

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 928 107**

51 Int. Cl.:

G05B 19/042 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.10.2018** **PCT/EP2018/078893**

87 Fecha y número de publicación internacional: **23.05.2019** **WO19096545**

96 Fecha de presentación y número de la solicitud europea: **22.10.2018** **E 18795387 (2)**

97 Fecha y número de publicación de la concesión europea: **03.08.2022** **EP 3710897**

54 Título: **Procedimiento y dispositivo para la protección contra ciberataques de grupos motobomba**

30 Prioridad:

15.11.2017 DE 102017220380

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

15.11.2022

73 Titular/es:

KSB SE & CO. KGAA (100.0%)
Johann-Klein-Straße 9
67227 Frankenthal, DE

72 Inventor/es:

BOSBACH, FRANZ GERHARD y
BRODERSEN, SÖNKE

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 928 107 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y dispositivo para la protección contra ciberataques de grupos motobomba

- 5 La presente invención se refiere a un procedimiento y a un dispositivo para la protección de un grupo motobomba, en particular un grupo de bomba centrífuga, contra ciberataques.

10 Influir específicamente en o destruir una bomba centrífuga es una forma de ciberataque. Los ciberataques son ataques dirigidos a una infraestructura específica de redes informáticas importantes desde el exterior. Este tipo de redes informáticas también se utilizan cada vez más para controlar plantas.

15 Las bombas centrífugas y en particular los grupos de bomba centrífuga, que comprenden una bomba, un motor, una electrónica de control y, en caso necesario, una válvula de regulación, desempeñan un papel importante en las plantas de producción. Generalmente, las bombas centrífugas se accionan por motores eléctricos regulados o no regulados.

20 Si los piratas informáticos atacan las plantas industriales mediante ciberataques, a menudo se interrumpe directamente el suministro de energía. El resultado es un paro de la producción. Para los ataques que tienen un efecto más diferenciado que una interrupción general, se requiere un enfoque más complejo. Si se trata de procesos concretos, se requiere un conocimiento preciso de su estructura y regulación. Esto hace más difícil un ataque a procesos concretos. Sin embargo, todos los procesos con fluidos presentan dispositivos conductores de fluidos de diseños más o menos estandarizados, que en general son más identificables y pueden sufrir ataques de manera más estructurada que los procesos completos.

25 Por ejemplo, mediante un ciberataque puede manipularse la velocidad de giro de la bomba centrífuga.

A través de esta manipulación, la bomba centrífuga puede llevarse a un grado de eficiencia desfavorable, que provoca altos costes de funcionamiento adicionales. También es concebible la destrucción parcial o total del accionamiento de la bomba centrífuga o de la propia bomba centrífuga o de otras partes de la planta.

30 Las bombas se diseñan y configuran con precisión para su uso específico en una planta. Algunas bombas son incluso construcciones a medida, por lo que tras un daño pueden pasar varias semanas o meses hasta que se disponga de piezas de repuesto o una bomba de sustitución. En el peor de los casos, la planta se paraliza hasta entonces. Por tanto, estos ataques a los dispositivos conductores de fluidos pueden dar lugar a grandes pérdidas de producción.

35 En el peor de los casos, este tipo de manipulaciones pueden provocar incluso explosiones. En el caso de una planta química, las consecuencias serían fatales. En el caso de las plantas con transporte de petróleo o gas, puede haber consecuencias de gran alcance para el medio ambiente.

40 En las bombas centrífugas, el ajuste controlado de la velocidad de giro se denomina regulación de la velocidad de giro. Esta regulación se utiliza para adaptar la velocidad de giro de la bomba de manera eficiente a los valores requeridos para el funcionamiento (datos de capacidad). La regulación de la velocidad de giro por medio de un convertidor de frecuencia es el método más eficaz para adaptar la capacidad de bombeo a los requisitos de caudal variable.

