(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 936 336**

(51) Int. CI.:

G08C 17/02 (2006.01)
H04Q 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.09.2020 E 20199473 (8)**

(97) Fecha y número de publicación de la concesión europea: **16.11.2022 EP 3809388**

(54) Título: **Contador de fluido que comunica con una válvula electromecánica**

(30) Prioridad:

15.10.2019 FR 1911488

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.03.2023

(73) Titular/es:

SAGEMCOM ENERGY & TELECOM SAS (100.0%)
250 Route de l'Empereur
92500 Rueil-Malmaison, FR

(72) Inventor/es:

TEBOULLE, HENRI y
LECAPPON, JEAN-PAUL

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Contador de fluido que comunica con una válvula electromecánica

La invención se refiere al campo de los contadores de fluido y, de forma más precisa, del control de válvulas situadas en las proximidades de contadores de fluido y destinadas a cortar o restablecer de forma selectiva la alimentación de fluido.

Antecedentes de la invención

Una red de distribución de fluido comprende tuberías conectadas a través de contadores de fluido a instalaciones consumidoras de fluido.

Se conoce montar una caja de corte en un conducto en las proximidades de un contador de fluido, en general aguas arriba del contador de fluido (es decir, en el lado de la instalación y no de la red de distribución). Dicha caja de corte comprende convencionalmente una válvula electromecánica controlada para cortar o restablecer de forma selectiva la alimentación de fluido de la instalación.

En el caso de un contador de agua, la válvula electromecánica se activa por ejemplo para cortar la alimentación cuando se detecta una fuga de agua o bien cuando está prevista que una vivienda permanezca vacía durante un cierto tiempo, tras una mudanza por ejemplo.

Para evitar que intervenga un operario en cada apertura y cierre de la válvula electromecánica, es conveniente que la misma pueda ser controlada a distancia.

El control a distancia debe ser seguro, para evitar que un individuo malintencionado accione fraudulentamente la válvula electromecánica. Por otro lado, los medios de comunicación utilizados en la caja de corte para adquirir este control a distancia deben ser poco consumidores de energía eléctrica, ya que la caja de corte está alimentada por una o más baterías y debe tener una vida útil importante sin cambiar la o las baterías.

Véase también la publicación US 2014/110613 que da a conocer un contador que integra una válvula cuya apertura y cierre pueden ser controlados a distancia.

Objeto de la invención

La invención tiene por objeto transmitir de manera segura una orden de apertura o de cierre de una válvula electromecánica integrada en una caja de corte montada en las proximidades de un contador de fluido y que limita el consumo de energía eléctrica de la caja de corte.

El objeto de la invención se define por las reivindicaciones 1-15.

Resumen de la invención

Con el fin de realizar este objetivo, se propone un contador de fluido que comprende medios de comunicación dispuestos para recibir desde el exterior una orden de apertura o de cierre de una válvula electromecánica que puede estar integrada en una caja de corte montada en las proximidades del contador de fluido, medios de autentificación dispuestos para autentificar una trama de orden que integra la orden de apertura o de cierre y una primera interfaz de comunicación dispuesta para transmitir a una segunda interfaz de comunicación de la caja de corte a través de un enlace radioeléctrico la trama de orden y una energía eléctrica adaptada para alimentar eléctricamente la segunda interfaz de comunicación de la caja de corte.

Los medios de autentificación del contador de fluido según la invención permiten autentificar la trama de orden y por tanto asegurar la transmisión de la orden de apertura o de cierre de la válvula electromecánica de la caja de corte. La segunda interfaz de comunicación de la caja de corte es alimentada por la primera interfaz de comunicación del contador de fluido, de manera que la transmisión de la trama de orden no aumenta el consumo eléctrico de la caja de corte. Se observa que la transmisión de la trama de orden y el control de la válvula electromecánica no necesitan ninguna presencia local humana.

Se propone además un contador de fluido tal como el descrito anteriormente, en el que la primera interfaz de comunicación está dispuesta para escribir la trama de orden en una memoria de la caja de corte y para leer una trama de acuse de recibo en la memoria de la caja de corte.

Se propone además un contador de fluido tal como el descrito anteriormente en el cual los medios de autentificación se disponen para cifrar al menos parcialmente la trama de orden.

Se propone además un contador de fluido tal como el descrito anteriormente, en el que los medios de autentificación se disponen para utilizar un algoritmo de cifrado que tiene una clave de cifrado simétrico que se almacena en una memoria del contador de fluido y en la memoria de la caja de corte.

Se propone además un contador de fluido tal como el descrito anteriormente, en el que el algoritmo de cifrado es un algoritmo de cifrado AES que utiliza un modo de funcionamiento GCM.

Se propone además un contador de fluido tal como el descrito anteriormente, en el que la primera interfaz de comunicación está dispuesta para recibir una trama de cambio de clave que puede transmitirse por un dispositivo móvil puesto en las proximidades del contador de fluido, el contador de fluido que se dispone para descifrar la trama de cambio de clave y para reemplazar la clave de cifrado simétrico almacenada en la memoria del contador de fluido por una nueva clave de cifrado simétrico integrada en la trama de cambio de clave.

Se propone además un contador de fluido tal como el descrito anteriormente, en el que la trama de orden integra un valor actual de un contador de tramas de orden, que se incrementa en cada transmisión de trama de orden por el contador de fluido en la caja de corte.

Se propone además una caja de corte que puede montarse en las proximidades de un contador de fluido, la caja de corte que comprende:

- una válvula electromecánica;
- una memoria;
- una segunda interfaz de comunicación dispuesta para recibir a través de un enlace radioeléctrico y para almacenar en la memoria una trama de orden que integra una orden de apertura o de cierre de la válvula electromecánica, la segunda interfaz de comunicación que está además dispuesta para recibir y para ser alimentada por una energía eléctrica transmitida a través del enlace radioeléctrico;
- un componente de procesamiento dispuesto para adquirir en la memoria la trama de orden, para descifrar la trama de orden y extraer la orden de apertura o de cierre, para controlar una apertura y un cierre de la válvula electromecánica y para escribir en la memoria (23) una trama de acuse de recibo.

