

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 400 893**

21 Número de solicitud: 201130753

51 Int. Cl.:

H04L 12/28 (2006.01)

H04L 29/06 (2006.01)

12

SOLICITUD DE PATENTE

A2

22 Fecha de presentación:

11.05.2011

43 Fecha de publicación de la solicitud:

15.04.2013

71 Solicitantes:

MYTECH INGENIERIA APLICADA, S.L. (100.0%)
Avenida de Peruleiro, nº 53, planta 5, puerta 8
15011 A CORUÑA ES

72 Inventor/es:

PAZ LOPEZ, Alejandro;
VARELA FERNANDEZ, Gervasio;
VAZQUEZ RODRIGUEZ, Santiago;
FAIÑA RODRIGUEZ-VILA, Andrés;
BECERRA PERMUY, José Antonio;
DEIBE DIAZ, Alvaro;
DURO FERNANDEZ, Richard J. y
LOPEZ PEÑA, Fernando

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

54 Título: **NODOS CENTRAL Y TERMINAL DE INSTRUMENTACIÓN Y SISTEMA DOMÓTICO AUTOCONFIGURABLE Y SEGURO.**

57 Resumen:

Nodo terminal de instrumentación (2) con:

- medios de conexión (30, 31, 35) para acoplarse con un aparato externo (10) para generar una señal eléctrica de actuación, medios de comunicación (28, 29) para recibir o enviar mensajes,
- medios de cifrado para cifrar los mensajes de envío generados y para descifrar los mensajes recibidos,
- medios de almacenamiento (33) para almacenar claves para cifrado y descifrado de los mensajes e información sobre el funcionamiento del propio nodo (2), sobre los estados de los dispositivos de la red (4, 5, 9, 10) y asociaciones entre estados,
- medios de procesamiento (34) para actualizar la información de los medios de almacenamiento (33) según los mensajes recibidos y para identificar eventos definidos por cambios de estado ocurridos en los dispositivos (4, 5, 9, 10), a fin de generar mensajes de envío según dichos eventos y controlar la generación de señales eléctricas en los medios de conexión (30, 31, 35).

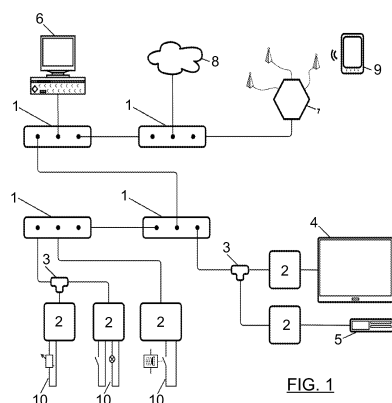


FIG. 1

DESCRIPCIÓN

Nodos central y terminal de instrumentación y sistema domótico autoconfigurable y seguro.

Sector de la técnica

5 La presente invención pertenece al campo de la domótica y está relacionada con la instrumentación de entornos domésticos y ofimáticos.

Estado de la técnica

10 Atendiendo a aspectos estrictamente estructurales, el término instrumentación del entorno comprende la comunicación e integración de dispositivos de campo para la sensorización y actuación, tanto discreta (todo/nada) como proporcional, dispositivos electrónicos basados en microcontroladores así como dispositivos de más alto nivel para el tratamiento de la información y de contenidos multimedia.

Atendiendo a aspectos estrictamente funcionales, el término instrumentación comprende la gestión e integración de información que, proveniente de la interacción con las personas y el entorno, está relacionada con el confort, la energía, la seguridad de las instalaciones, la seguridad de las personas, el ocio y todos aquellos aspectos domóticos y de automatización de tareas.

15 En la actualidad se pueden encontrar en el mercado numerosos sistemas y tecnologías destinados a la automatización del hogar y la oficina. Dichos sistemas se encuentran dominados por tecnologías que se encuadran dentro de lo que se puede considerar domótica clásica. Se trata generalmente de tecnologías propietarias, no interoperables entre sí, que se basan en la instalación de buses de comunicaciones propios a los que se conectan nodos terminales en los que se encuentran sensores o actuadores que operan sobre los diferentes elementos de la instalación.

20 Existen dos aproximaciones principales para dotar a dichos nodos de comportamiento. En algunas tecnologías existe un nodo central del sistema que contiene la lógica de operación del mismo y se encarga de controlar los nodos terminales. En otras existe la opción de que los propios nodos terminales cuenten con una programación que define su comportamiento. En ambos casos la programación se establece durante la instalación del sistema, no suele ser posible la modificación del comportamiento del mismo por parte de los usuarios finales ni la adaptación automática de éste a las necesidades o preferencias de los usuarios.

Dentro de este tipo de sistemas se encuentran tecnologías de domótica con cierta penetración en el mercado como EIB/KNX, Lonworks o X10.

30 En el documento de patente ES2078831, "Sistema domótico de control para una serie de instalaciones y/o aparatos eléctricos" se presenta un sistema domótico con operación distribuida que cuenta con diferentes unidades, cada una de ellas con una funcionalidad particular asociada. Estas unidades están conectadas a un nodo central que es donde se encuentra y ejecuta la lógica de operación del sistema. La conexión con dicho nodo central se realiza mediante un bus de comunicaciones propio, y el sistema requiere la programación y configuración específica del mismo según las tareas a realizar y las unidades disponibles.

35 En el documento de patente US6735619, "Home network gateway apparatus and home network device" se presentan dos dispositivos. Por un lado un dispositivo que se conecta a electrodomésticos y otros aparatos del hogar para actuar como adaptador de los mismos a la red de control del hogar. Por otro lado un dispositivo gateway con capacidad para conectarse a Internet que contiene el software necesario para detectar los dispositivos conectados a la red de automatización y hacer posible su control remoto a través de Internet. Así, el gateway proporciona a los usuarios una interfaz gráfica web desde la que controlar los dispositivos de su hogar.

40 En el documento de patente ES2300231, "Sistema de control domótico multiprotocolo con interfaz de usuario", se presenta un sistema de control domótico cuya principal característica es el hecho de ser compatible con múltiples tecnologías domóticas, permitiendo así el control integrado de dispositivos pertenecientes a tecnologías heterogéneas como X10 o EIB/KNX.

