(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 550 193**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.06.2012 E 12728460 (2)**

(97) Fecha y número de publicación de la concesión europea: **29.07.2015 EP 2710782**

(54) Título: **Procedimiento y dispositivo para vigilar un túnel VPN**

(30) Prioridad:

29.06.2011 DE 102011078309

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.11.2015

(73) Titular/es:

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

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y DISPOSITIVO PARA VIGILAR UN TÚNEL VPN

DESCRIPCIÓN

La invención se refiere a la protección de aplicaciones relevantes para la seguridad en un túnel VPN/red privada virtual. Las aplicaciones VPN industriales se conocen ya en múltiples formas. Con ellas pueden proporcionarse por ejemplo enlaces protegidos criptográficamente entre células de fabricación de un sistema de automatización de la fabricación. Igualmente pueden proporcionarse así enlaces con equipos como por ejemplo sistemas de control de agujas o señales para dar vía libre al tráfico en la automatización ferroviaria, que se controlan y vigilan desde un puesto central de control como una cabina de maniobra, así como enlaces para el mantenimiento a distancia seguro de un sistema de automatización.

Los túneles VPN, que conectan entre sí tales sistemas de automatización y sus componentes y/o sistemas de control y aparatos de control para la comunicación de datos, deben funcionar correctamente. Esto es necesario para garantizar fiablemente las llamadas exigencias de seguridad (safety) de la correspondiente instalación.

Por la técnica de comunicación se conocen por ejemplo distintas clases de redes privadas virtuales. Hay diferentes clases de redes privadas virtuales relacionadas con la codificación de la comunicación. Ejemplo de ello son protocolos de seguridad, como MACsec/MediumAccess-security, IPsec/InternetProtocol-security o SSL/TLS, así como protocolos Layer2 tuneleados sobre un protocolo de IP utilizando protocolos de comunicación, como L2TP o PPTP.

Bajo safety o seguridad funcional se entiende en general la seguridad del servicio. El objetivo es la inexistencia de peligro en un lugar y subjetivamente la certeza de estar protegidos frente a posibles peligros. Expresado de otra forma, la seguridad significa estar protegido frente a amenazas o daños. En relación con ello, pueden dividirse los objetivos de protección para un sistema de comunicación por ejemplo en categorías como confidencialidad, integridad, autenticidad o compromiso. Al respecto la confidencialidad puede consistir en que un mensaje no pueda ser leído por terceros. La integridad quiere decir que un mensaje no está manipulado. La autenticidad está relacionada con la comprobación de la identidad del emisor y/o del receptor. El compromiso se relaciona con la autoría de un mensaje.

En el ejemplo de la vigilancia de una carcasa para detectar una variación no autorizada, puede procederse como sigue:

Se establece un firewall (cortafuegos) industrial con función VPN/red privada virtual integrada, que proporciona a través de un contacto de señalización una señal de estado para vigilar la funcionalidad del aparato. Por medio de este contacto de señalización se realiza la señalización al interrumpirse el contacto. Al respecto pueden presentarse a modo de ejemplo los siguientes fallos funcionales:

- la caída de tensiones de alimentación,
- una avería permanente en el aparato, como fuente de alimentación interna,
- el estado defectuoso del enlace de al menos un puerto (port)/conexión correspondiente a un enlace interrumpido con un aparato de la red,
- sobrepasar o quedar por debajo de los valores de umbral ajustados para la temperatura, o
- la retirada de un adaptador de autoconfiguración ACA.

Una red privada virtual VPN convencional sirve para conectar abonados de una red a otra red. Al respecto no tienen que ser compatibles estas redes entre sí. Expresado sencillamente, se reduce la red originaria desde el punto de vista del enlace VPN a la función de un cable de prolongación que conecta el abonado VPN exclusivamente con el punto de conexión de la otra red, por lo general una pasarela VPN/acoplador de red. En función del protocolo VPN utilizado, puede complementarse por ejemplo una codificación adicional, que posibilita una comunicación segura frente a la escucha y a la manipulación entre los interlocutores VPN.

