(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 508 520**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/46 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.01.2011 E 11701035 (5)**

(97) Fecha y número de publicación de la concesión europea: **17.09.2014 EP 2524487**

(54) Título: **Sistema para llevar a cabo servicios remotos para una instalación técnica**

(30) Prioridad:

12.01.2010 DE 102010000824

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.10.2014

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München , DE

(72) Inventor/es:

BALINT, THOMAS;
BAUER, JÖRG y
KISSLING, JAN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema para llevar a cabo servicios remotos para una instalación técnica

La invención se refiere a un sistema para llevar a cabo servicios remotos para una instalación técnica conforme a la reivindicación 1.

Los servicios remotos (llamados con frecuencia también “Remote Services”) ofrecen en el ciclo de vida de una instalación técnica (por ejemplo de una instalación productiva industrial, una central de energía, una instalación de transporte y distribución de mercancía en piezas o de la técnica de edificios en un gran edificio) una multitud de posibilidades de aplicación. Entre éstas se encuentran por ejemplo actualización remota de software (Remote Update Services), vigilancia remota (Remote Conditioning Monitoring), mantenimientos remotos (Remote Maintenance) y sin olvidar el apoyo remoto a la eliminación de errores

Para poder ofrecer estos servicios se necesita un enlace de comunicación a través de una red pública (por ejemplo de la Internet) en la instalación, habitualmente en una red interna no pública de la instalación. A las redes internas en instalaciones de este tipo se imponen requisitos de seguridad especiales. Desde el punto de vista IT estos son capacidad de comprensión, transparencia y seguridad IT. Desde el punto de vista del desarrollo empresarial se trata de la seguridad de funcionamiento de la instalación.

El enlace desde el exterior con la red no pública interna de la instalación, a través de la red pública, se realiza por ello con frecuencia mediante un llamado “enlace de túnel”. Por enlace de túnel se entiende aquí un enlace de comunicación entre un dispositivo alejado de la instalación a través de una red pública y por lo tanto no segura, como por ejemplo la Internet, y un dispositivo interno de la instalación, en el que se realizan una identificación y una autentificación de los interlocutores de la comunicación y en el que se garantiza, mediante codificación de datos, la confidencialidad de los datos (es decir, no existe ningún acceso a los datos por parte de terceros) así como la integridad de los datos (es decir, no es posible una modificación de los datos por parte de terceros). Un enlace de túnel de este tipo es posible por ejemplo a través de la Internet mediante un enlace VPN (Virtual Private Network), que usa un protocolo de seguridad de Internet, como por ejemplo IPsec (Internet Protocol Security). Con ello, aunque se atiende suficientemente la seguridad IT, sin embargo no se dan o solamente de una manera condicionada la capacidad de comprensión y la transparencia del enlace.

Si para una instalación se llevan a cabo varios servicios remotos diferentes, estos se materializan en la instalación a través de correspondientemente numerosos y casi siempre diferentemente seguros enlaces de túnel. Mediante estos numerosos enlaces se produce por parte del gestor de la instalación una elevada complejidad administrativa, para garantizar un mínimo de seguridad en especial en cuanto a la transparencia y capacidad de comprensión. Por este motivo los gestores de instalaciones desean los menos enlaces posibles de este tipo y, de este modo, son escépticos con respecto a nuevos servicios remotos.

Del documento WO 2007/070154 A2 se conoce una solución para un mantenimiento remoto de un entorno productivo a través de una “remote network”, para el que a un suministrador de servicios puede garantizarse un acceso seguro.

Por ello la tarea de la presente invención consiste, en un sistema para llevar a cabo servicios remotos para una instalación técnica conforme al preámbulo de la reivindicación 1, reducir la complejidad administrativa por parte del gestor de la instalación con una elevada seguridad IT y una elevada seguridad de funcionamiento de la instalación y, de este modo, hacer posible llevar a cabo una multitud de servicios remotos en una instalación.

La solución de esta tarea se consigue mediante un sistema conforme a la reivindicación 1. Unas configuraciones ventajosas son objeto de las reivindicaciones subordinadas.

