2 del aparato de red 1 representada en la figura 3, pudiendo realizarse la carga de un fichero de configuración y/o de los datos de configuración a través de una segunda interfaz de red, en particular a través de la interfaz de red externa 3 representada en la figura 3, desde un servidor de configuración de aparatos de campo destinado a la dirección de red.

En una variante presenta el ajuste de configuración protegido una clave criptográfica asociada al servidor de configuración KS.

En una variante utiliza el aparato de red la dirección de red protegida de un servidor de aparatos de campo KS sólo cuando existe una conexión y/o cableado correcto del aparato de red.

La figura 4 muestra un diagrama secuencial para representar una variante de realización del procedimiento de acuerdo con la invención para la modificación asegurada de un ajuste de la configuración de un aparato de red 1.

Después de una etapa de arranque S0 se comprueba primeramente en una etapa S1, por ejemplo mediante un dispositivo de detección 8 del aparato de red 1, un cableado y/o una conexión de las interfaces del aparato de red 1.

Si la comprobación en la etapa S2 da como resultado que el cableado y/o la conexión están correctos, se bloquea primeramente en la etapa S3 una posibilidad de modificación para modificar los datos de configuración. A continuación se activa en una etapa S4 un modo de funcionamiento regular o servicio regular según los datos de configuración memorizados.

Si por el contrario la comprobación da como resultado que el cableado y/o la conexión del aparato de red 1 no son correctos o bien que el estado de la conexión física no puede presentarse en un funcionamiento regular del aparato de red 1, se admite o libera en una etapa S5 la posibilidad de modificación del ajuste de la configuración y ello se señaliza dado el caso a otros aparatos de red. En otra etapa S6 se reciben mediante el aparato de red 1 los datos de configuración previstos para la configuración y/o reconfiguración y se memorizan en la etapa S7 en la memoria local de configuración 7 para la reconfiguración. El proceso finaliza en la etapa S8.

Por ejemplo se realiza la configuración de la dirección de un servidor de configuración KS en el procedimiento de acuerdo con la invención como sigue. Se comprueba mediante un aparato un de codificación de campo o bien una VPN-Box, que constituye un aparato de red 1 según la figura 3, si tiene una conexión correcta el aparato de codificación de campo 1. Si es éste el caso, se activa un modo de funcionamiento regular u Operation Mode en la etapa S4. Si la conexión no es correcta, se activa en la etapa S5 un mecanismo de autoconfiguración, es decir, se libera o permite una modificación del ajuste de la configuración de la dirección del servidor de configuración. Esto puede realizarse también sin una autentificación mediante una palabra de paso o mediante una clave criptográfica. El aparato de codificación de campo 1 recibe a continuación los datos de configuración, por ejemplo una URL del servidor de configuración KS y memoriza estos datos de configuración localmente en su memoria de configuración 7.

En una variante ventajosa posible se borra cuando se activa la dirección de red del nuevo servidor de configuración KS la configuración completa definida por el servidor de configuración válido hasta ahora. Así se evita que queden restos de datos correspondientes a la configuración hasta ahora existente.

La secuencia de la configuración puede repetirse en una forma de realización posible, por ejemplo automáticamente a intervalos de tiempo regulares. Además puede realizarse la secuencia de la configuración al conectar el aparato de codificación de campo 1 o bien al aplicar una tensión de alimentación al aparato de red.

