(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 663 295**

(51) Int. CI.:

G06F 19/00 (2008.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.05.2007 E 10172615 (6)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2018 EP 2381377**

(54) Título: **Dispositivo y procedimiento para la protección de un aparato médico y de un paciente tratado con dicho aparato, contra influencias peligrosas procedentes de una red de comunicaciones**

(30) Prioridad:

25.05.2007 DE 102007024720
03.06.2006 DE 102006026088

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.04.2018

(73) Titular/es:

B. BRAUN MELSUNGEN AG (100.0%)
Carl-Braun-Strasse 1
34212 Melsungen, DE

(72) Inventor/es:

STEINKOLGER, ALEXANDER;
LAUER, HANS-MARTIN y
PREUS, NIKO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo y procedimiento para la protección de un aparato médico y de un paciente tratado con dicho aparato, contra influencias peligrosas procedentes de una red de comunicaciones

La presente invención se refiere a un dispositivo para su integración en un aparato médico, el cual es apropiado para su conexión en una red de comunicaciones que presenta, como mínimo, una zona no segura y también, en el lado que corresponde al aparato, una zona segura. Además, la presente invención se refiere a un aparato médico el cual es apropiado para su conexión en una red de comunicaciones que tiene, como mínimo, una zona no segura y, en el lado que corresponde al aparato una zona segura, así como a un sistema médico con múltiples aparatos médicos o aparatos parciales del tipo mencionado. Además, la invención se refiere a un procedimiento para el control de un dispositivo correspondiente para su integración en un aparato médico.

En el campo médico, la mayor parte de los aparatos han sido concebidos en el pasado en forma de aparatos autónomos. No obstante, en la actualidad, una proporción creciente de dichos aparatos están conectados a redes de comunicaciones. La razón de ello consiste parcialmente en una mayor conciencia en cuanto a costes en los aparatos médicos, en la mejora de los procesos utilizados, el almacenamiento parcialmente central de datos y, por lo tanto, la necesidad de utilización de redes de comunicaciones y también la creciente complejidad de los aparatos médicos, que hacen que su materialización con su propio sistema de ordenador no se pueda realizar o que sea muy costoso. Por esta razón, los aparatos médicos individuales complejos son, de hecho, sistemas que se basan en una serie de subsistemas de ordenador propios, los cuales están unidos entre sí mediante una red de comunicaciones y que contribuyen conjuntamente a la funcionalidad general del aparato médico. Por otra parte, se conocen muchos sistemas compuestos de aparatos médicos individuales que consiguen una funcionalidad conjunta solamente por la interacción de los aparatos médicos individuales contenidos en el sistema, cuya funcionalidad no se podría conseguir por los aparatos individuales. Por esta razón, estos sistemas constituyen aparatos médicos, incluso aparatos médicos que presentan una complejidad más elevada que los subsistemas/aparatos médicos que contienen. Por ejemplo, en el campo de las bombas de infusiones, se puede conseguir un valor adicional sensible cuando se pueden reunir bombas en un sistema de bombas conjunto dentro del cual las bombas comunican entre sí. Cuando este sistema de bombas puede comunicar también aún con el entorno, posibilita la transmisión de datos de las infusiones que se producen por el sistema de bombas en los pacientes atendidos mediante las infusiones, hacia un sistema de información hospitalario. En este caso, es posible el considerar el sistema de bombas de infusiones como un aparato médico en el sentido que se describe en la presente invención.

También se observa en los últimos años, a causa de la reducción de costes, un traslado creciente de pacientes desde los cuidados estacionarios a cuidados ambulantes que, no obstante, solamente pueden conducir a una reducción evidente de los costes que se originan cuando los datos médicos que se generan pueden ser transmitidos con el objeto de análisis y evaluación a la instalación médica correspondiente de manera rápida y eficaz. Esto tiene lugar también de manera creciente con ayuda de redes de comunicaciones.

En este contexto aparecen, no obstante, una serie de dificultades y fuentes de peligros que aumentan la importancia de una elevada seguridad necesaria, especialmente por el tratamiento de pacientes o en el servicio de aparatos médicos. Mediante la utilización de redes de comunicaciones en este campo se produce, por lo tanto, un nuevo tipo de peligro para los pacientes, o bien para los operadores de los aparatos médicos. Es posible que, mediante la interacción que se produce por la red de comunicaciones, el aparato médico sufra alteraciones de tal manera que puedan conducir a poner en peligro al paciente objeto de tratamiento o a un fallo de las funciones del aparato médico. Este tipo de interacción, que puede llevar a que se produzca una posible situación de peligro por el aparato médico, se designará a continuación como “ataque” al aparato médico. Un ataque de este tipo puede ser provocado, por ejemplo, por el software, que intente de manera intencionada conseguir fallos de seguridad para entrar en datos contenidos en el sistema de ordenador del aparato médico, que son confidenciales y utilizables solo de forma delictiva por terceros o para falsificar dichos datos. Este tipo de software se designará a continuación con la expresión “malware”. Dado que el “malware” altera o corrompe los objetivos de la funcionalidad de un sistema de ordenador para espiar los datos o falsificar los mismos, se debe evitar en ese caso en especial el riesgo para los pacientes o para el funcionamiento correcto del aparato médico cuando éstos son atacados por el “malware”.

Para poder garantizar la seguridad de los datos y el mantenimiento del secreto de los datos contenidos en la red, se parte habitualmente, en el desarrollo de redes de comunicaciones, de partes de la red de comunicaciones con diferentes niveles de seguridad. En los interfaces entre estas zonas se instalan habitualmente mecanismos de seguridad tales como, por ejemplo, los llamados cortafuegos. El centro de gravedad de un aseguramiento de este tipo de los mecanismos de seguridad antes mencionados se encuentra justificado en la actualidad, no obstante, en su mayor parte en el sector comercial, para garantizar la seguridad de datos y el mantenimiento del secreto y no es apropiado o lo es solo de manera incompleta para las exigencias que caracterizan los aparatos médicos.

Es incluso posible que se genere un ataque a un aparato médico a través de otro participante en la comunicación, habitualmente aparatos médicos, dentro de la parte considerada como segura de una red de comunicaciones, aunque los participantes en la comunicación individuales funcionen sin fallos y muestren un comportamiento de comunicaciones que se considere por su parte como cooperativo, puesto que, no obstante, en suma y por determinadas situaciones se puede producir una alteración. Esto es comparable a las colas que se forman en una

autopista, que se producen por una determinada densidad de vehículos de forma espontánea, es decir, sin una causa externa identificable. De manera alternativa, un ataque a un aparato médico puede tener lugar por parte de otros aparatos médicos dentro de la parte considerada como segura de una red de comunicaciones cuando los protocolos de comunicación de dos tipos de aparatos médicos conducen a posibles fallos de interpretación o por la comunicación de los aparatos médicos, el otro aparato médico quede sobrecargado.

De manera específica, aumenta el peligro potencial cuando para la fabricación del aparato médico se utilizan componentes de software de tipo general ("Allround"), tal como, por ejemplo, sistemas operativos habituales que han sido desarrollados para una serie de posibles casos de utilización, que presentan una elevada complejidad intrínseca y, por lo tanto, están sometidos de manera especial al riesgo de un ataque. El fabricante de un aparato médico se encuentra, en este caso, ante el dilema de que los componentes de software utilizados presentan, por una parte, un peligro potencial, pero, por otra parte, el desarrollo de los aparatos médicos sin la utilización de este tipo de componentes es tan compleja que de ello se genera un elevado riesgo potencial para los pacientes o para el funcionamiento correcto del aparato médico. Lo que hace incluso más peligrosa la utilización de dichos componentes de software es el hecho de que el malware está destinado principalmente a dichos componentes de software y, por lo tanto, actúa de manera específica en los puntos débiles existentes en cuanto a seguridad. En este caso, el malware puede llegar por una ruta indirecta a través de la conexión de la parte segura de la red de comunicaciones a una parte no segura o bien por rutas directas con intermedio del soporte de datos o mediante una combinación de ambas rutas en el aparato médico.

El documento US 2002/133721 es estado de la técnica adicional. Es un objetivo de la presente invención el suprimir estas dificultades o bien, como mínimo, solucionarlas parcialmente y proporcionar un dispositivo que permite la protección de aparatos médicos contra las acciones de peligro antes mencionadas procedentes de una red de comunicaciones.

La invención se define mediante las reivindicaciones independientes.

La presente invención posibilita cumplir con las exigencias especiales que presentan los aparatos médicos para su aseguramiento contra ataques procedentes de la red o fallos de funcionamiento determinados y se refiere a un dispositivo, de acuerdo con el preámbulo de la reivindicación 1, que presenta medios de transmisión para transmitir paquetes de comunicaciones hacia y desde el aparato médico, con intermedio de la red de comunicaciones, que presenta medios de monitorización para monitorizar la situación de la conexión del aparato con la red y que presenta medios de interrupción para interrumpir la conexión existente entre las zonas segura y no segura de la red en el caso que, durante la monitorización, se detecte una situación en la conexión con la red que signifique un peligro para el paciente tratado con el aparato o bien para el funcionamiento correcto del aparato. Esto tiene la ventaja de que en base a las específicas exigencias en el campo médico, así como por las características habituales típicas de los cortafuegos se puede separar en especial la conexión de la zona segura de la red de comunicaciones con respecto a la zona no segura de modo completo, en el caso en que se compruebe la existencia de un peligro de cualquier tipo para el paciente o para el aparato.

En una realización preferente del dispositivo objeto de la invención, los medios de transmisión disponen de un filtro de paquetes que lleva a cabo el filtrado de paquetes en los paquetes de comunicaciones transmitidos entre la zona no segura y la zona segura de la red de comunicaciones, de manera que el filtro de paquetes es apropiado para no dejar pasar paquetes de comunicaciones que pongan en peligro potencial el aparato médico. Además, los medios de interrupción pueden estar realizados, como mínimo, mediante un dispositivo interruptor, los medios de monitorización presentan, como mínimo, una lógica de control que, en caso de comprobación de una situación de la conexión con la red que presenta un peligro para el paciente o para la función correcta del aparato, pone en marcha la interrupción del dispositivo o dispositivos de interrupción para separar la zona no segura con respecto a la zona segura de la red de comunicaciones conectada de modo directo al aparato médico.

El filtro de paquetes mencionado puede estar constituido de forma tal que posibilite un filtrado de paquetes bidireccional de los paquetes de comunicaciones transferidos entre la zona no segura y la zona segura de la red de comunicaciones. Esto garantiza, por lo tanto, el control y filtrado de los datos transferidos en ambas direcciones. Además, en este caso, la separación entre la zona segura y la zona no segura de la red de comunicaciones puede ser realizada preferentemente en forma de segmentación lógica.

De este modo, el filtro de paquetes puede sustituir en especial de forma parcial o bien de forma completa el dispositivo de monitorización antes citado y/o el dispositivo de interrupción, dado que no permite los desplazamientos del paquete de comunicaciones o de la totalidad de los paquetes de comunicaciones en el proceso de filtrado.

Sin embargo, la separación entre la zona segura y la zona no segura de la red de comunicaciones puede ser llevada a cabo asimismo por segmentado físico, en especial en forma de diferentes rutas de transferencia de tipo físico en la zona segura o bien en la zona no segura de la red o bien mediante diferentes realizaciones de la misma ruta de transferencia en esta zona. En caso de que las rutas de comunicación utilizadas en la red de comunicaciones sean de tipo cableado será especialmente ventajoso utilizar fibra óptica para las rutas de transferencia, tal como se explicará y justificará en detalle en la siguiente descripción.

En otra forma de realización de la presente invención, el presente dispositivo presenta el medio de lógica de control mencionado para la realización de una comprobación estática y/o dinámica de los datos que se transfieren en la red de comunicaciones, cuyo resultado conduce al mantenimiento o separación de la conexión existente entre la zona no segura y la zona segura de la red poniendo en marcha el dispositivo o dispositivos de interrupción.

El dispositivo de interrupción mencionado puede ser dispuesto en el lado conectado a la zona segura de la red de comunicaciones y/o al lado conectado a la zona no segura de la red de comunicaciones del dispositivo de la invención. De esta manera es posible separar solamente el aparato médico y/o tanto el aparato médico como también el dispositivo en sí mismo con respecto a la zona no segura de la red.

En una forma de realización especialmente ventajosa de un dispositivo, según la invención, éste presenta una arquitectura redundante para lo cual en los medios de monitorización se ha integrado un modelo de las funciones de un medio de transferencia que permite comprobar su funcionamiento correcto. Un dispositivo, según la invención, puede presentar también, como mínimo, dos canales distintos con los correspondientes medios propios de transferencia, medios de monitorización, así como medios de interrupción, de manera que cada canal puede ser monitorizado en sí mismo y también con independencia de los otros canales y en la comprobación de una situación de la conexión de red, que muestra un peligro para el paciente o bien para la función completa del aparato, puede llevar a cabo la separación con respecto a la zona no segura de la red de comunicaciones. Ambas formas de realización mencionadas de un dispositivo, según la invención, se caracterizan por una seguridad especialmente elevada contra ataques desde la zona no segura de la red de comunicaciones o de determinadas funciones de fallo.

La presente invención está dirigida además a un aparato médico que es apropiado para la conexión a una red de comunicaciones que presenta, como mínimo, una zona no segura, así como por el lado que corresponde al aparato, una zona segura y un dispositivo, según la invención, de acuerdo con una de las realizaciones que se han indicado. En cuanto al aparato médico, se puede tratar en especial de bombas de infusiones o monitores de pacientes.

La presente invención está dirigida también a sistemas médicos dotados de múltiples aparatos médicos del tipo anteriormente mencionado o partes de dichos aparatos de manera que el sistema presenta, como mínimo, un dispositivo, según la invención, del tipo que se ha descrito.

Finalmente, la presente invención se dirige a un procedimiento para el control de un dispositivo de este tipo, de manera que el procedimiento monitoriza la transferencia de paquetes de comunicaciones hacia y desde el aparato médico con intermedio de la red de comunicaciones, monitoriza la situación de la conexión del aparato con respecto a la red de comunicaciones e interrumpe la conexión existente entre la zona segura y la zona no segura de la red en caso de que durante la monitorización se detecte una situación de la conexión de la red que muestra un peligro para el paciente o bien para la función correcta del aparato. Las diferentes realizaciones y ventajas de un procedimiento de este tipo se explicarán en detalle en la siguiente descripción.

Las figuras adjuntas muestran, a título de ejemplo, diferentes formas de realización de un dispositivo, según la invención, de un aparato médico o bien sistema, según la invención, y de un procedimiento, según la invención.

La figura 1 muestra la conexión, habitual en el estado de la técnica, de un aparato médico que se encuentra en la vivienda del paciente, en el domicilio del paciente;

La figura 2 muestra esquemáticamente y a título de ejemplo el principio del dispositivo, según la invención;

La figura 3 muestra un dispositivo, según la invención, con filtrado de paquetes bidireccional, a título de ejemplo;

La figura 4 muestra esquemáticamente el algoritmo de un filtro de paquetes utilizado en un dispositivo, según la invención;

La figura 5 muestra la separación de monitores de pacientes de una central;

La figura 6 muestra, a título de ejemplo, la construcción de un sistema de aparatos médicos que están unidos entre sí mediante una parte no segura de una red de comunicaciones;

La figura 7 muestra la utilización de paquetes de comunicación modificados en la parte no segura de la red de comunicaciones;

La figura 8 muestra la utilización de paquetes de comunicaciones codificados en la parte no segura de la red de comunicaciones;

La figura 9 muestra una configuración en la que el dispositivo de la invención puede ser separado de la parte no segura de la red de comunicaciones;

La figura 10 muestra una configuración que posibilita la separación por ambos lados del dispositivo de la invención;

La figura 11 muestra un ejemplo de una arquitectura redundante del dispositivo, según la invención;

La figura 12 muestra una configuración de un dispositivo, según la invención, con una arquitectura redundante distinta;

La figura 13 muestra una posible realización distinta del dispositivo objeto de la invención;

La figura 14 muestra, a título de ejemplo, el aseguramiento de un sistema de bombas de infusión contra las acciones procedentes de la zona no segura de la red de comunicaciones;

La figura 15 muestra la forma convencional de conexión de monitores de pacientes a un monitor central;

La figura 16 muestra la conexión de monitores de pacientes a un monitor central con intermedio de dispositivos, según la invención;

La figura 17 muestra de manera esquemática y a título de ejemplo, un dispositivo, según la invención, construido de forma modular;

La figura 18 muestra a título de ejemplo un aseguramiento jerárquico de un dispositivo médico mediante la presente invención.

A continuación, se explicará la presente invención haciendo referencia de manera detallada a las figuras. En primer lugar, se hará referencia a la figura 1, que muestra la conexión habitual hasta el momento de un aparato médico de captación de datos que está dispuesto en la vivienda del paciente. En este caso, la vivienda 1 del paciente y el dispositivo médico 2, cuyos límites de sistema se han mostrado mediante líneas de trazos, están unidos entre sí mediante una red WAN 3, por ejemplo Internet. El aparato médico de captación de datos 4 está acoplado con intermedio de la red LAN 5 a la red WAN 3. De esta manera, la red LAN 6 está acoplada al dispositivo médico y al aparato médico de evaluación 7. La zona 8 de la red de comunicaciones que, desde el punto de vista del dispositivo médico no es segura, se ha representado en la figura 1 de forma simbólica mediante una flecha gris. El objetivo de la presente invención es el de proteger el aparato médico dispuesto en la zona segura de la red de comunicaciones contra las acciones de la zona no segura 8 de la red. Esto se realiza de manera simple y eficaz y, no obstante, se cumplen las normas habituales de alta seguridad en el campo médico.