Una llamada SSL-VPN, también denominada VPN basada en web, apoya un modo VPN en el sentido de la VPN convencional. Al respecto se utiliza un protocolo SSL o un protocolo TLS. Bajo la misma denominación corren también sistemas con un acceso a distancia sobre aplicaciones de empresa y recursos de utilización conjunta. Esto significa que por ejemplo un interlocutor SSL-VPN puede acceder a través de un enlace asegurado, pero sin obtener un acceso directo a la red de la empresa.

En general puede considerarse una red VPN como una red autónoma, encapsulada en otra red. Al respecto se utiliza en el uso diario por lo general una red IP virtual, que dentro de otra red IP, la mayoría de las veces la Internet pública, forma una sección de red cerrada en sí misma.

Se conocen las llamadas herramientas de monitorización VPN para vigilar un túnel VPN. También se sabe que mediante SNMP puede vigilarse el estado de un túnel VPN. De esta manera se dispone en un sistema de gestión de la red separado de una información sobre enlaces de red VPN que no funcionan, para por ejemplo informar a un administrador de red. Además se conocen herramientas que finalizan determinados procesos de aplicación en un PC de un puesto de trabajo bajo Windows, caso de que no exista ningún túnel VPN en el PC del puesto de trabajo. Con ello se impide el envío de mensajes confidenciales mediante un proceso de aplicación del PC del puesto de trabajo a través de un enlace desprotegido.

Las llamadas herramientas (tools) de monitorización de red para la vigilancia general de componentes de red y/o del estado de la red, se conocen igualmente. Con ellas se comprueba por ejemplo si están conectados aparatos ajenos a una determinada red, o si se han conectado a posteriori. Se conocen herramientas de gestión de la red para vigilar sistemas IP y redes, vigilándose en particular componentes VPN y/o funciones de red. Bajo sistemas NAC se entienden sistemas de vigilancia del acceso a red que detectan si están conectados a la red aparatos conforme a las reglas.

El documento US 2003/200456 A1 describe una vigilancia de un túnel IP-sec entre pasarelas o terminales, impidiendo una comunicación de falta el envío de más paquetes cuando se detectan paquetes no codificados en el túnel IP-sec.

No se conoce hasta ahora una vigilancia integral de túneles VPN que se utilice para controlar aparatos de control en relación con funciones de seguridad/funciones safety.

La invención tiene como objetivo básico vigilar un túnel VPN tal que queden garantizadas funciones de control en un aparato de control con seguridad de servicio correspondiente a las llamadas funciones safety.

Este objetivo se logra mediante la correspondiente combinación de características de las reivindicaciones formuladas independientemente.

La invención se basa en la comprensión de que el mando de un aparato de control mediante un sistema de control puede configurarse con seguridad de servicio cuando esto se realiza mediante un túnel VPN que por lo general está asegurado criptográficamente. Para ello, en un sistema de control que utiliza en o para el túnel VPN uno o varios terminales (boxes) VPN, resulta posible una comunicación disponible para transmitir órdenes de control sólo cuando se dispone también realmente de un túnel VPN adecuado.

Un túnel VPN en condiciones de funcionar puede constituir la base para procesos de control relevantes para la seguridad de funcionamiento seguro. Las eventuales faltas se detectan tempranamente y no solamente mediante un fallo total cuando por ejemplo ya no llega ningún dato.

Se propone un mecanismo que vigila la funcionalidad y en un perfeccionamiento también la calidad de un túnel VPN establecido. Para ello se emite una información generada por una unidad de evaluación en forma de la correspondiente señal física o lógica a un sistema de control y/o un aparato de control. Esta señal puede también mostrarse en diversos puntos.

Para la evaluación en el curso de la vigilancia del túnel VPN, pueden utilizarse distintos procedimientos de comprobación. Los procedimientos considerados presentan por lo general componentes de codificación. Para la protección criptográfica de una comunicación de datos se conocen distintos procedimientos. El túnel VPN se prueba por ejemplo con datos usuales, evaluándose determinadas características de la transmisión de datos, determinados valores de umbral, tasas de retardo o de falta.