La recepción de los datos de configuración puede realizarse en una variante de realización posible tal que el aparato de codificación de la comunicación de campo 1 envíe a través de una interfaz interna 2 un mensaje de broadcast/multicast (difusión general/multidifusión), para determinar la dirección de red de un segundo servidor de configuración al que puede llegarse a través de la interfaz interna 2. Puede tratarse al respecto de un llamado mensaje PING a la dirección de IP de broadcast 255.255.255.255. A la misma contesta el servidor de configuración interno con su dirección de IP, por ejemplo 192.168.15.7. Además formula el aparato de codificación de la comunicación de campo 1, por ejemplo mediante http, una consulta para solicitar una configuración. Por ejemplo, se realiza esto mediante llamada por medio de GET a la URL http://192.168.15.7/Config. Opcionalmente puede entonces transmitirse a la vez una información de identificación relativa al fabricante o un número de serie del aparato de codificación de campo 1, por ejemplo puede codificarse la URL (http://192.168.15.7/Config?Siemens-VPN-Box-071382456). El segundo servidor de configuración interno puede contestar al respecto en una forma de realización posible proporcionando una información de configuración. Entonces puede incluir en particular la dirección de red, es decir, la dirección de IP, el nombre DNS o la URL, la dirección del primer servidor de configuración al que puede llegarse a través de la primera interfaz de red. El aparato de codificación de campo 1 memoriza esta información de configuración localmente en su memoria de configuración 7. Durante el funcionamiento regular o servicio regular se carga entonces la configuración de esta dirección de red.

La figura 5 muestra un diagrama secuencial para representar una variante de realización del procedimiento de acuerdo con la invención. Las etapas S0 – S2 son las mismas que en la variante de realización representada en la figura 4. Si la comprobación de la etapa S2 da como resultado que el cableado es correcto, se bloquea en la etapa S3a primeramente una modificación de la configuración “Address-Config-Server”. A continuación se cargan en la etapa S3b los datos de configuración de la dirección de red “Address-Config-Server”. A continuación se activa en la etapa S4 un modo de funcionamiento regular o servicio regular según los datos de configuración cargados. Si por el contrario la comprobación da como resultado una conexión y/o cableado incorrecta/o, se posibilita o permite en la etapa S5 una modificación de la configuración “Address-Config-Server”.

A continuación se reciben en la etapa S6 los datos de configuración relativos al “Address-Config-Server”.

Los datos de configuración se memorizan en relación con el “Address-Config-Server” en la etapa S7. Tras esta etapa S7, retorna el proceso a la etapa S1.

En el procedimiento de acuerdo con la invención para la modificación asegurada de un ajuste de configuración, no es posible o bien se impide con fiabilidad una modificación de la configuración por descuido o incluso una manipulación intencionada del ajuste de la configuración protegido frente a modificaciones del aparato de red 1 correctamente instalado que se encuentra en funcionamiento regular. En particular se impide con fiabilidad una manipulación mediante instancias externas que no tienen ningún acceso físico al aparato de red 1, sino sólo remoto a través de una conexión de red al aparato de red 1.

La activación de la dirección de un servidor de configuración de aparatos de campo KS con dos interfaces de red a través de una interfaz interna sólo es posible cuando la configuración de red en la interfaz de red interna y/o externa 2, 3 cumple un determinado criterio de prueba. Al respecto se comprueba si existe una configuración de red que no puede presentarse en un funcionamiento regular del aparato de red 1. De esta manera se impide una modificación inadvertida, inadmisible durante el funcionamiento regular del aparato de red 1. Una modificación del ajuste de la configuración sólo es posible mediante un acceso físico directo al aparato de red 1. Entonces se alcanza de acuerdo con la invención un nivel de protección que es comparable con un pulsador de reset (reinicio), sin tener que prever para ello el correspondiente pulsador de reset en el aparato de red 1. Por ello puede utilizarse un aparato de red 1 de acuerdo con la invención también en un entorno que podría originar un fuerte ensuciamiento de un tal pulsador de reset. Además se excluye así el peligro de que puedan producirse disparos intempestivos, por ejemplo debido a vibraciones del pulsador de reset. Además, mediante la posibilidad de renunciar a un pulsador de reset, se reduce el coste técnico en circuitos del aparato de red 1.

REIVINDICACIONES

1. Procedimiento para modificar de manera asegurada un ajuste de configuración de un aparato de red (1) que mediante al menos una interfaz (2; 3) puede conectarse a otros aparatos de red, en el que puede modificarse el ajuste de la configuración del aparato de red (1), siempre que exista un estado de conexión física captado de al menos una interfaz (2; 3) del aparato de red (1), que durante un funcionamiento regular del aparato de red (1) no se presenta.

