(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **1 263 334**

(21) Número de solicitud: 202032575

(51) Int. CI.:

H04L 12/28 (2006.01)
G05B 15/02 (2006.01)

(12) SOLICITUD DE MODELO DE UTILIDAD U

(22) Fecha de presentación:

24.10.2019

(43) Fecha de publicación de la solicitud:

23.03.2021

(71) Solicitantes:

UNIVERSIDAD DE HUELVA (80.0%)
C/ Dr. Cantero Cuadrado 6
21071 Huelva ES y
UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED) (20.0%)

(72) Inventor/es:

SÁNCHEZ HERRERA, Maria Reyes;
MEJÍAS BORRERO, Andrés;
MÁRQUEZ VÁZQUEZ, Alejandro;
DE LA TORRE CUBILLO, Luis y
ANDUJAR MARQUEZ, José Manuel

(74) Agente/Representante:

RODRIGUEZ QUINTERO, José

(54) Título: **SISTEMA PARA EL ACCESO A REDES DE DATOS SEGURAS**

ES 1 263 334 U

DESCRIPCIÓN

SISTEMA PARA EL ACCESO A REDES DE DATOS SEGURAS

Objeto de la invención

Es un objeto de la invención un sistema que permite implementar servicios en la nube para gestionar los datos de sensores, actuadores o controladores de cualquier tipo de planta o sistema sensorizable y actuable a partir de señales eléctricas, de tal forma que el acceso es seguro porque se realiza de forma encriptada y con los correspondientes perfiles de usuario. Es un acceso controlado porque puede ser sometido a filtros con distintos criterios de explotación, como, por ejemplo, el huso horario. Es un acceso ordenado porque el acceso puede ser secuenciado mediante, por ejemplo, un gestor de reservas. Finalmente, es un acceso colaborativo porque se permite el acceso concurrente a un mismo recurso.

Estado de la técnica

Las redes de datos han ido apareciendo y siguen creciendo conforme se presenta un problema o necesidad. Debido a esta peculiaridad, no hay un diseño integral de las redes de datos y, por tanto, se trata de redes desestructuradas. Cuando apareció la necesidad de acceder desde redes no seguras a elementos conectados a redes seguras (normalmente redes internas de empresas y/o instituciones), cada fabricante lo resolvió de una forma distinta y particular, adaptada a sus equipos y sistemas. Además, esas soluciones parciales aportadas por los distintos fabricantes no garantizan el acceso seguro, controlado, ordenado y colaborativo porque hay redes con medidas de seguridad reforzada que impiden el buen funcionamiento de los equipos propuestos por otros fabricantes.

Por tanto, en el estado de la técnica existe la necesidad de un sistema de acceso a elementos conectados a redes internas (seguras) desde redes públicas (no seguras) que sea general y válido independientemente del fabricante de cada red y que funcione en cualesquiera circunstancias aunque las redes involucradas tengan implementadas medidas de seguridad específicas. Hoy en día las soluciones comerciales al problema del acceso a dispositivos desde Internet siguen siendo específicas de cada fabricante. Este problema se soluciona mediante el método y el dispositivo descrito en las reivindicaciones que acompañan a la presente memoria descriptiva.

Explicación de la invención

El sistema que es objeto de la presente invención, de acuerdo con el enunciado de la presente memoria descriptiva, permite implementar servicios en la nube para gestionar los datos de sensores, actuadores o controladores de cualquier tipo de planta o sistema sensorizable y actuable a partir de señales eléctricas. El acceso a esos dispositivos es seguro, controlado, ordenado y colaborativo (en adelante SCOC). La presente invención, por tanto, se constituye como un elemento de frontera entre Internet (red pública) y una o varias redes privadas LAN (*Local Area Networks*, Redes de Área Local). Este elemento de frontera convierte los accesos a la(s) LAN en accesos SCOC. Además, los elementos (bases de datos, equipos físicos, u otros dispositivos electrónicos) a los que, estando conectados a la/s LAN/s, se implemente acceso desde Internet, serán accesibles como servicio en la nube. Por último, en cuanto se conecta un dispositivo mediante el sistema o el método de la invención en una LAN, el mismo sistema informa de todos los elementos conectados a esa LAN con posibilidad de implementación de acceso.

El paradigma de servicio en la nube rompe con el modelo tradicional de computación local. Tradicionalmente, era necesario tener instalada en el ordenador la aplicación asociada a un determinado tratamiento de datos. Con el modelo de servicio en la nube, el usuario no debe tener instalada ninguna aplicación específica en su ordenador, sino que accede al procesamiento requerido a través del navegador web. La aplicación está instalada en un servidor en Internet y se ejecuta de forma remota. La transformación de los datos puede quedar en internet (en el servicio en la nube) o ser transferida al equipo local. Las aplicaciones que permiten la gestión de los datos a través del navegador constituyen lo que se denomina servicio en la nube. Por tanto, el servicio en la nube está constituido por un conjunto aplicaciones que se ejecutan en el lado del servidor y un conjunto de aplicaciones ejecutables en el lado del navegador.