Se controlan por ejemplo aparatos de control tal como los que se utilizan en la automatización en la energía o en un sistema de automatización ferroviario o en un sistema de control de tráfico, por ejemplo control de semáforos, rótulos cambiantes o interruptores para accionar agujas o barreras ferroviarias o para conectar una estación distribuidora de energía o una estación transformadora, así como sensores para captar un consumo de electricidad, una temperatura o una señal de estado de un actuador, por ejemplo "barrera cerrada".

Una VPN-Box aporta una señal de liberación/Safe-For-Use que reproduce un determinado estado. Cuando se ha emitido esta señal, funciona correctamente el túnel VPN. La señal se realiza preferiblemente como señal de hardware separada. Alternativamente puede señalizarse la información relacionada con la misma también mediante una señal física de una interfaz de comunicación en dirección hacia el sistema de control y/o el aparato de control. Con ello se proporciona tras una comprobación una información que indica si existe un túnel VPN en condiciones de funcionar.

Es especialmente ventajoso dificultar y/o impedir mediante el envío de mensajes de comprobación a través de un túnel VPN por ejemplo un análisis del flujo de tráfico y ataques de canal lateral.

Precisamente con ello se impide que desde el exterior puedan extraerse conclusiones relativas al estado del sistema en ese momento y/o a las acciones de automatización.

Puesto que entre un sistema de control, por ejemplo una cabina de maniobra, y un aparato de control es necesaria una comunicación de datos, se intercambian por ejemplo mensajes de mando. La comunicación se realiza ventajosamente a través de una red Ethernet o IP. Estos mensajes de mando se transmiten a través de una red que está sometida a potenciales ataques. Por esta razón se sitúa en el túnel VPN, en cada caso en el lado del sistema de control y en el lado del aparato de control una VPN-Box, que codifica criptográficamente mensajes de mando cuando se transmiten a través de la red. Una VPN-Box dispone de claves criptográficas fijas o configurables, para establecer cuando se crea un enlace VPN claves de sesión, que son necesarias para proteger los mensajes VPN.

Una señal que indica la seguridad del servicio/Safe-for-use, es generada por una VPN-Box. La misma puede sacarse hacia fuera como señal física separada, como señal de conexión. Alternativamente puede proporcionarse la misma como señal lógica a través de la interfaz de comunicación hacia el aparato de control.

Para detectar la señal de la seguridad del servicio se utilizan distintas formas de vigilancia. En el marco de la vigilancia se intercambian mensajes de comprobación a través del túnel VPN y/o con la otra VPN-Box. Éstos pueden igualmente estar protegidos mediante claves de sesión o preferiblemente estar afectados por una clave de sesión de monitorización Mo-SK separada. Esta codificación puede establecerse mediante una función de deducción de clave. Alternativamente puede establecerse un acuerdo de claves separado. En otra variante están configuradas para la monitorización claves criptográficas separadas.

Resultan ventajas especiales cuando la señal de seguridad del servicio que indica que la funcionalidad del túnel VPN es correcta se lleva al sistema de control central de la correspondiente VPN-Box asociada.

En el marco de la invención puede utilizarse una VPN-Box también para otros escenarios de control. En el mando de aparatos de control para la automatización en la energía desde un puesto de mando o para el control de un ferrocarril industrial que no dispone de un conductor del tren, puede utilizarse una VPN-Box con túnel VPN.

Para aumentar la seguridad en la vigilancia de un túnel VPN puede ventajosamente establecerse un canal de comprobación separado, a través del que por ejemplo se transmitan o desarrollen avisos de falta o comprobaciones de estado. Esto puede utilizarse también para un túnel inactivo, que por ejemplo sólo opera en standby, en el que por lo tanto no se transmite ningún dato de usuario.

Ventajosamente se transmiten mensajes de comprobación cuando no se transmite ningún dato de mando del aparato de control y/o datos de mando del sistema de control a través del túnel VPN. En una variante se transmiten mensajes de comprobación cuando la carga de la red correspondiente a los datos de mando del aparato de control y/o a los datos de mando del sistema de control a través del túnel VPN se encuentran por debajo de un valor de umbral predeterminado, por ejemplo por debajo de 5 mensajes por segundo o por debajo de 1000 bytes por segundo.