Se propone además una caja de corte tal como la que se acaba de describir, en la cual el componente de procesamiento se encuentra por defecto en un modo de espera, la segunda interfaz de comunicación que se dispone para producir una señal de activación del componente de procesamiento cuando la segunda interfaz de comunicación recibe la energía eléctrica.

Se propone además una caja de corte tal como la que se acaba de describir, en la cual una clave de cifrado simétrico de un algoritmo de cifrado se almacena en la memoria de la caja de corte, el componente de procesamiento que se dispone para descifrar la trama de orden utilizando la clave de cifrado simétrico.

Se propone además una caja de corte tal como la que se acaba de describir, en la que la segunda interfaz de comunicación se dispone para recibir una trama de cambio de clave que puede ser transmitida por un dispositivo móvil puesto en las proximidades del elemento de corte, el componente de procesamiento que se dispone para descifrar la trama de cambio de clave y para reemplazar la clave de cifrado simétrico almacenada en la memoria del elemento de corte por una nueva clave de cifrado simétrico integrada en la trama de cambio de clave.

Se propone también un sistema de medida que comprende un contador de fluido tal como el descrito anteriormente y una caja de corte tal como la descrita anteriormente.

Se propone además un procedimiento de transmisión de una orden de apertura o de cierre de una válvula electromecánica integrada en la caja de corte situada en las proximidades de un contador de fluido, el procedimiento de transmisión que se implementa por un componente de procesamiento del contador de fluido tal como el descrito anteriormente, y que comprende las etapas de:

- adquirir la orden de apertura y de cierre;
- autentificar una trama de orden que integra la orden de apertura o de cierre;
- hacer trasmitir por la primera interfaz de comunicación a una segunda interfaz de comunicación de la caja de corte a través del enlace radioeléctrico la trama de orden y una energía eléctrica adaptada para alimentar eléctricamente la segunda interfaz de comunicación de la caja de corte.

Se propone también un programa de ordenador que comprende instrucciones que hacen que el componente de procesamiento del contador de fluido, como el que se ha descrito, ejecute las etapas del procedimiento de transmisión anterior.

Se propone además un soporte de grabación legible por ordenador, sobre el que se graba el programa de ordenador anterior.

Se propone por otro lado un procedimiento de cambio de clave, implementado por un componente de procesamiento de un contador de fluido tal como el que se acaba de describir, una clave de cifrado simétrico que se almacena en una memoria del contador de fluido, que comprende las etapas de:

- adquirir una trama de cambio de clave transmitida por un dispositivo móvil puesto en las proximidades del contador de fluido, la trama de cambio de clave que comprende una nueva clave de cifrado simétrico y que está cifrada gracias a la clave de cifrado simétrico almacenada en la memoria del contador de fluido;
- descifrar la trama de cambio de clave;
- reemplazar la clave de cifrado simétrico almacenada en la memoria del contador de fluido por la nueva clave de cifrado simétrico.

Se propone también un programa de ordenador que comprende instrucciones que hacen que el componente de procesamiento del contador de fluido, tal como el descrito anteriormente, ejecute las etapas del procedimiento de cambio de clave que se acaba de describir.

Se propone además un soporte de grabación legible por ordenador, sobre el que se graba el programa de ordenador que se acaba de describir.

La invención se comprenderá mejor a la luz de la descripción siguiente de un modo de implementación particular no limitativo de la invención.

Breve descripción de los dibujos

Se hará referencia a los dibujos adjuntos, entre los cuales:

La figura 1 representa un sistema de información, una *gateway* LoRa, un contador de agua según la invención y una caja de corte;
La figura 2 representa una caja de corte;
La figura 3 representa intercambios de órdenes, de tramas y de mensajes entre las entidades de la figura 1;
La figura 4 representa una trama de orden de la válvula electromecánica de la caja de corte;
La figura 5 representa una trama de acuse de recibo;
La figura 6 representa una trama de cambio de clave.

Descripción detallada de la invención

Con referencia las figuras 1 y 2, un contador de fluido según la invención es en este caso un contador 1 de agua que se monta en una tubería 2 de una red de distribución de agua y que se utiliza para medir el consumo de agua de una instalación.

Una caja 2 de corte se monta en el conducto 2 en las proximidades del contador 1 de agua. La distancia L entre el contador 1 de agua y la caja 3 de corte está por ejemplo comprendida entre 1 cm y 10 cm. La caja 3 de corte comprende una válvula 4 electromecánica que se utiliza para cortar o restablecer de forma selectiva la alimentación de agua de la instalación.

Las órdenes de apertura o de cierre de la válvula 4 electromecánica se emiten por un SI (para sistema de información) 5 que transmite las órdenes de apertura o de cierre al contador 1 de agua a través de una *gateway* Lora 6 (*gateway* o pasarela; LoRa para *Long Range*). El contador 1 de agua transmite estas órdenes de apertura o de cierre a la caja 3 de corte.

Se describe ahora cada una de estas entidades.

El SI 5 comprende un servidor 8 de aplicación y un servidor 9 LNS (para *LoRa Network Server*). El servidor 9 LNS está destinado en especial a gestionar las comunicaciones con el conjunto de las *gateway* LoRa y con todos los contadores de agua a los cuales se conecta el servidor 9 LNS. El servidor 9 LNS se comunica en este caso con la *gateway* LoRa 6 a través de una red 2G, 3G o 4G.

La *gateway* LoRa 6 comprende por tanto primeros medios 10 de comunicación para comunicarse con el servidor 9 LNS a través de una red 2G, 3G o 4G y de segundos medios 11 de comunicación para comunicarse con el contador 1 de agua. Los segundos medios 11 de comunicación en este caso están adaptados para comunicarse a través de una red LoRaWAN (para *Long Range Wide Area Network*).

El contador 1 de agua comprende en primer lugar medios 14 de comunicación que también están adaptados para comunicarse a través de una red LoRaWAN. El contador 1 de agua recibe las órdenes de apertura o de cierre de la válvula 4 electromecánica gracias a estos medios 14 de comunicación.