45 Las bombas de velocidad de giro regulada sólo consumen la cantidad de energía que necesitan para una tarea específica. En comparación con otros métodos de regulación, la regulación de la velocidad de giro por la frecuencia ofrece la mayor eficiencia del sistema y así el uso más eficiente de energía para un fin determinado.

50 Las bombas de velocidad de giro regulada sustituyen el proceso habitual de una bomba de velocidad de giro fija para el punto de funcionamiento máximo, cuyo exceso de capacidad se regula mediante una válvula. Esta válvula de regulación sigue estando presente para pequeños cambios y para la regulación del proceso, aunque no sea necesario debido a la regulación de la velocidad de giro de la bomba.

55 La regulación de la velocidad de giro de una bomba centrífuga se produce con el convertidor de frecuencia descrito mediante la variación de la frecuencia y tensión para el motor asíncrono trifásico utilizado, por ejemplo. Este método ofrece un beneficio óptimo con relativamente poco esfuerzo y alta eficiencia. El convertidor de frecuencia convierte la tensión y la frecuencia de la red eléctrica según unos patrones predeterminados para que el motor pueda funcionar a diferentes velocidades de giro. En este tipo de regulación de frecuencia pueden aparecer los siguientes problemas:

- ruidos en el motor, que a veces se transmiten al sistema como ruidos de interferencia,
- picos de alta tensión en la salida del convertidor de frecuencia hacia el motor.

65 Para medir, controlar y regular las secuencias, por ejemplo para automatizar los procesos y monitorizar grandes sistemas, en muchos ámbitos de la industria se emplean los denominados *industrial control systems* (ICS; español:

sistemas de control industrial, sistemas de automatización). Estos se utilizan a menudo en la industria de la producción. A través de este tipo de sistemas puede influirse, por ejemplo, en la velocidad de giro de una bomba o la posición de una válvula que regula el flujo.

- 5 En el pasado, los SCI estaban físicamente desvinculados de otros sistemas y redes TI y, así, protegidos de las influencias externas. Por tanto, su seguridad TI era de importancia secundaria.

Con la llegada de los sistemas TI del entorno de oficina y el aumento de la conexión en red de los SCI, estos sistemas están ahora expuestos a amenazas similares a las de los sistemas de la TI corporativa clásica.

- 10 En función del objetivo de los atacantes, su enfoque es diferente. En el caso de los sistemas que son directamente accesibles a través de Internet, se lanzan ataques dirigidos al sistema. Esto significa que se explotan directamente las vulnerabilidades del sistema atacado. Estos pueden afectar al sistema operativo o a las aplicaciones del servidor.

- 15 En muchos de los ataques que se han dado a conocer en los últimos años, los denominados ataques de *spear phishing* sirven como punto de entrada a la empresa. De este modo, se dirige una especie de “cabeza de puente” a un ordenador de la empresa. Desde esta cabeza de puente, se explora la red y se identifican otros sistemas. Una vez que los atacantes han llegado al sistema objetivo real, sacan la información que buscan de allí y llevan a cabo la manipulación. Una vez que el atacante ha alcanzado su objetivo, intenta eliminar sus huellas y no ser detectado.

- 20 Otros ataques se dirigen a sistemas cerrados propagándose a través de memorias de datos móviles que se conectan por descuido a un sistema cerrado. Al leer la memoria de datos móvil, la rutina se instala.

- 25 En el documento EP 3 242 033 A1 se describe un procedimiento para hacer funcionar un grupo motobomba controlado electrónicamente, en el que se registran y evalúan los datos de funcionamiento.

En el documento US 2016/0330225 A1 se describe un procedimiento para detectar anomalías en un sistema de control industrial.

- 30 En el documento WO 2017/090045 A1 se describe un sistema y un procedimiento para detectar un ciberataque en plantas gestionadas por SCADA/SCI.