En la vigilancia pueden medirse y comprobarse en general retardos, tasas de falta y similares como parámetros. Una etapa adicional consiste en la comprobación de si se cumplen los valores de umbral.

Es especialmente ventajosa para vigilar un túnel VPN la marca de tiempo correspondiente a diversos mensajes entre un sistema de control y un aparato de control o bien entre distintas VPN-Boxes. Así puede filtrarse la representación de datos en el sentido de que sólo existan datos codificados o bien que se compruebe si en el túnel todos los datos que allí deben transmitirse también existen en el túnel. Visto de otra manera, no debe presentarse ninguno de los datos en cuestión fuera del túnel.

Otra posibilidad adicional ventajosa para vigilar un túnel VPN consiste en vigilar el canal de texto explícito, pudiéndose detectar entonces componentes ajenos inesperados. Así puede detectarse por ejemplo una falta de la VPN-Box en base a que los datos de mando del aparato de control conectado no se transmitan codificados, sino en texto explícito.

En el caso de que en una VPN-Box se detecte un problema en la vigilancia del correspondiente túnel VPN, al existir una desviación entre un perfil predeterminado de un sistema o de un aparato y un perfil detectado, puede forzarse con un ·Reset" un rearranque de los componentes de software. Alternativamente puede desactivarse la VPN-Box, con lo que solamente puede ejecutarse una reactivación a través de una interfaz de mantenimiento. Este estado corresponde a una ausencia de señal de seguridad del servicio/Safe-for-Use. En este caso se coloca o activa en un aparato de control un programa de emergencia que garantiza un estado de servicio seguro. Entonces se traslada un aparato de control unido con la VPN-Box a un estado seguro para el servicio.

La generación de un llamado mensaje “Log”, por ejemplo a través de SNMP o mediante “syslog”, puede ser ventajosa para posibilitar un posterior análisis del funcionamiento incorrecto.

Además de generar una señal de seguridad del servicio, puede emitir una VPN-Box también la correspondiente señal de alarma a través de un segundo y/o alternativo canal de comunicación. Como ejemplo de aplicación citemos un control de agujas por línea física que señaliza el fallo de un enlace de comunicaciones VPN a través de una interfaz inalámbrica a un puesto central o a trenes que se encuentran en el tramo correspondiente.

Es ventajoso que una VPN-Box informe a un sistema local sobre el fallo del enlace de comunicaciones en la red. Con ello puede detenerse controladamente el sistema local. El objetivo de ello es mantener regularmente un estado de servicio seguro en un aparato de control.

A continuación se describirá en base a figuras esquemáticas la invención en base a ejemplos de ejecución no limitativos. La

figura 1 muestra esquemáticamente la vigilancia de un túnel VPN criptográfico 8 entre el sistema de control 1 y el aparato de control 2, que puede significar una señal, una aguja o una barrera,
figura 2 muestra la estructura básica de una VPN-Box 6,
figura 3 muestra la secuencia de una rutina en el túnel VPN 8 mediante una VPN-Box 6 cuando se inicia un módulo de comprobación VPN interno, que comprueba continuamente el correcto funcionamiento del túnel VPN.

La figura 1 muestra una representación correspondiente a la invención de un túnel VPN 8. Entre un sistema de control 1 y un aparato de control 2 se ha establecido un túnel VPN 8. El sistema de control 1 puede ser por ejemplo una cabina de maniobra. Como aparato de control se controlan distintos componentes o sistemas, como por ejemplo en el tráfico ferroviario: señales, agujas, barreras o en el ámbito industrial: aparatos para controlar aparatos de automatización en la energía o similar. La distancia entre el sistema de control 1 y el aparato de control 2 se cubre mediante el túnel VPN 8. Éste puede realizarse parcialmente o por completo mediante enlaces por línea física. Las circunstancias locales pueden hacer necesarios enlaces inalámbricos para transmitir datos.

Debido a la pluralidad de enlaces de datos, se constituyen para determinados sistemas redes claramente delimitadas por ejemplo en cuanto a las características técnicas, al operador y a la calidad.