2. Procedimiento de acuerdo con la reivindicación 1, en el que se comprueba el estado de conexión física captado de al menos una interfaz (2; 3) del aparato de red (1) en base a criterios de prueba predeterminados en el sentido de si el estado de conexión física puede presentarse o no puede presentarse durante un funcionamiento regular del aparato de red (1).

3. Procedimiento de acuerdo con la reivindicación 1 ó 2, en el que se permite una modificación del ajuste de la configuración del aparato de red (1) incluso sin una autentificación del aparato de red (1) en el caso de que el estado de conexión física determinado no se presente durante un funcionamiento regular del aparato de red (1).

4. Procedimiento de acuerdo con la una de las reivindicaciones 1 a 3, en el que se permite una modificación del ajuste de la configuración del aparato de red (1) en el caso de que el estado de conexión física determinado pueda presentarse en un funcionamiento regular del aparato de red (1), siempre que se haya realizado con éxito una autentificación del aparato de red (1).

5. Procedimiento de acuerdo con la una de las reivindicaciones precedentes 1 a 4, en el que el ajuste de la configuración del aparato de red (1) presenta una dirección de red de un servidor de configuración (KS).

6. Procedimiento de acuerdo con la reivindicación 5, en el que se borran en una modificación de la dirección de red del servidor de configuración (KS) los datos de configuración del aparato de red (1) proporcionados por el servidor de configuración que actuaba hasta ahora.

7. Procedimiento de acuerdo con la una de las reivindicaciones precedentes 1 a 6, en el que se señaliza una posibilidad de modificación del ajuste de la configuración del aparato de red (1) a al menos otro aparato de red correspondiente a la red o a un aparato de configuración, a continuación de lo cual se transmiten los datos de configuración previstos para una reconfiguración del aparato de red (1) automáticamente al aparato de red (1).

8. Procedimiento de acuerdo con la reivindicación 7, en el que se memorizan los datos de configuración transmitidos para modificar el ajuste de la configuración del aparato de red (1) en una memoria de datos de configuración (7) del aparato de red (1).

9. Procedimiento de acuerdo con la reivindicación 1, en el que la interfaz (2; 3) del aparato de red (1), de las que al menos hay una, se conecta con un aparato de configuración, que origina un estado de conexión física en el aparato de red (1) que en un funcionamiento regular del aparato de red (1) no se presenta, para permitir una modificación del ajuste de la configuración del aparato de red (1).

10. Procedimiento de acuerdo con la reivindicación 9, en el que el aparato de configuración u otro aparato de red, tras permitirse la modificación del ajuste de la configuración del aparato de red (1), transmite datos de configuración, previstos para una reconfiguración del aparato de red (1) a través de la misma interfaz o de otra interfaz del aparato de red (1).

11. Aparato de red (1) que puede conectarse a través de al menos una interfaz (2; 3) a otro aparato de red, en el que sólo puede modificarse un ajuste de la configuración del aparato de red (1) cuando exista un estado de conexión física captado de al menos una interfaz (2; 3) del aparato de red (1) que no se presenta durante un funcionamiento regular del aparato de red (1).

12. Aparato de red de acuerdo con la reivindicación 11, en el que la interfaz (2; 3) es una interfaz inalámbrica o una interfaz ligada a línea física.

13. Aparato de red de acuerdo con la reivindicación 11 ó 12, en el que el aparato de red (1) presenta un dispositivo detector (8) para detectar el estado de conexión física de la interfaz (2; 3) del aparato de red (1), de las que al menos hay una.

14. Aparato de red de acuerdo con una de las reivindicaciones 11 a 13,
en el que el aparato de red (1) es un aparato de automatización de una instalación de automatización, en particular un aparato de campo.

