



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS  
ESPAÑA



⑪ Número de publicación: **2 236 942**

⑯ Int. Cl.:  
**G05B 23/02**  
(2006.01)

⑫

## TRADUCCIÓN DE PATENTE EUROPEA MODIFICADA

T5

- ⑯ Número de solicitud europea: **98947574 .4**  
⑯ Fecha de presentación: **07.10.1998**  
⑯ Número de publicación de la solicitud: **1027635**  
⑯ Fecha de publicación de la solicitud: **16.08.2000**

⑭

Título: **Método y dispositivo para verificar la capacidad de funcionamiento de un dispositivo de seguridad**

⑯ Prioridad:  
**17.10.1997 FI 973990**

⑬ Titular/es:  
**METSO AUTOMATION OY  
TULPPATIE 1  
00880 HELSINKI, FI**

⑯ Fecha de publicación de la mención y de la traducción de patente europea: **16.07.2005**

⑭ Inventor/es:  
**WINCHCOMB, John y  
HÖGSTRÖM, Karl-Kristian**

⑯ Fecha de la publicación de la mención de la patente europea modificada BOPI: **30.03.2012**

⑯ Fecha de publicación de la traducción de patente europea modificada: **30.03.2012**

⑭ Agente/Representante:  
**Molero Moraleda, Felipe**

## DESCRIPCIÓN

Método y dispositivo para verificar la capacidad de funcionamiento de un dispositivo de seguridad.

### Campo de la invención

5 La invención se refiere al mantenimiento de dispositivos de seguridad. Particularmente, la invención se refiere a la verificación del comportamiento correcto de dispositivos de seguridad controlados por un accionador, que comprenden piezas móviles, especialmente las denominadas válvulas de interrupción automática de emergencia y sus dispositivos de control, de tal manera que no se degrada la continuidad de producción ni la condición en espera de los dispositivos.

### Antecedentes de la invención

10 En la industria, particularmente en la industria del proceso petroquímico, se utilizan sistemas en los que el equipo de proceso, que tiene posibilidad de ocasionar riesgos al fallar, está provisto de válvulas y otros medios mecánicos diseñados para llevar al proceso rápidamente a una condición segura si se exceden los límites del parámetro de proceso preestablecidos. Por ejemplo, tal sistema por lo general incluye válvulas con accionadores de acción única, cuya apertura o cierre libera una sobrepresión acumulada, desvía una peligrosa corriente de proceso a un depósito de 15 retención, o similar. En lo sucesivo, tales válvulas se denominan válvulas de interrupción automática (siendo válvulas de emergencia que tienen una función de apertura o cierre). Estas válvulas normalmente mantienen siempre la misma posición, como otros dispositivos de seguridad mecánicos correspondientes, y en consecuencia tienen riesgo de quedar atascados si las situaciones que fuerzan una interrupción no son, como se espera en este caso, muy frecuentes. La seguridad general de las válvulas de interrupción automática no se considera satisfactoria cuando se usan el equipo 20 y los métodos de la técnica anterior. La mayor desventaja en los sistemas actuales consiste en que un fallo existente - por ejemplo, que un componente mecánico se quede atascado - no se observa necesariamente cuando el sistema se encuentra en una condición en espera, y en una situación de emergencia el sistema puede estar dañado o inoperativo.

25 Para verificar el funcionamiento apropiado, es habitual probar, por ejemplo, las válvulas de interrupción automática de un modo que simule una situación de emergencia real. Esta práctica puede de hecho ocasionar enormes riesgos, puesto que la capacidad de funcionamiento del sistema de válvula de interrupción automática se bloquea temporalmente y, si el dispositivo no se activa apropiadamente, la situación puede permanecer así.