En la figura 2 se ha mostrado una representación esquemática de un dispositivo, según la invención. El dispositivo 9, según la invención, asegura a un aparato médico 10 contra posibles ataques que pueden proceder de la zona no segura 11b de la red de comunicaciones 11. Presta servicio además en la ruta desde la zona no segura de la red de comunicaciones 11 al aparato médico un filtro de paquetes 12 que no deja pasar los paquetes de comunicaciones que pueden poner en peligro potencialmente al aparato médico 10. Una lógica de control 13 permite separar la zona no segura 11b de la red de comunicaciones 11 con respecto al aparato médico 10 con ayuda del dispositivo de interrupción 14. En este caso, se ha mostrado a título de ejemplo una forma de separación en la cual el dispositivo, según la invención, se puede separar también por sus medios con respecto a la zona segura 11a de la red de comunicaciones 11.

El aparato médico 10 puede, en caso deseado, ser realizado en forma de sistema con varios aparatos médicos parciales 15, 16 que están conectados en una zona segura 11a de la red de comunicaciones 11.

El dispositivo objeto de la presente invención puede estar constituido de manera ventajosa de forma que el filtrado de paquetes sea realizado de manera bidireccional, es decir, tanto en la dirección de la zona no segura 11b hacia la zona segura 11a de la red de comunicaciones 11 como también en dirección opuesta. En este caso, no solamente reasegurará el aparato médico contra un ataque que puede proceder de la parte no segura de la red de comunicaciones 11, sino que adicionalmente minimizará la influencia que el aparato médico ejerce en caso de fallo sobre la parte no segura de la red de comunicaciones 11. En la figura 3 se ha mostrado una representación esquemática de un dispositivo, según la presente invención, con filtrado de paquetes bidireccional.

El dispositivo, según la invención, dotado de filtrado de paquetes bidireccional 18 asegura a un aparato médico 10 contra posibles ataques que se pueden producir desde la zona no segura 11b de la red de comunicaciones 11 y procura, simultáneamente, una carga mínima en caso de fallo de la parte no segura 11 de la red de comunicaciones 11 por el aparato médico 10. Se constituye de esta forma un filtro de paquetes 12 que se compone de dos filtros de paquetes que monitorizan las diferentes direcciones de flujo de paquetes. En la ruta desde la parte no segura de la red de comunicaciones 11 hacia el aparato médico se utilizará un filtro de paquetes 12a que no deja pasar los paquetes de comunicaciones que pueden ser peligrosos potencialmente para el aparato médico 10. En la dirección contraria se utiliza un filtro de paquetes 12b que puede minimizar el retroefecto del aparato médico sobre la parte no segura de la red de comunicaciones 11. Una lógica de control 13 posibilita que el propio dispositivo 9 y la zona no segura 11b de la red de comunicaciones 11 queden separados del aparato médico 10 con ayuda del dispositivo de interrupción 14, de manera que éste está compuesto de dos partes 14a, 14b para las diferentes direcciones del flujo de comunicación. Ambas partes del dispositivo de interrupción son accionadas simultáneamente en caso normal, pudiendo ser aconsejable también, no obstante, una conmutación alternada en casos especiales, por ejemplo, para la minimización de la descarga de la red de comunicaciones 11.

El aparato médico 10 puede estar constituido también eventualmente como sistema a base de varios aparatos parciales 15, 16 médicos que están conectados a la zona segura 11a de la red de comunicaciones 11.

La separación completa a través del dispositivo de interrupción 14 o separación parcial mediante el filtro de paquetes 13 (puesto que permanecen paquetes de comunicación) del aparato médico 10 con respecto a la zona no segura 11b de la red de comunicaciones 11, debe ser tenida en cuenta dentro del campo de análisis de riesgos del aparato médico 10, conduciendo a una situación segura de éste en la que se excluya un peligro específico del operador o del paciente del aparato médico 10 para permitir la utilización del dispositivo 9, según la presente invención. En la práctica, estas limitaciones de utilización del dispositivo 9, según la invención, tendrán poca relevancia, puesto que se debe contar en todo momento con una rotura de la conexión de red, por ejemplo, en base a fallos en el cableado y otros procedimientos para la minimización de riesgos, tales como, por ejemplo, arquitecturas de red redundantes que son demasiados costosas en la mayor parte de casos.

Para que el filtro de paquetes 12 y el dispositivo de interrupción 14 puedan garantizar sus cometidos, debe existir una segmentación, es decir, una separación lógica y/o física entre la zona no segura 11b y la zona segura 11a de la red de comunicaciones 11. De otro modo, los paquetes de comunicaciones tendrían, sin intención o posibilidad de influencia, que ser transportados al azar a través del filtro de paquetes 12 y el dispositivo de interrupción 14 entre la zona no segura 11b y la zona segura 11a de la red de comunicaciones 11.

El tipo y forma en la que en un dispositivo, según la invención, puede tener lugar la segmentación de ambas partes 11 y 17 de la red de comunicaciones 11, puede ser completamente distinta. Como ejemplos para segmentaciones posibles, se brinda la utilización de otras redes de comunicaciones 11, que se basan en otros principios físicos (por ejemplo, LAN/WLAN) de otro protocolo, para el transporte de datos o la conversión de paquetes TCP/IP, pero se puede contar con otros tipos de segmentación.

La forma de funcionamiento del dispositivo de interrupción 14 depende esencialmente del tipo de segmentación utilizada entre la zona no segura 11b y la zona segura 11a de la red de comunicaciones 11.

Si se utiliza un dispositivo, según la invención, con filtrado de paquetes bidireccional 18, la segmentación entre la zona segura 11a y la zona no segura 11b de la red de comunicaciones 11 puede tener lugar de manera lógica, por ejemplo, por el hecho de que detrás del dispositivo 18, según la invención, se utiliza otro protocolo de comunicaciones con respecto a la red de comunicaciones 11 que delante del dispositivo objeto de la invención. En caso normal, el filtro de paquetes 12, que desempeña también el análisis de protocolo, lleva a cabo también la transformación entre los diferentes protocolos de comunicaciones.

El filtro de paquetes 12a, por ejemplo en caso necesario, puede no desempeñar la transformación de protocolo para los paquetes de comunicaciones a filtrar. De este modo, no se generará en la zona segura 11a de la red de comunicaciones 11 para el paquete de comunicaciones correspondiente ningún paquete de comunicaciones traducido aceptable. Se puede prever incluso que en este caso la función del dispositivo de interrupción 14 sea desempeñada por el filtro de paquetes 12a, dado que éste dispone la transformación de manera duradera y para todos los paquetes de comunicaciones. El aparato médico 10 se encuentra entonces separado de forma lógica con respecto a la zona no segura 11b de la red de comunicaciones 11 incluso cuando no ha tenido lugar una separación física. En la dirección opuesta, el filtro de paquetes 12b debe desempeñar las correspondientes funciones y son válidos los mismos principios en la dirección opuesta. De esta manera, se puede realizar una construcción muy favorable en cuanto a costes del dispositivo, según la invención.

Teóricamente, se puede prever, no obstante, que paquetes de comunicaciones del protocolo de comunicación utilizado en la zona no segura 11b de la red de comunicaciones 11 muestren paquetes de comunicaciones aceptables también en el protocolo de comunicación que se utiliza en la zona segura 11a de la red de comunicaciones 11, que producen un ataque al aparato médico 10. Concretamente, este riesgo se puede minimizar por la elección cuidadosa de los protocolos de comunicación utilizados, pero un determinado riesgo residual permanece siempre cuando tiene lugar un ataque de la zona segura 11a de la red de comunicaciones 11 por medio de un “ataque por fuerza bruta” o un “Bubbling Idiot” (“Idiota balbuceante”) que envía un paquete de comunicaciones accidental. En este caso, se pueden “adivinar” después de un tiempo determinado secuencias de comunicaciones aceptables para el protocolo de comunicaciones que se utilizarán en la zona segura 11a de la red de comunicaciones 11.

De esta manera, se puede conseguir una especialmente elevada seguridad del aparato médico 10 cuando existe una segmentación física entre la zona no segura 11b y la zona segura 11a de la red de comunicaciones 11.

Una segmentación física de este tipo puede ser realizada de manera que se utilicen diferentes rutas de transferencia física para la zona no segura 11b y para la zona segura 11a de la red de comunicaciones 11. Así, por ejemplo, la zona no segura 11b de la red de comunicaciones 11 podría utilizar transferencia por radio y la zona segura 11a podría utilizar transferencia por red de cableado. No obstante, se pueden utilizar también diferentes realizaciones de las mismas rutas de transferencias, para lo cual se pueden considerar, por ejemplo, dos cableados de red separados, o frecuencias de transmisión por radio distintas, para ambas zonas 11a y 11b de la red de comunicaciones 11.

Una utilización especialmente ventajosa del aparato 9 que se ha descrito resulta, no obstante, en redes de comunicaciones eléctricas 11, unidas por cables cuando se utiliza una segmentación física de ambas zonas 11a y 11b de la red de comunicaciones 11. En este caso, el dispositivo descrito puede introducir también principalmente un

aseguramiento de los aparatos médicos contra alteraciones eléctricas que se pueden aplicar mediante la zona no segura 11b de la red de comunicaciones 11 en el aparato médico y provocar una función de fallo de los mismos y, por lo tanto, un peligro para el paciente o usuario.

También puede tener lugar, en este caso, el aseguramiento, que es importante para los aparatos médicos contra descargas por contacto a causa de elevadas tensiones por fallo de la zona no segura 11b de la red de comunicaciones 11, cuyo aseguramiento puede tener lugar mediante el dispositivo 9, según la presente invención.

Si un aseguramiento de las tensiones de contacto en las utilizaciones determinadas es especialmente crítico, puede ser ventajoso para la zona segura 11a de la red de comunicaciones 11 utilizar una red de comunicaciones 11 basada en fibra óptica para el transporte de luz, ya que de esta manera, en principio, no tienen lugar compensaciones de potencial.

Tanto la zona no segura 11b de la red de comunicaciones 11 como también la zona segura 11a de la red de comunicaciones 11 pueden estar unidas por cableado, pero se puede prever también otro tipo de realizaciones que envían los datos mediante luz, radio, sonido u otras rutas de transporte. Los métodos de transferencia no pueden ser los mismos en ambas zonas 11a y 11b de la red de comunicaciones 11; en este caso, es ventajoso que el dispositivo, según la invención, pueda llevar a cabo una conversión entre estos métodos de transferencia por sí mismo, de manera que no se requiera un aparato adicional para esta conversión.

En la figura 4 se ha mostrado un algoritmo básico posible simplificado para el filtro de paquetes 12. El filtro de paquetes espera la recepción de paquetes de comunicación desde la zona no segura 11b de la red de comunicaciones 11. Tan pronto como se dispone de un paquete de comunicaciones, lo recibe y comprueba si el paquete es aceptable para su envío al aparato médico 10. En este caso, el paquete de comunicaciones será enviado y, en caso contrario, será descartado. A continuación, el filtro de paquetes 12 espera nuevamente la recepción del paquete siguiente.

En este caso, puede ser ventajoso para la capacidad de seguimiento del comportamiento del dispositivo 9, según la invención, que se lleve a cabo un registro de los paquetes de comunicaciones recibidos y rechazados y, de esta manera, se pueda comprobar la configuración correcta del filtro de paquetes 12.

Para poder recibir los paquetes de comunicaciones de la zona no segura 11b de la red de comunicaciones 11, pueden recibir en la zona segura 11a de la red de comunicaciones 11, se evaluará, por el filtro de paquetes 12, el conocimiento adicional de la estructura del dispositivo médico, la estructura interna del aparato médico y de sus sub-aparatos, sus características, situación momentánea y otros.

En el caso más sencillo, podrían pasar por el filtro de paquetes 12, por ejemplo, solo los paquetes de comunicaciones con direcciones fijas MAC o direcciones IP, o solamente aquellos que lleven a cabo la comunicación a través de puertos autorizados. También se pueden llevar a cabo otras pruebas de la comunicación, tal como una inspección de la situación (“Stateful”). El comportamiento del dispositivo 9, según la invención, en la etapa de la monitorización de las conexiones de la red sería en este caso similar a la correspondiente a un cortafuegos de hardware; las reglas para el filtrado de paquetes podrían, no obstante, especificarse sustancialmente de manera más exacta y adaptarse al aparato médico a proteger. A diferencia de los cortafuegos habituales, en este caso, si se comprueba la existencia de paquetes de comunicación peligrosos, se interrumpe la unión con la zona no segura 11b de la red 11.

Se muestra especialmente ventajoso además que el dispositivo 9, según la invención, lleve a cabo un análisis de protocolo del protocolo de comunicación para la transferencia al aparato médico 10 y que el filtro de paquetes 12 deje pasar solamente los paquetes de comunicación que corresponden al protocolo de comunicaciones del aparato médico 10. De esta manera, se reduce sensiblemente el peligro de un ataque al aparato médico 10.

Además, el análisis de protocolo posibilita también, dentro del ámbito de los datos que se producen en el protocolo, la comprobación de valores de datos aceptables y permiten solamente el paso de los paquetes de comunicación por el filtro de paquetes 12 cuyos datos se encuentran en la zona de evaluación autorizada.

Al contrario que en los cortafuegos que aseguran redes de comunicaciones 11 para sistemas de ordenadores de utilización general, el filtro de paquetes 12 puede ser adecuado de manera precisa a los protocolos de comunicación a utilizar, puesto que la instalación de programas aleatorios en sistemas de ordenadores incorporados en aparatos médicos no son, en general, ni posibles ni autorizados por el fabricante cuando dichos aparatos médicos generan posibles peligros para los operadores o pacientes del aparato médico. Por esta razón, los protocolos de comunicaciones utilizados por un aparato médico sufren raramente modificaciones, que en caso deseado, requieren la adecuación del filtro de paquetes, tal como es el caso en los sistemas de ordenadores de utilización general.

Una realización especialmente ventajosa del dispositivo 18, según la presente invención, con filtrado de paquetes bidireccional se consigue cuando se utiliza simultáneamente la comprobación de los protocolos de comunicación utilizados para convertir los datos de otros protocolos de comunicación utilizados en otros aparatos médicos en una red de comunicaciones 11 que se basa en otros principios físicos, posibilitando de esta manera la comunicación entre sí de aparatos propiamente incompatibles.

Asimismo, para poder decidir cuándo debe ser llevada a cabo la separación con respecto a una parte potencialmente no segura de la red de comunicaciones 11, se evalúa adicionalmente el conocimiento de la estructura del dispositivo médico, de la estructura interna o de los aparatos médicos, sus características y otros.

Además, el dispositivo descrito puede, en caso de un peligro potencial conocido, producido por la zona no segura 11b de la red de comunicaciones 11, interrumpir la unión de éste con el aparato médico 10 de manera completa, de modo que es posible la limitación de muchas de sus funciones, permaneciendo, no obstante, su funcionalidad principal o de núcleo.

En base a un ejemplo de monitor de paciente, mostrado esquemáticamente en la figura 5, se mostrará claramente una separación de este tipo. Una central 19 que se encuentra en la zona no segura 11b de la red de comunicaciones 11 está unida con los monitores de pacientes 20, 21 y 22 asegurados mediante dispositivos 9, según la invención, encontrándose dichos monitores en la zona segura 11a de la red de comunicaciones 11. En el caso de reconocimiento de un peligro potencial, mediante los dispositivos 9, según la invención, se puede interrumpir la unión con respecto a la zona no segura 11b de la red de comunicaciones 11 y, de esta manera, con respecto a la central 19, lo cual muestra una limitación de la funcionalidad de los monitores de paciente 20, 21 y 22, cuya funcionalidad principal se encuentra, no obstante, a disposición de la monitorización aunque de manera menos confortable. En el momento de la interrupción, no se pueden llevar a cabo ataques desde los monitores de pacientes 20, 21 y 22 a la central 19 y a la inversa.

Una separación de este tipo puede ser muy ventajosa cuando se utilizan, por ejemplo, aparatos médicos más antiguos que están preparados solamente de manera no accesible para las redes de comunicación actuales 11 con elevadas velocidades de datos, puesto que en el desarrollo del aparato se ha partido de redes de comunicaciones 11 especializadas para dichos aparatos, pero estas previsiones no existen a causa de la infraestructura de los dispositivos médicos. Si se utilizan, por ejemplo, complejas rutinas de manipulación de la interrupción en los aparatos médicos, ello puede conducir ente otros a una pura sobrecarga de la red de comunicaciones 11 que generará una sobrecarga excesivamente elevada de los procesadores de los aparatos médicos, incluso cuando los propios datos transferidos son completamente inocuos. Mientras que un aparato médico individual en este caso se debe encontrar en una situación segura, la simultánea transmisión de un número elevado de aparatos médicos en la misma situación puede generar una situación general crítica suscitada por la complejidad del grupo. Cuando, por ejemplo, un monitor de paciente individual presenta un fallo en una estación intensiva, reconoce ésta por sus propios medios y dispara una alarma que pone en aviso al servicio no pudiéndose clasificar esta situación en sí misma necesariamente como crítica. Lo mismo es válido para una bomba de infusión. No obstante, si fallan en la misma estación de cuidados intensivos a causa de averías, que han sido provocadas a través de la red de comunicaciones 11, poniendo fuera de servicio todos los monitores de pacientes y todas las bombas de infusión, el peligro que se genera es de distinta gravedad para la totalidad de los pacientes tratados.