45 La revisión del estado actual de la técnica en el sector al que se destina la presente invención ha permitido identificar las características principales de las invenciones más relevantes. De estas características se pueden extraer algunas de las principales carencias que presentan este tipo de sistemas. Estas son:

- 50 1. Numerosas tecnologías, especialmente las tecnologías de domótica clásica, requieren la instalación de buses de comunicaciones propios, así como la obligación de utilizar dispositivos terminales también propietarios, lo cual encarece enormemente la instalación eléctrica de las viviendas y oficinas y limita la oferta de dispositivos disponibles.
2. Otra carencia de numerosas tecnologías es que, o bien no cuentan con capacidades de operación autónoma, limitándose exclusivamente a permitir el control remoto de la instalación, o las posibilidades de operación autónoma de la instalación son bastante básicas, limitándose a operaciones reactivas ante cambios directos

detectados por los sensores. La definición de dichas programaciones suele ser estática, y decidida por los instaladores del sistema durante la puesta en marcha del mismo. En muchos casos, dicha lógica de operación autónoma se encuentra alojada en dispositivos centrales, lo que puede dificultar la operación del sistema en caso de fallos en algunas partes de la red o en el propio dispositivo central.

- 5 3. Finalmente, otro aspecto ignorado en las tecnologías existentes es la seguridad del sistema de instrumentación, tanto con respecto a la confidencialidad de las comunicaciones, como al acceso a las capacidades de control de los dispositivos disponibles.

Analizando de forma global el estado de la técnica en el ámbito de esta invención, todas las invenciones presentan alguna de las carencias mencionadas.

- 10 Estos inconvenientes han sido algunos de los principales escollos en la integración de este tipo de tecnologías en los hogares y oficinas, pues suponen incrementos muy elevados en los costes de construcción e instalación para conseguir funcionalidades muy limitadas.

Descripción de la invención

- 15 Sería por tanto deseable obtener un sistema de instrumentación distribuida en entornos domésticos y ofimáticos de coste reducido, tanto en lo referente a los componentes como en lo referente a la instalación, que disponga de capacidades de operación autónoma sin requerir la utilización de control centralizado, que disponga de herramientas y capacidades para modificar y adaptar fácilmente la operación del sistema a las preferencias de sus usuarios, y que garantice la seguridad tanto de los datos manejados por el sistema como del acceso a las propias funcionalidades del mismo.

- 20 Para ello, la presente invención propone la utilización de componentes de uso común para el diseño de una red de instrumentación no propietaria y la construcción de nodos terminales de instrumentación que faciliten la conexión de dispositivos genéricos. Esta configuración hace posible la concepción de sistemas para la instrumentación de coste reducido.

- 25 Finalmente, la presente invención propone también una serie de mecanismos encaminados a, por un lado, mejorar la autonomía de la red de instrumentación con respecto a la operación funcional de la misma, así como a su instalación y configuración. Y, por otro lado, mecanismos encaminados a garantizar la seguridad de las comunicaciones dentro de la red de instrumentación y con sistemas externos, así como garantizar la seguridad en el acceso a la funcionalidad proporcionada por la red.

Éste y otros objetivos se consiguen mediante las características definidas en las reivindicaciones independientes.

- 30 Otras realizaciones concretas o particularmente ventajosas se definen en las reivindicaciones dependientes.

Es por tanto objeto de la presente invención un dispositivo (o nodo) terminal de instrumentación distribuida. La invención también se refiere a un dispositivo (o nodo) central de instrumentación distribuida. Se expone también un sistema que integra ambos dispositivos bajo una red de comunicaciones.

Descripción de las figuras

- 35 Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica del mismo, se acompaña como parte integrante de este documento un conjunto de dibujos con carácter ilustrativo y no limitativo, donde se ha representado lo siguiente:

- 40 En la Figura 1 se muestra un ejemplo esquemático de una instalación de red de instrumentación según la propuesta de la presente invención. En la figura se puede apreciar la topología de red híbrida entre topología en estrella mediante switches (1) y topología de bus mediante hubs pasivos en forma de T (3). Se pueden ver también los diferentes elementos que habitan la red de instrumentación, como un nodo central (6), diversos nodos de instrumentación con diferentes dispositivos conectados, como un televisor (4), un reproductor multimedia (5) o diversos dispositivos electrónicos como interruptores, sensores de presencia, termómetros, entre otros (10), un punto de acceso inalámbrico (7) para soportar el acceso sin cables a la red de instrumentación desde dispositivos portátiles (9), así como la opción de contar con acceso a internet (8) para poder acceder a los dispositivos de forma remota.

- 45 En la Figura 2 se muestra una representación de una posible realización de un dispositivo que permita transferir las claves de identificación y cifrado en un nodo de instrumentación de la presente invención. En dicha figura se pueden apreciar el propio dispositivo de claves (11), la pantalla (12) para visualizar la información de las claves disponibles, el botón (13) de transferencia de claves, el conector (14) para la conexión I2C con el nodo de instrumentación, el conector USB para el ordenador (15) y el compartimento de la batería (16).

En la Figura 3 se muestra un diagrama de la secuencia de operación del mecanismo de seguridad de las comunicaciones descrito para la presente invención. La secuencia es la siguiente, (17) el instalador conecta el

dispositivo de transferencia de claves mediante USB al nodo central (usualmente un ordenador) y solicita la generación de N claves, (18) el nodo central genera y transfiere las claves, (19) el instalador conecta un dispositivo con las claves a un nodo de instrumentación mediante I2C y pulsa el botón de transferencia, (20) se transfieren las claves al nodo de instrumentación y (21) se eliminan del dispositivo de transferencia de claves, (22) el nodo de instrumentación almacena las claves, (23) el nodo de instrumentación envía el mensaje de anuncio a la red de instrumentación cifrado con la clave pública del nodo central, (24) el nodo central recibe el mensaje y lo descifra con su clave privada, (25) el nodo central envía el mensaje de respuesta con la clave simétrica, cifrado con la clave pública del nodo de instrumentación, (26) el nodo de instrumentación descifra el mensaje de respuesta con su clave privada y almacena la clave simétrica.