30 Un método para comprobar una válvula de interrupción automática consiste en limitar mecánicamente su recorrido, para evitar así que tenga cualquier efecto significativo sobre el proceso, y verificar la movilidad de la válvula dentro de ciertos límites. Este procedimiento requiere el uso de, por ejemplo, una llave tangible, y evitar la activación del sistema de emergencia durante el procedimiento de comprobación, al menos en lo que respecta a la unidad pertinente.

35 La prueba se realiza a intervalos preestablecidos, por ejemplo dos veces al año, pero la prueba sólo demuestra que los dispositivos son capaces de funcionar en el momento de la prueba. Un fallo se puede desarrollar brevemente después de la prueba, y persistir hasta la siguiente prueba. Esta forma de comprobación no es un modo fiable de verificar la capacidad de funcionamiento del sistema.

40 El diagnóstico de la válvula, que usa el detector actual y la tecnología digital, es un campo en rápido desarrollo. Por ejemplo, en la solicitud de patente finlandesa 96 2406 y en la solicitud de patente europea 95 306546, se describen los métodos para la vigilancia de la condición de las válvulas de control, usando detectores en el accionador y medios de control de la válvula, y el análisis de señales a partir de dichos detectores en un microprocesador para analizar la capacidad de funcionamiento de la unidad de válvula como un todo.

45 Según se describe más arriba, la vigilancia de la condición de una válvula u otro dispositivo mecánico que forma parte de un sistema de seguridad comprende ciertos requisitos.

50 En la patente noruega 152314, se describen un método y un dispositivo para comprobar la función de los dispositivos de seguridad. Según dicha patente, una válvula de interrupción automática de emergencia o el relé de control de un motor eléctrico se comprueba periódicamente sin afectar al proceso al cual se adapta el sistema de seguridad. Durante, por ejemplo, el corte temporal de la señal de una válvula piloto solenoide que afecta a una válvula de interrupción automática, la válvula de interrupción automática se desplaza, por ejemplo, 10 grados, y la posición de la válvula de interrupción automática se monitoriza mediante un detector o un disyuntor. Si se observa un funcionamiento defectuoso, se activa la función de seguridad. La secuencia de comprobación se controla por un conjunto de circuitos lógicos situados fuera del campo, y puestos en marcha por medio de temporizadores y elementos lógicos estándares.

### **50 Descripción de la invención**

#### *Descripción general*

Se ha inventado un método según la reivindicación 1, el cual proporciona la verificación del funcionamiento libre de error de un dispositivo mecánico de seguridad, por ejemplo una válvula de interrupción automática, al tiempo que la condición en espera del sistema de seguridad se mantiene constantemente sin alteración. En dicho método, la

función de seguridad y la vigilancia o función de diagnóstico se combinan en tiempo real, teniendo la función de seguridad no obstante una prioridad mayor que la función de diagnóstico. En un método según la invención, un componente montado directamente en el dispositivo de seguridad para activar la función de seguridad es controlado mediante el sistema de seguridad de alto nivel de la planta que es responsable de las operaciones de seguridad, o alternativamente por una unidad lógica integrada en el dispositivo según la invención, adaptándose una unidad de diagnóstico a dicho componente de activación. Se permite a la unidad de diagnóstico realizar el diagnóstico sin perturbar las funciones del proceso siempre que el proceso esté en una condición normal. En una situación de emergencia, se evita la unidad de diagnóstico, con lo que, por ejemplo, ni un fallo o perturbación en la prueba de diagnóstico ni una comprobación de rutina en marcha pueda alterar la función de seguridad. El alcance y periodicidad del diagnóstico se puede programar en el sistema para alcanzar un nivel deseado de fiabilidad.