El contador 1 de agua comprende también una primera interfaz 15 de comunicación que en este caso es una interfaz NFC maestra. La primera interfaz 15 de comunicación comprende un primer componente de procesamiento, en este caso un primer microcontrolador 16, una primera memoria 17, un emisor/receptor 18 NFC y una primera antena 19. El emisor/receptor 18 NFC comprende en este caso un amplificador, un modulador y un demodulador.

El contador 1 de agua comprende además medios de autentificación que comprenden en este caso un módulo de software programado en el primer microcontrolador 16 y una primera zona de la primera memoria 17.

La caja 3 de corte, a su vez, comprende, además de la válvula 4 electromecánica una segunda interfaz 20 de comunicación que en este caso es una interfaz NFC esclava, un segundo componente de procesamiento, en este caso un segundo microcontrolador 21 y una batería 22.

La segunda interfaz 20 de comunicación comprende una segunda memoria 23, un receptor 24 NFC y una segunda antena 25. El receptor 24 NFC comprende por ejemplo un demodulador.

El segundo microcontrolador 21 se dispone para controlar (a través de un *driver* no representado) una apertura o un cierre de la válvula 4 electromecánica. El segundo microcontrolador 21 comprende en este caso una interfaz I2C para acceder a la segunda memoria 23 de lectura y de escritura.

La batería 22 de la caja 3 de corte se utiliza para alimentar el segundo microcontrolador 21 y la válvula 4 electromecánica (así como el *driver*).

Se describe ahora, con referencia la figura 3, la manera en la que cooperan las entidades que se acaban de citar.

El servidor 8 de aplicación produce una orden de apertura o de cierre de la válvula 4 electromecánica de la caja 3 de corte y el servidor 9 LNS transmite la orden de apertura o de cierre a la *gateway* LoRa 6 utilizando una petición HHTP POST (etapa E1). La *gateway* LoRa 6 retransmite la orden de apertura o de cierre al contador 1 de agua sobre la red LoRaWAN (etapa E2). La orden de apertura o de cierre se asegura de acuerdo con un protocolo LoRa.

El contador 1 de agua adquiere la orden de apertura o de cierre y la descifra, de acuerdo de nuevo con el protocolo LoRa.

El primer microcontrolador 16 del contador 1 de agua genera una trama de orden, que integra la orden de apertura o de cierre.

Los medios de autentificación del contador 1 de agua por tanto van a autentificar la trama de orden. La autentificación consiste en cifrar al menos parcialmente la trama de orden.

Los medios de autentificación utilizan un algoritmo de cifrado que tiene una clave de cifrado simétrico (secreta) que se almacena en la primera zona de la primera memoria 17 de la primera interfaz 15 de comunicación.

El algoritmo de cifrado es un algoritmo de cifrado AES (para *Advanced Encryption Standard*) que utiliza el modo de funcionamiento GCM (para *Galois Counter Mode*). El algoritmo de cifrado permite cifrar y descifrar los datos por bloques de 128 bits. La clave de cifrado simétrico es una clave de 128 bits.

La clave de cifrado simétrico también se almacena en una primera zona de la segunda memoria 23 de la segunda interfaz 20 de comunicación de la caja 3 de corte y por tanto es conocida a la vez por la primera interfaz 15 de comunicación y la segunda interfaz 20 de comunicación. El contador 1 de agua y la caja 3 de corte se asocian a través de esta misma clave de cifrado simétrico. La asociación es por ejemplo realizada en fábrica, al final de la fabricación del contador 1 de agua y de la caja 3 de corte, por cambio de la clave de cifrado simétrico en la primera memoria 17 del contador 1 de agua en la segunda memoria 23 del elemento 3 de corte. La asociación también se puede realizar durante la instalación in situ.

El contador 1 de agua transmite entonces la trama de orden a la caja 3 de corte utilizando la tecnología NFC (etapa E3). La primera interfaz 15 de comunicación produce gracias al emisor/receptor 18 NFC y a la primera antena 19 un campo electromagnético que va a inducir una corriente en la segunda antena 25 de la segunda interfaz 20 de comunicación. El campo electromagnético permite formar un enlace radioeléctrico que permite a la primera interfaz 15 de comunicación transmitir a la segunda interfaz 20 de comunicación la trama de orden, pero también una energía eléctrica que alimenta a la segunda interfaz 20 de comunicación. La segunda interfaz 20 de comunicación por tanto no es alimentada por la batería 22 de la caja 3 de corte sino únicamente por esta energía eléctrica trasmitida a través del enlace radioeléctrico.

Se observa en este caso que de forma ventajosa, para optimizar la transmisión de energía eléctrica, la primera antena 19 y la segunda antena 25 se sitúan enfrentadas entre sí y se extienden cada una en un plano perpendicular al eje que pasa por sus centros respectivos.

La primera interfaz 15 de comunicación escribe por tanto la trama de orden en una segunda zona de la segunda memoria 23 de la segunda interfaz 20 de comunicación.

El segundo microcontrolador 21 de la caja 3 de corte se encuentra en general, por defecto, en un modo de espera. Cuando la segunda interfaz 20 de comunicación recibe la energía eléctrica trasmitida por la primera interfaz 15 de comunicación, la misma produce una señal de activación que va a despertar al segundo microcontrolador 21.

La señal de activación es una señal de interrupción aplicada a una patilla del segundo microcontrolador 21. Como variante, una señal de tipo "*memory busy*" generada por la segunda interfaz 20 de comunicación, podría también utilizarse para despertar al segundo microcontrolador 21.

El segundo microcontrolador 21 por tanto va a acceder a la trama de orden leyendo en la segunda zona de la segunda memoria 23. El segundo microcontrolador 21 descifra gracias a su conocimiento de la clave de cifrado simétrico la trama de orden, extrae de la trama de orden la orden de apertura o de cierre, y controla la válvula 4 electromecánica en función de dicha orden de apertura o de cierre.