En la Figura 4 se muestra un diagrama de bloques del nodo de instrumentación (2) que se compone de una placa electrónica (27) que contiene una funcionalidad mínima: módulo de comunicaciones (28), conector de comunicaciones (29), entradas y salidas digitales (30), entradas analógicas (31), módulo de alimentación (32) y capacidad de almacenar (33) y procesar datos (34). La ampliación de la funcionalidad de esta placa se realiza, en caso necesario, conectando nuevas placas específicas a un conector de expansión (35) situado en la placa base.

En la Figura 5 se muestra diagrama de bloques del nodo central (6) que consta de un protocolo de acceso externo (37) a la funcionalidad del módulo, herramientas gráficas (38) de configuración de la red y nodos de instrumentación, mecanismos de autoconfiguración (39), repositorio de software de control (40) para placas de expansión, base de datos de dispositivos (41), mecanismos de seguridad y privacidad (42), protocolo de comunicaciones (43).

Realización preferente de la invención

Con el objetivo de complementar la descripción que se está realizando, se acompaña a continuación una descripción detallada de una posible realización de la presente invención sin carácter limitativo.

En la figura 1 se ilustra un diseño de red para instrumentación de coste reducido y alta eficiencia, y un dispositivo para la instrumentación distribuida (2) con un coste y consumo energético reducidos, así como extensible y adaptable. Por ejemplo, con la posibilidad de ser desplegado en cajas de montaje empotrables de tamaño 50x50x20 mm, o incluso de integrarse directamente en los dispositivos electrónicos finales, formando parte de éstos.

Una de las ventajas de la presente propuesta es proporcionar una red de instrumentación que posibilite obtener instalaciones de coste reducido, con operación distribuida y de altas prestaciones.

También es otra de las ventajas conseguir consumos reducidos e integrar todo tipo de dispositivos en una instalación de instrumentación, especialmente aquellos dispositivos de uso común.

Para lograr las ventajas anteriormente mencionadas, se recurre preferentemente a la utilización de tecnologías de red como la familia Ethernet, IEEE 802.3, con una topología de red híbrida, en la que se utiliza topología en estrella, mediante switches (1), para la conexión entre sí de diferentes áreas de la instalación, tales como salas, plantas, etc. Dentro de dichas áreas se utiliza una topología en forma de bus en la que las bifurcaciones se realizarán mediante conectores T (3) que contendrán electrónica básica para permitir la comunicación. Estas T podrán ser concentradores Ethernet pasivos.

Adicionalmente, en la topología de red también se contempla la posibilidad de utilizar tecnologías inalámbricas, como la familia IEEE 802.11, integrando puntos de acceso (7) en la instalación con el objetivo de soportar la comunicación con dispositivos inalámbricos o portátiles (9) en la instalación. En figura 1 se puede ver un diagrama esquemático de un ejemplo de red de instrumentación según la propuesta.

Conectados entre sí mediante dicha red se encontrarían los diversos dispositivos externos (10) que se desean controlar con el sistema de instrumentación. Entre estos dispositivos se encuentran todo tipo de aparatos instalados en entornos habitables tales como hogares u oficinas, incluyendo dispositivos destinados al confort, la energía, la seguridad de las instalaciones, la seguridad de las personas, el ocio y todos aquellos aspectos domóticos y de automatización de tareas.

Se ha diseñado en particular un nodo terminal de instrumentación extensible y adaptable mediante la utilización de componentes electrónicos genéricos. La utilización de dicho tipo de componentes, es decir, componentes fabricados en grandes cantidades y disponibles para el público en general, permite abaratar considerablemente los costes de componentes con respecto a la utilización de componentes fabricados específicamente, como es el caso de las tecnologías de instrumentación y domótica clásicas.

El nodo terminal de instrumentación (2) realiza dos tipos de tareas con respecto a los dispositivos externos (10) que tiene conectados. Por un lado proporciona acceso distribuido a los mismos, de forma que otros componentes del sistema puedan controlar dichos dispositivos remotamente, y por otro lado contiene la lógica de control y configuración que permite la operación autónoma de los dispositivos externos conectados, incluso pudiendo interactuar con otros nodos directamente para, en conjunto, llevar a cabo tareas complejas que un solo nodo terminal de instrumentación (2) con sus dispositivos externos conectados (10) no podría completar.

Preferentemente, el nodo terminal de instrumentación (2) se compone de una placa electrónica (27) que contiene una funcionalidad mínima: módulo de comunicaciones (28), conector de comunicaciones (29), entradas y salidas digitales

(30), entradas analógicas (31), módulo de alimentación (32) y un módulo con capacidad de almacenar (33) y un módulo para procesar datos (34). La ampliación de la funcionalidad de esta placa se realiza, en caso necesario, conectando nuevas placas específicas a un conector de expansión (35) situado en la placa base. De esta manera, el sistema es escalable y permite adaptarse a las distintas necesidades de actuación/sensorización.