Un sistema conforme a la invención para llevar a cabo servicios remotos para una instalación técnica comprende

- un primer sistema de servicios remotos con un primer dispositivo alejado de la instalación para llevar a cabo un primer servicio remoto, un primer dispositivo interno de la instalación y un primer enlace de túnel para transmitir datos entre el primer dispositivo alejado de la instalación y el primer dispositivo interno de la instalación, y

- un segundo sistema de servicios remotos con un segundo dispositivo alejado de la instalación para llevar a cabo un segundo servicio remoto, un segundo dispositivo interno de la instalación y un segundo enlace de túnel para transmitir datos entre el segundo dispositivo alejado de la instalación y el segundo dispositivo interno de la instalación.

Con ello el segundo enlace de túnel discurre conforme a la invención a través del primer enlace de túnel.

El enlace de datos con el segundo dispositivo interno de la instalación se realiza de este modo gráficamente mediante un “doble enlace de túnel”, respectivamente “un túnel en un túnel”. Desde el exterior en la instalación sólo se requiere físicamente el primer enlace de túnel, a través del cual después discurre a su vez también el segundo enlace de túnel. Para el gestor de la instalación se produce por medio de esto fundamentalmente solo una complejidad administrativa para el primer enlace de túnel y, de esta forma, sólo para un enlace de túnel en lugar de para dos enlaces de túnel. El primer enlace de túnel puede configurarse con ello de forma especialmente segura, de tal modo que incluso un segundo enlace de túnel relativamente poco seguro puede adquirir el nivel de seguridad del primer enlace de túnel. Por medio de esto puede conseguirse también una elevada seguridad de funcionamiento de la instalación. Mediante el primer enlace de túnel pueden discurrir adicionalmente también otros enlaces de túnel de otros sistemas de servicios remotos, sin que aumente esencialmente la complejidad administrativa por parte del gestor de la instalación y se limite la seguridad de funcionamiento. El primer sistema de servicios remotos se utiliza desde el punto de vista del segundo y dado el caso de otros sistemas de servicios remotos, en sí mismo, como infraestructura de transporte y materializa un enlace seguro de componentes de instalación con un segundo y dado el caso otros suministradores de servicios remotos. Los protocolos del segundo sistema de servicios remotos y dado el caso de otros sistemas de servicios remotos pueden intercambiarse a través de esta infraestructura. Desde el punto de vista del gestor de la instalación se trata de una única solución de servicios remotos integrada.

Con ello se realiza el primer enlace de túnel a través de una plataforma de comunicación segura, que está enlazada con la Internet. Por medio de esto puede instalarse en la instalación en todo el mundo un enlace de túnel desde cada conexión de Internet.

Para aumentar la seguridad la plataforma de comunicación segura se encuentra de forma preferida en una zona desmilitarizada.

Conforme a una configuración especialmente ventajosa, para aumentar todavía más la seguridad se realiza una reflexión de datos en la plataforma de comunicación segura.

La invención puede usarse de forma especialmente ventajosa si el primer enlace de túnel usa una codificación de datos distinta a la del segundo enlace de túnel.

Para que un usuario del segundo sistema de servicios remotos no tenga que autentificarse ante el primero y tampoco ante el segundo sistema de servicios remotos, sino sólo una vez ante uno de los dos sistemas de servicios remotos, los dos sistemas de servicios remotos pueden estar enlazados con un trámite de autentificación común.

A continuación se explican con más detalle la invención y configuraciones ventajosas de la invención, con base en un ejemplo de ejecución en la figura.

Un sistema 1 mostrado en la única figura para llevar a cabo servicios remotos para una instalación técnica 2 (por ejemplo una instalación productiva industrial, una central de energía, una instalación de transporte y distribución de mercancía en piezas o la técnica de edificios en un gran edificio) comprende un primer sistema de servicios remotos 10 y un segundo sistema de servicios remotos 20. A continuación se parte de la base de que los dos sistemas de servicios remotos 10, 20 son usados por el mismo suministrador de servicios remotos para llevar a cabo servicios remotos. Sin embargo, esto es sólo a modo de ejemplo. De forma correspondiente los dos sistemas de servicios remotos 10, 20 pueden ser usados también por suministradores de servicios remotos en cada caso diferentes para llevara cabo servicios remotos.