Según una realización de la presente invención, se proporciona un dispositivo que permite la verificación del funcionamiento sin perturbar de un dispositivo de seguridad mecánico, al tiempo que se mantiene totalmente la condición en espera del sistema de seguridad. La unidad de campo de un sistema de seguridad según la invención comprende de un microprocesador que proporciona procedimientos de diagnóstico y de autocomprobación preestablecidos. La unidad de campo incluye además una unidad de control que proporciona el control de un accionador. Mediante medios de comunicaciones apropiados dicha unidad de control se conecta, por un lado, al sistema de seguridad de nivel elevado o a la unidad lógica integrada en la unidad de campo, y, por otro lado, al suministro de energía del dispositivo de seguridad, por ejemplo un suministro de aire comprimido. El sistema de seguridad de nivel elevado o la unidad lógica integrada activa la función de seguridad directamente, evitando la función de diagnóstico.

Además de dicha unidad de campo, otro componente principal del sistema de seguridad según la presente invención consiste en una unidad de monitorización. El enlace de comunicación procedente del sistema de seguridad de nivel elevado se hace pasar a través de la unidad de monitorización. Preferiblemente, la tarea de la unidad de monitorización es monitorizar la condición de la unidad de campo en línea, y proporcionar el medio para presentar información de la condición al usuario.

## 25 *Descripción detallada*

La invención se describe más exactamente a continuación haciendo referencia a los dibujos adjuntos, en los que

- la figura 1 es una representación esquemática de un sistema para realizar el método de la presente invención;
- la figura 2 es una representación de una unidad de campo según la presente invención conectada a un accionador de válvula en una situación normal;
- la figura 3 es una representación de una unidad de campo y un accionador según la presente invención, en una situación de emergencia.

En la figura 1, (1) representa una unidad de monitorización de un sistema según la presente invención, y (2) es una unidad de campo que comprende una unidad (7) de control según la invención, una interfaz (3) de comunicación, una unidad (19) electrónica que incluye un microprocesador, y los detectores requeridos y componentes neumáticos (no mostrados). La unidad (7) de control controla un dispositivo (24) de seguridad que comprende un accionador (8) y una válvula (22). La comunicación entre la unidad (1) de monitorización y la unidad (7) de control se mantiene preferiblemente a través del enlace (5) de comunicación, según se describe más abajo. El enlace (5) de comunicación puede ser analógico o digital, o una combinación de ambos por medio de, por ejemplo, un cable pareado. Puesto que el área de campo por lo general es un área de riesgo de explosión, en este caso el sistema incluye una unidad (6) de barrera.

La unidad (2) de campo se suministra con tensión eléctrica, preferiblemente 24 V, a partir del sistema (18) de seguridad de nivel elevado encargado de las funciones de seguridad o, en caso de que el sistema de seguridad según la presente invención incluya una unidad lógica, a partir de un enlace de comunicación digital. Preferiblemente, la unidad (1) de monitorización está provista de luces indicadoras que reflejan la condición de la unidad de campo, controlada por la señal proporcionada por el enlace (5) de comunicación y las salidas (21) de relé correspondientes a dichas luces indicadoras. Por ejemplo, una luz verde puede indicar que la señal es normal y que el sistema de seguridad según la invención se encuentra en una condición en espera. A intervalos programables, el microprocesador incluido en la unidad (19) electrónica realiza el diagnóstico. De ese modo, la señal en el enlace (5) cambia, según se indica por, por ejemplo, una luz amarilla. Cuando el diagnóstico ha revelado un fallo, esto se indica correspondientemente por, por ejemplo, una luz roja. Las señales correspondientes a las luces indicadoras pueden ser enviadas a través, por ejemplo, de las salidas (21) de relé. El comportamiento de los indicadores de luz y las salidas de relé puede por ejemplo ser verificado por medio de un botón pulsador local sobre la unidad de monitorización.

Preferiblemente, la unidad (1) de monitorización está conectada a un ordenador (23) que ejecuta un programa de mantenimiento de sistema de seguridad, que permite la determinación del carácter de un fallo por análisis de los datos almacenados por el sistema de diagnóstico. La comunicación requerida por esta función se proporciona también preferiblemente por el enlace 5 de comunicación.