La principal proporciona un método general para acceder a aplicaciones y dispositivos de forma SCOC. Por tanto, la invención proporciona acceso seguro y controlado desde internet a cualquiera de sus sistemas físicos (líneas de producción, plantas piloto, laboratorios, o cualquiera que se decida). Esa empresa podrá usar para ello un servidor privado o constituirse como proveedor IaaS (*Infraestructure-as-a-Service*). Además los sistemas accesibles pueden ser redes móviles.

El equipo se ha desarrollado de forma que para su configuración no sea necesario ser experto

en comunicaciones y electrónica, sino que puede ser configurado por cualquier persona con conocimientos mínimos en esos temas.

Finalmente, cabe destacar que la invención puede ser implementada en un computador de tarjeta simple (*Single-Board Computer*, SBC) como por ejemplo una Raspberry Pi o similares con el software correspondiente. La invención también puede ser implementada en un conjunto de servidores cada uno con el software correspondiente a un módulo. Entre esos dos casos límite, son posibles todos los casos intermedios.

A lo largo de la descripción y de las reivindicaciones, la palabra «comprende» y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos. Para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la invención y en parte de la práctica de la invención. Los siguientes ejemplos y dibujos se proporcionan a modo de ilustración y no se pretende que restrinjan la presente invención. Además, la invención cubre todas las posibles combinaciones de realizaciones particulares y preferidas aquí indicadas.

Breve descripción de los dibujos

A continuación, se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención, que se ilustra como un ejemplo no limitativo de ésta.

La figura 1 muestra la arquitectura del sistema para el acceso seguro, controlado, ordenado y colaborativo a redes de datos seguras, objeto de la presente invención.

La figura 2 muestra la arquitectura del módulo CDAS (1).

La figura 3 muestra la arquitectura del módulo SCRA (3).

Explicación de un modo detallado de realización de la invención

Tal y como se muestra en la figura 1, el sistema objeto de la invención es un sistema escalable y modular que comprende, en esta realización práctica, al menos, los siguientes módulos:

El primer módulo 1 o módulo CDAS (*Convergent Data Acquisition System*), que es un dispositivo electrónico configurado para hacer accesible en red los datos de sensores y

actuadores de un equipo físico. Así pues, un equipo o dispositivo con un módulo CDAS 1 pasaría a ser un equipo convergente (i.e. accesible desde red). Este módulo CDAS 1 no sería necesario en el caso de dispositivos cuyo fabricante los hace convergentes a través de un software específico (software propietario).

El segundo módulo (2) o módulo UI (*User Interface*, interfaz de usuario) es una aplicación que permite la gestión de los datos asociados a los dispositivos físicos desde la red.

El tercer módulo (3) o módulo SCRA (*Server to Control the Remote Access)* es un servidor que se encarga de controlar el acceso a una red con varios conjuntos de equipos físicos o plantas, todos ellos convergentes.

El cuarto módulo (4) o módulo CPD (*Cloud Publishing Device*) es un dispositivo electrónico configurado para solicitar la publicación en la nube del acceso a equipos físicos convergentes que constituyan un conjunto o planta.

El quinto módulo (5) o módulo CPS (*Cloud Publishing Server*) es un servidor configurado para hacer visible desde internet las solicitudes de publicación realizadas por el o por los módulos CPD 4.

Un sexto módulo (6) o módulos IIMS (*Integration on Information Management System*) es un módulo que comprende las distintas aplicaciones (*plugins*) necesarias para integrar el acceso a los dispositivos físicos o conjuntos de dispositivos en el gestor de contenidos de la empresa o institución. En el ámbito de la educación, por ejemplo, el gestor de contenidos será un *Learning Management System* (LMS). Las aplicaciones comprendidas en el módulo IIMS (6) son tres: una para integrar el módulo UI (2), otra para ordenar el acceso mediante la correspondiente reserva y otra para aceptar la validación diferida de los perfiles de usuario.

El séptimo módulo o módulo IRS (*International Registration Server*) es un servidor único que tiene registrados todos los módulos IIMS (6) en los que funciona el sistema y/o método objeto de la presente invención.

Finalmente, el octavo módulo o módulo LSRAC (*Local Service to Remote Access Control*) es un módulo de software que se instala en el ordenador del usuario y que está configurado para eliminar las limitaciones de comunicación impuestas por los navegadores.

El sistema o el método que son objeto de la presente invención comprenderá:

- Una combinación de al menos uno de cada uno de los módulos.
- Una combinación de módulos SCRA (tantos como redes internas distintas existan), CDAS e UI (en número variable con los dispositivos a implementar su acceso), uno o varios módulos IIMS, LSRAC e IRS.
- Una combinación de módulos CDAS e UI, CPD (tantos como redes internas distintas existan), un módulo CPS, IIMS, LSRAC e IRS.