La lógica de control 13 puede llevar a cabo la decisión sobre la realización de la separación de las zonas de la red de comunicaciones 11 en base a pruebas estáticas de los datos a enviar. Como tales, se brindan, por ejemplo, la comprobación de las direcciones IP de los asociados en las comunicaciones, las direcciones MAC utilizadas para éstos, la utilización de determinados puertos y/o en especial una comprobación de los datos enviados en cuanto a sintaxis y/o semántica y consistencia.

En un caso normal, una prueba estática de los paquetes de comunicaciones a enviar conducirá directamente a la eliminación de los paquetes en el filtro de paquetes y también a la separación de la zona no segura 11b de la red de comunicaciones 11. En caso de exigencias de seguridad especialmente elevadas para el aparato médico 10 puede ser, no obstante, aconsejable cuando se producen infracciones demasiado frecuentes de las pruebas de aceptación estáticas, llevan a cabo una separación temporal o incluso duradera de la zona no segura 11b de la red de comunicaciones 11.

La decisión sobre la realización de las zonas 11a y 11b de la red de comunicaciones 11 puede tener lugar también por el hecho de que se ha realizado una prueba dinámica de los datos a enviar. Estas pruebas pueden ser, por ejemplo, los tiempos de respuesta del asociado de comunicación, un flujo de datos máximo permisible a los aparatos médicos a proteger o también un flujo de datos mínimo que indica un funcionamiento correcto del asociado de comunicación. También son ventajosas en este caso monitorizaciones basadas en la situación que contienen un modelo de los aparatos involucrados en la comunicación.

Una forma específica de utilización del aparato 9, según la invención, se produce cuando funcionan conjuntamente varios subaparatos médicos que, en su conjunto funcionan como una sistema/aparato médico, estando unidos mediante una parte no segura 11b de la red de comunicación 11 entre sí. En esta constelación se recomienda dotar a los aparatos o subaparatos médicos de manera correspondiente e individualmente con dispositivos 9, según la invención. En este caso puede ser más aconsejable utilizar dispositivos 18, según la invención con filtrado de paquetes bidireccional, tal como se mostrará más adelante.

En la figura 6 se ha mostrado la construcción de un sistema de aparatos médicos que están unidos entre sí mediante una parte no segura de la red de comunicaciones 11. Con intermedio de la zona no segura 11b de la red de comunicaciones 11 están unidos entre sí ambos aparatos médicos 10a y 10b, que conjuntamente forman un sistema médico. Se encuentran de manera correspondiente con intermedio de los dispositivos, según la invención, con

filtrado de paquetes bidireccional 18a y 18b en las zonas aseguradas 11a.1 y 11b.2 de la red de comunicaciones 11. Un aparato médico adicional 10c, pero no perteneciente al sistema médico citado anteriormente está asegurado mediante el dispositivo 18c, según la invención, asociado al mismo y está unido con la zona no segura 11b de la red de comunicaciones 11.

Si los filtros de paquetes de los dispositivos 18a, 18b y 18c, según la invención, se han ajustado de manera óptima y se utilizan protocolos de comunicación apropiados, puede tener lugar entre los aparatos médicos 10a y 10b una comunicación sin que ésta sea detectada por el aparato médico 10c. De manera inversa, puede tener lugar entre el aparato médico 10c y otros aparatos que se encuentran en la parte no segura de la red de comunicaciones 11 una comunicación, sin que ésta influya en los aparatos médicos 10a y 10b. No obstante, cuando los protocolos de comunicación utilizados por los aparatos 10a, 10b y 10c son iguales y, por ejemplo, además una parte de la comunicación tiene lugar como emisión (“broadcast”), es decir, que afecta a todos los participantes de la red de comunicaciones 11 simultáneamente, se puede renunciar a los métodos antes indicados.

En este caso, es recomendable que el filtro de paquetes 13 de los aparatos 10a y 10b, según la invención, asociados a los aparatos médicos 18a y 18b lleven a cabo una conversión de los protocolos de comunicación que son utilizados en la zona no segura 11b de la red de comunicaciones 11 en comparación con los paquetes de comunicación modificados, según el protocolo original. En la figura 7 se ha mostrado el desarrollo de un proceso de este tipo con referencia a la figura 6 de modo esquemático.

Un paquete de comunicaciones 26, que contiene datos que se han designado con la expresión “Data” es transformado por el dispositivo 18b, según la invención, en la transición de una zona segura 11a.2 de la red de comunicaciones 11 en otro paquete de comunicaciones 27 que será transportado dentro de la zona no segura 11b de la red de comunicaciones 11. La conversión puede ser muy simple y rápida, dado que el paquete de comunicaciones original 26 será incorporado en otro paquete de comunicaciones 27. En este caso, puede ser ventajoso que se comprueben datos adicionales 28, tales como, por ejemplo, la firma, que están incorporados en el paquete de comunicaciones 27, para separar por ejemplo en los mismos protocolos diferentes grupos de aparatos médicos entre sí y/o para poder confirmar como dispositivo 18a, según la invención, que los datos dentro de la parte no segura 11b de la red de comunicaciones 11 no han sido variados. El aparato objeto de la invención 18a convierte en un desarrollo adicional el paquete de comunicaciones modificado 27 en un paquete de comunicaciones 29 utilizable en el aparato médico 10a, cuyo paquete debe ser, para igual protocolo de comunicación utilizado, básicamente idéntico con el paquete de comunicación inicial 26.

De esta manera, es posible, de manera eficaz, reducir la influencia por ambos lados de diferentes comunicaciones a un valor mínimo. Si se comprueba por el aparato 18a, según la invención, por ejemplo mediante la prueba de la firma, que el paquete de comunicaciones entrante 27 ha sufrido una falsificación, el paquete correspondiente 29 no será generado. Existe entonces eventualmente un indicio de un ataque y la lógica de control 13 podría llevar a cabo la separación de la parte no segura de la red, eventualmente, solo después de una aparición más frecuente de estos sucesos.

En la estructura de red que se ha descrito, en la que se utiliza la zona no segura 11b de la red de comunicaciones 11 para permitir la comunicación de dos subaparatos médicos entre sí, se pueden prever, no obstante, además de los peligros potenciales descritos con anterioridad para el paciente y/o para el usuario, exigencias de aseguramiento de datos contra espionaje por terceros no autorizados. Esta exigencia puede ser cumplida por una ampliación del proceso mostrado en la figura 7. En la figura 8 se ha mostrado el desarrollo de este proceso ampliado.

Un paquete de comunicación 26 contiene los datos designados “Data”. Serán transformados por el dispositivo, según la invención 18b, en la transición de una zona segura 11a.1 de la red de comunicaciones 11 a la zona no segura 11b en otro paquete de comunicación modificado 31. Al contrario que en el proceso de la figura 7, el paquete de comunicaciones adicional no será incorporado simplemente en el nuevo paquete de comunicaciones, sino que se transformará la zona de datos en una zona de datos codificada 30 que se ha designado “dATA”. En este caso, se pueden utilizar procedimientos simétricos y/o asimétricos con respecto a otras áreas de utilización, eventualmente con una firma adicional incorporada para la diferenciación de diferentes grupos de aparatos médicos o para una comprobación rápida de la inaccesibilidad de los paquetes de comunicación. En la transición a la segunda zona segura 11a.2 de la red de comunicaciones 11, el paquete de comunicación 31 codificado y modificado será transformado en un paquete de comunicación 29 utilizable por el aparato médico 23, cuyo paquete para igual protocolo de comunicación utilizado será básicamente idéntico al paquete de comunicación inicial 26.

Se produce, por lo tanto, una especie de red privada virtual (VPN) entre los aparatos 10a y 10b, de manera que los contenidos de la comunicación de otros aparatos susceptibles de comunicar en la zona no segura 11b de la red de comunicaciones 11 no pueden ser modificados de manera inadvertida ni tampoco pueden ser leídos. Este procedimiento determina de manera especialmente ventajosa cuando la zona no segura 11b de la red de comunicaciones 11 es Internet, tal como debería ser en la conexión de un aparato médico en la vivienda del paciente en la mayor parte de casos.

Esta seguridad puede ser utilizada de manera muy ventajosa incluso dentro de un dispositivo médico para transportar datos a través de una “parte abierta” de la red de comunicaciones 11, sin dar posibilidad a terceros no autorizados de acceder a los datos. Cuando se lleva a cabo un análisis muy detallado de los datos transferidos a

efectos de aseguramiento, la invención que se ha descrito puede conseguir una separación especialmente eficaz de los datos en una parte no codificada “abierta” y una parte codificada “privada”.

Si se tienen que intercambiar datos entre subaparatos médicos 10a y 10b que presentan un elevado potencial de peligro en caso de una posible falsificación, puede ser ventajoso impedir dicha potencial falsificación en la zona no segura 11b de la red de comunicaciones 11 mediante el almacenamiento y envío de paquetes de comunicación “anticuados”, de manera que en cada paquete de comunicación enviado, con intermedio de la zona no segura 11b de la red de comunicaciones 11 se contenga una parte variable cuya corrección es comprobada en la recepción, antes de que el paquete de comunicación pase por el filtro de paquetes. Este puede ser, por ejemplo, un número simple con una sucesión definida. Si se utiliza como parte variable el tiempo horario, se puede comprobar incluso si el paquete es válido todavía o ha requerido demasiado tiempo para el transporte en la red de comunicaciones 11.

Cuando uno de los subaparatos médicos 10a y 10b requiere una reacción específica en caso de rotura de la comunicación con otro sub-aparato médico, pero la comunicación no contiene ninguna trama de tiempo determinada, los correspondientes dispositivos 18a y 18b, según la invención, pueden enviar en periodos de tiempo fijos indicaciones de vida para comprobar el funcionamiento de la comunicación. Si estas indicaciones de vida no se producen, entonces el aparato a monitorizar correspondiente 10a o 10b debe ser avisado de manera adecuada. Esto puede tener lugar, por ejemplo, por la generación de un paquete de comunicación adecuado o también por la utilización de conductores de control específicos.

En el caso de exigencias todavía más elevadas en cuanto a seguridad de manipulación de los datos a transferir, se puede enviar desde los dispositivos emisores, según la invención, 18a o 18b a cada paquete de comunicación relevante un número de transacción (TAN) en base al cual el dispositivo 18b o 18a receptor, según la invención, puede determinar de manera indudable la llegada del paquete de comunicación. Entonces se debe enviar una lista de los TAN a ambos dispositivos, según la invención 18a y 18b de manera previa mediante otra ruta segura, por ejemplo, soportes de datos. Con cada uno de los TAN enviados al asociado de comunicación correspondiente, éste será borrado de la lista por ambos dispositivos 18a y 18b, según la invención.

Una forma adicional de facilitar datos que deben ser enviados a la zona no segura 11b de la red de comunicaciones 11, puede tener lugar también por el hecho de que las direcciones en la parte protegida de la red de comunicaciones 11 no se dan a conocer al exterior. Esto dificulta notablemente posibles actuaciones desde la red de comunicaciones potencialmente no segura 11.

Dada la forma de funcionamiento del dispositivo descrito, éste puede desempeñar de manera muy ventajosa también otros objetivos que hasta el momento han sido desempeñados por otros aparatos especiales. Así, por ejemplo, es posible, sin importantes complicaciones adicionales, integrar un escáner de virus en el aparato, puesto que el tráfico global de datos comprueba la existencia de virus de ordenador.

El dispositivo que se ha descrito puede también desempeñar una función de reserva de los datos transferidos con intermedio del protocolo de comunicaciones, almacenando éstos de manera permanente o solamente para la duración de la separación con respecto a la zona potencialmente no segura 11b de la red de comunicaciones 11 para transferirlos después de la reconstrucción satisfactoria de la conexión de manera automática con el asociado de comunicación.

Puede desempeñar una función de “Proxy” y así, por ejemplo, un aparato, que debe ser un aparato en una interfaz serie conectado con tiempos de respuesta correspondientemente rápidos, en la situación de una transformación de protocolo y conexión con intermedio de Internet debe enviar con tiempos de respuesta correspondientemente lentos confirmaciones de la recepción de paquetes en principio de forma global y solamente para permanencias más prolongadas de estas señales colocar el aparato a proteger en una modalidad en la que se considere la conexión como interrumpida.

Otros objetivos posibles adicionalmente que pueden ser realizados de manera ventajosa con el aparato que se ha descrito son, por ejemplo, un control de acceso para los datos que se encuentran de manera asegurada en la red de comunicaciones 11 o bien incluso la protección de autorizaciones SW en la red de comunicaciones 11.

Por el contacto directo con la zona no segura 11b de la red de comunicaciones 11 existe, no obstante, el peligro de que el aparato descrito sea alterado incluso por un ataque procedente de la red de comunicaciones 11 en su forma de funcionar y, por lo tanto, no pueda realizar su función de protección o solamente la pueda desempeñar de forma limitada.

Por lo tanto, puede ser aconsejable que el dispositivo, según la invención, se pueda separar con ayuda del dispositivo de interrupción con respecto a la zona no segura 11b de la red de comunicaciones 11 cuando la lógica de control 13 confirma un ataque potencial al aparato médico o al aparato objeto de la invención. En la figura 9 se ha mostrado esquemáticamente la construcción de un dispositivo, según la invención, realizado de la forma indicada.

Por ejemplo, en este caso, se ha dispuesto un filtrado de paquetes bidireccional 12, pero también se puede prever, un filtrado de paquetes unidireccional, tal como se ha mostrado en la figura 2. En el dispositivo, según la invención 32 se encuentra el dispositivo de interrupción 14 en el lado que se encuentra en la zona no segura 11b de la red de

comunicaciones 11. De esta forma, la lógica de control 13 puede separar el aparato, según la invención 32 conjuntamente con el aparato médico 10 con respecto a la zona no segura 11b de la red de comunicaciones 11.

A causa de la separación completa de la zona no segura 11b de la red de comunicaciones 11 se excluye un ataque adicional al dispositivo, según la invención 32. La situación de la separación con respecto a la zona no segura 11b de la red de comunicaciones 11 debe mostrar la situación segura para el aparato médico 10 y se debe tener en cuenta, incluso para el fallo de la tensión de alimentación del aparato 32, según la invención.

Puede constituir una ampliación aconsejable del concepto inventivo que la lógica de aseguramiento 13 tenga la posibilidad de llevar a cabo una reposición o “reset” y por lo tanto, relacionado con ello, un nuevo inicio del dispositivo 32, según la invención, puesto que de esta manera se asegura que el dispositivo quedará dispuesto en una situación inicial definida y correcta, de manera que se combatiría un ataque potencial al dispositivo objeto de la invención por la apertura del dispositivo interruptor 14.

Una situación todavía más crítica se podría producir cuando el aparato objeto de la invención 9, por un fallo funcional, lleve a cabo por sí mismo un ataque al aparato médico a proteger 10. Se muestra, por lo tanto, como ventajoso, tal como se representa en la figura 2, que la lógica de control 13, con la ayuda del dispositivo de interrupción 14, separe el dispositivo 9, según la invención, conjuntamente con la zona no segura 11b de la red de comunicaciones 11 de la zona segura 11a de la propia red de comunicaciones 11 tan pronto como se comprueba una limitación del funcionamiento del aparato 9, según la invención. Como situación segura del dispositivo 9, según la invención, se comprenderá, por lo tanto, la apertura del dispositivo de interrupción 14 y, por lo tanto, la separación de la parte no segura 11 y el dispositivo, según la invención 9, con respecto a la zona segura 11a de la red. Esta situación se debe tener en cuenta, por lo tanto, por ejemplo, para el caso de fallo de alimentación del aparato 9, según la invención.

Para poder comprobar una limitación de este tipo del propio funcionamiento se pueden utilizar, por ejemplo, los siguientes procedimientos:

- Controles “Watchdogs” de hardware o software
- Supervisión del desarrollo lógico y/o temporal del programa del software utilizado
- Supervisión del apilamiento del software utilizado
- Comprobación de la forma de funcionamiento correcta de memorias ROM y RAM
- Supervisión de la alimentación de corriente
- Comprobación de la integridad del código de programa y de los datos

Dado que tanto la estructura esquematizada, según la figura 2, como también la estructura, según la figura 9, presentan ventajas en la realización del dispositivo, según la invención, se muestra ventajoso para exigencias de seguridad especialmente elevadas una combinación de ambas estructuras, tal como se ha mostrado en la figura 10. En la configuración que se ha mostrado, la lógica de control 13 puede separar el dispositivo 33, según la invención, tanto con respecto a la zona no segura 11b como también con respecto a la zona segura 11a de la red de comunicaciones 11 con ayuda del dispositivo de interrupción 14a y 14b.

En este caso, una separación de este tipo puede tener lugar mediante ambos dispositivos de interrupción acoplados entre sí o con independencia uno de otro. Como apoyo puede ser aconsejable una segmentación física de ambas zonas 11a y 11b de la red de comunicaciones 11 permitiendo que los interruptores 14a y 14b lleven a cabo el cierre siempre de forma alternada, puesto que de esta manera permanece la segmentación física incluso en el caso de un fallo funcional del dispositivo 33, según la invención, en cualquier momento.

En caso de una funcionalidad comprobada por la lógica de control del aparato 33, es aconsejable abrir ambos dispositivos de interrupción 14a y 14b simultáneamente y llevar a cabo una reposición (“Reset”) para conseguir la situación segura y definida del aparato 33, según la invención, después de un nuevo arranque. La separación de ambas partes de la red de comunicaciones 11 debe mostrar también la situación segura del aparato médico 10 y, por ejemplo, tenerlo en consideración en caso de que continúe el suministro eléctrico del aparato 33.

Una realización del dispositivo, según la invención, especialmente ventajosa en el sentido de la seguridad se consigue cuando el dispositivo, según la invención, se construye de forma redundante. Para ello, se ofrecen una serie de procedimientos posibles.