- 35 En el documento EP 2 279 465 B1 se describe un procedimiento implementado por ordenador para la gestión de la ciberseguridad para un sistema de control industrial. A este respecto, se proporciona un módulo de programa centralizado gestor de seguridad del sistema. Éste puede introducirse mediante un dispositivo de procesamiento. El módulo de programa centralizado gestor de seguridad del sistema está integrado en una interfaz de usuario integrada de mando y control en una unidad de monitorización, control y adquisición de datos.

- 40 En el documento EP 2 500 579 A1 se describe un procedimiento para monitorizar una bomba centrífuga accionada por un motor eléctrico. Se explica que el consumo de energía y la corriente de carga del motor eléctrico son decisivos para la formación del par. Dado que los valores del consumo de energía o de la corriente de carga suelen estar disponibles de todos modos en los sistemas de control del motor, no se necesitan sensores adicionales para monitorizar la bomba centrífuga.

- 45 En el documento EP 2 433 010 B1 se describe un procedimiento y un dispositivo para determinar el punto de funcionamiento de una máquina de trabajo. A este respecto, una potencia absorbida por la máquina de trabajo o su caudal caracterizan un punto de funcionamiento. En el procedimiento se registran las magnitudes medidas dependientes del punto de funcionamiento de la máquina de trabajo mediante sensores. Los valores medidos se almacenan y evalúan durante el funcionamiento.

- 50 El objetivo de la invención es proporcionar un procedimiento y un dispositivo mediante los cuales puedan evitarse de manera eficaz los ciberataques a los grupos motobomba descritos anteriormente, en particular los grupos de bomba centrífuga, que comprenden un dispositivo transportador de fluidos, en particular una bomba centrífuga, un motor, una electrónica de control y, en caso necesario, una válvula de regulación. A este respecto, se protegerán de manera fiable los componentes del grupo motobomba en sí mismos así como los componentes utilizados en la planta, de modo que se evite un fallo de la planta. El procedimiento o el dispositivo se implementarán en la planta de manera sencilla, de modo que la instalación o el reequipamiento se asocie con los menores costes posibles para el fabricante y el operador.

- 60 Este objetivo se alcanza según la invención mediante un procedimiento para la protección de un grupo motobomba en el caso de ciberataques con las características de la reivindicación 1 y una unidad para realizar el procedimiento con las características de la reivindicación 12. Por las reivindicaciones dependientes, la descripción y los dibujos se deducirán variantes preferidas.

- 65 Por consiguiente, por un lado, se propone un procedimiento para la protección de un grupo motobomba que comprende un dispositivo transportador de fluidos de velocidad de giro regulada, en particular una bomba centrífuga,

un accionamiento y un control, en el caso de ciberataques. Según la invención, en primer lugar, se registra al menos una primera señal, que se refiere a la velocidad de giro y/o la regulación de la velocidad de giro del dispositivo transportador de fluidos. El registro de la primera señal también puede realizarse opcionalmente con ayuda de sensores.

5 La al menos una primera señal se transmite a una unidad o se registra por una unidad y aquí se evalúa. En la unidad, en el contexto de una evaluación, se comparan al menos una magnitud teórica y al menos una magnitud real derivada de la primera señal. Si se producen desviaciones significativas o si se superan o no se alcanza unos valores límite predeterminados, la unidad puede utilizar la evaluación para determinar si se ha producido un ciberataque en el grupo motobomba, por ejemplo en el accionamiento del dispositivo transportador de fluidos o en otro componente unido al mismo.

15 En caso de que, durante esta evaluación, la unidad determine un funcionamiento irregular del grupo motobomba inducido deliberadamente, en particular del accionamiento, del control y/o del dispositivo transportador de fluidos, reacciona emitiendo al menos una segunda señal y así pone el grupo motobomba en un estado de seguridad, mediante el cual se evitan eficazmente los ciberataques actuales y/o futuros. Al mismo tiempo, en respuesta a la al menos una segunda señal, el dispositivo transportador de fluidos se transfiere a un funcionamiento según las normas mediante el ajuste correspondiente de los componentes del dispositivo transportador de fluidos y/o del control y/o del accionamiento.