Además, el alojamiento de la unidad de monitorización incluye preferiblemente medios (por ejemplo, un teclado y un visualizador LED) para el control local del microprocesador incluido en la unidad (19) electrónica. La tarea de la interfaz (3) de comunicación es separar las señales, descritas más abajo, transmitidas por el enlace (5) de comunicación. Además, puede incorporar la unidad lógica integrada en la unidad de campo.

5 En la interfaz (3) de comunicación, el enlace de comunicación se divide en un enlace (10) directo a la unidad (7) de control y un enlace (25) a la unidad (19) electrónica. Además, la unidad (19) electrónica se conecta por el elemento (26) a la unidad de control.

10 Durante la operación normal, se llevan a cabo pruebas sobre la unidad (7) de control y sobre el dispositivo (24) de seguridad a intervalos definidos bajo el control del programa que reside en el microprocesador dentro de la unidad (19) electrónica. Las pruebas también se pueden llevar a cabo ad hoc, por medio del ordenador (23).

15 En una situación en la que se activa la función de emergencia, la señal se realiza directamente desde el sistema (18) de seguridad de nivel elevado, vía los enlaces (5) y (10), a la unidad (7) de control, por ejemplo de la manera descrita más abajo. Alternativamente, una unidad lógica, integrada dentro de la interfaz (3) de comunicación, puede transmitir una señal a lo largo del enlace (10) directamente a la unidad (7) de control.

20 15 En la figura 2, (7) es la válvula principal de la unidad (2) de campo. La figura representa una situación de funcionamiento normal. Puesto que la conexión (10) está viva con una tensión de control de 24 V, la válvula (11) de control neumática permanece cerrada, y la platina (14) permanece empujada a la derecha contra el muelle (15). Por este medio, la presión de aire de funcionamiento del accionador actúa libremente a través de las conexiones (12) y (13), y el cilindro (8) accionador de la válvula se presuriza, comprimiéndose el muelle (9). Se permite al microprocesador (17) dentro de la unidad (19) electrónica realizar el diagnóstico por medio de la válvula (16) de control neumático, según se describe más abajo.

25 20 La figura 3 representa una situación en la que se ha activado la función de seguridad. La tensión en la conexión (10) ha descendido a cero, y la presión se libera a través de la válvula (11). El muelle (15) empuja la platina (14) a la izquierda, la presión del accionador se libera a través de la abertura (20), y el accionador (8), por medio de la energía en el muelle (9) comprimido, lleva a la válvula de interrupción automática a su posición de seguridad, la cual puede estar abierta o cerrada. La función del microprocesador (17) no tiene influencia sobre la situación. Preferiblemente, el microprocesador se desactiva en esta situación, puesto que se le suministra con energía a partir de la misma conexión que la válvula (11) de control. Naturalmente, la unidad (19) electrónica de campo de la válvula de interrupción automática está provista normalmente de circuitos de memoria no volátiles capaces de almacenar los datos de medición que se refieren 30 a la función de seguridad, antes de que desaparezca la energía.

35 El microprocesador (17) recibe al menos los siguientes datos de entrada:

- posición de la válvula de control
- posición de la válvula de interrupción automática
- presión del cilindro del accionador
- comandos introducidos a partir de un teclado local.

40 45 El microprocesador (17) puede ser programado para llevar a cabo funciones de diagnóstico a intervalos preestablecidos, por ejemplo 15 ms - una semana. En la realización preferida descrita más abajo, estos comprenden una denominada prueba de histéresis. Antes de comenzar la prueba, el microprocesador transmite, alterando la señal de enlace (5) de comunicación, un mensaje a la unidad (1) de monitorización, que cambia para indicar que se está realizando una prueba. Despues, la presión de control se disminuye por medio de la válvula (16), durante un intervalo de tiempo previamente definido, hasta un nivel preestablecido, y de nuevo al nivel de inicio, con lo cual se observará una disminución correspondiente en la presión del accionador dentro de un retraso de tiempo definido, según se indica por los detectores (no mostrados). Según la presión disminuye y retorna a la condición inicial dentro de un intervalo de tiempo definido, se observará un cambio correspondiente en la posición de la válvula de interrupción automática dentro de un retraso de tiempo definido. Si no se alcanzan los valores objetivo, el microprocesador (17) transmite, alterando la señal en el enlace (5) de comunicación, un mensaje a la unidad (1) de monitorización, la cual cambia para indicar la alarma de fallo. Los movimientos de la válvula de interrupción automática durante el ciclo de prueba están limitados para no interferir con el proceso.