15. Red, en particular red para una instalación de automatización que presenta aparatos de red (1),
en la que los aparatos de red (1) pueden conectarse mediante respectivas interfaces (2; 3) a otros aparatos de red conectados a la red,
en la que un ajuste de la configuración de un aparato de red (1) sólo puede modificarse en el caso de que exista un estado de conexión física de la interfaz (2; 3) del aparato de red (1), de las que al menos hay una, que no se presenta durante un funcionamiento regular del aparato de red (1) dentro de la red.

16. Aparato de configuración para un aparato de red (1) que puede conectarse a al menos una interfaz (2; 3) del aparato de red (1) para provocar un estado de conexión física en el aparato de red (1) que no se presenta durante un funcionamiento regular del aparato de red (1), con lo que se permite una modificación de un ajuste de la configuración del aparato de red (1).

FIG 1

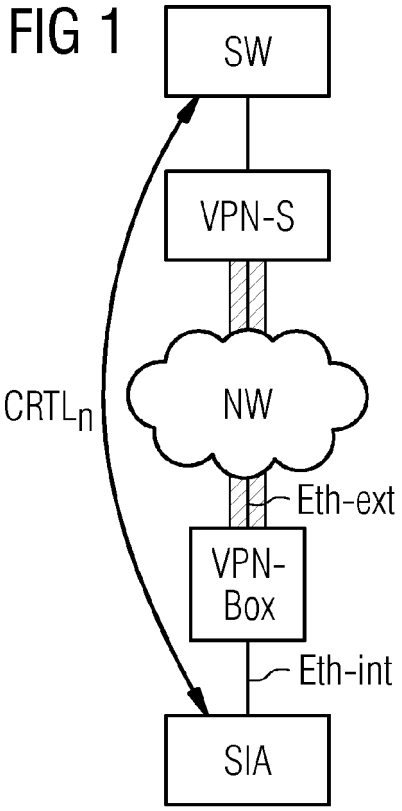
SW
VPN-S
NW
CRTL$_n$
Eth-ext
VPN-
Box
Eth-int
SIA