El primer sistema de servicios remotos 10 comprende un dispositivo alejado de la instalación 2 en forma de un router de acceso 11, un dispositivo interno de la instalación en forma de un router de acceso 12 y una plataforma de comunicación segura 14, que comprende un servidor de acceso 15 y un servidor de datos 16 y que se encuentra en una zona desmilitarizada 17 de la Internet. El router de acceso 12 está conectado a una red 4 no pública interna de la instalación, a la que están también conectados por ejemplo unos componentes 5 de un sistema de automatización de la instalación 2 y un Computerized Maintenance Management System (CMMS) 6 de la instalación 2. El router de acceso 11 se encuentra en una zona desmilitarizada 27 del suministrador de servicios remotos y está enlazado con una red no pública interna 24 (por ejemplo una Intranet) del suministrador de servicios remotos.

Entre el router de acceso 11 y el router de acceso 12 puede establecerse, con ayuda de la plataforma de comunicación segura 14, un enlace de túnel 13 a través de la Internet 3. Los datos de la instalación 2, por ejemplo los datos sobre un proceso de fabricación, procedentes de los aparatos de automatización 5 o del sistema CMMS 6, pueden transmitirse a través del enlace de túnel 13 al suministrador de servicios remotos y, a la inversa, los datos del suministrador de servicios remotos transmitirse a estos componentes. Los datos pueden transmitirse con ello automáticamente o tras una solicitud explícita por parte del suministrador de servicios remotos.

El enlace de túnel 13 no está con ello “transconectado” en la plataforma de comunicación 14, sino interrumpido en el servidor de acceso 5 mediante una funcionalidad “Reverse-Proxy”. Un enlace establecido desde la instalación 2 a

través del router de acceso 12 o por parte del suministrador de servicios remotos a través del router de acceso 11 se termina en el servidor de acceso 15. Los datos con ello transmitidos se archivan en el servidor de datos 16. El servidor de acceso 15 establece después el otro enlace con el suministrador de servicios remotos, respectivamente con la instalación 2, y transmite a través de la misma los datos archivados en el servidor de datos 16.

En la plataforma de comunicación segura 14 se “refleja” de este modo la comunicación entrante. Esta reflexión, sin embargo, sólo tiene lugar para protocolos predefinidos. De esta forma se garantiza que una comunicación entre el suministrador de servicios remotos y la instalación 2 sólo tenga lugar a través de unos protocolos explícitamente autorizados. La citada reflexión y el establecimiento del enlace con la instalación 2, respectivamente con el suministrador de servicios remotos, se realizan exclusivamente una vez realizadas con éxito la autentificación y la autorización en el respectivo router de acceso 11 ó 12, en donde las informaciones de enlace y las claves para ello necesarias se transmiten de forma segura.

Esta arquitectura ofrece una protección fiable contra accesos no autorizados por parte del suministrador de servicios remotos en la instalación y a la inversa, contra accesos desde la Internet, contra la transmisión de virus y programas dañinos similares por parte del suministrador de servicios remotos a la instalación y a la inversa, así como contra un abuso de datos de acceso confidenciales.

Para asegurar la confidencialidad, autenticidad e integridad de la comunicación a través del enlace de túnel se usa de forma preferida el protocolo IPSec. En los routers 1, 12 se encuentran después los puntos finales IP-Sec. Para intercambiar informaciones clave puede usarse el Internet Security Association and Key Management Protocol (ISAKMP).

En el caso del enlace de túnel 13 se trata de forma preferida de un enlace de túnel VPN (Virtual Private Network), es decir, los routers 11 y 12 están configurados como routers VPN con acceso a Internet en banda ancha. De este modo se dispone, con unos costes de comunicación muy reducidos, de grandes anchuras de banda para servicios remotos potentes y también para futuros servicios con valor añadido.