- 5 En la red, además de nodos de instrumentación, existen los nodos centrales (6), como se aprecia en la figura 5. El cometido de estos nodos es, entre otros, proporcionar acceso a la red de instrumentación a componentes externos al sistema, como puede ser software de aplicación que haga uso de la red de instrumentación para llevar a cabo tareas de alto nivel: como la configuración de la propia red de instrumentación, su monitorización, proporcionar interfaces gráficas de gestión de la instalación, etc.
- 10 La presente realización propone incorporar mecanismos de autoconfiguración del sistema que faciliten la conexión de dispositivos externos (10), tales como electrodomésticos, luminarias, sistemas de seguridad, sistemas multimedia, sensores y actuadores en general, etc., al sistema de instrumentación, requiriendo la mínima intervención posible por parte de los instaladores y usuarios. Para ello, los nodos de instrumentación y los nodos centrales incorporan software que implementa un protocolo de anuncio y descubrimiento automático de dispositivos.
- 15 Parte de la lógica de operación de dichos mecanismos de autoconfiguración se encuentra en los nodos centrales (6). Estos nodos cuentan preferiblemente con interfaces gráficas de usuario que permiten a los instaladores y usuarios modificar la configuración de la instalación, la cual, a su vez, como se verá a continuación, presenta mecanismos para detectar automáticamente cambios en la configuración física de la misma, facilitando la conexión de nuevos dispositivos a la instalación.
- 20 Cuando un nodo de instrumentación es conectado a la red de instrumentación, o bien, cuando una nueva placa de expansión o dispositivo es conectado a un nodo de instrumentación, este último iniciará un protocolo de anuncio. Dicho protocolo consiste en el envío de un mensaje de anuncio de nodo a todos los nodos conectados a la red de instrumentación, tanto nodos de instrumentación como nodos centrales, lo cual se lleva a cabo mediante el envío de un paquete UDP a la dirección de difusión de la red.
- 25 Dicho mensaje de anuncio es recibido por los nodos centrales (6), los cuales agregan, o modifican si ya existía, el nuevo nodo terminal (2), y la información acerca de éste, a una base de datos de dispositivos disponibles. A partir de ese momento el nuevo nodo terminal de instrumentación (2) estará disponible para que el sistema haga uso del él.
- 30 Como se ha comentado anteriormente, los nodos terminales de instrumentación (2) son extensibles mediante placas de expansión. Debido a limitaciones de memoria y a que el sistema está abierto para aceptar nuevas placas de expansión en el futuro, no es posible desplegar en los nodos terminales de instrumentación (2) todo el software necesario para controlar cada una de las posibles placas de expansión. Así pues, durante el proceso de anuncio y descubrimiento de dispositivos, el nodo central (6) identifica las placas de expansión conectadas a un nodo terminal de instrumentación (2). En caso de que este último no disponga del software controlador necesario para operar alguna de las placas de expansión que tiene conectadas, el nodo central inicia un proceso de transferencia de software. Mediante este mecanismo se transfiere al nodo terminal de instrumentación (2) el software que éste necesita para controlar las nuevas placas de expansión que tiene conectadas. Dicho software incluye la lógica que debe ejecutar el nodo terminal de instrumentación (2) para manejar el hardware disponible en la placa de expansión. Esta lógica es dependiente de cada placa de expansión e incluye el protocolo de interacción entre el nodo de instrumentación y los dispositivos concretos disponibles en cada placa de expansión.
- 35 El nodo central (6) incorpora un repositorio de software de control (40) para placas de expansión, así como herramientas software para que los instaladores y usuarios puedan gestionar dicho repositorio. Se ha tenido especialmente en cuenta la posibilidad de que se instalen en el sistema nuevas versiones de un software controlador ya existente. En dichos casos, el sistema iniciará de forma autónoma un protocolo similar al descrito anteriormente para la transferencia de software de control de placas de expansión. A diferencia del caso anterior, en este caso será el nodo central (6) el que establezca la comunicación con aquellos nodos terminales de instrumentación (2) que contengan software de control de placas de expansión anticuado, y procederá a transferirles la nueva versión.
- 40 El nodo central (6) incorpora un repositorio de software de control (40) para placas de expansión, así como herramientas software para que los instaladores y usuarios puedan gestionar dicho repositorio. Se ha tenido especialmente en cuenta la posibilidad de que se instalen en el sistema nuevas versiones de un software controlador ya existente. En dichos casos, el sistema iniciará de forma autónoma un protocolo similar al descrito anteriormente para la transferencia de software de control de placas de expansión. A diferencia del caso anterior, en este caso será el nodo central (6) el que establezca la comunicación con aquellos nodos terminales de instrumentación (2) que contengan software de control de placas de expansión anticuado, y procederá a transferirles la nueva versión.
- 45 El nodo central (6) incorpora un repositorio de software de control (40) para placas de expansión, así como herramientas software para que los instaladores y usuarios puedan gestionar dicho repositorio. Se ha tenido especialmente en cuenta la posibilidad de que se instalen en el sistema nuevas versiones de un software controlador ya existente. En dichos casos, el sistema iniciará de forma autónoma un protocolo similar al descrito anteriormente para la transferencia de software de control de placas de expansión. A diferencia del caso anterior, en este caso será el nodo central (6) el que establezca la comunicación con aquellos nodos terminales de instrumentación (2) que contengan software de control de placas de expansión anticuado, y procederá a transferirles la nueva versión.

Una vez descubierto el dispositivo (4,5,9,10) y llevado a cabo el proceso inicial de autoconfiguración, que incluye la transferencia del software de control de placas de expansión necesario, éste ya estará accesible en las herramientas de configuración de la red que están disponibles para los instaladores y usuarios, así como disponible para ser utilizado en la instalación.

Se consigue proporcionar una red de instrumentación que opere de forma autónoma y distribuida, de forma que un fallo de algún componente afecte únicamente a los dispositivos controlados por dicho componente. Así pues, los nodos terminales de instrumentación (2) no sólo posibilitan la conexión de los dispositivos externos (10) al sistema de instrumentación, sino que también contienen el protocolo que posibilita la interacción autónoma.

Dicho protocolo se define en base a un sistema de eventos de forma que los nodos terminales de instrumentación (2) reaccionan autónomamente a eventos de cambio de estado que tienen lugar en otros nodos terminales de instrumentación (2). Este protocolo permite especificar asociaciones entre estados de distintos dispositivos (4,5,9,10) de

la red de instrumentación, de forma que cuando se detecte un cambio de estado en un dispositivo, el nodo terminal de instrumentación (2) enviará un evento a la red de instrumentación que será recibido por el resto de nodos terminales de instrumentación (2). Aquellos nodos terminales de instrumentación (2) cuyos dispositivos (4,5,9,10) tengan especificada una asociación con el estado del evento recibido, reaccionaran autónomamente modificando el estado de sus dispositivos locales (4,5,9,10) de acuerdo a lo especificado en la asociación.

Estas asociaciones son definidas por instaladores o usuarios mediante las herramientas de configuración disponibles en los nodos centrales (6), o bien de forma autónoma por software de aplicación de alto nivel que se ejecuta también en dichos nodos centrales. Una vez definidas, las asociaciones son transferidas automáticamente desde el nodo central a los nodos de instrumentación implicados que, a partir de ese momento, podrán operar de forma autónoma sin necesidad de ser controlados por el nodo central.

Se proponen mecanismos que garanticen la confidencialidad de la información manejada por el sistema de instrumentación, así como la seguridad en el acceso al control de los dispositivos desplegados en la red de instrumentación. Esto es, garantizar que sólo los usuarios o sistemas autorizados tienen la capacidad de comunicarse con los nodos de instrumentación y nodos centrales desplegados en la red, así como controlar los dispositivos accesibles mediante éstos, y acceder a la información transferida entre ellos.