Después, tras la apertura o el cierre de la válvula 4 electromecánica, el segundo microcontrolador 21 escribe en una tercera zona de la segunda memoria 23 de la segunda interfaz 20 de comunicación, con destino a la primera interfaz 15 de comunicación del contador 1 de agua, una trama de acuse de recibo que integra un acuse de recibo (etapa E4). Se observa que la tercera zona de la segunda memoria 23 y la segunda zona de la segunda memoria 23 son posiblemente pero no necesariamente iguales.

El segundo microcontrolador 21 autentifica la trama de acuse de recibo utilizando el algoritmo de cifrado citado anteriormente.

La primera interfaz 15 de comunicación accede a la tercera zona de la segunda memoria 23 de la segunda interfaz 20 de comunicación para intentar leer en la tercera zona de la segunda memoria 23 una trama de acuse de recibo (etapa E5). La lectura se realiza por un método de *polling*: a intervalos regulares, la primera interfaz 15 de comunicación accede al contenido de la tercera zona de la segunda memoria 23 para determinar si una trama de acuse de recibo se encuentra en la tercera zona de la segunda memoria 23.

Si la trama de acuse de recibo está presente durante el primer intento de lectura, el contador 1 de agua por sí mismo va a enviar un mensaje de acuse de recibo a la *gateway* LoRa 6 (etapa E6). La *gateway* LoRa 6 retransmite el mensaje de acuse de recibo al servidor 8 de aplicación del SI 5 a través del servidor 9 LNS (etapa E7).

Tras la transmisión de la trama de orden a la caja 3 de corte, si alguna trama de acuse de recibo no es almacenada en la tercera zona de la segunda memoria 23 (etapa E8), el primer intento de lectura falla (etapa E9). La primera interfaz 15 de comunicación efectúa por tanto un segundo intento de lectura (etapa E10). Si este falla, la primera interfaz 15 de comunicación efectúa un tercer intento de lectura (etapa E11). Cada intento de lectura está separado de la anterior una duración predeterminada, en este caso igual a 1 mn. Después de un número predeterminado de intentos de lectura, infructuosos, en este caso igual a 3, el contador 1 de agua envía un mensaje de error a la *gateway* LoRa 6 (etapa E12). La *gateway* LoRa 6 retransmite el mensaje de error al servidor 8 de aplicación del SI 5 a través del servidor 9 LNS (etapa E13).

El primer microcontrolador 16 de la primera interfaz 15 de comunicación utiliza un contador de tramas de orden cuyo valor actual está integrado en la trama de orden. El contador de tramas de orden es incrementado por el primer microcontrolador 16 en cada transmisión de trama de orden por el contador 1 de agua a la caja 3 de corte.

Este contador de tramas de orden permite evitar la "repetición" de una trama de orden, es decir evitar que una trama de orden antigua, escuchada y adquirida por un individuo malintencionado, sea utilizada para producir una orden de apertura o de cierre destinadas a controlar de forma fraudulenta la caja 3 de corte. Por tanto, cuando el segundo microcontrolador 21 de la caja de corte adquiere una trama de orden, verifica que el valor actual del contador de tramas de orden, integrado en la trama de orden, e superior estrictamente a la integrada en la trama de orden precedente.

Del mismo modo, el segundo microcontrolador 21 de la caja 3 de corte utiliza un contador de tramas de acuse de recibo que se incrementa cada vez que el segundo microcontrolador 21 produce una trama de acuse de recibo y cuyo valor actual se integra en la trama de acuse de recibo.

Es posible cambiar la clave de cifrado simétrico utilizada por el contador 1 de agua y por la caja 3 de corte. La modificación de la clave de cifrado simétrico se realiza localmente. Un operario se aproxima al contador 1 de agua y por tanto a la caja 3 de corte y utiliza un dispositivo móvil, por ejemplo un *Smartphone* que ha recuperado con anterioridad la clave de cifrado simétrico actualmente en vigor. El dispositivo móvil programa una nueva clave de cifrado simétrico a la vez en el contador 1 y en la caja 3 de corte. El dispositivo móvil envía para ello una trama de cambio de clave, por un lado, al contador 1 de agua y por otro lado, de manera independiente, a la caja 3 de corte. La nueva clave de cifrado simétrico se integra en la trama de cambio de clave. La trama de cambio de claves autentifica gracias al algoritmo de cifrado citado anteriormente, utilizando la clave de cifrado simétrico actualmente en vigor.

El primer microcontrolador 16 de la primera interfaz 15 de comunicación del contador 1 de agua adquiere la trama de cambio de clave y la almacena en una segunda zona de la primera memoria 17. El segundo microcontrolador 21 de la caja 3 de corte adquiere la trama de cambio de clave y la almacena en una cuarta zona de la segunda memoria 23.

El primer microcontrolador 16 y el segundo microcontrolador 21 utilizan por tanto la clave de cifrado simétrico actualmente en vigor y almacenada en la primera memoria 17 y en la segunda memoria 23 para descifrar la trama de cambio de clave. El primer microcontrolador 16 y el segundo microcontrolador 21 adquieren y almacenan por tanto la nueva clave de cifrado simétrico respectivamente en la primera zona de la primera memoria 17 y en la segunda zona de la segunda memoria 23.

El dispositivo móvil implementa un contador de tramas de cambio de clave cuyo valor actual está integrado en la trama de cambio de clave. El contador de tramas de cambio de clave se incrementa por el dispositivo móvil en cada transmisión de trama de cambio de clave por el dispositivo móvil al contador 1 de agua y a la caja 3 de corte. La trama de cambio de clave es autentificada gracias al algoritmo de cifrado citado anteriormente que utiliza la clave de cifrado simétrico actualmente en vigor.

Se describe ahora más en detalle la estructura de una trama de orden, de una trama de acuse de recibo y de una trama de cambio de clave.

Con referencia a la figura 4, una trama 30 de orden comprende en primer lugar un valor 31 inicial IV (para *Initial Value*) que no está cifrado y que está de acuerdo con la recomendación NIST *Special Publication* 800-38, capítulo 8.2.1.