En la figura 11 se ha mostrado una realización redundante posible de características simples del dispositivo objeto de la invención, que a efectos de simplicidad se muestra nuevamente a modo de ejemplo con un filtrado de paquetes bidireccional.

El dispositivo, según la invención 34 consiste, en este caso, en un canal de trabajo 35 y un canal de monitorización 36 que están alojados en subsistemas separados entre sí. El canal de trabajo 35 adopta las funciones del filtro de

paquetes 12 y todas las funciones relacionadas del mismo, es decir, por ejemplo, también la conversión de los protocolos de comunicación utilizados. El canal de monitorización 36 no adopta función alguna. Su función consiste solamente en monitorizar el funcionamiento correcto del canal de trabajo 35. Esto puede tener lugar de manera que exista un modelo (simplificado) de la asignación de tarea en el canal de trabajo en el canal de monitorización o que el canal de monitorización 36 efectúe la comprobación solamente según un principio de control ("watchdog") de la función del canal de trabajo 35. Si el canal de monitorización 36 comprueba un fallo del canal de trabajo 35 puede separar con ayuda del dispositivo de interrupción 14, con respecto a la red de comunicaciones 11 y en su caso generar una reposición ("Reset") para llevarlo nuevamente a un estado definido y que, por lo tanto, cumple su función.

En este caso se ha mostrado, en la figura 11, por ejemplo, una separación en el lado de la parte segura 17 de la red de comunicaciones 11; no obstante, son asimismo igualmente posibles variantes con una separación de la zona no segura 11b o ambas zonas de la red de comunicaciones 11.

Una variante muy segura consiste en canales "distintos" completamente independientes entre sí, cada uno de los cuales puede separarse a sí mismo y al otro canal con respecto a la parte potencialmente no segura de la red de comunicaciones 11 y monitorizar el correcto funcionamiento del otro canal.

Una variante de este tipo se ha mostrado de manera simplificada en la figura 12. La parte completa que transporta los paquetes de comunicación desde la zona segura 11a a la zona no segura 11b de la red de comunicaciones 11, se ha suprimido en este caso. Se puede realizar en el caso de un filtrado de paquetes bidireccional de forma simétrica a la parte que se ha mostrado o bien por el simple envío de los paquetes de comunicación. También en este caso tiene lugar la separación nuevamente a título de ejemplo, en el lado de la zona segura 11a de la red de comunicaciones 11.

El dispositivo, según la invención, 37 comprende dos subsistemas independientes entre sí 38 y 39 que contienen de manera correspondiente, un dispositivo de interrupción 40 o 41, una lógica de control 42 o 43 y un filtro de paquetes 44 o 45. Si ambos filtros de paquetes 44, 45 han llegado al resultado de traducir y enviar un paquete de comunicación, ambos resultados parciales son comprobados por un comparador 46 y si coinciden, son enviados de manera uniforme. Ambos elementos 42 y 43 de la lógica de control pueden, de manera correspondiente, con independencia uno de otro, llevar a cabo la separación de ambas zonas 11a y 11b de la red de comunicaciones 11. De esta forma, pueden evaluar las informaciones que proceden de los subsistemas propios 38 o 39 con respecto a ataques que pueden tener lugar o una funcionalidad limitada de los correspondientes subsistemas. No obstante, es especialmente ventajoso que entre ambos subsistemas 38 y 39 exista una ruta de comunicación 47 con cuya ayuda ambos elementos 42 y 43 de la lógica de control reciban indicaciones sobre el funcionamiento correcto de los otros subsistemas 39 o 39, para que puedan llevar a cabo la separación de las partes 11b y 11a del sistema de comunicaciones 11.

También en ese caso es ventajoso que ambos elementos 42 y 43 de la lógica de control puedan poner en marcha una reposición ("Reset") de los otros subsistemas correspondientes o incluso del dispositivo 37 en su conjunto.

Si para el desarrollo del dispositivo 37, según la invención, se deben utilizar, por ejemplo, sistemas operativos para minimizar el tiempo de desarrollo y los fallos de desarrollo, es recomendable disponer en ambos canales sistemas operativos independientes uno de otro y si es posible, utilizar asimismo hardware de red distinto, puesto que la probabilidad de que ambos canales sean influidos simultáneamente y de la misma manera por la red de comunicaciones potencialmente no segura 11, es extremadamente reducida y, por lo tanto, la seguridad contra fallos es muy elevada. Además, la realización con diversidad del aparato descrito, presenta también la ventaja de que los fallos que tienen lugar en el diseño y desarrollo del software y/o generados por el mismo hardware o por variaciones casuales de los contenidos de datos de las memorias del ordenador son reconocidos en casos normales y conducen a una separación con respecto a la red de comunicaciones potencialmente no segura 11 hasta una corrección duradera.

De esta manera se minimiza el riesgo de que un fallo dificulte la función del aparato, ello, no obstante, hasta que no se haya reconocido todavía una influencia posible del aparato médico por la red de comunicaciones 11 potencialmente no segura y que tenga lugar realmente una acción que provoque un riesgo para el paciente.

En la figura 13 se ha representado una constitución posible, esquemática, de un dispositivo 48, según la invención, de tipo diferenciado; también en este caso, nuevamente para una dirección de transporte desde la zona no segura 11b a la zona segura 11a de la red de comunicaciones 11.

Desde la zona no segura 11b de la red de comunicaciones 11, los datos llegan a través del sistema operativo 53 al primer canal 51, desde allí atraviesan el cortafuegos 55, un escáner de virus 57 y el análisis de protocolo 59. Cada una de estas capas rechaza los datos si estos son potencialmente peligrosos. A continuación, los datos llegan al comparador 61. Paralelamente a ello, los datos llegan al segundo canal 52 a través del segundo sistema operativo 54, el segundo cortafuegos 56, el segundo escáner de virus 58 y el segundo análisis de protocolo 60 igualmente al comparador 61. Exclusivamente para el caso de que ambos canales lleguen al resultado de que los datos son correctos y no dañinos, son enviados a la zona segura 11a de la red de comunicaciones 11. Ambos canales conducen a una monitorización opuesta 62 que eventualmente pone en marcha la reposición y pueden de forma

contraria, mediante las rutas de desconexión 49 y 50 efectuar la separación de la zona no segura 11b de la red de comunicaciones 11.

Posibles formas de realización del aparato descrito 9 pueden ser un aparato independiente y también un aparato conectado a un aparato médico. Una realización del dispositivo 9, según la invención, se conseguirá en la mayor parte de casos mediante una combinación de software y hardware específico o una combinación de firmware específico y hardware (por ejemplo, con ayuda de un FPGA). Una realización mediante software puramente sería solamente posible cuando el aparato médico a monitorizar contiene ya el hardware necesario para su realización. En muchos microcontroladores se podría conseguir, por ejemplo, una separación completa de la zona no segura 11b de la red, de forma que las patillas I/O que están asociadas a la comunicación con la zona segura 11a de la red de comunicaciones 11, estén conmutadas a una modalidad pasiva.

A continuación se indicarán algunos ejemplos posibles de áreas de utilización del dispositivo de la invención:

En la figura 14, se ha mostrado a título de ejemplo y de forma esquemática el aseguramiento de un sistema de bombas de infusión mediante el aparato objeto de la invención. Un sistema de bombas de infusión comprende en el ejemplo mostrado un módulo de comunicación 63 que está conectado a un CAN-Bus 64 central con topología de bus lineal y resistencias de expulsión 65 y 66, así como un sistema de alarma central 67 y las bombas de infusión 68 a 72. El módulo de comunicación 63 puede convertir el protocolo de comunicación P_1 utilizado en el CAN-Bus de las bombas de infusión 68 a 72 en otro protocolo de comunicación P_2, por ejemplo, basado en Ethernet. Ese sistema de bombas de infusión representa un aparato médico 62 en el sentido de las definiciones anteriores debido a las capacidades adicionales aportadas por el sistema (comunicación central y alarma central). Para asegurar contra posibles ataques procedentes de la zona no segura 11b de la red de comunicaciones 11, se utiliza un dispositivo 73, según la invención. En la zona no segura 11b de la red de comunicaciones 11, está conectado un PC 74 que puede desempeñar funciones tales como la monitorización central de la alarma o una distribución central de datos de terapia.

En este caso, es especialmente ventajoso escoger un dispositivo, según la invención, con filtrado de paquetes bidireccional y un cierre conocido por el PC 74 para impedir un posible conocimiento de datos relativos a personas susceptibles de protección en la parte no segura de la red e impedir una manipulación no autorizada de datos de terapia en la zona no segura 11b de la red de comunicaciones 11. Los interruptores 14a y 14 de la figura 3 pueden llevar a cabo en este caso la separación de la conducción de Ethernet para un cierre correcto. De esta manera, se puede realizar una separación física del aparato médico 62 con respecto a la zona no segura 11b de la red 11. En una realización correspondiente a la figura 3, el dispositivo 73, según la invención, permanece conectado con la zona no segura 11b de la red de comunicaciones 11 y puede reconocer por esta razón (eventualmente después de una reposición o “Reset” propio) cuando deja de existir un ataque potencial al aparato médico 62. Solamente en este caso se cerrarán nuevamente los dispositivos interruptores y el aparato médico 62 quedará conectado nuevamente con la zona no segura 11b de la red de comunicaciones 11.

En este ejemplo se puede observar que se pueden conseguir ventajas de seguridad y/o de costes en una realización cuando el dispositivo 73, según la invención, y el módulo de comunicación 63 constituyen una unidad 75 que unifica las funciones de ambos aparatos individuales. Esto se puede conseguir, por ejemplo, para costes comparables de forma redundante para conseguir una elevada seguridad. Al contrario que en la realización con dos aparatos individuales, se puede evitar en este caso incluso que el módulo de comunicación 63 lleve a cabo a causa de una función de fallo, un ataque a los otros subaparatos del aparato médico 62. Un dispositivo 75 de este tipo puede funcionar como aparato independiente o puede ser integrado en el aparato médico 62, por ejemplo, en forma de tarjeta acoplable. En ambos casos, es recomendable que los interruptores 14a y 14b lleven a cabo una separación con respecto al CAN-Bus 64 ya correctamente desconectado.

Como ejemplo adicional, se citará la conexión de un grupo de monitores de pacientes a un monitor central.

Se pueden conseguir ventajas específicas, en especial por la utilización del dispositivo, según la invención, cuando un parque de aparatos médicos existente más antiguo, por ejemplo, después de un traslado a otro edificio, deben ser conectados nuevamente a la red. Los aparatos más viejos presentan frecuentemente todavía interfaces serie (por ejemplo, RS-485) que facilitan una conexión directa entre todos los participantes de la comunicación. En la figura 15 se ha mostrado, a título de ejemplo, una conexión en red de este tipo de varios monitores de pacientes que están unidos a un monitor central 76.

El monitor central 76 está unido mediante una serie de interfaces en serie RS-485 77 a 81 con los monitores conectados de pacientes 82 a 86. Para cada conexión individual está instalado un cable especializado entre el monitor central 76 y el monitor de paciente correspondiente.

Si resulta que dentro de un dispositivo médico se tiene que poner a disposición todavía una serie de otros grupos de aparatos médicos a parte de los monitores de pacientes, los elevados costes de este proceso son evidentes. Por el contrario, se ha mostrado en la figura 16 la estructura resultante con la utilización del dispositivo, según la invención, y la aplicación de una infraestructura Ethernet existente.

El monitor central 76 está conectado en este caso a un dispositivo 87, según la invención, el cual presenta varias interfaces RS-485. El dispositivo 87, según la invención, está unido a un conmutador Ethernet 88 al que están conectados los dispositivos 89 a 93, según la invención. Con sus interfaces RS-485 están nuevamente conectados los monitores de pacientes 82 a 86.

En primer lugar, esa forma de conexión, en ese caso el cableado, es sensiblemente más complicada que el cableado en forma de estrella de la figura 15. No obstante, es importante no perder de vista que los componentes que se encuentran en las casillas de trazos 94 y las conexiones de la red de comunicaciones 11 a la infraestructura IT corresponden a cualquier dispositivo médico moderno y, por lo tanto, se pueden utilizar sin costes adicionales sustanciales. Además, una estructura en red de este tipo posibilita un desplazamiento muy simple de monitores de pacientes y/o monitores centrales, puesto que éstos pueden ser acoplados conjuntamente con sus dispositivos, según la invención, en otros enchufes Ethernet del dispositivo médico.

La utilización de los dispositivos, según la invención 87 y 89 hasta 93 puede conseguir en este caso, por ejemplo, los efectos siguientes:

- Los datos de comunicaciones originales RS-485 serán transportados en paquetes envolventes TCP/IP por Ethernet,
- Los datos están protegidos mediante codificación contra una observación no autorizada en Ethernet,
- Los datos están protegidos contra una falsificación no autorizada en Ethernet,
- Mediante la variación de datos dentro de los paquetes TCP/IP envolventes, almacenados, no podrán ser utilizados por otros participantes de la red en un momento de tiempo posterior,
- Un comportamiento temporal que pueden alcanzar sin problemas los sistemas 76 y 82 a 86 en una comunicación en serie (por ejemplo, tiempos de respuesta a indicaciones de vida que a causa de circunstancias técnicas son contestados y, por lo tanto, esperados frecuentemente de manera mucho más rápida a lo que sería necesario en base a los riesgos), pero que por principio no se pueden garantizar en un transporte por Ethernet, se garantizan mediante los dispositivos objeto de la invención, mediante reserva (“Caching”) y autorización (“Proxying”). Solamente en la identificación de una verdadera alteración de la comunicación (por la permanencia de las indicaciones de vida del otro aparato médico) dejarán de facilitarse las respuestas a las indicaciones de vida por parte de los dispositivos según la invención,
- Diferentes grupos de pacientes y monitores centrales, tal como aparece por ejemplo por diferentes estaciones, no pueden influir dentro de la red de comunicaciones 11 del dispositivo médico de modo adverso,
- En la aparición de tráfico de datos potencialmente peligroso en Ethernet, los monitores de pacientes y del monitor central son separados de Ethernet. Esto hace que el monitor central no pueda funcionar, pero mantiene, no obstante, la capacidad funcional local de los monitores de pacientes.

En base a la figura 16, se puede observar que el dispositivo, según la presente invención, se puede realizar de manera ventajosa en múltiples configuraciones distintas. Estas configuraciones pueden ser distintas, por ejemplo, en:

- el tipo de los principios de trasferencia física utilizados en los lados de entrada o de salida,
- el tipo del protocolo de comunicaciones utilizado,
- el tipo de protocolo de aplicación utilizado,
- el número de entradas y salidas distintas del dispositivo, según la invención,
- las circunstancias accesorias temporales y/o lógicas para la separación del conmutador de interrupción,
- las circunstancias accesorias temporales y/o lógicas para el cierre del dispositivo conmutador de interrupción, y
- las circunstancias accesorias temporales y/o lógicas para la realización de una reposición del aparato objeto de la invención.

Una multiplicidad de configuraciones posibles de este tipo se puede conseguir de manera ventajosa para lo cual se pueden utilizar conceptos modulares para el dispositivo objeto de la invención. Un ejemplo para dicho dispositivo modular, según la invención, se ha mostrado en la figura 17.

El dispositivo modular, según la invención, 103 está compuesto por el módulo 94 de filtrado de paquetes que contiene un filtro de paquetes bidireccional 12, así como dos módulos activadores 95 y 96 que de manera correspondiente están conectados de forma independiente a un lado del módulo del filtro de paquetes con intermedio de una interfaz de comunicaciones. Los módulos de activación 95 a 96 contienen cada uno de ellos un convertidor 97 o bien 98 que lleva a cabo la conversión en los medios físicos necesarios y eventualmente una

implementación del plano inferior del protocolo de comunicación. Además, los módulos de activación 95 y 96 contienen cada uno de ellos una lógica de aseguramiento 99 o 100 que accionan los conmutadores de interrupción 101 o 102 y eventualmente pueden iniciar la reposición del dispositivo 103, según la invención.

Una construcción modular de este tipo, del dispositivo según la invención, simplifica claramente la adaptación a diferentes casos de utilización. En este caso, es especialmente aconsejable realizar también el software del dispositivo, según la invención, de forma modular, por ejemplo, de manera que se implemente una arquitectura del controlador para efectuar la activación de los diferentes módulos activadores. Asimismo es muy ventajoso el desarrollo de un generador de códigos o un API/ de un armazón con el que se puedan implementar las diferentes funciones de los filtros de paquetes en diferentes planos del modelo ISO/OSI o bien de un plano de un protocolo de aplicación, de manera sencilla, con independencia de la constitución precisa del dispositivo objeto de la invención.

A diferencia del dispositivo modular mostrado en la figura 17, de acuerdo con la presente invención, puede ser ventajoso en una realización redundante que los dispositivos lógicos de aseguramiento 99 y 100 estén contenidos parcialmente en el módulo de filtro de paquetes 94 y que a través de las interfaces de comunicaciones correspondientes las piezas simplificadas de la lógica de control contenidas en los módulos de activación puedan provocar la apertura o cierre de los correspondientes conmutadores de interrupción.

La aplicación de un dispositivo, según la invención, dentro de un dispositivo médico, puede ser utilizada en muchos aparatos/sistemas médicos que comprenden varias subredes asociadas junto con tecnología de redes conocida para el aseguramiento jerárquico de zonas parciales de la red de comunicaciones 11 de manera correspondiente a su división en diferentes zonas de seguridad. En la figura 18, se ha mostrado a título de ejemplo, un aseguramiento jerárquico de este tipo, mediante un dispositivo, según la presente invención.