Así pues, los nodos, tanto los terminales de instrumentación (2) como los centrales (6), incorporan un mecanismo para cifrar las comunicaciones que se establecen entre ellos. Dicho mecanismo se basa en un sistema híbrido entre un sistema de clave pública/clave privada y un sistema de clave simétrica.

Así pues, se utilizará un sistema de cifrado de clave simétrica para cifrar las comunicaciones entre nodos (2,6), y se utilizará un sistema de cifrado de clave pública/clave privada para autenticar a los nodos durante el proceso de establecimiento de la clave simétrica necesaria para las comunicaciones.

Cada nodo (2,6) de la red de instrumentación tendrá un conjunto de clave pública/clave privada, conjunto que debe ser instalado en el nodo durante su instalación física en la red. Dicho conjunto de clave pública/clave privada se genera en un nodo central, que será el encargado de llevar a cabo el proceso de establecimiento de claves simétricas para el cifrado de las comunicaciones.

Durante el proceso de anuncio de un nuevo nodo de instrumentación en la red, el nodo de instrumentación utiliza la clave pública del nodo central para cifrar los mensajes de anuncio (22, 23). El nodo central (2) responderá al mensaje de anuncio con un mensaje que contendrá la información de la clave simétrica que el nodo debe utilizar para las comunicaciones con la red de instrumentación (25). Dicho mensaje de respuesta se cifra utilizando la clave pública del nodo de instrumentación (24).

Desde el momento en que el nodo de instrumentación conoce la clave simétrica (26), comienza a utilizarla para cifrar y descifrar todas las comunicaciones que mantenga con otros nodos de la red de instrumentación.

La clave simétrica (26) es renovada cada cierto tiempo mediante un proceso que es gestionado por un nodo central (6), el cual genera una nueva clave simétrica y se la comunica al resto de nodos terminales (2) de la red utilizando el procedimiento de clave pública/clave privada anteriormente descrito.

Este sistema de seguridad requiere que el instalador de la red de instrumentación inicialice adecuadamente cada uno de los nodos de la red, instalando una pareja de clave pública/clave privada, así como la clave pública de alguno de los nodos centrales encargados de la gestión del sistema de cifrado.

La inicialización de los dispositivos (4,5,9,10) debe llevarse a cabo físicamente y dispositivo a dispositivo durante la fase de instalación física de la red. Esto debe ser así para poder garantizar completamente la seguridad en el proceso de transmisión inicial de las claves, que no puede llevarse a cabo a través de un canal de comunicaciones no seguro, como sería en ese momento la propia red de instrumentación.

Para ello, se propone la utilización de un dispositivo diseñado a tal efecto que permita el almacenamiento y transferencia de las claves, utilizando una interfaz USB para su conexión a un ordenador y una interfaz I2C para la conexión con nodos terminales de instrumentación (2).

Utilizando el software de gestión de la red de instrumentación que estará habilitado en los nodos centrales (6), en concreto en aquéllos que dispongan de la posibilidad de gestionar el sistema de seguridad de la red, el instalador podrá generar un número N de pares clave pública/clave privada y almacenarlas, junto con la clave pública del nodo central (6), en un dispositivo de transferencia de claves (11).

Una vez hecho esto, el instalador tendrá que desplazarse hasta cada nodo (2) (o bien realizar este proceso antes de montarlos físicamente en la instalación), conectar un dispositivo de transferencia de claves (11) a través del conector de placas de expansión (35) del nodo terminal de instrumentación (2) (el cual debe estar encendido) y realizar el proceso de transferencia de claves hacia el nodo de instrumentación (2).

A partir de ese momento, el nodo terminal de instrumentación (2) ya cuenta con el conjunto de claves que necesita para autenticarse contra el nodo central (6) y obtener de éste la clave simétrica mediante el procedimiento descrito anteriormente. En la Figura 3 se puede ver el esquema de la operación del mecanismo de seguridad de las comunicaciones descrito.

5 Volviendo a la Figura 1, aparece allí representando un diagrama de bloques funcional de la presente invención. En dicho diagrama se puede apreciar un ejemplo de implementación de los tres elementos principales de los que se conforma la presente invención.

- a. la red de instrumentación,
- b. el nodo central (6),
- 10 c. el nodo de instrumentación (2).

La red de instrumentación está construida utilizando una topología de red híbrida entre topología en estrella mediante switches 802.3 (1) y topología de bus mediante hubs 802.3 pasivos en forma de T (3). Opcionalmente, existe también la posibilidad de utilizar puntos de acceso 802.11 (7) en lugar de los hubs pasivos, soportando así el acceso a la red de instrumentación mediante dispositivos inalámbricos (9), así como la utilización de nodos de instrumentación con módulos de comunicaciones bajo tecnología inalámbrica 802.11.

El nodo central (6) está compuesto de un PC empotrado que cuenta con un microprocesador compatible con las instrucciones Intel x86, como por ejemplo Intel Atom o VIA EPIA, al menos 256Mb de memoria RAM, interfaz de red 802.3 e interfaz RS-232. Instalado en dicho PC se encuentra el software de control del nodo central, que está implementado utilizando el lenguaje de programación JAVA.

20 El nodo de instrumentación (2) está constituido por diferentes módulos de los cuales se expone a continuación una posible realización.

El módulo de alimentación (32) del nodo de instrumentación está formado por un convertor dc/dc que rebaja la tensión de 24V de corriente continua a una tensión constante de 3.3V para alimentar al resto de sistemas. Este convertor dc/dc está controlado por el reductor de voltaje LT3502AIDC. Otras opciones posibles son la alimentación por medio de "Power over Ethernet" o alimentación a baterías. Este módulo de alimentación contiene un LED para indicar la existencia de alimentación y el correcto funcionamiento de la fuente.