El router de acceso 12 comprueba la autorización del suministrador de servicios remotos para acceder a la instalación 2. En el caso de una autorización entrega al suministrador de servicios remotos una contraseña temporal para acceder al servidor de acceso 15. El suministrador de servicios remotos solicita al servidor de acceso 15 el acceso a la instalación 2 mediante la indicación de su contraseña. El servidor de acceso 15 compara la contraseña con la contraseña obtenida por el router de acceso 12 y, en el caso de una coincidencia, establece el enlace de túnel 13 del suministrador de servicios con la instalación 2. El router de acceso 12 puede estar con ello también ajustado de tal modo, que sólo autorice enlaces entre la instalación 2 y la plataforma de comunicación segura 14.

El primer sistema de servicios remotos 10 ofrece la posibilidad de, mediante una comunicación de datos con los componentes de automatización 5 o el sistema CMMS 6, llevar a cabo servicios remotos como por ejemplo una vigilancia remota, un diagnóstico remoto o actualizaciones de software en los aparatos de automatización 5 o en el sistema CMMS 6 de la instalación 2. Para esto el suministrador de servicios remotos puede acceder, a través de una Engineering-Station 18 conectada a su red interna 24 o un Remote-Service-PC 19 a través del enlace de túnel 13, a los componentes de automatización 5 y al sistema CMMS 6. El primer sistema de servicios remotos 10, sin embargo, tiene sus puntos fuertes sobre todo en una transmisión de datos fiable y segura a través del enlace de túnel 13.

El segundo sistema de servicios remotos 20 comprende un servidor 25 alejado de la instalación, que al igual que el router de acceso 11 del primer sistema de servicios remotos 10, está conectado a la red no pública 24 del suministrador de servicios remotos, y un Client-PC 21 que está enlazado con el servidor 25.

Mediante el sistema de servicios remotos 20 se proporcionan unos servicios, que están disponibles en la instalación 2 por ejemplo en un control CNC 7, un control 8 de la automatización básica o en un Standard-PC 9, que están conectados a la red 4 y a través de la misma están enlazados con el router de acceso 12. El control CNC 7, el control 8 de la automatización básica y el Standard-PC 9 presentan para esto en cada caso un agente de software 22, que es un componente interno de la instalación del sistema de servicios remotos 20. Además de esto pueden estar ligados al sistema de servicios remotos 20 otros componentes, como por ejemplo controles de la automatización de procesos, sistemas MES y sistemas CMMS.

Entre un agente de software 22, aquí el agente de software del control CNC 7, y el Client-PC 21 puede establecerse un enlace de túnel 23, a través del cual pueden transmitirse los datos desde el suministrador de servicios remotos al agente de software 2 del control CNC 7 y a la inversa. La codificación de los datos en el enlace de túnel 23 se realiza con ello por ejemplo con SSL y, de este modo, con una técnica de codificación distinta a en el caso del enlace de túnel 13. Con ello se usa un protocolo como por ejemplo el protocolo https, que permite el uso de un Proxy en el enlace 23.

El enlace de túnel 23 discurre con ello en el enlace de túnel 13 del primer sistema de servicios remotos 10. Desde el exterior en la instalación 2 sólo se dispone de esta forma físicamente de un único enlace de túnel 13 y, de este modo, sólo de un único enlace de túnel. Desde el punto de vista del gestor de la instalación los dos sistemas de servicios remotos 10, 20 forman de este modo una única solución de servicios remotos. Para el gestor de la instalación se obtiene por medio de esto fundamentalmente sólo una complejidad administrativa para el primer enlace de túnel 1. Si éste está configurado con más seguridad que el segundo enlace de túnel 23, el segundo enlace de túnel 23 puede adquirir adicionalmente también el nivel de seguridad del primer enlace de túnel 13. A través del primer enlace de túnel 13 pueden discurrir adicionalmente también otros enlaces de túnel de otros sistemas de servicios remotos.