50 Además de la prueba descrita anteriormente para verificar la capacidad de funcionamiento mecánico de una válvula de interrupción automática, el diagnóstico incluye otras funciones fuera del alcance de la presente invención, por ejemplo diagnóstico interno de los componentes electrónicos y caracterización de fugas de válvula y movimiento de válvula, usando un detector acústico distinto.

Según una realización de la presente solicitud, toda comunicación entre el cuarto de control y el campo puede tener lugar a lo largo del mismo enlace (5) de comunicación. Preferiblemente, éste es un cable pareado para

a) mantener la tensión de control, por ejemplo 24 V, del sistema (18) de seguridad de nivel elevado, manteniendo simultáneamente la condición en espera de la unidad (2) de campo;

b) controlar las luces indicadoras y salidas de relé de la unidad (1) de monitorización, por medio de cambios de señal;

5 c) comunicación entre el programa de mantenimiento del sistema de seguridad en el ordenador (23) y la unidad (19) electrónica que usa, por ejemplo, el protocolo HART bien conocido por personas expertas en la técnica.

La disposición antes mencionada es preferible debido a que es conveniente la actualización del sistema dentro de las plantas existentes.

10 A diferencia del método y dispositivo descrito en el documento NO 152314, la presente invención proporciona las siguientes ventajas:

- los componentes "inteligentes" se localizan en el campo, lo cual permite la conexión de dispositivos de seguridad a un sistema de bus de campo;

- si se observa un funcionamiento defectuoso, la función de seguridad no se activa incondicionalmente, sino que es posible el mantenimiento, y la planta puede permanecer en funcionamiento;

15 - la señal en espera principal (por ejemplo, la tensión principal de 24 V en el ejemplo anterior) no se ve afectada durante la prueba, sino que siempre se mantiene el contacto directo con el sistema a cargo de las funciones de seguridad. La comprobación se realiza usando una señal dedicada y un cableado distinto.

- Es posible la puesta en marcha de pruebas autónomas individuales, así como diagnósticos detallados que comprenden diversos detectores, opcionalmente en la forma de autodiagnóstico.

20 - El cableado a la unidad de campo se mantiene en un mínimo; con frecuencia es suficiente un cable pareado existente.

La invención se describe en este documento usando un sistema instalado a un válvula, pero es obvio que la invención se puede, sin desviarse de su concepto general, instalar en otros dispositivos de seguridad que comprenden piezas mecánicas, que no controlan necesariamente flujos de fluidos sino que proporcionan una condición segura por otros medios.