El valor 31 inicial IV se divide en un primer campo 32 y en un segundo campo 33.

El primer campo 32 es un campo de 4 octetos que contiene un identificador del emisor del mensaje, en este caso un identificador del contador 1 de agua.

El segundo campo 33 es un campo de 8 octetos que contiene el valor actual del contador de tramas de orden. El segundo campo 33 permite más de 18 x 10^{18} órdenes sin cambio de clave de cifrado simétrico y se reinicia liza a 0 Durante cada cambio de clave de cifrado simétrico.

La trama 30 de orden comprende a continuación una *payload* 34 que es un campo funcional destinado a identificar la función de la trama: orden de apertura, orden de cierre o acuse de recibo. La *payload* 34 está cifrada por el algoritmo de cifrado AES que utiliza el modo de funcionamiento GCM y comprende 4 octetos.

La *payload* 34 comprende un octeto de orden que toma los valores siguientes:

“0”: para una orden de apertura de la válvula 4 electromecánica. Se trata por tanto de una trama de orden que viene del contador 1 de agua;
“1”: para una orden de cierre de la válvula electromecánica. Se trata por tanto de una trama de orden que viene del contador 1 de agua;
“2”: para un acuse de recibo, se trata por tanto de una trama de acuse de recibo que viene de la caja 3 de corte.

El octeto de control de la *payload* 34 de la trama 30 de orden tiene por tanto como valor “0” en el caso de una orden de apertura y como valor “1” en el caso de una orden de cierre.

La *payload* 34 comprende además 3 octetos no utilizados.

Se observa que el algoritmo de cifrado utilizado genera un suceso aleatorio de 16 octetos sobre el octeto de orden.

La trama 30 de orden comprende entonces un código 35 de autentificación de mensaje (también denominado *tag*) sobre 16 octetos generados por el algoritmo de cifrado AES que utiliza el modo de funcionamiento GCM. El código 35 de autentificación de mensaje permite autentificar la trama 30 de orden, asegurar la integridad de los datos que la misma contiene y confirmar que la trama 30 de orden proviene de un emisor esperado (en este caso del contador 1 de agua).

En referencia la figura 5, una trama 40 de acuse de recibo comprende en primer lugar un valor 41 inicial IV dividido en un primer campo 42 y en un segundo campo 43.

El primer campo 42 es un campo de 4 octetos que contiene un identificador del emisor del mensaje, en este caso un identificador de la caja 3 de corte.

El segundo campo 43 es un campo de 8 octetos que contiene el valor actual del contador de tramas de acuse de recibo. Este segundo campo 43 permite más de 18 x 10^{18} acuses de recibo sin cambio de clave de cifrado simétrico y se reinicia liza a 0 durante cada cambio de clave de cifrado simétrico.

La trama 40 de acuse de recibo comprende a continuación una *payload* 44 cifrada por el algoritmo de cifrado AES que utiliza el modo de funcionamiento GCM y comprende 4 octetos.

El octeto de orden de la *payload* 44 de la trama 40 de orden tiene por valor “2”.

La *payload* 44 comprende además 3 octetos no utilizados.

Se observa que el algoritmo de cifrado utilizado genera un suceso aleatorio de 16 octetos sobre el octeto de orden.

La trama 40 de acuse de recibo comprende entonces un código 45 de autentificación de mensaje (también denominado *tag*) sobre 16 octetos generado por el algoritmo de cifrado AES que utiliza el modo de funcionamiento GCM. El código 45 de autentificación de mensaje permite autentificar la trama 40 de acuse de recibo, asegurar la integridad de los datos que la misma contiene y confirmar que la trama 40 de acuse de recibo proviene de un emisor esperado (en este caso de la caja 3 de corte).

Con referencia la figura 6, una trama 50 de cambio de clave comprende en primer lugar un valor 51 inicial IV (para *Initial Value*) que no está cifrado y que está de acuerdo con la recomendación NIST *Special Publication* 800-38, capítulo 8.2.1.

El valor 51 inicial IV está dividido en un primer campo 52 y en un segundo campo 53.

El primer campo 52 es un campo de 4 octetos que contiene un identificador del emisor del mensaje, en este caso se elige un mismo identificador fijo para todos los aparatos móviles.

El segundo campo 53 es un campo de 8 octetos que contiene el valor actual del contador de tramas de cambio de clave. El contador se inicializa a 0 durante el primer cambio de clave realizado por el dispositivo móvil.

La trama 50 de cambio de clave comprende a continuación una *payload* 54 cifrada por el algoritmo de cifrado. La *payload* 54 está cifrada por el KMS (*Key Management System*) utilizando la clave de cifrado simétrico actualmente en vigor que está almacenada en la primera memoria 17 del contador 1 de agua y en la segunda memoria 23 de la caja 3 de corte y que es conocida por el dispositivo móvil.

La *payload* 54 comprende 17 octetos que comprenden un octeto de orden que toma el valor “3” y 16 octetos de clave (es decir 128 bits).

La trama 50 de cambio de clave comprende a continuación un código 55 de autentificación de mensaje (también denominado *tag*) sobre 16 octetos generado por el algoritmo de cifrado AES que utiliza el modo de funcionamiento GCM. El código 55 de autentificación de mensaje permite autentificar la trama 50 de cambio de clave, asegurar la integridad de los datos que la misma contiene y confirmar que la trama 50 de cambio de clave proviene de un emisor esperado (en este caso de un dispositivo móvil previsto para este uso).

Por supuesto, la invención no está limitada al modo de realización descritos sino que engloba cualquier variante que entra en el campo de la invención tal y como se define por las reivindicaciones.

Las tecnologías y los protocolos de comunicación que permiten conectar entre sí el SI, la *gateway,* el contador de fluido y la caja de corte podrían ser diferentes a los descritos en este caso.