En la figura 1 se utiliza una red 3 que sirve para realizar el túnel VPN 8. Es decir, el tráfico de datos entre un sistema de control 1 y un aparato de control 2 puede desarrollarse mediante intercambio de mensajes de mando. La comunicación se realiza por ejemplo a través de una red Ethernet o de una red IP. Estos mensajes de mando se transmiten a través de la red 3, que está sometida a ataques potenciales. Esto resulta en particular de que se utilizan redes públicamente accesibles, como Internet, WLAN, redes de telefonía móvil. Por esta razón se prevén en el túnel VPN 8, en las proximidades del sistema de control 1 y en las proximidades del aparato de control 2 respectivas VPN-Box 6, que protegen criptográficamente mensajes de mando 4 en la transmisión a través de la red 3. Además puede disponer una VPN-Box por ejemplo de claves criptográficas fijas o configurables, para generar al establecer un enlace VPN claves de sesión, que se utilizan para proteger criptográficamente los mensajes de mando. La VPN-Box 6 decodifica y/o codifica mensajes de mando del aparato de control 2, con lo que los mismos quedan protegidos criptográficamente durante la transmisión a través de la red 2. Un mensaje de mando en texto explícito se transmite entre la VPN-Box 6 y el aparato de control 2 mediante un enlace de comunicaciones local no protegido criptográficamente, por ejemplo una red Ethernet. Este enlace de comunicaciones puede estar protegido por ejemplo físicamente, colocando la VPN-Box 6, el aparato de control 2 y el enlace de comunicaciones local situado entre ambos en un armario de maniobra cerrado.

Para la transmisión a través de una red pueden utilizarse distintos protocolos.

En la figura 1 se representa además una señal de seguridad en el servicio/señal Safe-for-Use 7 entre la VPN-Box 6 y el aparato de control 2 en forma de una flecha. Esta VPN-Box 6 genera la señal de seguridad en el servicio SFU 7, en el caso de que la comprobación del túnel VPN 8 haya dado como resultado que es posible una transmisión de datos correcta, es decir, que el túnel VPN 8 funciona correctamente.

Una variante para vigilar el túnel VPN 8 prevé la utilización de mensajes de comprobación 5 entre las VPN-Boxes 6. Con ello se dificulta por ejemplo un análisis del flujo de tráfico o un ataque de canal lateral, que permitiría sacar conclusiones relativas al estado del sistema en ese momento y/o a acciones de automatización. Aún cuando en la figura 1 las flechas para mensajes de mando 4 y para mensajes de comprobación 5 se representan fuera de la zona central del túnel 8, se transmiten estos mensajes dentro del túnel VPN 8. Esto no impide la utilización de un túnel VPN adicional paralelo.

La VPN-Box 6 representada en la figura 2 reproduce la estructura interna de una VPN-Box 6. Ésta contiene los siguientes componentes:

20 hardware (HW Security Modul),
21 IKE (V1/V2),
22 Management Interface (interfaz de gestión),
23 USB,
24 IPsec,
25 IP,
26 activador de Ethernet,
27 NIC, interfaz de comunicación,
28 Monitor VPN
7 señal de seguridad en el servicio/Safe-for-Use/SfU

Al respecto interactúan los distintos componentes como sigue:

Dos interfaces de comunicación se realizan como interfaz de hardware 27/Network Interface Connector NIC 27 a través de Ethernet. El control se realiza mediante un activador de Ethernet 26. Una pila de comunicación de IP realiza la comunicación de IP 25 entre ambas interfaces. Un protocolo IPsec 24 protege la comunicación de IP y/o el túnel VPN 8. Las relaciones de seguridad Security Association SA e IPsec se establecen mediante un protocolo IKE 21. La o bien las clave/s criptográficas configurables o fijas, por ejemplo Secret Key SK, Private Key, Public Key o certificados, están memorizadas preferiblemente en un módulo de seguridad de hardware 20.