FIG 2

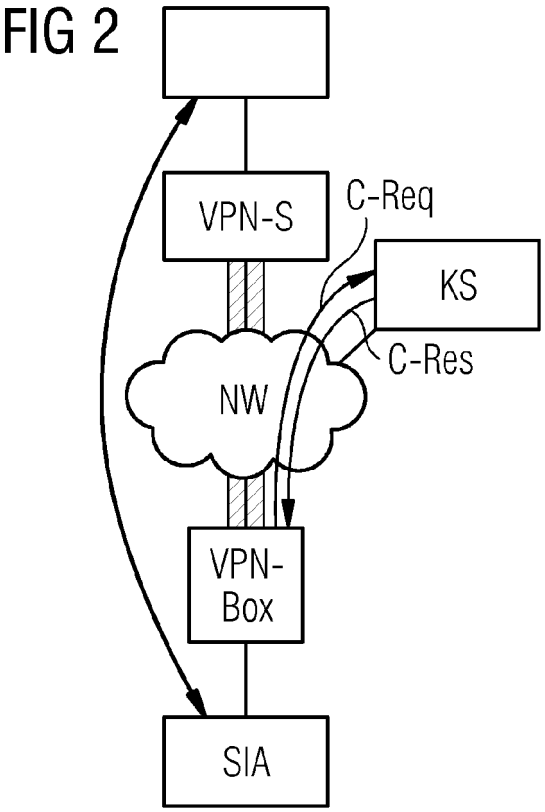
VPN-S
C-Req
KS
C-Res
NW
VPN-
Box
SIA

FIG 3

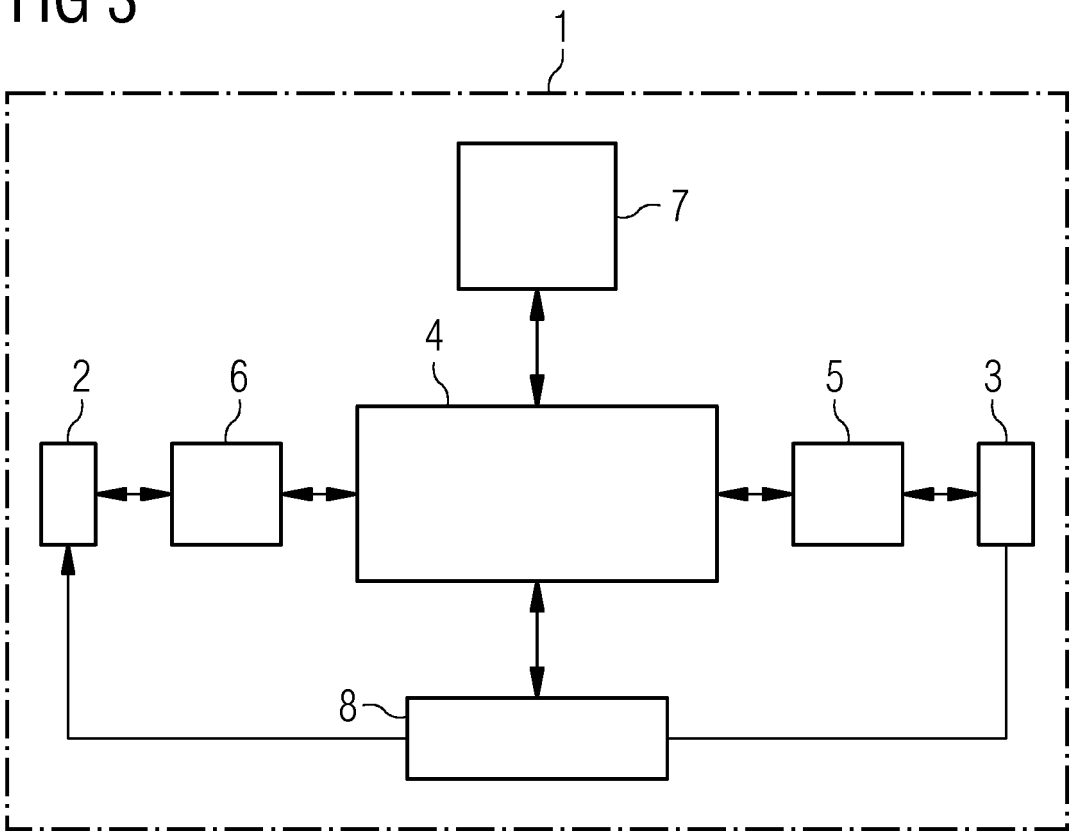

FIG 4

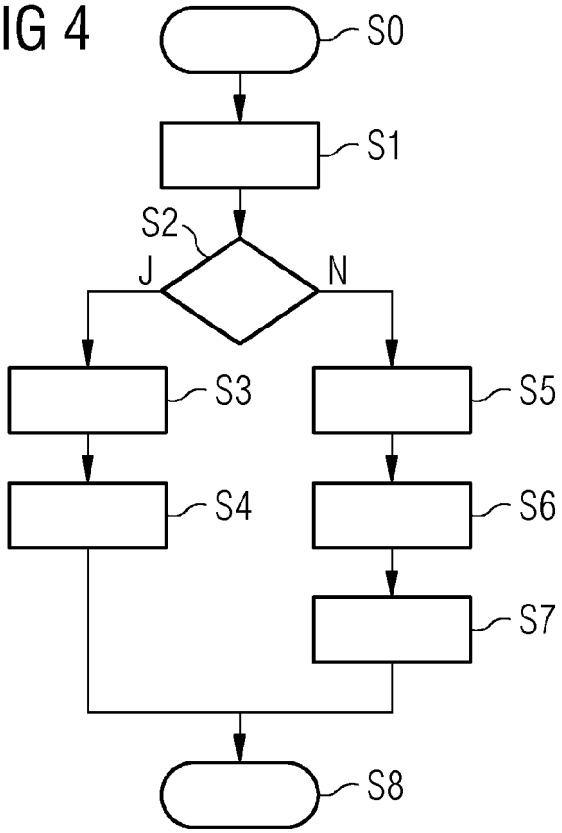

FIG 5