Las redes de comunicaciones 106 y 107 de dos lugares de un dispositivo médico están conectados con intermedio de dos aparatos 104 y 105 con funcionalidad de cortafuegos y VPN mediante Internet. En la red de comunicaciones 106 se encuentra un monitor central 110 conectado con intermedio de un dispositivo 108, según la invención y un PC de cálculo 114 con intermedio de un aparato 112 con funcionalidad de cortafuegos y VPN. Mediante el dispositivo objeto de la invención 128 es posible, por ejemplo, en este caso, conectar el recinto de cuidados intensivos A al que se debe considerar como aparato médico a la red de comunicaciones 116. En ella, están conectados un ordenador de coordinación 118, así como un sistema de bombas de infusión 122 o bien un monitor de paciente 126 conectados con intermedio de los dispositivos 120 y 124, según la invención. El monitor del paciente 126 facilita los datos del paciente al monitor central 110 para permitir su supervisión por el monitor central junto con los datos de los pacientes de otros monitores de pacientes. El PC de coordinación 118 sirve para la transferencia de listas completas de datos de infusiones al sistema de bombas de infusiones 122 para su distribución a las bombas individuales. Esto posibilita configurar fácilmente todas las bombas del sistema de bombas de infusión 122 para su puesta en marcha o para la adaptación de la terapia de infusión. Con el ordenador de coordinación 118 se pueden enviar asimismo, eventualmente, datos a otros sistemas de bombas de infusión que se encuentran en el recinto de cuidados intensivos. En la red de comunicaciones 107 del segundo lugar considerado, se encuentra la misma estructura de red de comunicaciones 11. En este caso, un monitor central 111 está conectado con intermedio de un dispositivo, según la invención y un PC de cálculo 115 con intermedio de un aparato 113 con funcionalidad de cortafuegos y VPN. Con intermedio del dispositivo, según la invención, 129 el recinto de cuidados intensivos B está conectado a esta red de comunicaciones 117. En su interior, se encuentra un PC de coordinación, así como un sistema de bombas de infusión 123 o bien un monitor de paciente 127 conectados con intermedio de los dispositivos, según la invención, 121 y 125.

Esta arquitectura de red puede ser utilizada, por ejemplo, para las siguientes rutas de comunicación:

- Los lugares de referencia A y B comparten una red de comunicaciones común 11, la cual se compone de dos partes 106 y 107. A efectos de que en Internet no se puedan observar o manipular datos de forma no autorizada, se utiliza una VPN. Los cortafuegos en 104 y 105 aseguran ambas redes de comunicaciones 11 contra ataques en Internet.

- Los PC de cálculo 114 y 115 están conectados entre sí mediante una VPN. Ésta impide que los datos confidenciales a adaptar no puedan ser observados o manipulados de manera no autorizada dentro de las partes 106 y 107 de la red de comunicaciones 11. Dado que una parte no despreciable del malware y de los ataques generados por el mismo llegan mediante una red con intermedio de los soportes de datos por detrás de los cortafuegos de empresas, es aconsejable, en este caso, un aseguramiento de la zona crítica de la red de comunicaciones 11 para el dispositivo médico por medio de los cortafuegos de los aparatos 112 y 113.

- Dentro del recinto de cuidados intensivos A comunican el sistema de bombas de infusiones 122 con el PC de coordinación 118 con intermedio de la red de comunicaciones 116. Puesto que en esta parte de la red de comunicaciones 11 pueden estar conectados también otros aparatos potencialmente peligrosos para el sistema de bombas de infusión 122, incluso el PC de coordinación podría encontrarse en contacto con el malware a través de soporte de datos, se asegurará mediante un dispositivo, según la invención, 120.

- Un monitor de paciente que está asegurado mediante el dispositivo, según la invención, 124 puede llevar a cabo una comunicación con el monitor central que está asegurado mediante el dispositivo, según la invención, 108.

• Para minimizar la influencia de otros participantes en las comunicaciones en la red de comunicaciones 106, se permitirá el paso a través del dispositivo 128, según la invención, de aquellos paquetes de comunicaciones en el recinto de cuidados intensivos A que son relevantes realmente para los aparatos médicos situados en el mismo.

Se explicarán a continuación algunas reacciones a posibles ataques. En este caso, se debe partir del hecho de que los ataques están dirigidos a aparatos conectados al sistema y por parte de la lógica de control de los correspondientes aparatos pueden ser reconocidos como suficientemente gravosos, que no se muestra suficiente la simple reducción de los paquetes de comunicaciones a través del filtro de paquetes, sino que se abrirá el correspondiente dispositivo de interrupción.

En caso de un ataque dentro de la red de comunicaciones 116, el dispositivo, según la invención, 120 acciona el dispositivo de interrupción, de manera que el sistema de bombas de infusión 122 puede continuar sin alteraciones sus infusiones, pero, no obstante, no es posible la comunicación con el ordenador de coordinación 118. El dispositivo 124, según la invención, acciona, en esta situación, igualmente el dispositivo de interrupción, de manera que el monitor de paciente 126 realiza también sin alternaciones la función de monitorización, pero no es posible la comunicación con el monitor central 110. Además, el dispositivo, según la invención, 128 acciona también el dispositivo de interrupción y no permite influencias de los ataques sobre el resto de la red de comunicaciones 106. De esta manera, la funcionalidad de otro recinto de cuidados intensivos, en la que no han aparecido los ataques dentro de la propia red, está asegurada sin alteraciones y también el monitor central 110 puede comunicar con los monitores de pacientes de los otros recintos de cuidados intensivos sin alteraciones.

En caso de un ataque que procede de la red de comunicaciones 106, los dispositivos de interrupción de los dispositivos, según la invención 112 y 128 serán accionados. El monitor central no tiene, por lo tanto, conexión alguna con el monitor del paciente 126 y tampoco con los monitores de pacientes en otros recintos de cuidados intensivos. La comunicación dentro de la red de comunicaciones 116 permanece, no obstante, inalterada, de manera que la utilización del ordenador de coordinación 118 sigue siendo posible de modo completo conjuntamente con el sistema de bombas de infusión 122.

Una utilización jerárquica de este tipo de los dispositivos, según la invención, posibilita en el caso de ataques que no se realicen solamente las funcionalidades imprescindibles y simultáneamente minimizar los efectos sobre otros participantes de la red de comunicaciones y de esta manera aumentar la disponibilidad.

Todas las características que se han dado a conocer en la documentación de la solicitud se reivindican como esenciales para la invención siempre que, individualmente o en combinación, sean nuevas con respecto al estado de la técnica.

Lista de símbolos de referencia

1 Vivienda del paciente

2 Dispositivo médico

3 Red WAN

4 Aparato médico de recogida de datos

5 Red LAN

6 Red LAN del dispositivo médico

7 Aparato médico de evaluación

8 Zona no segura de la red de comunicaciones considerada desde el dispositivo médico

9 Dispositivo según la invención

10 Aparato médico

11 Red de comunicaciones

11a Zona segura

11b Zona no segura

12 Filtro de paquetes

13 Lógica de control

14 Dispositivo de interrupción

15, 16 Aparato médico parcial

18 Filtro de paquetes bidireccional

19 Central de monitores de pacientes

20, 21, 22 Monitor de paciente

26 Paquete de comunicaciones enviado

27 Paquete de comunicaciones modificado

28 Datos adicionales

29 Paquete de comunicaciones utilizable por el aparato médico

30 Zona de datos codificados

31 Paquete de comunicaciones modificado codificado

32 Dispositivo, según la invención, con dispositivo de interrupción de la zona no segura de la red de comunicaciones

33 Dispositivo, según la invención, con dispositivos de interrupción a ambos lados

35 Canal de trabajo

36 Canal de monitorización

37 Dispositivo, según la invención, con dos subsistemas independientes entre sí

38, 39 Subsistemas independientes

40, 41 Dispositivo de interrupción

42, 43 Lógica de control

44, 45 Filtro de paquetes

46 Comparador

47 Ruta de comunicación entre los subsistemas

48 Aparato, según la invención, diversificado

49, 50 Dispositivo de interrupción

51, 52 Primer y segundo canal

53, 54 Primer y segundo sistemas operativos

55, 56 Primer y segundo cortafuegos

57, 58 Primer y segundo escáner de virus

59, 60 Primer y segundo análisis de protocolo

61 Comparador

62 Aparato médico

63 Módulo de comunicaciones

64 CAN-Bus

65, 66 Resistencia de bloqueo

67 Sistema de alarma

68-72 Bombas de infusiones

73 Dispositivo, según la invención

74 Ordenador

75 Unidad formada por el dispositivo, según la invención, 75 y módulo de comunicaciones 63

76 Monitor central

77–81 Interfaces RS-485

82-86 Monitores de pacientes

87 Dispositivo, según la invención

88 Conmutador Internet

89-93 Dispositivos, según la invención

94 Unidad formada por componentes y conexiones de la red de comunicaciones

95, 96 Módulo activador

97, 98 Activador

99, 100 Lógica de aseguramiento

101, 102 Dispositivo de interrupción

103 Aparato, según la invención

104, 105 Aparato con funcionalidad cortafuegos y VPN

106, 107 Redes de comunicaciones de dos lugares de referencia de un dispositivo médico

108, 109 Dispositivo según la invención

110, 111 Monitor central

112, 113 Aparato con funcionalidad de cortafuegos y VPN

114, 115 PC de cálculo

116, 117 Redes de comunicaciones

118, 119 PC de coordinación

120, 121 Dispositivos según la invención

122, 123 Sistema de bombas de infusión

124, 125 Dispositivos según la invención

126, 127 Monitores de pacientes

128, 129 Aparatos según la invención

REIVINDICACIONES

1. Dispositivo (9; 34; 37) para la interacción con un aparato médico (10) que es adecuado para conexión en una red de comunicaciones (11) que comprende como mínimo una zona no segura (11b) y una zona segura (11a) en el lado del aparato, de manera que el dispositivo (9) comprende medios de transmisión (12; 44, 45) para transmitir paquetes de comunicación hacia y desde el aparato médico (10) por medio de la red de comunicaciones (11), que comprende medios de monitorización (13; 42, 43) para monitorizar el estado de la conexión del aparato (10) a la red (11) y que comprende medios de interrupción (14; 40, 41) para la interrupción de la conexión existente entre el área segura (11a) y el área no segura (11b) de la red (11) en caso de que, durante el proceso de monitorización se detecte un estado de la conexión a la red que presente riesgo para un paciente tratado con el aparato (10) o en cuanto al funcionamiento correcto del aparato (10), **caracterizado** por que

el dispositivo presenta una arquitectura redundante que está configurada para lograr un medida mayor en seguridad, en el que la arquitectura redudante, constituida por al menos un canal de trabajo configurado a través de los medios de transmisión (12; 44, 45), que está dispuesto para transmitir paquetes de comunicación, y al menos un canal de monitorización formado por los medios de monitorización (13; 42, 43), que está dispuesto para monitorizar la forma correcta de funcionamiento del canal de trabajo, está construida en subsistemas separados uno de otro (35, 36; 38, 39), y un modelo de la función de los medios de transmisión (12; 44, 45) está integrado en los medios de monitorización (13; 42, 43) y los medios de monitorización (13; 42, 43) están dispuestos para verificar la manera correcta de funcionamiento de los medios de transmisión (12; 44, 45) sobre la base de una evaluación de informaciones procedentes de otro subsistema y del modelo.

2. Dispositivo, según la reivindicación anterior, **caracterizado** por que los medios de transmisión (12; 44, 45) comprenden un filtro de paquete que lleva a cabo el filtrado de paquete en los paquetes de comunicación transmitidos entre el área no segura (11b) y el área segura (11a) de la red de comunicaciones (11), de manera que el filtro de paquete es adecuado para bloquear paquetes de comunicación que presentan un riesgo potencial para el aparato médico (10), por que los medios de interrupción comprenden como mínimo un dispositivo de interrupción (14; 40, 41), y por que los medios de monitorización (12) comprenden como mínimo una lógica de control (13; 42, 43) que, cuando se detecta un estado de la red de conexión que presenta un riesgo para un paciente o para el correcto funcionamiento del aparato, activa la interrupción del dispositivo o dispositivos de interrupción (14; 40, 41) a efectos de separar el área no segura (11b) del área segura (11a) de la red de comunicaciones (11) que está conectada directamente al aparato médico (10).

3. Dispositivo, según la reivindicación anterior, **caracterizado** por que el filtro o filtros de paquetes (12; 44, 45) llevan a cabo un filtrado de paquetes bidireccional de los paquetes de comunicación transmitidos entre el área no segura (11b) y el área segura (11a) de la red de comunicaciones (11).

4. Dispositivo, según una de las reivindicaciones anteriores, **caracterizado** por que el filtro de paquetes (12; 44, 45) sustituye de manera parcial o completa los medios de monitorización (13; 42, 43) y/o los medios de interrupción (13, 14) para lo cual bloquea paquetes de comunicación perjudiciales o todos los paquetes de comunicación cuando se detecta una situación de conexión a la red que presenta riesgo para los pacientes o para el correcto funcionamiento del aparato.

5. Dispositivo, según la reivindicación anterior, **caracterizado** por que la separación entre el área segura (11a) y el área no segura (11b) de la red de comunicaciones (11) es implementada en forma de segmentación lógica.

6. Dispositivo, según una de las reivindicaciones 1 a 4, **caracterizado** por que la separación entre el área segura (11a) y el área no segura (11b) de la red de comunicaciones (11) es implementada en forma de segmentación física.

7. Dispositivo, según la reivindicación anterior, **caracterizado** por que dicha segmentación física es conseguida por diferentes rutas de transmisión físicas en el área segura (11a) o en el área no segura (11b) de la red de comunicaciones (11) o por diferentes casos de la misma ruta de transmisión.

8. Dispositivo, según la reivindicación 6 o 7, **caracterizado** por que la red de comunicaciones (11) comprende rutas de transmisión por cables y/o por radio.

9. Dispositivo, según la reivindicación anterior, **caracterizado** por que la ruta de transmisión en el área segura (11a) de la red de comunicaciones (11) consiste en fibra óptica.

10. Dispositivo, según una de las reivindicaciones 2 a 9, **caracterizado** por que el filtro de paquetes (12; 44, 45) es adecuado para llevar a cabo una traducción y/o encriptado de los protocolos de comunicación utilizados en la zona no segura (11b) o en la zona segura (11a) de la red de comunicaciones (11) de manera tal que paquetes de comunicación que han sido modificados con respecto a los paquetes de comunicación que se originan a partir del protocolo original son utilizados en la otra área respectiva de la red de comunicaciones (11).

11. Dispositivo, según una de las reivindicaciones anteriores 2 a 10, **caracterizado** por que dicha lógica de control (13) tiene medios para llevar a cabo una comprobación estática y/o dinámica de los datos a transmitir en la red de comunicaciones (11), de manera que los resultados de dicha comprobación conducen a que la conexión existente entre el área segura (11a) y el área no segura (11b) de la red (11) se mantenga o se corte por activación del dispositivo o dispositivos de interrupción (14; 40, 41).

12. Dispositivo, según una de las reivindicaciones anteriores, **caracterizado** por que el o los dispositivos de interrupción (14; 40, 41) están situados en el lado conectado al área segura (11a) de la red de comunicaciones (11) y/o en el lado del dispositivo (9) conectado al área no segura (11b) de la red de comunicaciones (11), a efectos de poder separar del área no segura (11b) solamente el aparato médico (10) y/o tanto el aparato médico (10) como el aparato (9) propiamente dicho.

13. Dispositivo según una de las reivindicaciones anteriores, caracterizado por que presenta al menos dos canales diversificados (38, 39) con respectivos medios de transmisión adecuados (12; 44, 45), medios de monitorización (13; 42, 43) y medios de interrupción (14; 40, 41), en el que cada canal puede monitorizarse a sí mismo como también al otro canal de manera independiente y puede separarse del área no segura (11b) de la red de comunicaciones (11) cuando se detecta una situación de la conexión de red que representa un peligro para el paciente o para el correcto funcionamiento del aparato.

14. Dispositivo según la reivindicación anterior, caracterizado por que presenta un comparador (46; 61) que es adecuado para comparar uno con otro los resultados del filtrado de paquetes en cada canal (38, 39) y reenviar los paquetes de comunicación a transmitir sólo si son los mismos en cada canal (38, 39).

15. Dispositivo, según una de las reivindicaciones 13 y 14, **caracterizado** por comprender en cada canal (38, 39) una lógica de seguridad que es adecuada para separar el área no segura (11b) de la red de comunicaciones (11) de su área segura (11a), independientemente de la lógica de seguridad de cualquier otro canal cuando se detecta una situación de la conexión de la red que presenta riesgo para los pacientes o para el funcionamiento correcto del aparato.

16. Aparato médico (10) apropiado para su conexión a una red de comunicaciones (11) que comprende como mínimo un área no segura (11b) y un área segura (11a) en el lado del aparato, **caracterizado** por comprender un dispositivo (9; 34; 37) según una de las reivindicaciones anteriores.

17. Aparato médico, según la reivindicación anterior, **caracterizado** por comprender una bomba de infusión (62) o un monitor de paciente.

18. Sistema médico que comprende una serie de aparatos médicos (10) o subaparatos (15, 16) que es apropiado para su conexión a una red de comunicaciones (11) que comprende como mínimo un área no segura (11b) y un área segura (11a) en el lado del aparato, **caracterizado** por que el sistema comprende como mínimo un dispositivo (9; 34; 37) según una de las anteriores reivindicaciones 1 a 16.

19. Sistema médico, según la reivindicación anterior, **caracterizado** por que cada uno de los aparatos individuales (10) o subaparatos (15, 16) tiene su propio dispositivo (9) de acuerdo con una de las reivindicaciones anteriores 1 a 16.