La primera interfaz de comunicación y la segunda interfaz de comunicación no son necesariamente interfaces NFC. Se podría utilizar otro tipo de tecnología o de protocolo y por ejemplo una tecnología y un protocolo “propietarios”. Cualquier enlace radioeléctrico que permita a la vez transmitir datos (órdenes, acuses de recibo, etc.) y una energía eléctrica suficiente para alimentar una interfaz de comunicación entra en el campo de la invención.

La invención se puede implementar por supuesto con un contador que no sea un contador de agua: contador de gas, de gasolina, etc.

Se podrían utilizar otros algoritmos de cifrado y por ejemplo los algoritmos *Twofish, Serpent, Blowfish*. De forma más general, los medios de autentificación podrían ser diferentes de los descritos en este caso. Se puede utilizar cualquier medio de autentificación que permita certificar la autenticidad de una trama.

El primer componente de procesamiento y el segundo componente de procesamiento no son necesariamente microcontroladores, sino que podrían ser componentes diferentes: FPGA, ASIC, procesador, etc.

REIVINDICACIONES

1. Contador (1) de fluido que comprende medios (14) de comunicación dispuestos para recibir del exterior una orden de apertura o de cierre de una válvula (4) electromecánica integrada en una caja (3) de corte montada en las proximidades de un contador (1) de fluido, medios de autentificación dispuestos para autentificar una trama (30) de orden que integra la orden de apertura o de cierre y una primera interfaz (15) de comunicación dispuesta para transmitir a una segunda interfaz (20) de comunicación de la caja (3) de corte, a través de un enlace radioeléctrico, la trama (30) de orden y una energía eléctrica adaptada para alimentar eléctricamente la segunda interfaz (20) de comunicación de la caja (3) de corte.

2. Contador de fluido según la reivindicación 1 en el que la primera interfaz (15) de comunicación está dispuesta para escribir la trama de orden en una memoria (23) de la caja (3) de corte y para leer una trama (40) de acuse de recibo en la memoria (23) de la caja (3) de corte.

3. Contador de fluido según una de las reivindicaciones anteriores, en el que los medios de autentificación se disponen para cifrar al menos parcialmente la trama de orden.

4. Contador de fluido según la reivindicación 3, en el cual los medios de autentificación se disponen para utilizar un algoritmo de cifrado que tiene una clave de cifrado simétrico que se almacena en una memoria (17) del contador (1) de fluido y en la memoria (23) de la caja (3) de corte.

5. Contador de fluido según la reivindicación 4, en el cual el algoritmo de cifrado es un algoritmo de cifrado AES que utiliza un modo de funcionamiento GCM.

6. Contador de fluido según la reivindicación 4, en el que la primera interfaz (15) de comunicación está dispuesta para recibir una trama (50) de cambio de clave que puede transmitirse por un dispositivo móvil puesto en las proximidades del contador (1) de fluido, el contador (1) de fluido que se dispone para descifrar la trama (50) de cambio de clave y para reemplazar la clave de cifrado simétrico almacenada en la memoria (17) del contador (1) de fluido por una nueva clave de cifrado simétrico integrada en la trama (50) de cambio de clave.

7. Contador de fluido según una de las reivindicaciones anteriores, en el que la trama (30) de orden integra un valor actual de un contador de tramas de orden, que es incrementado en cada transmisión de trama de orden por el contador de fluido a la caja de corte.

8. Caja (3) de corte que puede montarse en las proximidades de un contador (1) de fluido, la caja de corte que comprende:

- una válvula (4) electromecánica;
- una memoria (23);
- una segunda interfaz (20) de comunicación dispuesta para recibir a través de un enlace radioeléctrico y para almacenar en la memoria (23) una trama (30) de orden transmitida por el contador de fluido y que integra una orden de apertura o de cierre de la válvula (4) electromecánica, la segunda interfaz de comunicación que está además dispuesta para recibir y para ser alimentada por una energía eléctrica transmitida por el contador de fluido a través del enlace radioeléctrico;
- un componente (21) de procesamiento dispuesto para adquirir en la memoria (23) la trama de orden, para descifrar la trama de orden y extraer la orden de apertura o de cierre, para controlar una apertura o un cierre de la válvula electromecánica y para escribir en la memoria (23) una trama de acuse de recibo,

una clave de cifrado simétrico de un algoritmo de cifrado que se almacena en la memoria (23) de la caja (3) de corte, el componente (21) de procesamiento que se dispone para descifrar la trama de orden utilizando la clave de cifrado simétrico.

9. Caja de corte según la reivindicación 8, en la que el componente (21) de procesamiento se encuentra por defecto en un modo de espera, la segunda interfaz (20) de comunicación que está dispuesta para producir una señal de activación del componente (21) de procesamiento cuando la segunda interfaz de comunicación recibe la energía eléctrica.

10. Caja de corte según una de las reivindicaciones 8 a 9, en la que la segunda interfaz (20) de comunicación se dispone para recibir una trama (50) de cambio de clave que puede transmitirse por un dispositivo móvil puesto en las proximidades del elemento de corte, el componente (21) de procesamiento que se dispone para descifrar la trama de cambio de clave y para reemplazar la clave de cifrado simétrico almacenada en la memoria (23) del elemento de corte por una nueva clave de cifrado simétrico integrada en la trama de cambio de clave.

11. Sistema de medida que comprende un contador (1) de fluido según una de las reivindicaciones 1 a 7 y una caja (3) de corte según una de las reivindicaciones 8 a 10.

12. Procedimiento de transmisión de una orden de apertura o de cierre de una válvula (4) electromecánica integrada en una caja (3) de corte situada en las proximidades de un contador (1) de fluido, el procedimiento de transmisión que se implementa por un componente (16) de procesamiento del contador de fluido según una de las reivindicaciones 1 a 7, y que comprende las etapas de:

- adquirir la orden de apertura o de cierre;
- autentificar una trama (30) de orden que integra la orden de apertura o de cierre;
- hacer transmitir por la primera interfaz (15) de comunicación a una segunda interfaz (20) de comunicación de la caja (3) de corte a través de un enlace radioeléctrico la trama (30) de orden y una energía eléctrica adaptada para alimentar eléctricamente la segunda interfaz (20) de comunicación de la caja (3) de corte.