El microcontrolador (34) empleado es el PIC18F67J60-I/PT. Este microcontrolador contiene un controlador de Ethernet incluido en el mismo y, además, dispone de un oscilador externo (36) F330 de 25MHz, necesario para la comunicación Ethernet. Además, el microcontrolador puede comunicarse con la memoria externa (33) 24FC512T-I/SM de 512Kbits y almacenar datos de manera permanente. El microcontrolador se encarga de modificar las salidas digitales (30) correspondientes, informar al resto de la red de los valores de las señales de entrada, comunicar su presencia al resto de nodos de la red por medio del módulo de comunicaciones Ethernet, responder a las peticiones de otros nodos conectados a la red, guardar los datos que se requieran almacenar en la memoria y requerir datos a otros nodos de la red. Su firmware puede ser actualizado por medio de las comunicaciones Ethernet.

35 El sistema de comunicaciones Ethernet se compone por un controlador (en esta implementación este controlador está integrado en el microcontrolador) y de un transformador y resistencias para el filtrado de ruidos.

Las entradas digitales del nodo (30), ocho en total, se conectan a las entradas digitales del microcontrolador con resistencias de "pull-up" y resistencias para protección del microcontrolador. Un grupo de cuatro de estas entradas se conectan a conectores de dos vías con la masa de la placa. Este grupo se emplea como entradas a señales de dispositivos activos que dispongan de su propia alimentación o dispositivos pasivos, tales como, interruptores, pulsadores, sensores de presencia, etc. Las cuatro entradas del otro grupo se conectan a conectores de tres vías que disponen de masa y 3,3V y permite la alimentación de dispositivos activos que no dispongan de alimentación.

Este nodo dispone de una entrada analógica específica conectada a través de un conector de tres vías que dispone de masa y 3,3V. Además, las cuatro entradas digitales con conectores de tres vías se pueden configurar para convertirlas en entradas analógicas. Esta configuración permite la medición de señales en el rango de 0 a 3,3V en dispositivos tales como potenciómetros, sensores de luz, medidores de temperatura, etc.

El nodo proporciona dos tipos de salidas digitales distintas: salidas de colector abierto y salidas para activar relés de corriente continua. Las cuatro salidas de colector abierto se utilizan con conectores de dos vías (colector y masa) y permiten accionar dispositivos que tengan su propia alimentación. Las tres salidas para activar relés (elementos sin alimentación) disponen de conectores de dos vías (colector y tensión de alimentación). Estas salidas están pensadas para la activación de cargas inductivas de hasta 500mA y, por tanto, están equipadas de diodos de freewheeling para protección del circuito.

La ampliación de funcionalidad de esta placa básica se realizará añadiéndole placas de expansión a través de un conector (35). Dicho conector incorpora un bus de comunicaciones, las distintas tensiones de alimentación, y las

entradas y salidas que no están empleadas del microcontrolador. De esta manera, las placas de expansión pueden ser controladas por el microcontrolador de la placa base o bien llevar su propio microcontrolador y comunicarse con las restantes placas mediante dicho bus. El bus elegido en esta implementación es el I2C ya que existen muchos circuitos integrados que lo emplean (memorias, microcontroladores, sensores, etc.).

- 5 Las dimensiones del nodo de instrumentación permiten su montaje, junto con los cables necesarios para su conexionado, en el interior de cajas de montaje empotrables de tamaño 50x50x20 mm. Las sucesivas ampliaciones del dispositivo pueden o bien apilarse dentro de la misma caja empotrada o bien alojarse en cajas contiguas.

Las placas de expansión que se pueden acoplar al nodo base proporcionan un mayor número de entradas y salidas o nuevas funcionalidades al sistema. Las placas que proporcionan nuevas funcionalidades son, entre otras, las siguientes:

- 10
- Placas de comunicaciones:
 - Wireless
 - Zigbee
 - Bluetooth
 - RS232
- 15
- USB
- Placas de entradas:
 - entradas analógicas de 4-20mA
 - entradas analógicas de 0-10V
 - expansión de entradas digitales
- 20
- Placas de salidas:
 - Salidas de potencia de 220V
 - Salidas de potencia corriente continua
 - Salidas de contactos libre de tensión
 - Salidas analógicas
- 25
- Salidas de resistencia variable

Las placas de expansión disponen de sensores de intensidad consumida a nivel global y por cada una de las salidas. En el caso de que se utilicen relés de estado sólido también incluyen un sensor de temperatura para controlar que la placa no se calienta en exceso.