## REIVINDICACIONES

1. Un método para verificar la capacidad de funcionamiento de un dispositivo de seguridad y un sistema de seguridad que controla a dicho dispositivo, en el que el dispositivo de seguridad se proporciona con una unidad de campo comprendiendo una unidad de diagnóstico, para llevar a cabo operaciones para verificar la movilidad de las piezas móviles de dicho dispositivo de seguridad y para verificar la capacidad de funcionamiento de unidades eléctricas del sistema de seguridad, la señal que mantiene la condición en espera de la función de seguridad no se ve afectada por dichas operaciones; en el que, en una situación de emergencia, se evita la unidad de diagnóstico y se activa la función de seguridad directamente mediante el sistema de seguridad de nivel elevado de la planta,  
 5 caracterizado por
- 10 - montar un componente para activar la función de seguridad directamente al dispositivo de seguridad, y adaptar una unidad de diagnóstico a dicho componente, estando controlado dicho componente directamente por el sistema de seguridad de nivel elevado,  
 - permitir el funcionamiento de funciones de diagnóstico por la unidad de diagnóstico, siempre que, si se observa un funcionamiento defectuoso, el dispositivo de seguridad no se active incondicionalmente.
- 15 2. Un método según la reivindicación 1, caracterizado porque el procedimiento para verificar la movilidad de las piezas móviles y la capacidad de funcionamiento de componentes eléctricos en el sistema de seguridad se lleva a cabo continuamente según un programa preestablecido, o según acontecimientos únicos por medio de un enlace de comunicación.
- 20 3. Dispositivo para la verificación de un dispositivo de seguridad que comprende piezas móviles, que comprende  
 - una unidad de control para activar la función de seguridad,  
 - enlaces para controlar dicha unidad de control directamente por un sistema de seguridad de nivel elevado de la planta;  
 - electrónica para llevar a cabo diagnósticos, al tiempo que se mantiene totalmente la condición en espera del sistema de seguridad;  
 25 - medios para permitir, en una situación de emergencia, que el sistema de seguridad evite la electrónica de diagnóstico,  
 caracterizado por una unidad (2) de campo montada directamente al dispositivo de seguridad, incluyendo la unidad de campo
- 30 - la unidad (7) de control para activar la función de seguridad,  
 - una unidad (19) electrónica adaptada a dicha unidad (7) de control, para llevar a cabo diagnóstico sin activar incondicionalmente el dispositivo de seguridad si se observa un funcionamiento defectuoso,  
 - una interfaz de comunicación (3),  
 - enlaces (5, 10) para controlar la unidad de control directamente por el sistema (18) de seguridad de nivel elevado.  
 35
4. Dispositivo según la reivindicación 3, caracterizado por una unidad (2) de campo dispuesta sobre el dispositivo, una unidad (1) de monitorización situada en cualquier otra parte, y un enlace (5) de comunicación entre dichas unidades, siendo transmitidas las señales desde la unidad (19) electrónica y las señales desde el sistema (18) de seguridad en dicho enlace de comunicación.
- 40 5. Dispositivo según la reivindicación 3 ó 4, caracterizado porque el dispositivo de seguridad comprende un accionador y una válvula.