13. Procedimiento de transmisión según la reivindicación 12, una clave de cifrado simétrico que se almacena en una memoria (17) del contador de fluido, el procedimiento que comprende además las etapas de:

- adquirir una trama (50) de cambio de clave transmitida por un dispositivo móvil puesto en las proximidades del contador de fluido, la trama de cambio de clave que comprende una nueva clave de cifrado simétrico y que está cifrada gracias a la clave de cifrado simétrico almacenada en la memoria del contador de fluido;
- descifrar la trama (50) de cambio de clave;
- reemplazar la clave de cifrado simétrico almacenada en la memoria del contador de fluido por la nueva clave de cifrado simétrico.

14. Programa de ordenador que comprende instrucciones que hacen que el componente de procesamiento del contador de fluido según una de las reivindicaciones 1 a 7 ejecute las etapas del procedimiento de transmisión según una de las reivindicaciones 12 o 13.

15. Soporte de grabación legible por ordenador, en el que se graba el programa de ordenador según la reivindicación 14.

Fig. 1

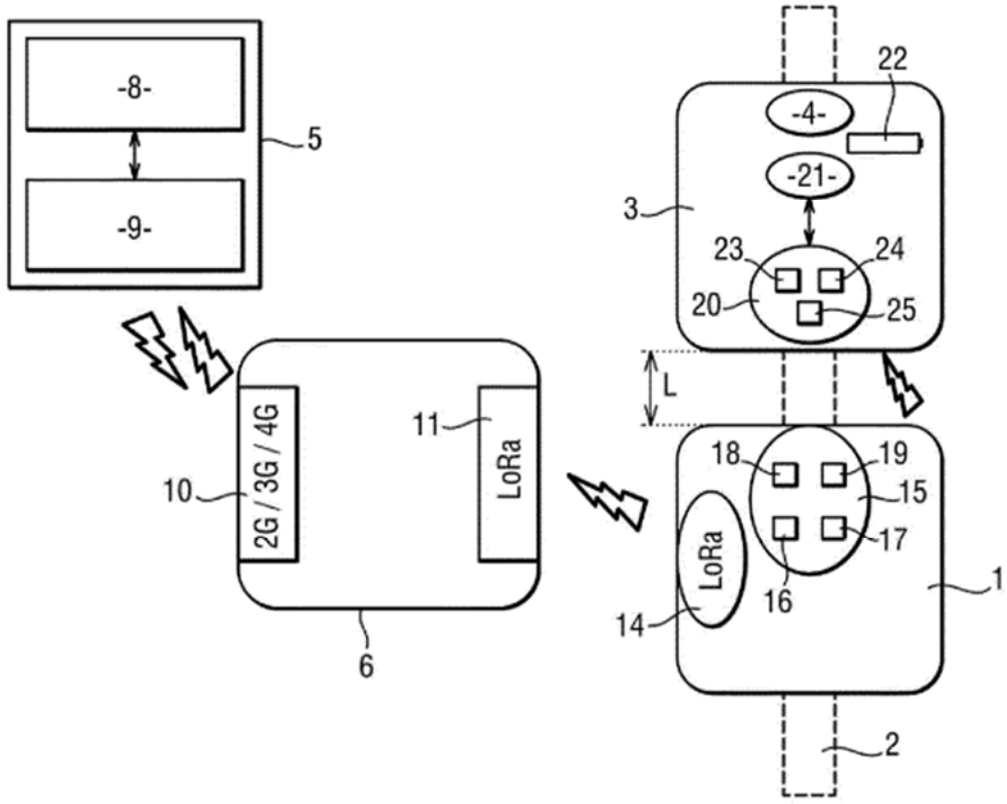

-8-
-9-
5
2G / 3G / 4G
10
LoRa
11
6
22
-4-
-21-
3
23
24
20
25
L
18
19
15
17
16
LoRa
14
1
2