REIVINDICACIONES

- 1.-** Nodo terminal de instrumentación (2) caracterizado por que comprende:
- medios de conexión (30,31,35) configurados para acoplarse eléctricamente con un aparato externo (10) para generar una señal eléctrica de actuación sobre dicho aparato externo (10),
 - medios de comunicación (28,29) configurados para recibir o enviar mensajes a través de una red local de datos,
- 5 - medios de cifrado configurados para cifrar los mensajes de envío generados en los medios de procesamiento y para descifrar los mensajes recibidos en los medios de comunicación para ser procesados,
- medios de almacenamiento (33) configurados para almacenar claves para cifrado y descifrado de los mensajes, dichos medios de almacenamiento configurados además para almacenar información sobre el funcionamiento del propio nodo de instrumentación (2), sobre los estados de los dispositivos de la red (4,5,9,10) y asociaciones entre estados,
- 10 - medios de procesamiento (34) configurados para actualizar la información de los medios de almacenamiento de acuerdo con los mensajes recibidos y para identificar eventos definidos por cambios de estado ocurridos en los dispositivos (4,5,9,10) de la red, a fin de generar mensajes de envío de acuerdo con dichos eventos y controlar la generación de señales eléctricas en los medios de conexión (30,31,35).
- 2.-** Nodo terminal (2) según reivindicación 1, caracterizado por que los medios de conexión comprenden además un módulo de expansión (35) configurado para ser conectado con otro módulo de expansión (35) para permitir el apilamiento de varios módulos de expansión sobre un mismo nodo de instrumentación.
- 15 **3.-**Nodo terminal (2) según reivindicación 2, caracterizado por que el módulo de expansión (35) comprende un microcontrolador propio configurado para implementar al menos uno de los dos modos siguientes:
- un modo autónomo configurado para establecer operaciones de control autónomo de las funciones de dicho módulo de expansión,
- 20 - un modo dependiente configurado para ser controlado desde el nodo terminal (2) anfitrión.
- 4.-**Nodo terminal (2) según reivindicaciones 2 ó 3, caracterizado por que los medios de conexión comprenden al menos una entrada analógica y una pluralidad de entradas y salidas digitales.
- 5.-**Nodo terminal (2) según una cualquiera de las reivindicaciones 2 a 4, caracterizado por que está configurado para implementar un proceso de inicialización basado en el envío de un mensaje de anuncio a todos los nodos (2,6) y/o módulos de expansión (35) disponibles en la red de instrumentación a fin de actualizar la información presente en los medios de almacenamiento.
- 25 **6.-**Nodo terminal (2) según una cualquiera de las reivindicaciones anteriores, caracterizado por que los medios de comunicación están configurados para implementar al menos uno de los siguientes protocolos: según IEEE 802.3 o según IEEE 802.11.
- 30 **7.-**Nodo terminal (2) según una cualquiera de las reivindicaciones anteriores, caracterizado por que los medios de cifrado están configurados para implementar un cifrado de clave simétrica y un cifrado de clave pública/clave privada para autenticar previamente los nodos durante el proceso de establecimiento de la clave simétrica.
- 8.-** Nodo central de instrumentación (6) caracterizado por que comprende:
- medios de comunicación (37,43) configurados para recibir o enviar mensajes a través de una red local de datos, dichos medios de comunicación (37,43) configurados además para transferir información sobre el funcionamiento de unos nodos terminales (2), sobre los estados de los dispositivos de la red (4,5,9,10) y asociaciones entre estados,
 - medios de cifrado (42) configurados para cifrar los mensajes de envío generados en unos medios de procesamiento y para descifrar los mensajes recibidos en los medios de comunicación (37,43) para ser procesados,
- 35 - medios de almacenamiento (41) configurados para almacenar información asociada a una pluralidad de dispositivos (2,4,5,9,10) que pueden ser conectados a la red, comprendiendo información sobre el funcionamiento de unos nodos terminales (2), sobre los estados de los dispositivos de la red (4,5,9,10) y asociaciones entre estados,
- medios de procesamiento (38,39,40) configurados para:
 - actualizar la información de los medios de almacenamiento (41) de acuerdo con los mensajes recibidos,
- 40 - establecer asociaciones basadas en cambios de estado de los dispositivos (4,5,9,10) de la red, de forma que se definen eventos para administrar dichos dispositivos (4,5,9,10),
- 45

- controlar la transferencia de información en los medios de comunicación (37,43).

9.- Nodo central (6) según reivindicación 8, caracterizado por que los medios de comunicación (37,43) están configurados para implementar al menos uno de siguientes protocolos: según IEEE 802.3 o según IEEE 802.11.

5 **10.-** Nodo central (6) según reivindicación 9, caracterizado por que comprende unos medios de control configurados para ampliar la capacidad de conexión de unos nodos terminales (2) anfitriones mediante la gestión de módulos de expansión (35) configurados para ser conectados con otros nodos terminales (2).

11.- Nodo central (6) según reivindicación 8, caracterizado por que comprende unos medios de monitorización de los dispositivos (2,4,5,6,9,10) de la red.

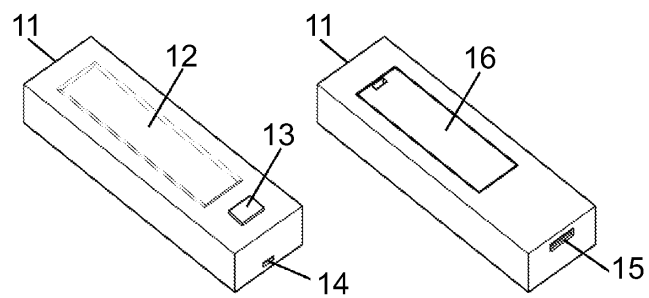
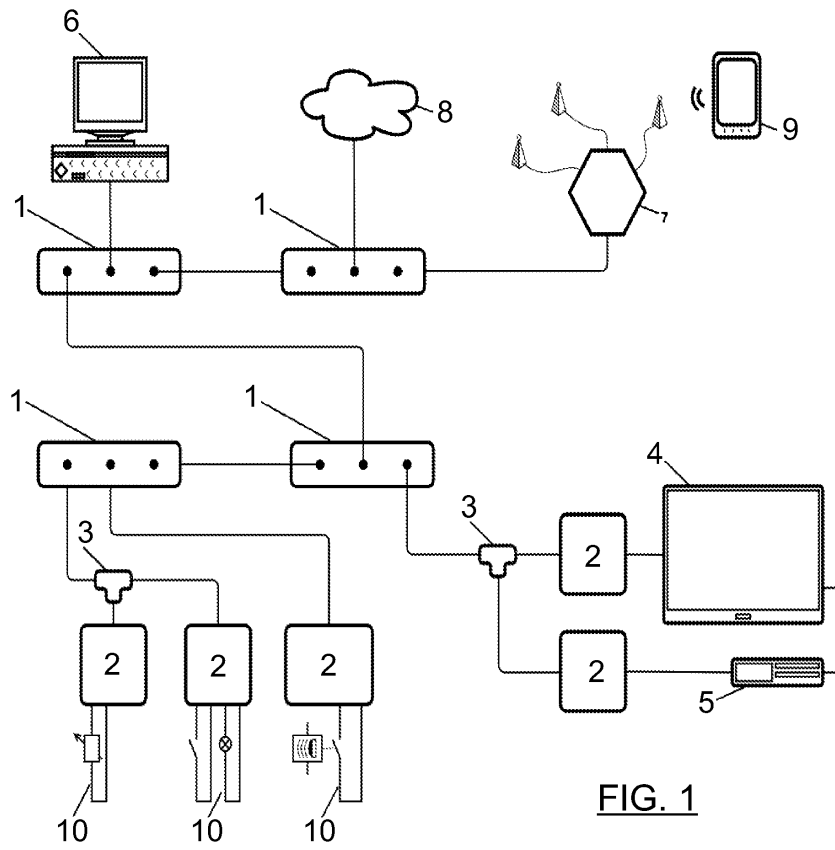
12.- Sistema domótico caracterizado por que comprende:

- 10
- una red local de datos,
 - un nodo terminal (2) según una cualquiera de las reivindicaciones 1 a 7,
 - un nodo central (6) según una cualquiera de las reivindicaciones 8 a 11.