20. Procedimiento para el control de un dispositivo (9; 34; 37) para interaccionar con un aparato médico (10) que es adecuado para conexión en una red de comunicaciones (11) que comprende como mínimo un área no segura (11b) y un área segura (11a) en el lado del aparato, de manera que el procedimiento asegura la transmisión de paquetes de comunicación hacia y desde el aparato médico (10) con intermedio de la red de comunicaciones (11), monitoriza la situación de la conexión del aparato (10) con la red (11) e interrumpe una conexión existente entre el área segura (11a) y el área no segura (11b) de la red (11) si durante el proceso de monitorización se detecta una situación de conexión a la red que representa riesgo para un paciente o para el funcionamiento correcto del aparato, **caracterizado** por que el procedimieneto trabaja de manera redundante en etapas de trabajo en al menos un canal de trabajo formado por medios de transmisión (12; 44, 45) para transmitir paquetes de comunicación y en etapas de monitorización en al menos un canal de monitorización formado por medios de monitorización (13; 42, 43) para monitorizar la correcta realización de las etapas de trabajo, en un canal de trabajo y un canal de monitorización interrumpidos en respectivos subsistemas (35, 36; 38, 39) separados uno de otro para lograr una medida más elevada en seguridad, en el que, en las etapas de monitorización, está integrado un modelo al menos parcial de la función de las etapas de transmisión y las etapas de monitorización se realizan de tal manera que se comprueba la manera correcta de funcionamiento de los medios de transmisión (12; 44, 45) sobre la base de una evaluación de informaciones procedentes de otro subsistema y del modelo.

21. Procedimiento, según la reivindicación anterior, **caracterizado** por que lleva a cabo un filtrado de paquetes durante la transmisión de los paquetes de comunicación transmitidos entre el área no segura (11b) y el área segura (11a) de la red de comunicaciones (11), de manera que este filtrado es adecuado para bloquear paquetes de comunicación que presentan riesgo potencial para el aparato médico (10).

22. Procedimiento, según una de las reivindicaciones 20 a 21, **caracterizado** por que lleva a cabo un filtrado de paquetes bidireccional en los paquetes de comunicación transmitidos entre el área no segura (11b) y el área segura (11a) de la red de comunicaciones (11).

23. Procedimiento, según una de las reivindicaciones 20 a 22, **caracterizado** por que permite la segmentación lógica entre el área segura (11a) y el área no segura (11b) de la red de comunicaciones (11).

24. Procedimiento, según una de las reivindicaciones 20 a 23, **caracterizado** por que permite que dichas etapas de monitorización y/o interrupción sean sustituidas parcial o completamente por el filtrado de paquetes durante la etapa de transmisión, para lo cual bloquea, durante el filtrado de paquetes, paquetes de comunicación perjudiciales o todos los paquetes de comunicación cuando se ha detectado una situación de la conexión de red que presente riesgo para el paciente o para el funcionamiento correcto del aparato.

25. Procedimiento, según una de las reivindicaciones 20 a 24, **caracterizado** por que el filtrado de paquetes es adecuado para llevar a cabo la traducción y/o encriptado de los protocolos de comunicación utilizados en el área no segura (11b) o en el área segura (11a) de la red de comunicaciones (11) de manera tal que los paquetes de comunicación que han sido modificados con respecto a los paquetes de comunicación que se originan a partir del protocolo original son utilizados en la otra área respectiva de la red de comunicación (11).

26. Procedimiento, según una de las reivindicaciones 20 a 25, **caracterizado** por que durante la etapa de monitorización se lleva a cabo una comprobación estática y/o dinámica de los datos a transmitir en la red de comunicación (11), conduciendo el resultado de dicha comprobación al mantenimiento o al corte de la conexión existente entre el área segura (11a) y el área no segura (11b) de la red (11).

27. Procedimiento según una de las reivindicaciones 20 a 26, **caracterizado** por que trabaja en al menos dos canales diversificados (38, 39) con una respectiva transmisión, monitorización e interrupción propias, en el que cada canal puede monitorizarse a sí mismo y también al otro canal de manera independiente y puede separarse del área no segura (11b) de la red de comunicaciones (11) cuando se detecta una situación de la conexión de red que representa un peligro para el paciente o para el correcto funcionamiento del aparato.

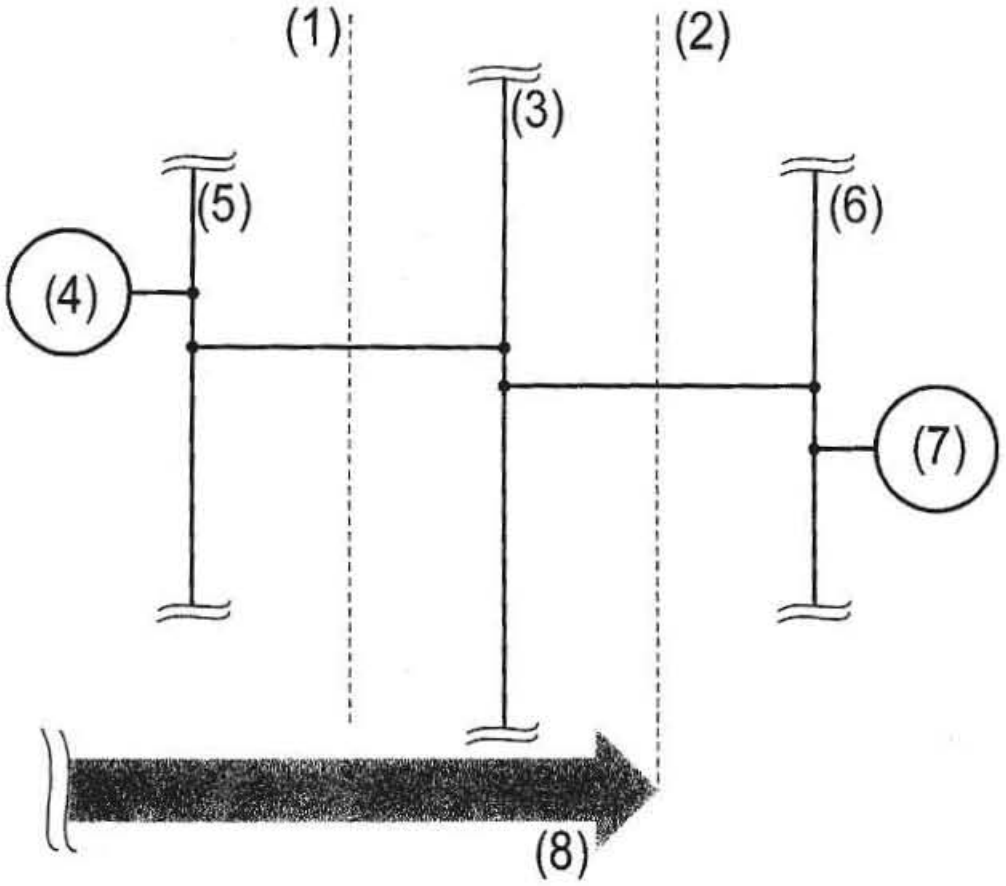

Fig. 1

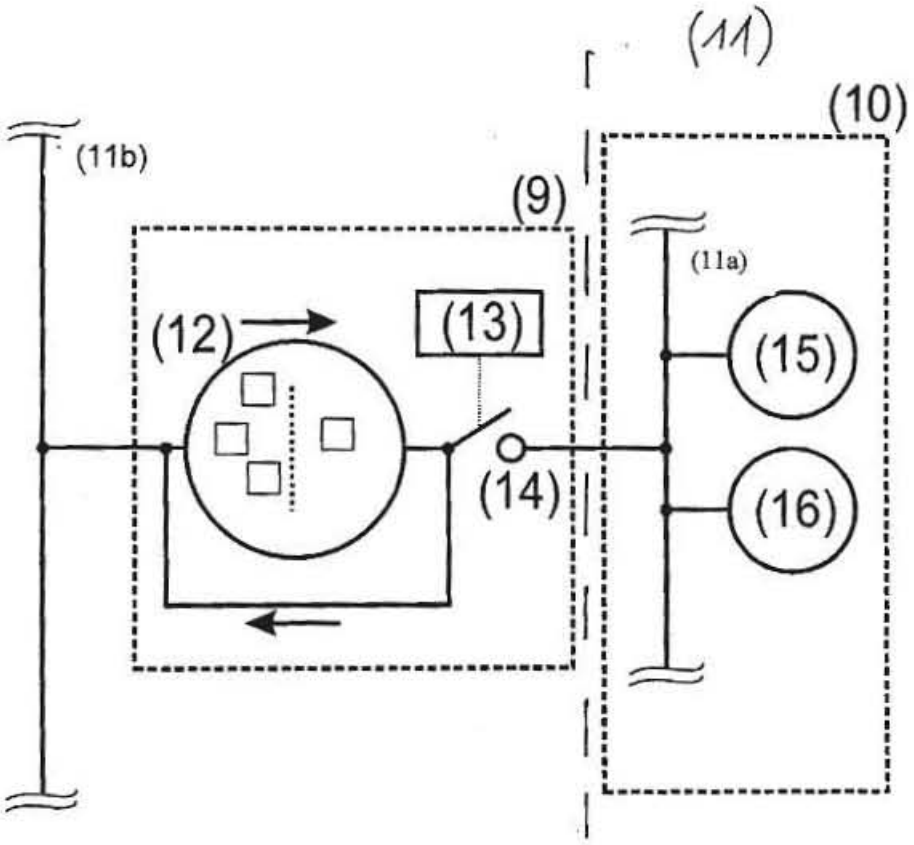

Fig. 2

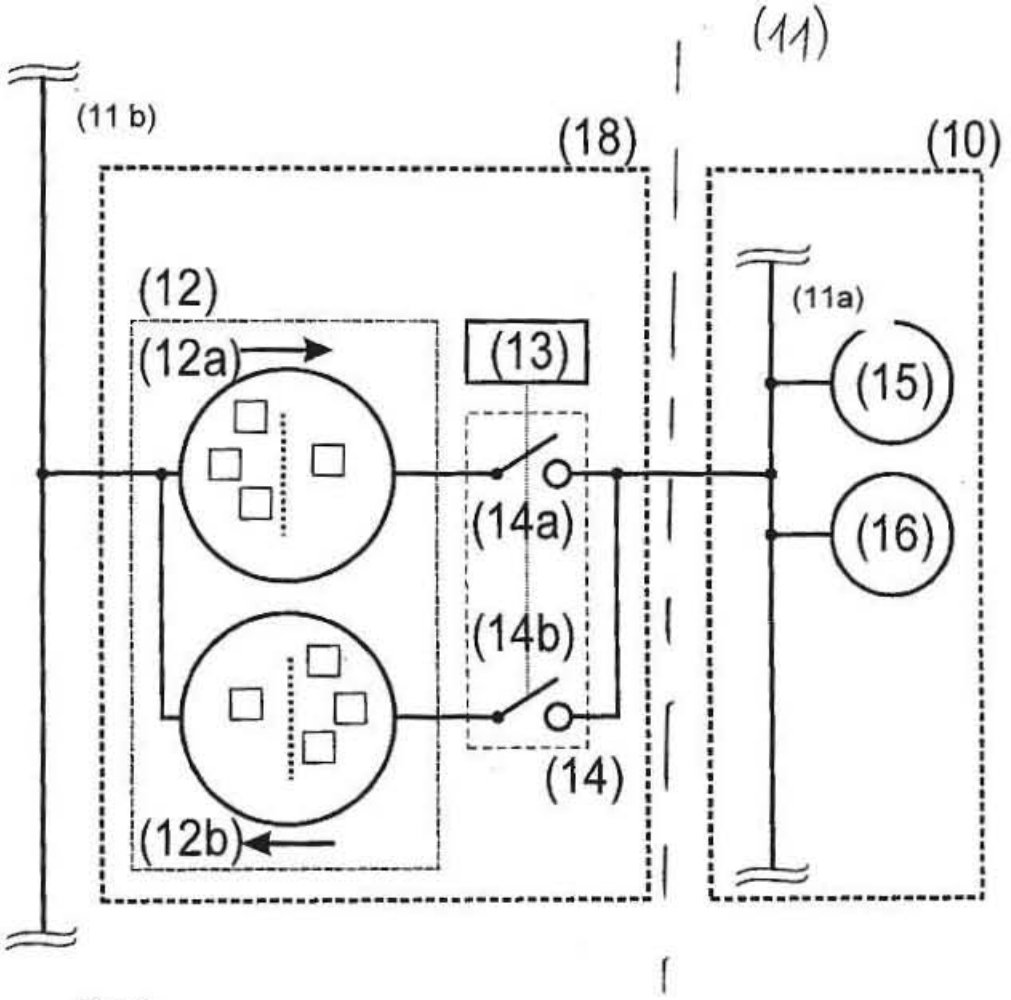

Fig. 3

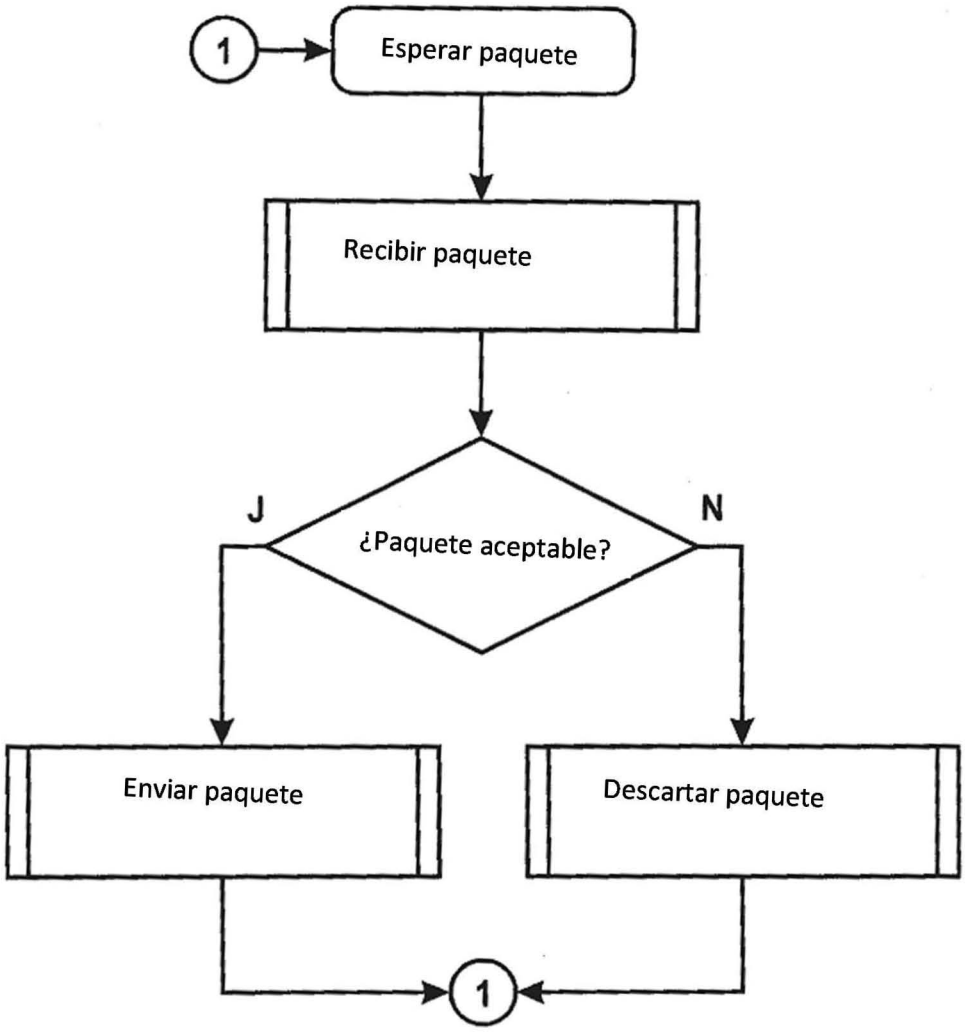
1
Esperar paquete
Recibir paquete
J
¿Paquete aceptable?
N
Enviar paquete
Descartar paquete
1