20 La unidad analiza preferiblemente señales, que recibe el dispositivo transportador de fluidos de velocidad de giro regulada o el control. Los siguientes fenómenos pueden indicar en particular un ciberataque:

- aproximación sistemática a los límites de velocidad de giro,
- 25 - ciclos rápidos de encendido o apagado,
- rampas rápidas con las que se aumenta o disminuye la velocidad de giro,
- excitación de vibraciones,
- anomalías en la activación, en comparación con el comportamiento habitual.

30 Tras un análisis de los datos de entrada correspondientes la unidad envía señales a los componentes del grupo motobomba para establecer un estado de seguridad protegido contra ciberataques. A este respecto, el procedimiento según la invención es adecuado para evitar ciberataques en una red central, así como ciberataques en componentes individuales del grupo motobomba.

35 Al control del grupo motobomba según la invención pertenecen además de una electrónica de control también al menos un componente de regulación, por ejemplo una válvula de regulación.

El término ciberataque se refiere en este caso a cualquier imposición intencionada de una operación irregular desde el exterior.

40 En una variante particularmente ventajosa de la invención la unidad presenta un módulo de monitorización. El módulo de monitorización puede disponer de una unidad de evaluación. La unidad de evaluación puede estar unida a su vez a una memoria. El módulo de monitorización comprende además preferiblemente una unidad de entrada o salida.

45 En una variante ventajosa de la invención el módulo de monitorización está unido a un módulo de motor. El módulo de monitorización y el módulo de motor pueden estar descentralizados y completamente separados del sistema de control de procesos o de una red o en una variante alternativa también pueden formar parte de un sistema de control de procesos o de una red. A este respecto, resulta fundamental que no haya ningún tipo de conexión en red, posiblemente incluso una separación estricta, de modo que el módulo de monitorización pueda monitorizar el grupo motobomba de una manera casi totalmente independiente, dado el caso, que pueda iniciar un estado de seguridad y pueda proporcionar una alarma correspondiente.

50 Preferiblemente un aparato de control de motor está unido a un módulo de motor, la unidad de evaluación del módulo de monitorización y el accionamiento, estando configurado el accionamiento preferiblemente como motor eléctrico.

60 Para proteger el grupo motobomba o toda la planta, una unidad de evaluación, control o regulación varía los parámetros de funcionamiento en el grupo motobomba de tal modo que el accionamiento del dispositivo transportador de fluidos entre en un estado estable y quede protegido de manera eficaz.

Opcionalmente se aplica un procedimiento iterativo, en el que se repiten etapas individuales o secuencias de etapas o todo el procedimiento una o varias veces.

65 Mediante el análisis de los parámetros de funcionamiento se detecta un posible ciberataque. Para ello se comparan los valores medidos con una serie de patrones de estado de funcionamiento almacenados en el aparato de control

de motor. En caso de detectar en el grupo motobomba un estado de funcionamiento no almacenado, automáticamente se iniciará un estado de emergencia. Entonces, preferiblemente, el accionamiento o el dispositivo transportador de fluidos o todo el grupo motobomba se desacopla de la red, a través de la que se ha producido el ciberataque, de modo que ya no sea posible que se produzca otro ciberataque. De este modo puede evitarse también un mal uso por errores accidentales de funcionamiento.

En una forma de realización está previsto que el accionamiento sea un motor eléctrico y que la regulación de la velocidad de giro del dispositivo transportador de fluidos se produzca por medio de un convertidor de frecuencia unido al accionamiento. Ventajosamente la al menos una primera señal se refiere en este caso a un estado o parámetro de funcionamiento del convertidor de frecuencia.