15 **13.-** Sistema domótico según reivindicación 12, caracterizado por que los medios de almacenamiento (34) de un nodo terminal (2) están configurados para ser inicializados mediante una transmisión inicial de las claves públicas de forma que los mensajes de envío son cifrados por dicho nodo terminal (2) y descifrados al ser recibidos por el nodo central (6) mediante la aplicación de una clave privada almacenada en los medios de almacenamiento (41) de dicho nodo central (6).

20 **14.-** Sistema domótico según reivindicación 13, caracterizado por que el nodo central (6) está configurado para enviar en respuesta al nodo terminal (2), un mensaje cifrado con la clave pública que comprende información sobre una clave simétrica necesaria para establecer posteriores comunicaciones a través de la red.

15.- Sistema domótico según reivindicación 14, caracterizado por que periódicamente se reemplaza la clave simétrica.



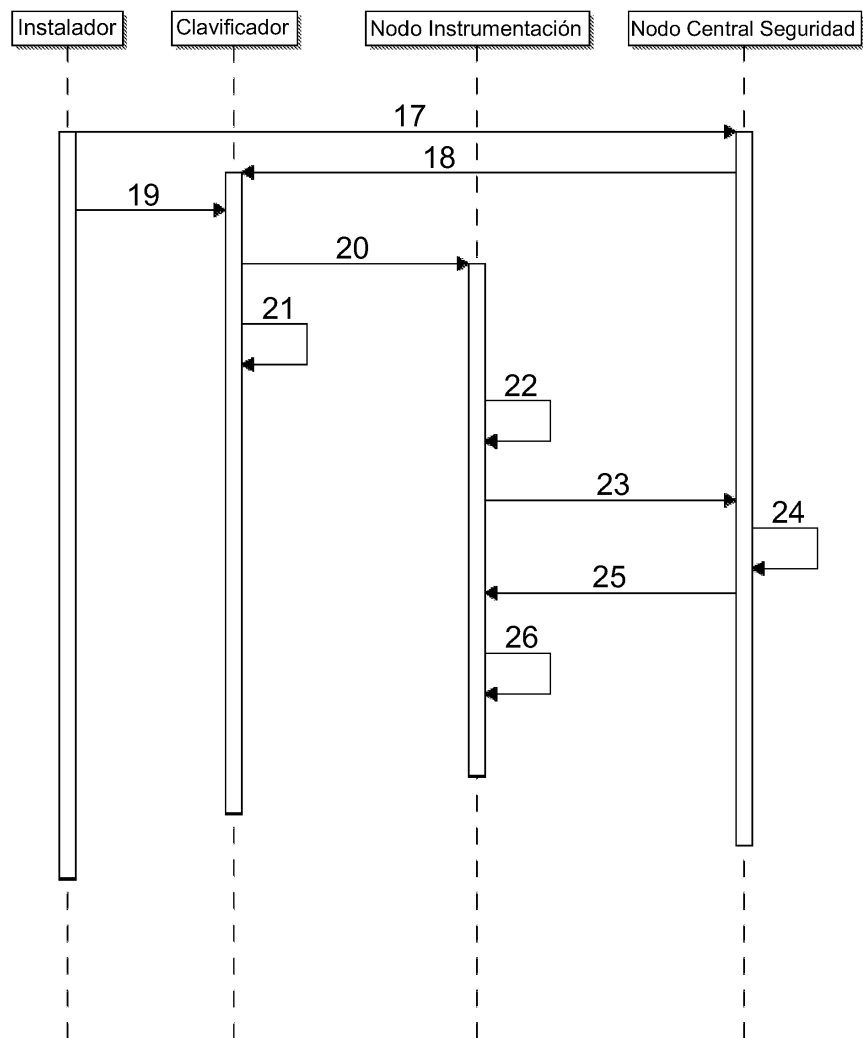


FIG. 3

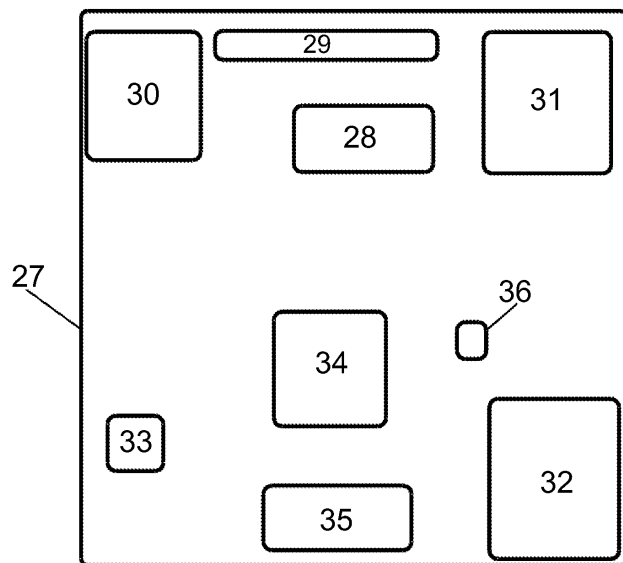


FIG. 4

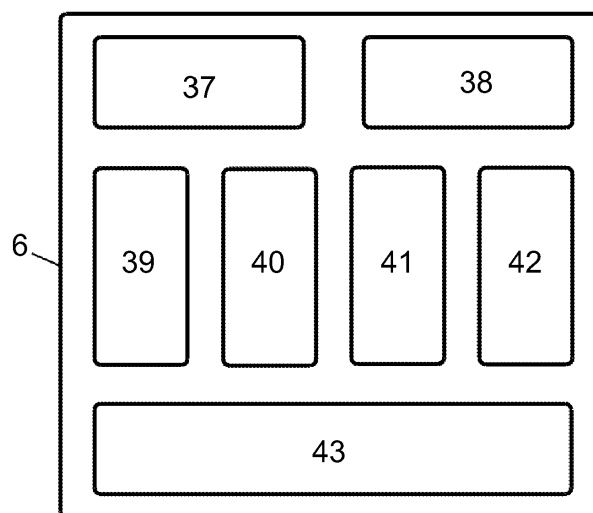


FIG. 5