El segundo sistema de servicios remotos 20 tiene sus puntos fuertes sobre todo en la aportación de servicios con valor añadido (added value), por ejemplo para clientes OEM de productos de automatización. Para estos productos se ofrecen por ejemplo los siguientes servicios remotos:

- Vigilancias remotas de aparatos de control con un registro de eventos en un historial con documentación del estado actual del control en ese momento. Mediante el historial de eventos es posible analizar el estado del control, por ejemplo en el caso de errores, y compararlo con estados anteriores.

- Vigilancias de estados: detección y documentación del estado actual de la máquina sobre la base de pruebas estandarizadas predefinidas y registro continuado de valores característicos de estado. Con ayuda de series de mediciones pueden reconocerse tendencias, para usar las mismas como base de una optimización de las actividades de reparación y mantenimiento. Un operador de máquina puede ejecutar de forma sencilla y rápida estas pruebas predefinidas, sin un equipamiento adicional.

- Acceso remoto a aparatos de control en la instalación.

- Servicios de datos: protección de archivos de control actuales en un servidor del suministrador de servicios, con la posibilidad de reproducir estos de forma controlada en el control, en casos de error, o usarlos como referencia para comparaciones.

- Servicios de workflow: activación de desarrollos de mantenimiento y reparación mediante avisos a través de medios internos y externos al sistema (SMS, e-mail, casos de mantenimiento), planificación, vigilancia y documentación de actividades de reparación en la máquina.

- Servicios administrativos: funciones para la administración del sistema, como por ejemplo instalación y gestión de máquinas, instalación y gestión de usuarios.

Para que un usuario del segundo sistema de servicios remotos 20 no tenga que autentificarse tanto en el segundo sistema de servicios remotos 20 como en el primer sistema de servicios remotos 10, es decir dos veces, puede disponerse de un mecanismo de autentificación común. Esto es posible por ejemplo por medio de que se proporcione un trámite de autentificación 28 común, que esté enlazado a ambos sistemas de servicios remotos 10, 20 de una manera no representada con más detalle. Un usuario sólo tiene que registrarse entonces una vez y después de esto puede conmutar entre ambos sistemas de servicios remotos 10, 20.

La instalación 2, respectivamente su red 4, la plataforma segura 14 y la red 24 del suministrador de servicios remotos están protegidas con ello mediante unos firewalls, no representados con más detalle, contra accesos no autorizados.

REIVINDICACIONES

1. Sistema (1) para llevar a cabo servicios remotos para una instalación técnica (2), que comprende

- un primer sistema de servicios remotos (10) con un primer dispositivo (11) alejado de la instalación (2) para llevar a cabo un primer servicio remoto, un primer dispositivo (11) interno de la instalación y un primer enlace de túnel (13) para transmitir datos entre el primer dispositivo (11) alejado de la instalación y el primer dispositivo (12) interno de la instalación, y

- un segundo sistema de servicios remotos (20) con un segundo dispositivo (21) alejado de la instalación para llevar a cabo un segundo servicio remoto, un segundo dispositivo (22) interno de la instalación y un segundo enlace de túnel (23) para transmitir datos entre el segundo dispositivo (21) alejado de la instalación (2) y el segundo dispositivo (22) interno de la instalación,

caracterizado porque el segundo enlace de túnel (23) discurre a través del primer enlace de túnel (13), y porque se realiza el primer enlace de túnel (13) a través de una plataforma de comunicación segura (14), que está enlazada con la Internet (3).

2. Sistema (1) según la reivindicación 1, caracterizado porque la plataforma de comunicación segura (14) se encuentra en una zona desmilitarizada (17).

3. Sistema (1) según la reivindicación 1 ó 2, caracterizado porque se realiza una reflexión de datos en la plataforma de comunicación segura (14).

4. Sistema (1) según una de las reivindicaciones anteriores, caracterizado porque el primer enlace de túnel (13) usa una codificación de datos distinta a la del segundo enlace de túnel (23).

5. Sistema (1) según una de las reivindicaciones anteriores, caracterizado porque los dos sistemas de servicios remotos (10, 20) están enlazados con un trámite de autentificación común (28).