En una variante de la invención, en el caso de la unidad se trata de un dispositivo de control y/o regulación descentralizada. La unidad puede estar colocada directamente en o dentro del dispositivo transportador de fluidos, el control o el accionamiento. Mediante esta unidad descentralizada es posible una protección contra ciberataques incluso cuando todo el sistema de control de procesos o toda la red ya se han infectado por el ciberataque. La unidad descentralizada independiente puede registrar estados de funcionamiento desfavorables del accionamiento o del dispositivo transportador de fluidos y así detectar un ciberataque. Además, esta unidad descentralizada puede desacoplar de la red o del sistema de control de procesos el accionamiento, el dispositivo transportador de fluidos o uno o varios otros componentes del grupo motobomba hasta que se haya descartado el ciberataque.

A este respecto, en una variante preferida de la invención la unidad está configurada de tal modo que en la estructura de mando es dominante con respecto al sistema de control de procesos o la red, a la que está unido el grupo motobomba o determinados componentes del mismo. Si la unidad detecta un ciberataque, entonces desacopla completamente los componentes correspondientes del grupo motobomba, por ejemplo el accionamiento o partes del control, del sistema de control de procesos o de la red y así protege el grupo motobomba de los ataques actuales y de otros ataques.

Además de establecer un estado de seguridad, adicional o alternativamente la unidad puede iniciar alertas para que el operador sea consciente del ciberataque detectado.

En una variante de la invención la unidad presenta una memoria de datos. La memoria de datos sirve para registrar y almacenar datos tecnológicos del accionamiento y/o del dispositivo transportador de fluidos y/o del control y/o de componentes adicionales del grupo motobomba.

Preferiblemente la unidad presenta al menos una conexión para un sensor. A este respecto, en particular para detectar ciberataques son adecuados los sensores de vibración, presión, flujo o temperatura.

Para alcanzar una conexión o desconexión rápida del accionamiento y así evitar el ciberataque, según la invención se emplea una unidad de almacenamiento de energía que, por ejemplo, puede estar realizada como combinación de condensador o batería.

Además deben evitarse las excitaciones por vibración en el dispositivo transportador de fluidos o el accionamiento. Debido a los cambios de carga provocados las interacciones, por ejemplo, entre el impulsor y la rueda guía del grupo motobomba (en particular en una configuración como grupo de bomba centrífuga), aunque también entre otros componentes, pueden dar lugar a vibraciones de presión que dentro del dispositivo transportador de fluidos o de toda la planta pueden experimentar una resonancia. Con una excitación específica de estas frecuencias de resonancia pueden obtenerse amplitudes de vibración, que pueden producir un daño o incluso una destrucción del dispositivo transportador de fluidos o de toda la planta, en la que está dispuesto el grupo motobomba.

Estos estados ya se conocen en los aparatos de control de los grupos de bomba centrífuga, ya que el objetivo al poner en marcha y apagar las plantas es precisamente superar estos estados de funcionamiento lo más rápido posible para no causar ningún daño. Por tanto, existe la posibilidad de utilizar los datos ya conocidos de la planta y evitar un daño específico en el contexto de un ciberataque o de un error humano.

En una variante de la invención se emplea un sistema de alimentación ininterrumpida (SAI), en inglés *Uninterruptible Power Supply* (UPS). De este modo, en caso de ciberataques, puede garantizarse el suministro de energía del accionamiento o de otras partes del grupo motobomba.

Otra característica fundamental de un SAI es el tiempo de reacción máximo que depende de la capacidad de los acumuladores. En función de las necesidades, puede ascender a unos pocos segundos o varias horas. Si hay una gran necesidad de energía y tiempo de reacción, también se emplean grupos electrógenos para recargar los acumuladores.

La presente invención se refiere además a una unidad para realizar el procedimiento según la invención, que está configurada para la protección de un grupo motobomba según el preámbulo de la reivindicación 1 en el caso de

ciberataques. A este respecto evidentemente se obtienen las mismas ventajas y propiedades que en el procedimiento según la invención, por lo que se prescinde aquí de una descripción repetitiva.