Fig. 4

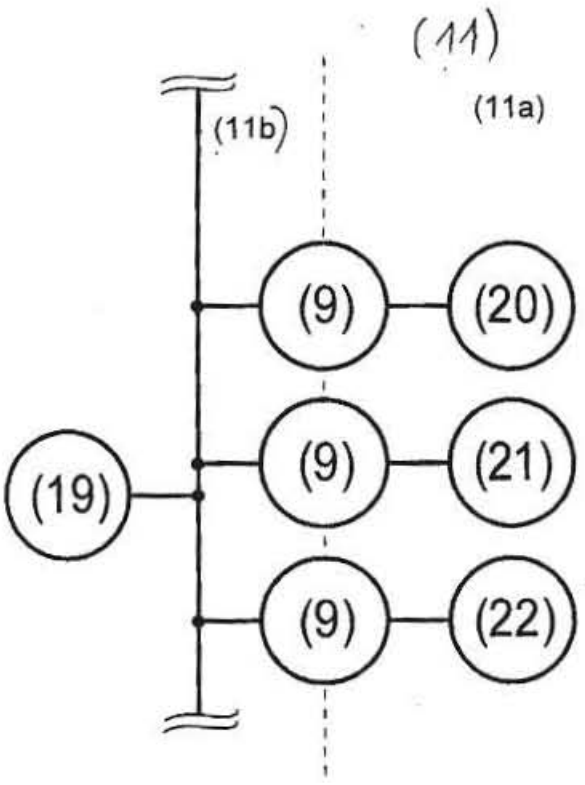

Fig. 5

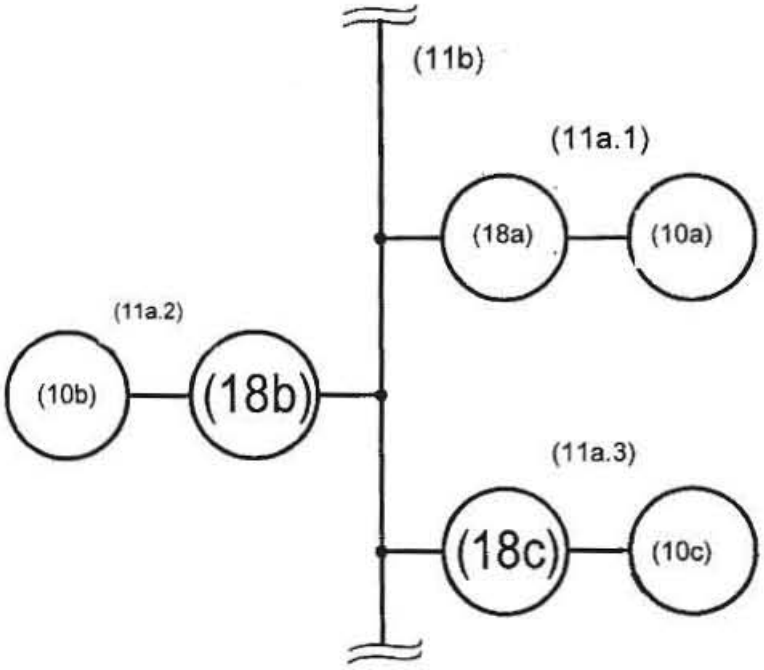

Fig. 6

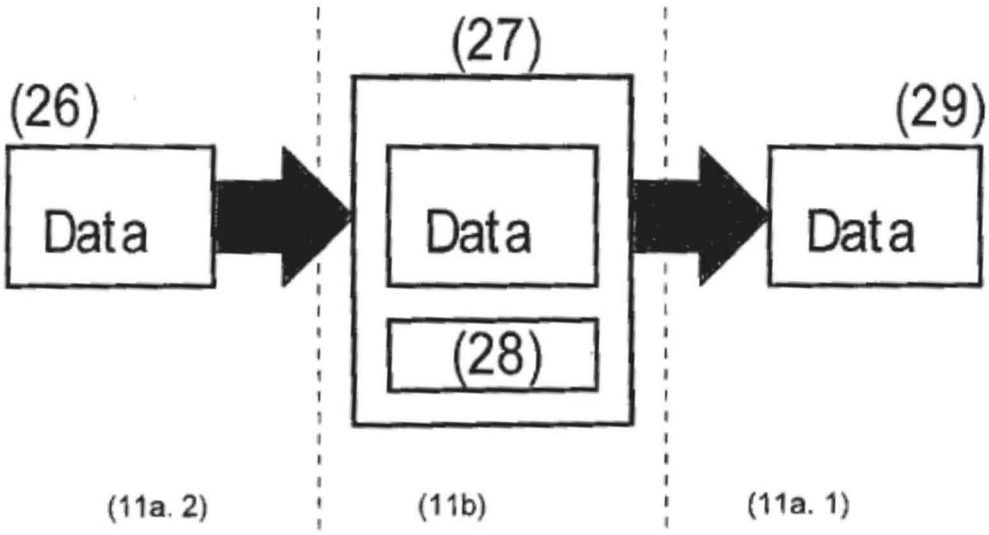

Fig. 7

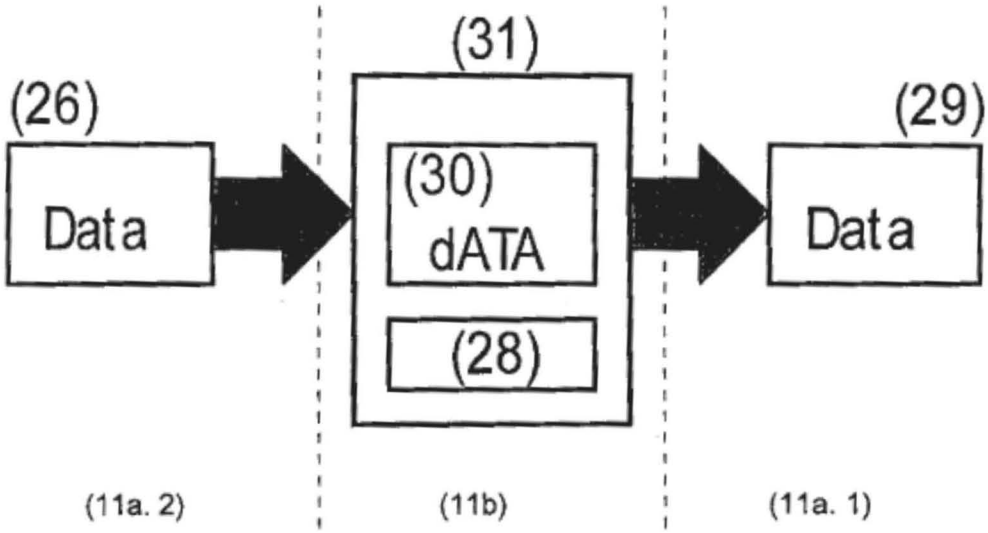

Fig. 8

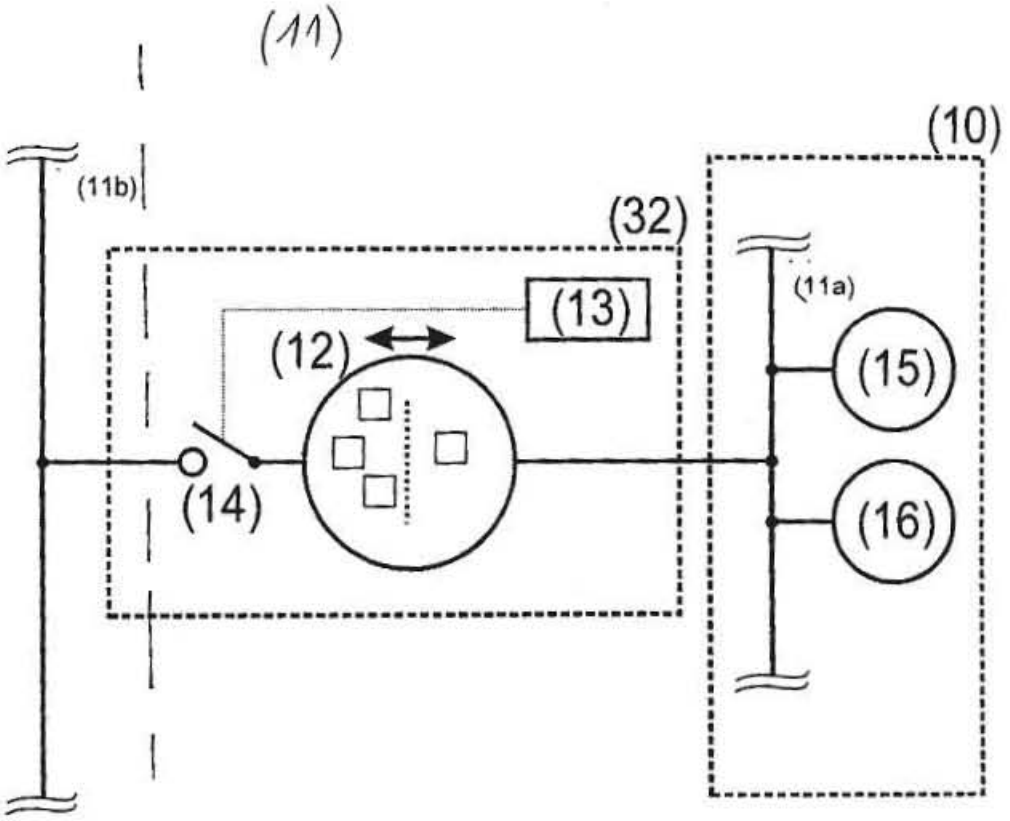

Fig. 9

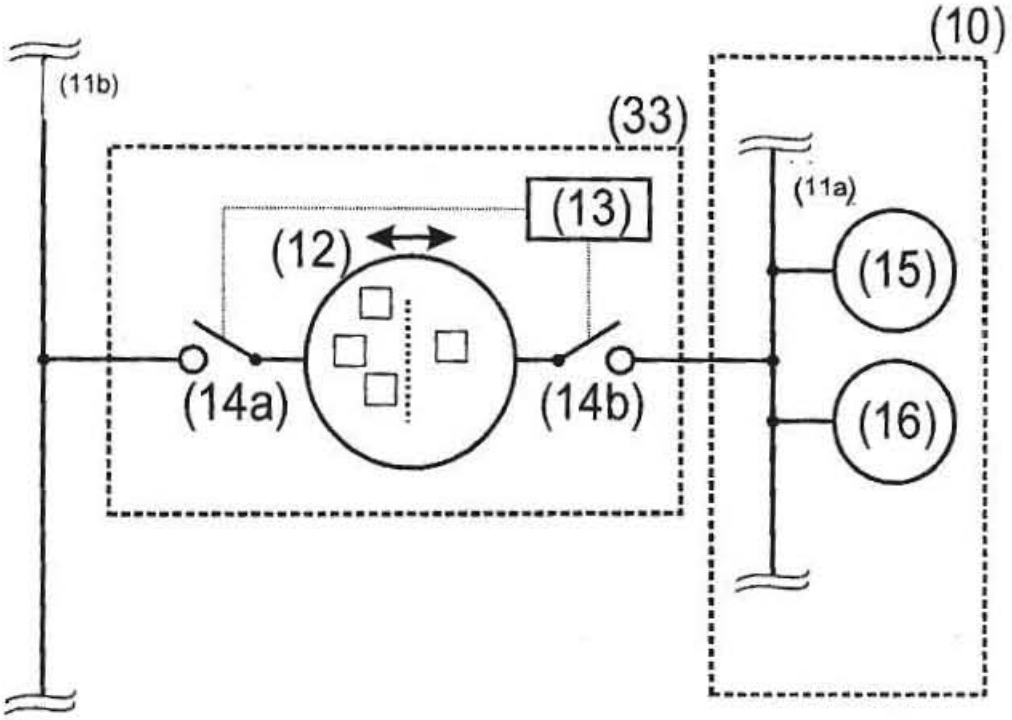

Fig. 10

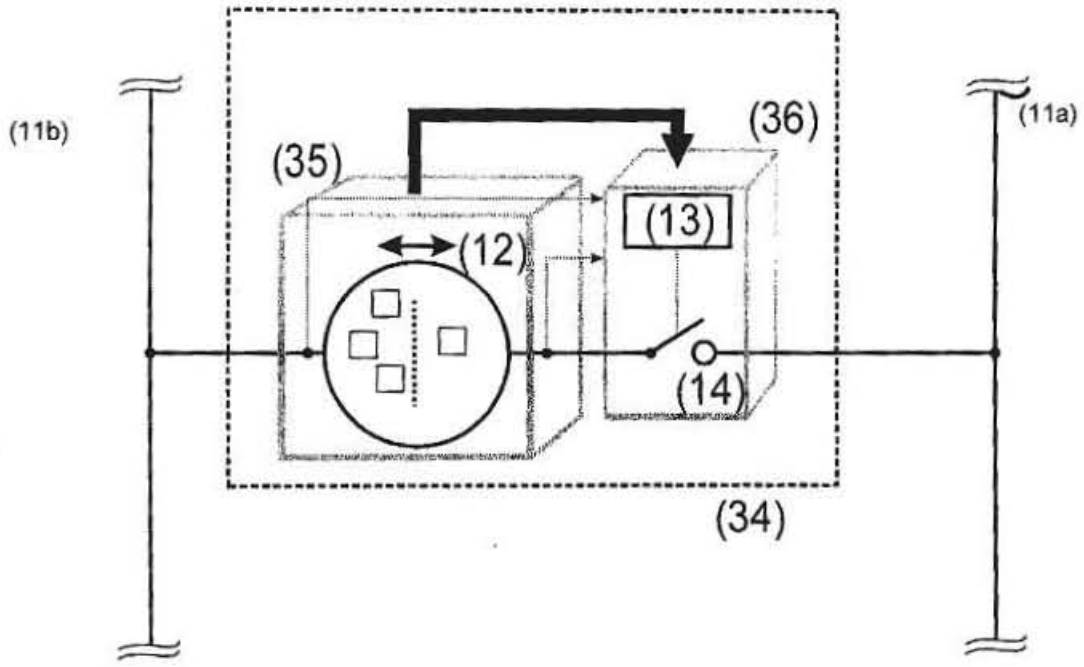

Fig. 11

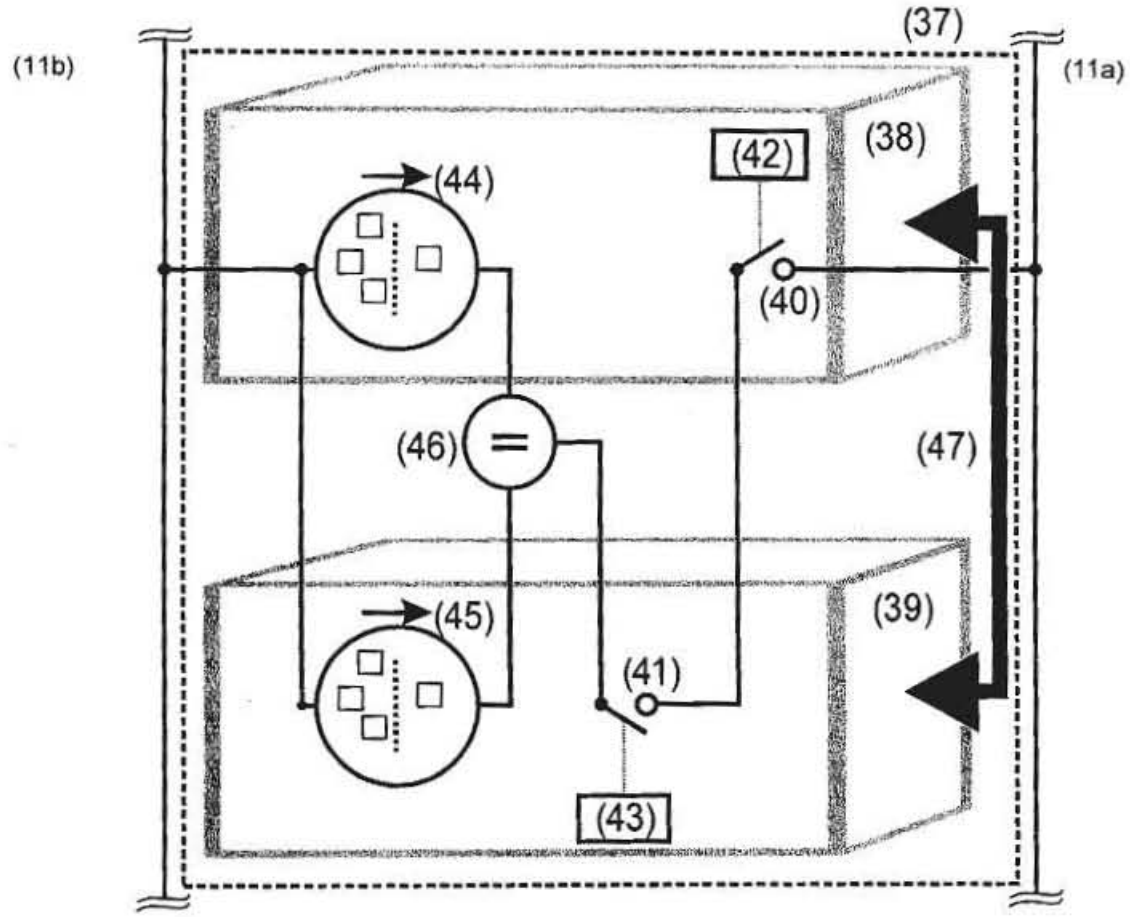

Fig. 12

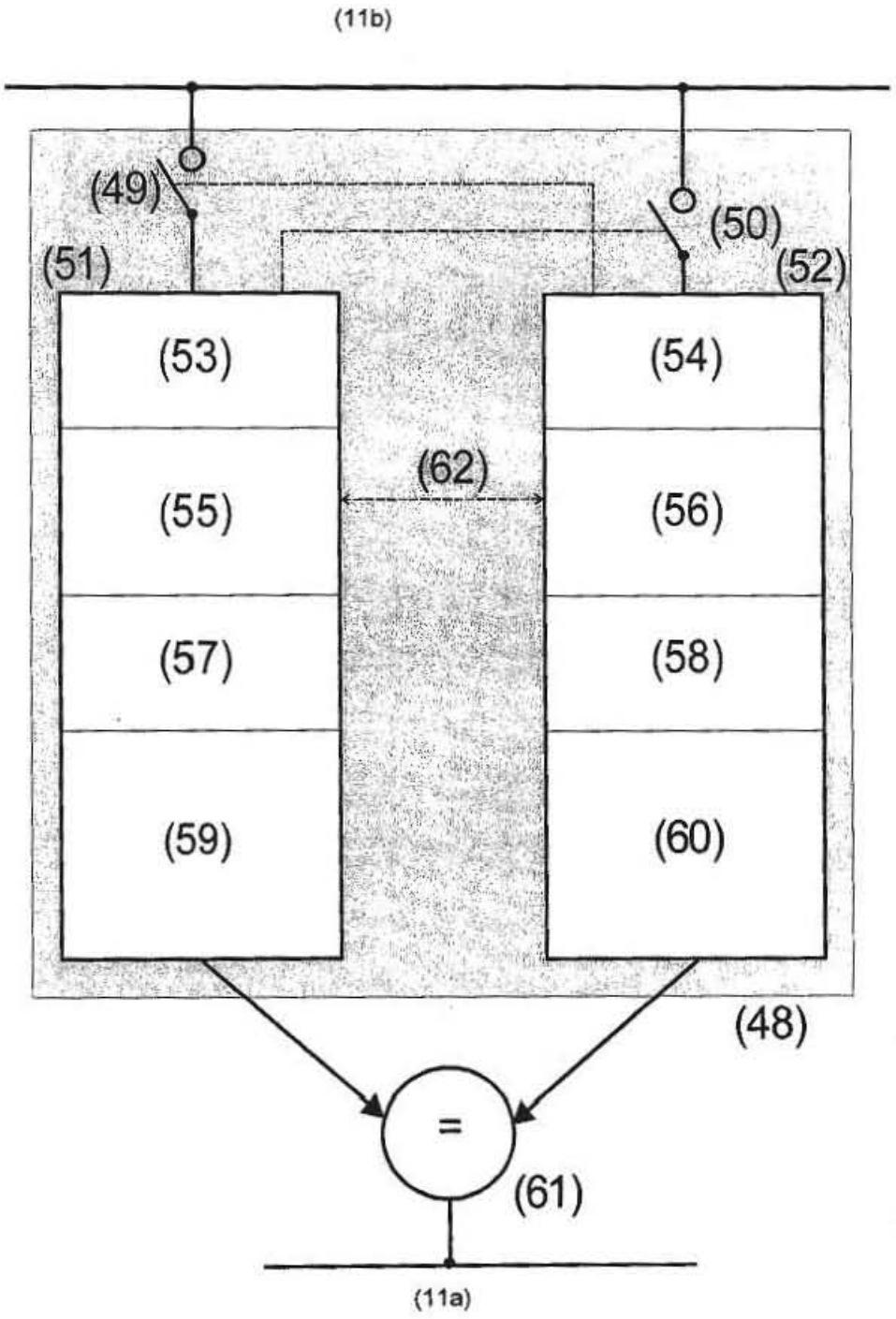