El monitor de VPN vigila un túnel VPN 8 establecido y preparado y proporciona en función del resultado de una comparación una señal de liberación o de seguridad en el servicio/señal Safe-For-Use SfU 7. Mediante una interfaz de gestión 22, por ejemplo USB 23, pueden realizarse ajustes de la configuración de la VPN-Box 6. Además pueden estar previstos sensores, que detectan la apertura de una carcasa o daños, así como un funcionamiento fuera de la gama de temperaturas prevista, etc.

La figura 3 muestra la estructura de un túnel VPN 8 con una VPN-Box 6. En paralelo a ello se arranca un módulo de comprobación VPN interno, que en base a un fichero de parámetros de comprobación leído comprueba continuamente el correcto funcionamiento del túnel VPN. En caso de falta, no se aporta ninguna señal Safe-for-Use 7. También puede informarse a un sistema central sobre una avería a través de un canal de comunicación alternativo.

La figura 3 muestra en conjunto los siguientes componentes:

30 arranque
31 lectura de parámetros VPN
32 arranque túnel VPN 8
33 lectura de los parámetros de comprobación VPN
34 arranque de los parámetros de comprobación VPN
35 vigilancia del túnel VPN 8 en función de los parámetros de comprobación
36 desviación
37 SÍ
38 señalización del estado al sistema central y/o sistema de control
39 NO
40 intercambio de mensajes

Según el esquema secuencial de la figura 3 se comprueba la funcionalidad de un túnel VPN 8. Esta comprobación puede realizarse por ejemplo comparando un perfil real, que caracteriza el estado actual efectivamente existente del enlace VPN, con un perfil archivado.

Si resulta una desviación en uno o varios parámetros, se emite en el nodo de decisión para una desviación 36 por ejemplo una señalización del estado 38 a un sistema central, como el sistema de control 1. Los resultados tomados como base de la comprobación se fundamentan en reglas VPN.

Si según la figura 3 la decisión relativa a si existe una desviación 36 o no es que “no” 39, entonces se realiza un intercambio de mensajes, por ejemplo un intercambio de mensajes de mando 4. Se aporta entonces una señal Safe-for-Use.

Si se vigila adicionalmente un túnel VPN 8 en cuanto a la calidad, ello puede realizarse por ejemplo como sigue:

Primeramente puede realizarse una vigilancia de una autentificación realizada con éxito de uno o varios interlocutores de comunicación, con lo que puede detectarse que existe el túnel VPN 8.

A continuación se realiza la vigilancia para comprobar que se cumple un acuerdo de seguridad predeterminado, por ejemplo Re-Keying, la utilización de Ciphersuites predeterminadas, autentificación o también autorización.

Los sensores de carcasa conectados directa o indirectamente con una VPN-Box 6 pueden asumir la vigilancia de un armario empotrado, en el que está alojada la VPN-Box.

Mediante el envío de mensajes de comprobación VPN 5 a través del túnel VPN 8 se aportan datos de usuario, así como mensajes de fondo que impiden o al menos dificultan un análisis del flujo de tráfico en las correspondientes pausas de emisión.

El componente de comprobación VPN puede realizar una vigilancia y señalización continua de los mensajes de comprobación intercambiados, así como de los datos de usuario propiamente dichos.

REIVINDICACIONES

1. Procedimiento para vigilar un túnel VPN (8) establecido y protegido criptográficamente en cuanto a funcionalidad, con al menos una VPN-Box (6) posicionada en el túnel VPN (8), **caracterizado porque** el túnel VPN (8) está establecido para la comunicación de datos entre un sistema de control (1) y un aparato de control (2) y la VPN-Box (6) aporta una señal de seguridad en el servicio (7) al aparato de control (2) cuando la vigilancia ha dado como resultado que el túnel VPN (8) cumple con las características predeterminadas, con lo que en el aparato de control (2) puede iniciarse o mantenerse un estado de servicio regular.

2. Procedimiento según la reivindicación 1, **caracterizado porque** en el túnel VPN (8), próxima espacialmente al sistema de control (1) y/o próxima espacialmente al aparato de control (2) se utiliza en cada caso la VPN-Box (6), de las que al menos hay una, transmitiéndose al menos un mensaje de mando (4) a través de una red (3).

3. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** a través del túnel VPN (8) se envía al menos un mensaje de comprobación (5).

4. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** la señal de seguridad en el servicio (7) de la VPN-Box (6), de las que al menos hay una, se lleva al sistema de control (1) y/o al aparato de control (2).

5. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** la señal de seguridad en el servicio (7) es una señal física que confirma la funcionalidad del túnel VPN (8).

6. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** en el sistema de control (1) se realiza la evaluación de la correcta funcionalidad del túnel VPN (8).

7. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** para la comunicación de datos en el túnel VPN (8) se utiliza una red Ethernet o una red IP (3).

8. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** la VPN-Box (6), de las que al menos hay una, dispone de claves criptográficas preparadas para proteger el mensaje VPN (4), de los que al menos hay uno.

9. Procedimiento según la reivindicación 8, **caracterizado porque** se establece un acuerdo de claves separado.

10. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** para vigilar el túnel VPN (8) se intercambia al menos un mensaje de comprobación (5) entre varias VPN-Boxes (6) unilateral o mutuamente.

11. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** la VPN-Box (6), de las que al menos hay una, emite para el mando de distintos aparatos de control (2) para distintas funciones electromecánicas, una señal de seguridad en el servicio (7) cuando la funcionalidad del túnel VPN (8) es la correcta.

12. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** adicionalmente a la vigilancia del túnel VPN (8) se vigila la funcionalidad de su calidad.

13. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** se establece un túnel VPN (8) separado como canal de comprobación para comprobaciones del estado o avisos de falta.

14. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** para la vigilancia del túnel VPN (8) se miden tasas de retardo de datos o tasas de falta y se comparan con valores de umbral fijados.

15. Procedimiento según una de las reivindicaciones precedentes, **caracterizado porque** se realiza una vigilancia de un túnel VPN (8) mediante comparación de la marca de tiempo de distintos mensajes que se transmiten a través del túnel VPN (8).

16. Procedimiento según una de las reivindicaciones precedentes,

caracterizado porque en la vigilancia de un túnel VPN (8) se conducen todos los datos previstos para transmitirlos en el túnel VPN (8) a través del túnel VPN (8).

17. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque se realiza una vigilancia del canal de texto explícito.

18. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque cuando se detecta un problema en el túnel VPN (8), se realiza un rearranque o una desactivación de una o varias de las VPN-Boxes (6), de las que al menos hay una.

19. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque para realizar un posterior análisis de una avería funcional se transmite un mensaje LOG a través de vías de transmisión separadas.

20. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque cuando falla la comunicación VPN, se envía un mensaje a un puesto central o local, para que pueda llevarse un sistema local a un estado seguro para el servicio.

21. Dispositivo para realizar una vigilancia de un túnel VPN (8) establecido y protegido criptográficamente en cuanto a funcionalidad y/o calidad según una de las reivindicaciones 1 - 20, con al menos una VPN-Box (6) posicionada en el túnel VPN (8),
caracterizado porque el túnel VPN (8) está preparado para la comunicación de datos entre un sistema de control (1) y un aparato de control (2) y existe la VPN-Box (6) para la vigilancia y mediante la misma puede aportarse una señal de seguridad en el servicio (7) al aparato de control (2), cuando el resultado de la vigilancia es que el túnel VPN (8) cumple con características prescritas, con lo que en el aparato de control (2) puede establecerse o mantenerse un estado de servicio regular.

22. Dispositivo según la reivindicación 21,
en el que existe una VPN-Box (6) posicionada en el túnel VPN (8) para la vigilancia,
la evaluación relativa a la correcta funcionalidad y/o calidad del túnel VPN (8) se realiza al menos parcialmente en el sistema de control (1) y puede aportarse una señal de seguridad en el servicio (7) al aparato de control (2) cuando el resultado de la vigilancia es que el túnel VPN (8) cumple con características prescritas, con lo que en el aparato de control (2) puede establecerse o mantenerse un estado de servicio regular.