Preferiblemente la unidad está conectada a una red informática y está configurada para interrumpir automáticamente la conexión a la red informática cuando, mediante la evaluación de la al menos una primera señal, se determina un funcionamiento irregular del grupo motobomba provocado deliberadamente.

Según una forma de realización está previsto que la unidad presente un módulo de procesamiento de señales para procesar la al menos una primera señal, un módulo de evaluación para evaluar la al menos una primera señal, una memoria con datos del dispositivo transportador de fluidos y/o del accionamiento y/o del control y preferiblemente una unidad de entrada/salida.

Ventajosamente la unidad está configurada además para llevar a cabo automáticamente una activación/regulación de los componentes de grupo motobomba cuando, mediante la evaluación de la al menos una primera señal, se determina un funcionamiento irregular del grupo motobomba provocado deliberadamente, para transferir el grupo motobomba a un funcionamiento según las normas y un estado protegido contra los ciberataques actuales y/o contra otros ciberataques.

A partir de la descripción de ejemplos de realización mediante dibujos y a partir de los propios dibujos se deducirán otras características y ventajas de la invención. A este respecto muestran:

la figura 1: una disposición de bomba centrífuga, y

la figura 2: un diagrama de bloques de una unidad para defenderse de un ciberataque.

La figura 1 muestra una disposición 1 con un dispositivo transportador de fluidos 2 realizado como bomba centrífuga, que a través de un árbol 3 está unido a un accionamiento 4. En el ejemplo de realización el accionamiento 4 está realizado como motor asíncrono, que acciona la bomba centrífuga 2. Un alimentador de red 5 alimenta el accionamiento 4. En una tubuladura de presión 6 de la bomba centrífuga 2 está dispuesto un sensor 7 para medir la presión en el lado de presión o la presión final de la bomba centrífuga 2. El sensor 7 está conectado a una unidad 9 a través de una línea 8.

La unidad 9 está conectada además al accionamiento 4 a través de una línea 22. La unidad 9 evalúa las señales del accionamiento 4 y/o del sensor 7 y así puede analizar estados de funcionamiento críticos que indiquen un ciberataque contra el accionamiento 4. Para ello, la unidad 9 utiliza el procedimiento según la invención.

Preferiblemente, para realizar el procedimiento según la invención se recurre a características del accionamiento 4, como por ejemplo la potencia nominal. A partir de estos parámetros también pueden derivarse o calcularse otros parámetros. Para registrar las señales de los sensores 7 la unidad 9 tiene unas conexiones 10 adecuadas. En el ejemplo de realización las conexiones 10 están realizadas como entradas de señal.

En el ejemplo de realización la unidad 9 tiene un módulo de procesamiento de señales 11. Por ejemplo el módulo de procesamiento de señales 11 también puede determinar una frecuencia de sonido rotacional con una precisión relativamente alta.

El procedimiento que tiene lugar en la unidad 9 se controla y coordina por un módulo informático 12. Además la unidad 9 presenta preferiblemente un elemento de visualización y mando 13.

En la disposición puede estar prevista una conexión de sensor de presión adicional, no representada en este caso, que por ejemplo sirve para registrar la presión de succión de bomba. Además, la disposición puede presentar entradas de señal adicionales, no representadas en este caso, y/o una interfaz de bus en serie o para la entrada o salida de parámetros.

La figura 2 representa un diagrama de bloques y muestra una unidad 9 para el control y/o la regulación de una bomba centrífuga 2. En la representación según la figura 2 la unidad 9 dispone de un módulo de evaluación 14, una memoria 15 conectada al módulo de evaluación 14 y una unidad de entrada/salida 16 conectada también al módulo de evaluación 14.