Fig. 13

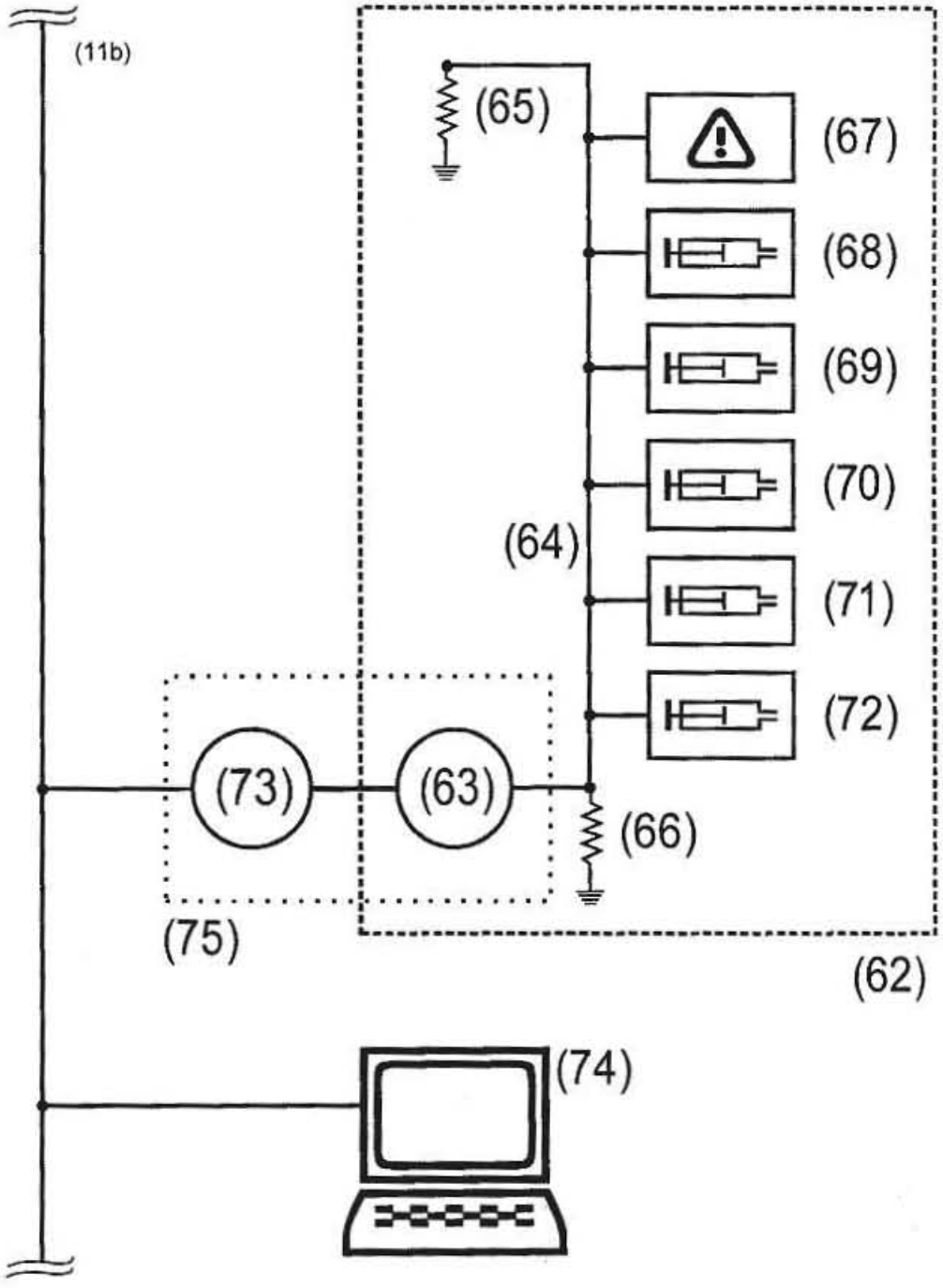

Fig. 14

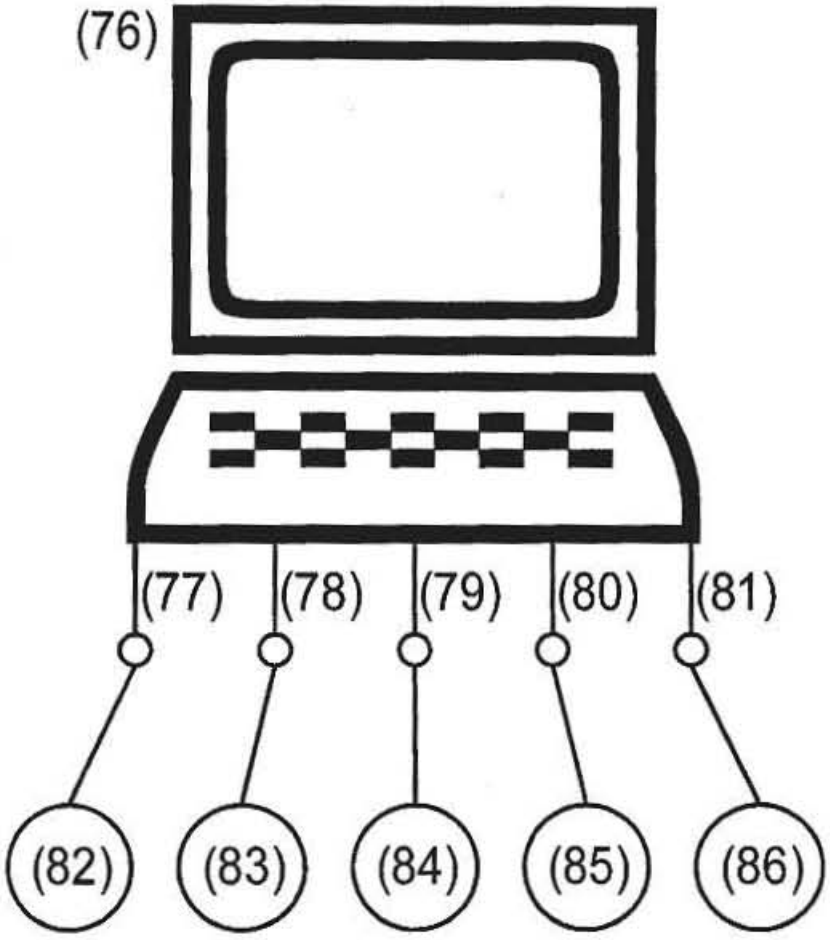

Fig. 15

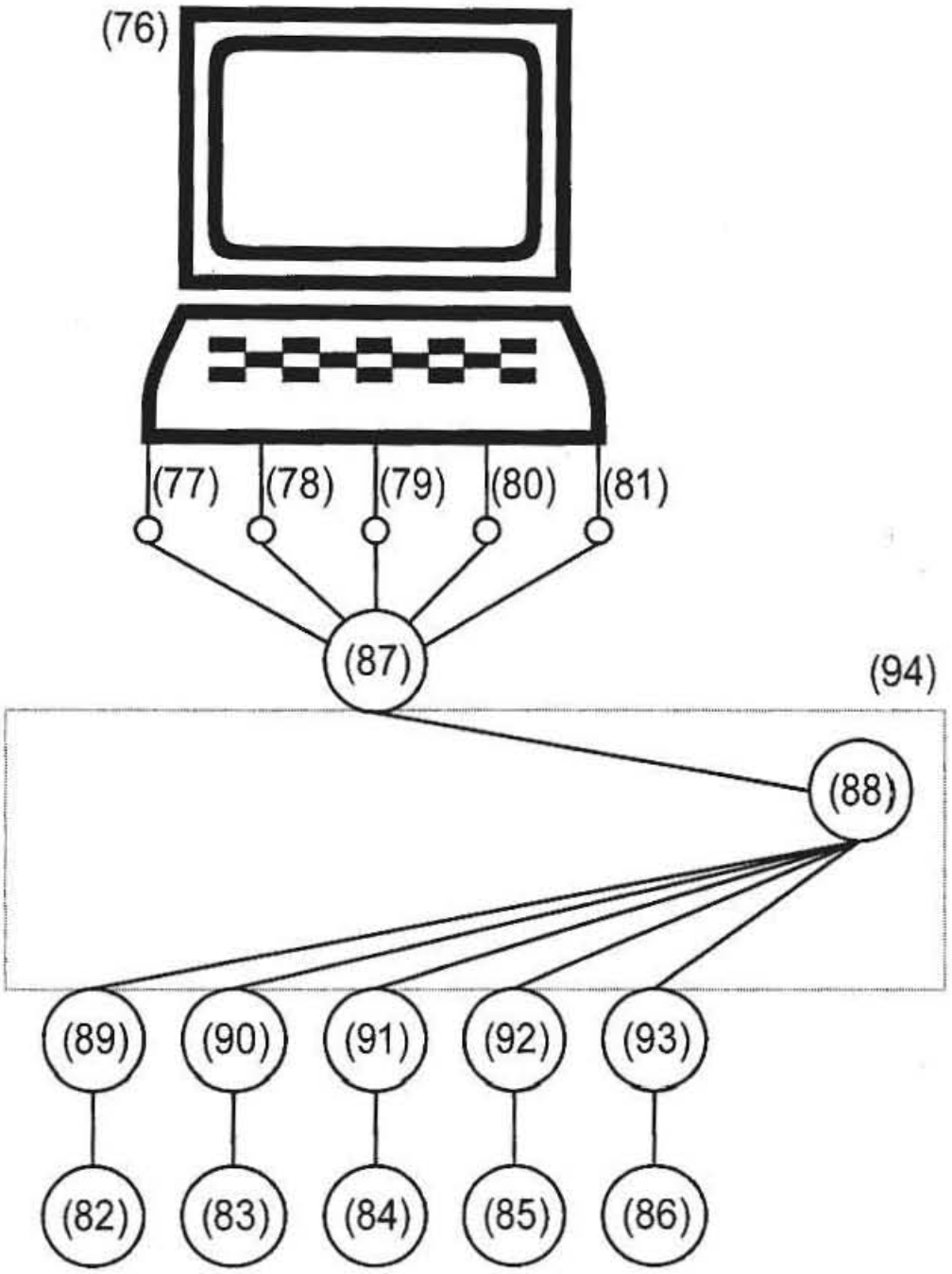

Fig. 16

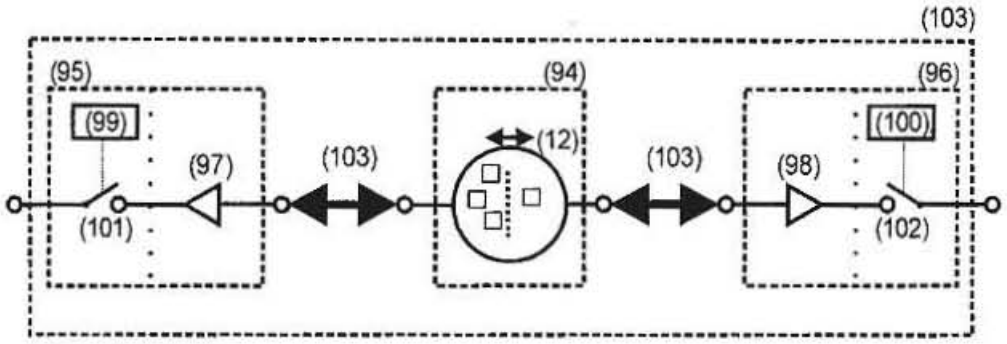

Fig. 17

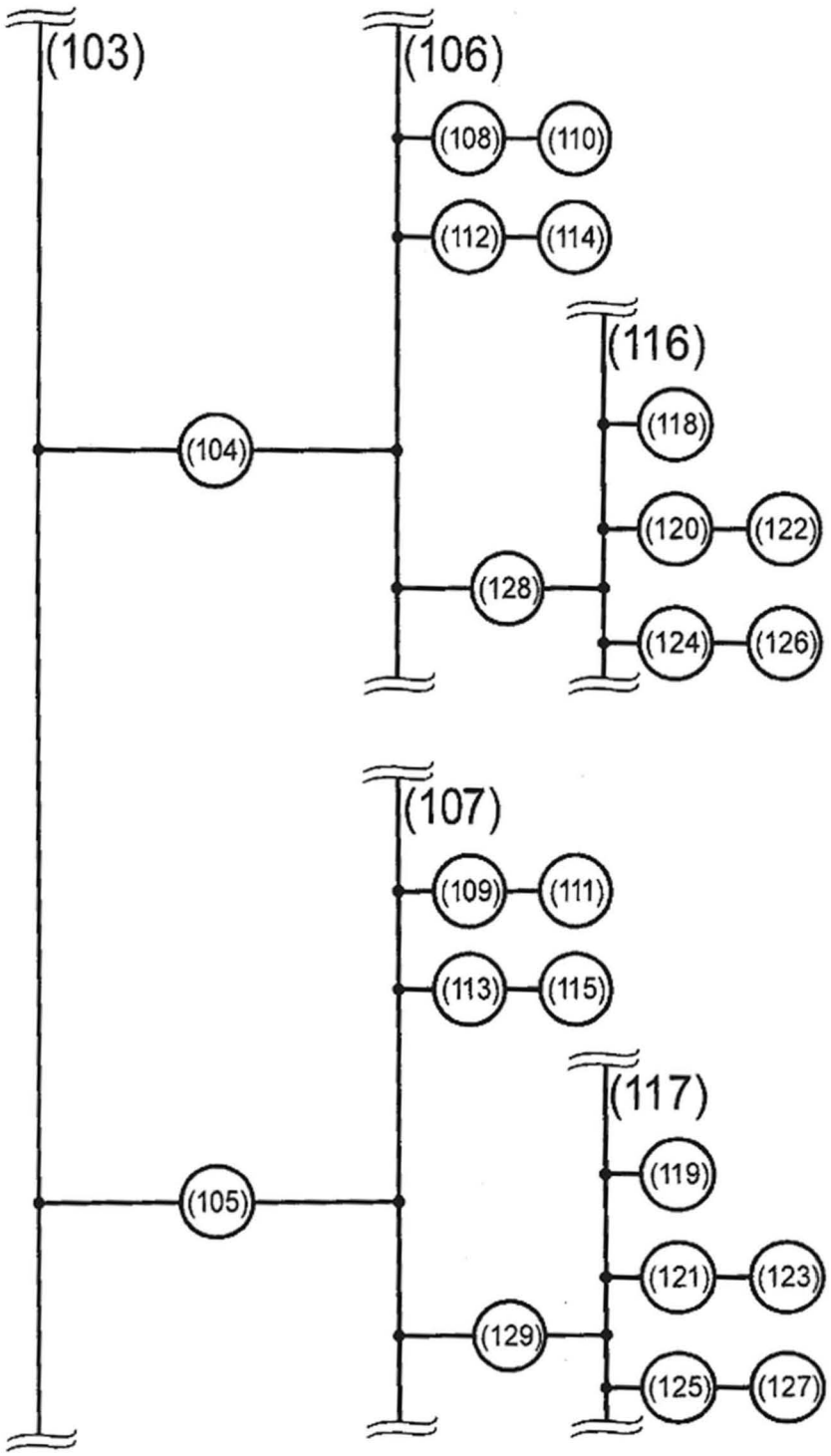
(103)
(106)
(108)
(110)
(112)
(114)
(116)
(118)
(104)
(120)
(122)
(128)
(124)
(126)
(107)
(109)
(111)
(113)
(115)
(117)
(119)
(105)
(121)
(123)
(129)
(125)
(127)

Fig. 18