Fig. 1

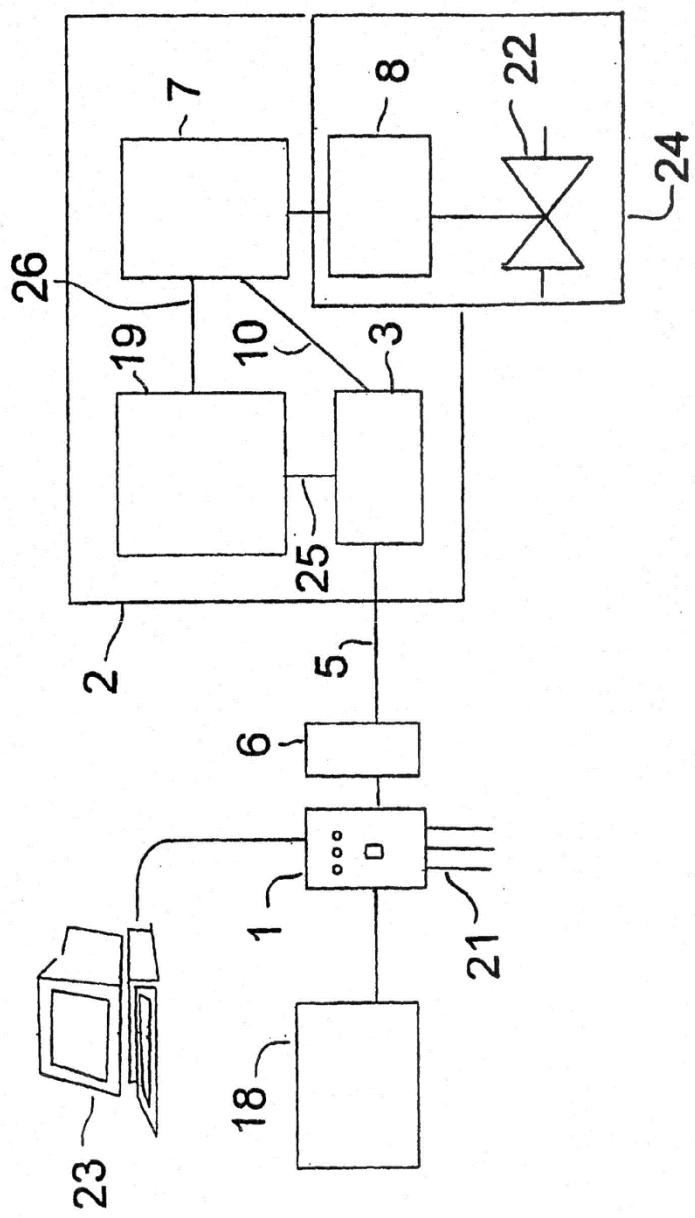


Fig. 2

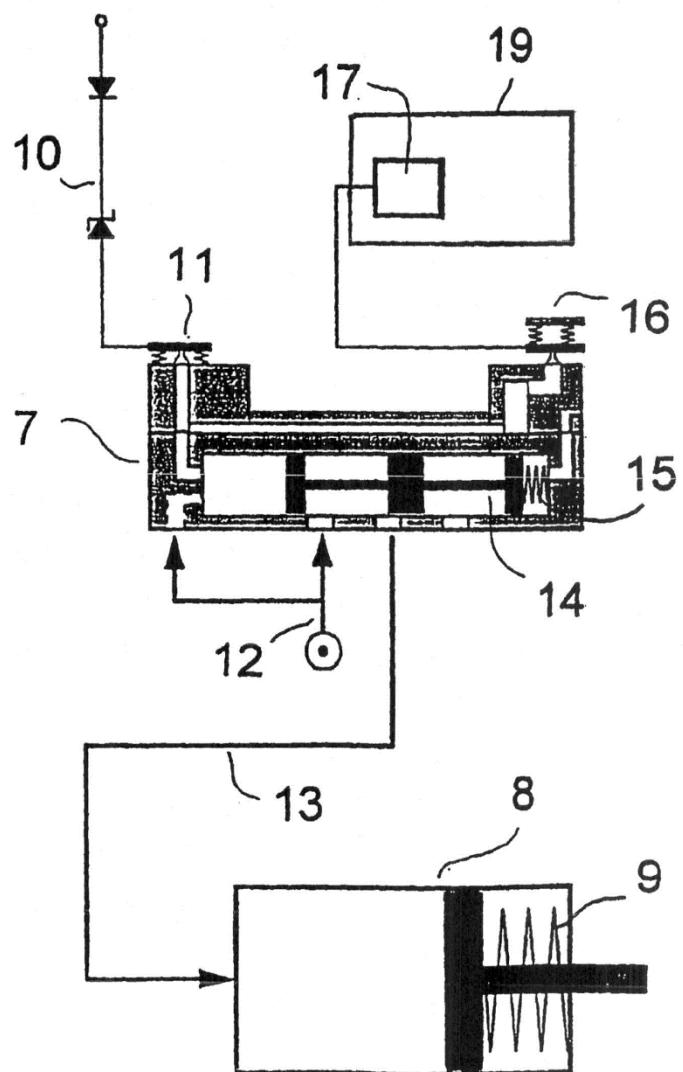


Fig. 3