La unidad 9 está conectada a un módulo de motor 17. La unidad 9 y el módulo de motor 17 pueden formar parte de un sistema de control de procesos 18, aunque no es obligatorio. Un aparato de control de motor 19 está conectado al módulo de motor 17, la unidad 9 de la bomba centrífuga 2 y el accionamiento 4. La bomba centrífuga 2 recibe un medio líquido a través de una línea de alimentación 20 y bombea el medio hacia fuera a través de una línea de descarga 21. El tráfico de datos entre dichos componentes se indica mediante flechas.

Lista de números de referencia:

- 1 disposición
- 2 dispositivo transportador de fluidos (bomba centrífuga)
- 5 3 árbol
- 4 accionamiento
- 5 alimentador de red
- 6 tubuladura de presión
- 7 sensor
- 10 8 línea
- 9 unidad
- 10 conexión
- 11 módulo de procesamiento de señales
- 12 módulo informático
- 15 13 elemento de mando
- 14 módulo de evaluación
- 15 memoria
- 16 unidad de entrada/salida
- 17 módulo de motor
- 20 18 sistema de control de procesos
- 19 aparato de control de motor
- 20 línea de alimentación
- 21 línea de descarga

REIVINDICACIONES

1. Procedimiento para la protección de un grupo motobomba que comprende un dispositivo transportador de fluidos (2) de velocidad de giro regulada, en particular una bomba centrífuga de velocidad de giro regulada, un accionamiento y un control, en el caso de ciberataques con las etapas siguientes:
 - (i) registrar al menos una primera señal que se refiere a la velocidad de giro y/o a la regulación de la velocidad de giro del dispositivo transportador de fluidos (2), preferiblemente por medio de al menos un sensor,
 - (ii) evaluar la primera señal por medio de una unidad (9), produciéndose con la evaluación una comparación de al menos una magnitud teórica y al menos una magnitud real derivada de la primera señal,
 - (iii) emitir al menos una segunda señal mediante la unidad (9), en caso de que la unidad (9), debido a la evaluación de la primera señal, determine un funcionamiento irregular del grupo motobomba provocado deliberadamente,
 - (iv) ajustar los componentes del dispositivo transportador de fluidos (2) y/o del control y/o del accionamiento para establecer un funcionamiento según las normas del dispositivo transportador de fluidos (2), caracterizado por que en respuesta a la segunda señal se establece un estado del grupo motobomba protegido contra el ciberataque actual y/o contra otros ciberataques, comprendiendo la etapa (iv) la activación de un dispositivo de almacenamiento de energía para mantener el suministro de energía del grupo motobomba durante un ciberataque.
2. Procedimiento según la reivindicación 1, caracterizado por que la unidad (9) es un dispositivo local de control y/o regulación, que preferiblemente está dispuesto en o dentro del dispositivo transportador de fluidos (2) y más preferiblemente está conectado o puede conectarse a una red informática.
3. Procedimiento según la reivindicación 1 o 2, caracterizado por que la regulación de la velocidad de giro del dispositivo transportador de fluidos (2) se produce por medio de un convertidor de frecuencia conectado al accionamiento, siendo el accionamiento un motor eléctrico.
4. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la unidad (9) registra los ciclos para una conmutación del dispositivo transportador de fluidos (2), límites de velocidad de giro, la pendiente de una variación de velocidad de giro, vibraciones y/o anomalías con respecto a un comportamiento almacenado y/o aprendido del dispositivo transportador de fluidos (2).
5. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la unidad (9) presenta una memoria de datos para los datos del dispositivo transportador de fluidos (2) y/o del accionamiento (4) y/o del control.
6. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la unidad (9) determina un funcionamiento irregular del grupo motobomba provocado deliberadamente, en caso de que la evaluación de la primera señal detecte una anomalía leve y/o de acción permanente y/o de ocurrencia regular y/o intensa a corto plazo y/o creciente y/o de ocurrencia estructural que no se produce durante el funcionamiento normal del grupo motobomba.
7. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el al menos un sensor es un sensor de radiación y/o acústico y/o de vibración y/o de presión y/o de flujo y/o de velocidad de giro y/o de temperatura.
8. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la etapa (iv) comprende desacoplar los componentes del grupo motobomba, en particular la unidad (9), de una red informática y/o el funcionamiento autárquico del grupo motobomba.
9. Unidad (9), configurada para realizar un procedimiento según una de las reivindicaciones 1 a 8, que está configurada para la protección de un grupo motobomba con un dispositivo transportador de fluidos (2) de velocidad de giro regulada, un accionamiento y un control, estando conectada la unidad (9) preferiblemente a una red informática y estando configurada para interrumpir automáticamente la conexión a la red informática, siempre que la unidad (9) esté conectada a una red informática, en caso de determinar, mediante la evaluación de la al menos una primera señal, un funcionamiento irregular del grupo motobomba provocado deliberadamente.
10. Unidad (9) según la reivindicación 9, caracterizada por que presenta un módulo de procesamiento de señales (11) para procesar la al menos una primera señal, un módulo de evaluación (14) para evaluar la al menos una primera señal, una memoria (15) con datos del dispositivo transportador de fluidos (2) y/o del accionamiento y/o del control y preferiblemente una unidad de entrada/salida (16).