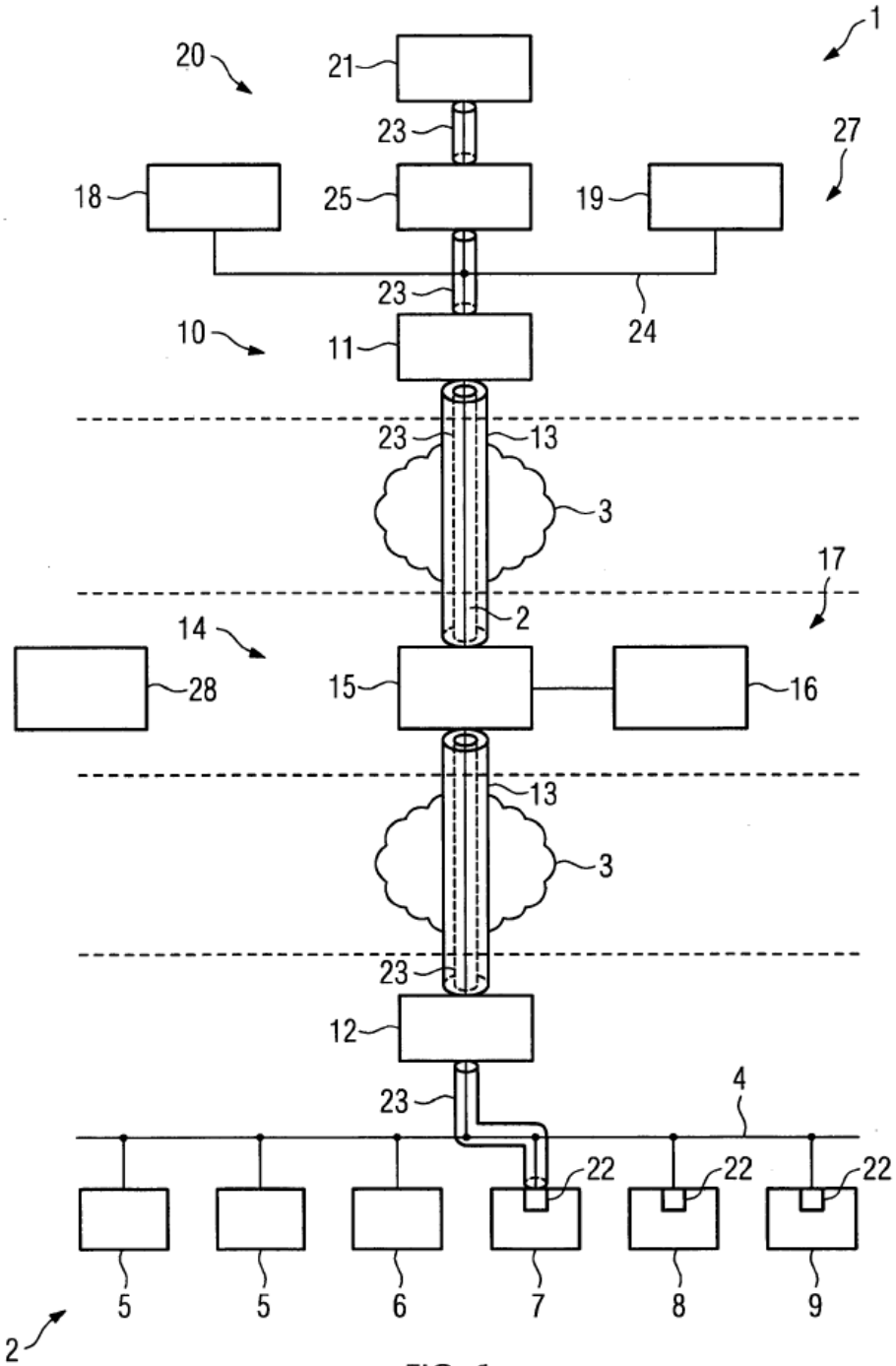
1
20
21
23
27
18
25
19
23
24
10
11
23
13
3
17
2
14
28
15
16
13
3
23
12
23
4
22
22
22
5
5
6
7
8
9
2

FIG. 1