Fig. 2

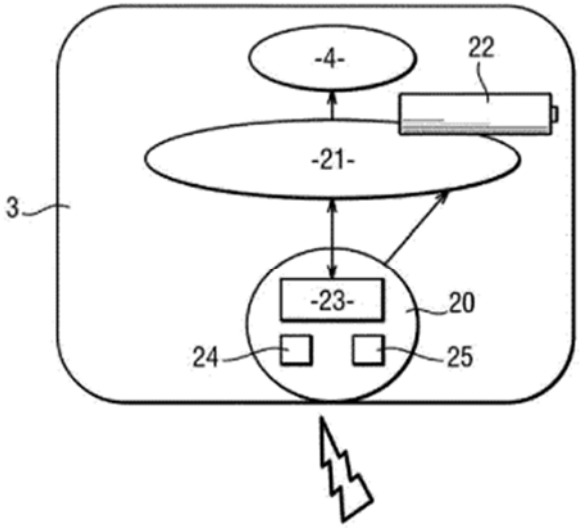

-4-
22
-21-
3
-23-
20
24
25

Fig. 3

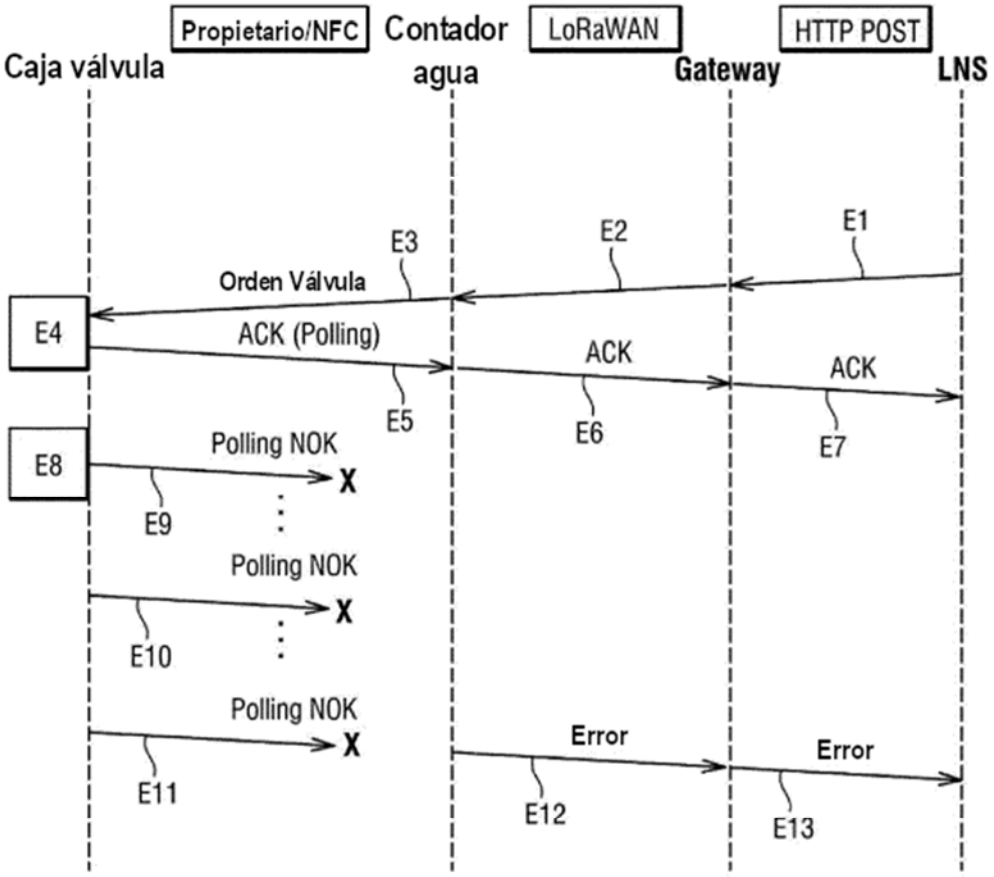

Propietario/NFC
Contador agua
LoRaWAN
HTTP POST
Caja válvula
Gateway
LNS
E1
E2
E3
Orden Válvula
E4
ACK (Polling)
ACK
ACK
E5
E6
E7
E8
Polling NOK
E9
Polling NOK
E10
Polling NOK
E11
Error
Error
E12
E13

Fig. 4

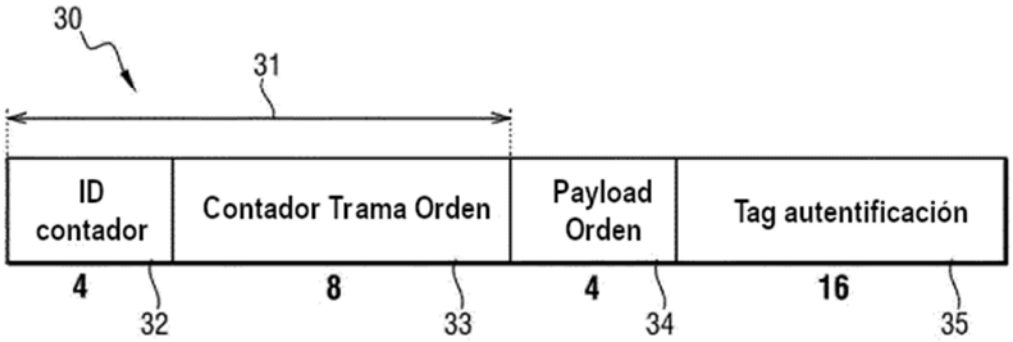

30
31
ID contador
Contador Trama Orden
Payload Orden
Tag autentificación
4
8
4
16
32
33
34
35

Fig. 5

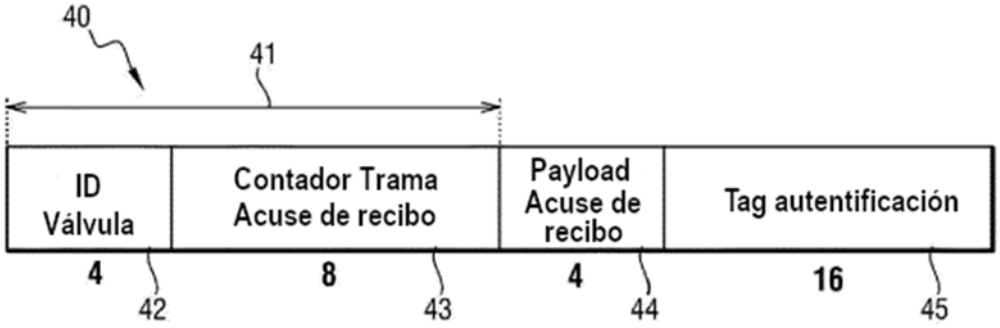
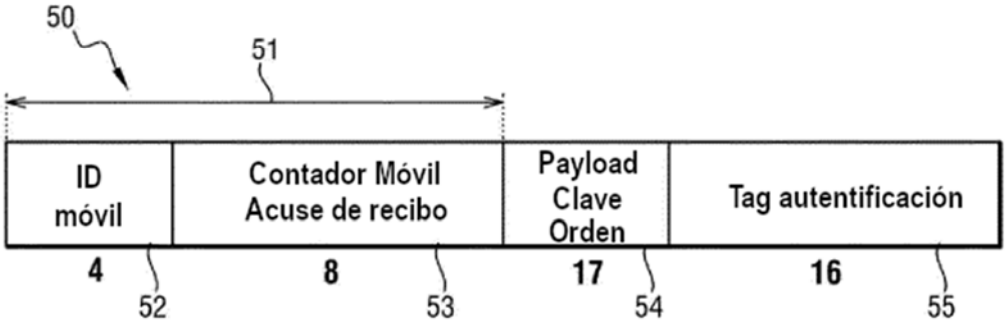

40
41
ID
Válvula
Contador Trama
Acuse de recibo
Payload
Acuse de
recibo
Tag autentificación
4
8
4
16
42
43
44
45

Fig. 6


50
51
ID
móvil
Contador Móvil
Acuse de recibo
Payload
Clave
Orden
Tag autentificación
4
8
17
16
52
53
54
55