Fig. 1

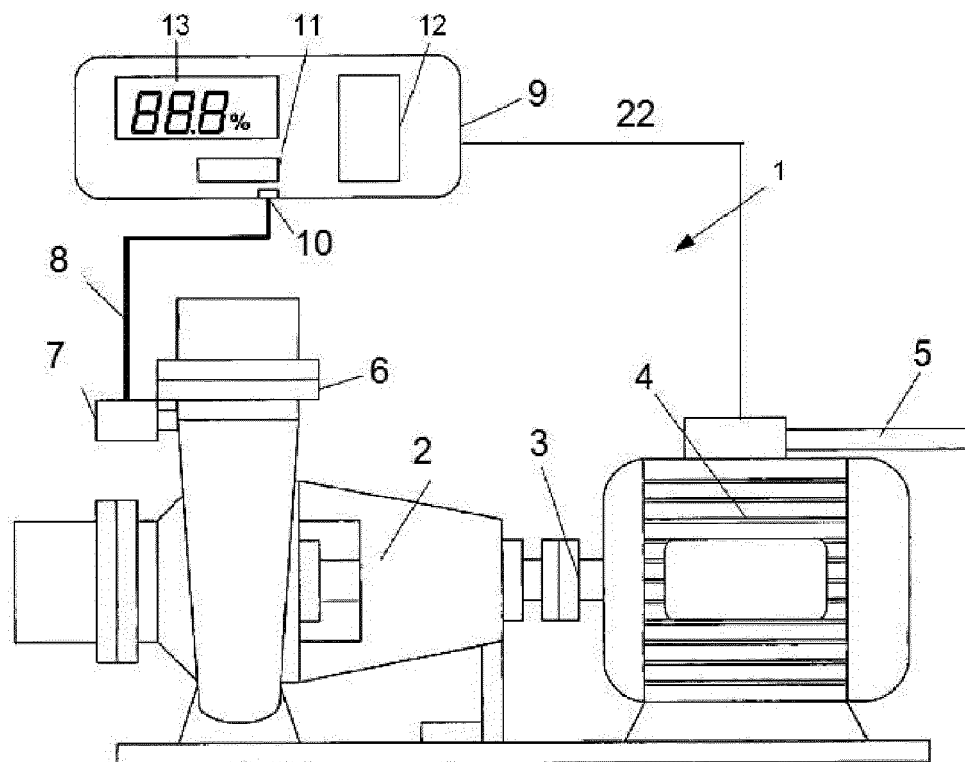


Fig. 2