FIG 1

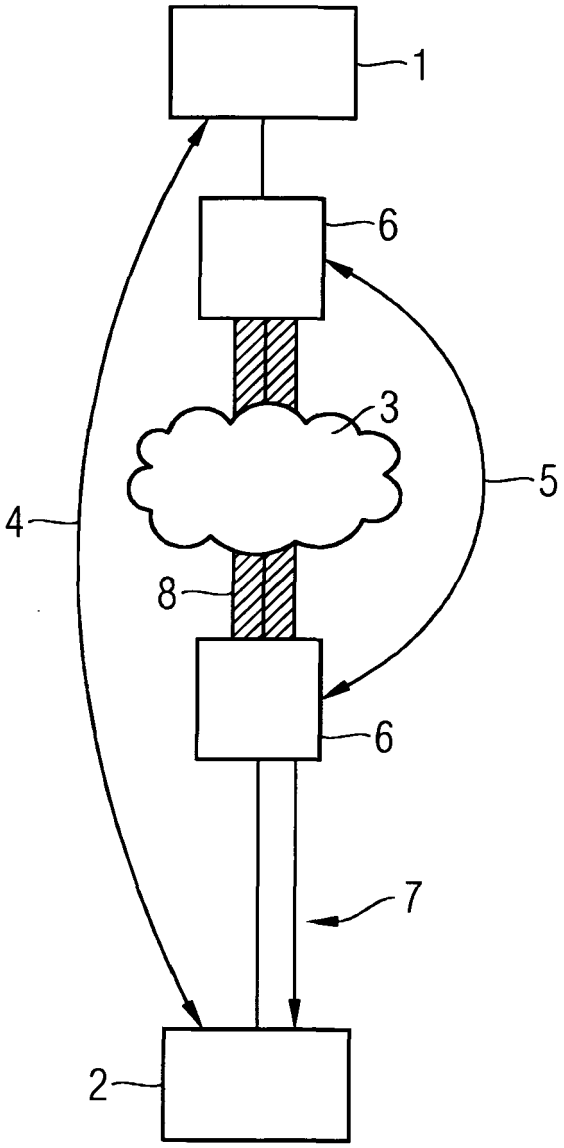

FIG 2

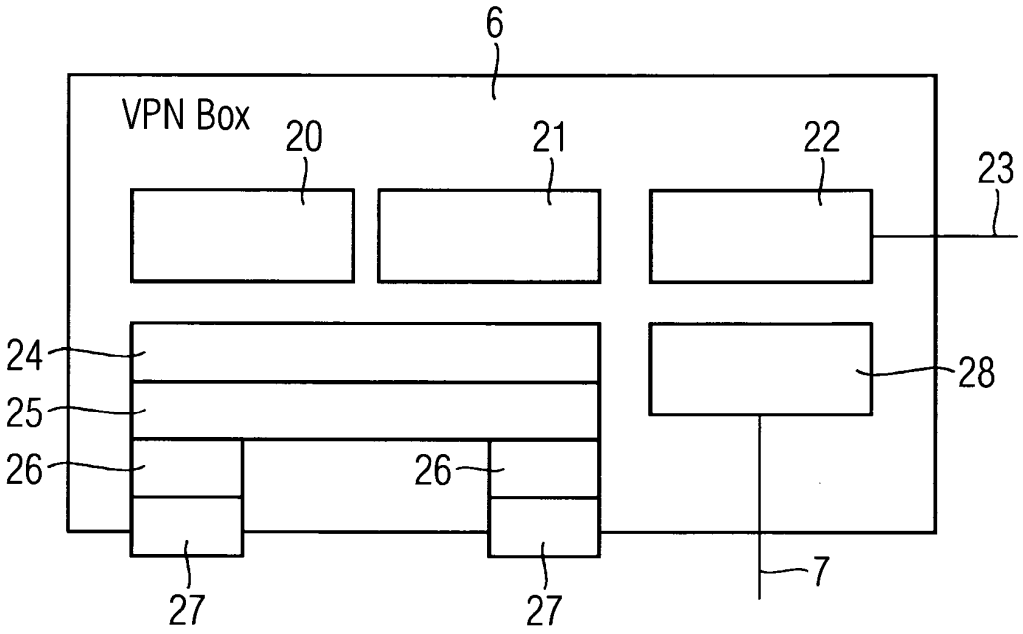

FIG 3