Módulos CDAS (1)

El módulo CDAS (1) es un módulo general para cualquier tipo de dispositivo, por lo que no comprende la sensorización y actuación de éste, sino que éste se supone como una «caja negra» con un conjunto de «n» variables de entrada y «m» variables de salida normalizadas, tal y como mejor se observa en la figura 2. El módulo CDAS (1) comprende, por tanto, al menos un procesador/computador necesario para la gestión de esas entradas y salidas. El módulo CDAS (1) presenta dos posibles arquitecturas que lo hacen totalmente escalable: una primera arquitectura para sistemas sencillos y una segunda arquitectura para sistemas complejos, donde los términos «sencillo» o «complejo» hacen referencia a las necesidades de procesamiento de información y/o cómputo. En cualquiera de esas dos posibles arquitecturas, el módulo CDAS (1) comprende una pluralidad de capas: (a) una primera capa interfaz de red (1.1) que puede ser de tipo Ethernet o inalámbrica, mediante la cual el módulo CDAS (1) se conectará a la red; (b) una segunda capa de procesamiento y computación de datos (1.2) que aporta la torre de protocolos TCP/IP (Transport Control Protocol / Internet Protocol), la capacidad de procesamiento necesaria para el mantenimiento de las comunicaciones por la red y las necesidades de procesamiento de datos; (c) una tercera capa de adquisición de datos (1.3) que proporciona la interfaz necesaria para que la capa de procesamiento y computación (1.2) reciba y envíe información; y (d) una cuarta capa de adaptación de niveles (1.4) que ajusta los rangos de tensiones de las señales eléctricas de los sensores y actuadores a valores óptimos de entrada en la capa de adquisición (1.3).

Para sistemas sencillos, como la activación de un equipo, imponer un nivel de consigna determinado o mostrar a través de la UI el valor adquirido por un sensor, se propone un único componente como arquitectura de las tres primeras capas del módulo CDAS: una placa de desarrollo de bajo coste basada en microcontroladores. Estos dispositivos disponen de entradas y salidas digitales, entradas y salidas analógicas y buses digitales de comunicación serie, además de capacidad de procesamiento e interfaces de red.

En el caso de aplicaciones complejas, se propone una arquitectura alternativa para la implementación esas tres capas, que incluye un sistema operativo embebido para la gestión del almacenamiento de información y para aumentar la concurrencia de los accesos por red. Asimismo, este sistema posibilita el uso de herramientas de desarrollo rápido para diseñar las aplicaciones de control necesarias.

Módulo UI (2)

El módulo UI (2) es la aplicación que permite la gestión de los datos asociados a los dispositivos físicos y que se ejecuta en un navegador de internet (a modo de ejemplo no limitativo, Google Chrome, Mozilla Firefox, Opera, Internet Explorer u otros cualesquiera). Un módulo UI (2) está configurado para convertir las acciones de los usuarios en señales sobre ellos y muestra los valores de datos asociados a magnitudes físicas relevantes. El marco de ejecución de esta interfaz es el navegador o el software propietario. La integración en la nube en el primer caso es trivial, pero en el segundo caso se hace necesario el uso del módulo LSRAC.

Módulo SCRA (3)

El módulo SCRA (3) está constituido por un servidor con dos interfaces de red. Una de ellas lo conecta a internet con una dirección válida y la otra crea una red controlada. La misión de este módulo SCRA (3) es servir de frontera entre el tráfico que llega de internet con destino a los dispositivos convergentes situados en la red controlada y validar los accesos de forma SCOC. El módulo SCRA (3) le aporta a la red controlada funcionalidades básicas (por ejemplo, DHCP, DNS, entre otros) y un conjunto de funcionalidades de comunicación (3.1) que controlan el acceso con dos estrategias distintas. Los accesos con protocolos derivados de HTTP (HTML, XHR, SSE o WebSocket) se gestionan por un servidor proxy transparente para estos protocolos (3.2). Los accesos a dispositivos convergentes que utilicen protocolos propietarios se gestionan mediante un servidor de túneles que permite utilizar el software propietario para la visualización, configuración y programación de los dispositivos (3.3).

El servidor proxy utiliza una estrategia de validación distribuida (filtro de control de acceso 3.4 y 3.5), lo que le permite, en caso necesario, delegar las validaciones a los gestores de contenidos. El servicio proxy establece las comunicaciones con protocolos derivados de HTTP. Los accesos correspondientes se inician en el navegador y terminan en el dispositivo situado en la red controlada. El uso de aplicaciones propietarias hace necesario el servicio de túneles para establecer las comunicaciones entre las mismas y los dispositivos que controlan. Por razones de seguridad, los túneles se establecen desde un socket de entrada en el equipo

del cliente y un socket concreto en la red controlada. Por lo tanto, no es necesario habilitar reglas de control de tráfico en la electrónica de la red controlada.

Además de los servicios proxy y de túneles, el módulo SCRA (3) incluye un servicio de configuración automática de los equipos que se conectan a la red controlada (3.6). El servicio de configuración automática (3.6) trata de minimizar la intervención manual en la configuración de los dispositivos. Este servicio de configuración automática (3.6) está basado en: (a) la asignación automática de direcciones IP, que puede ser realizada por el servicio DHCP, incluido en el módulo SCRA (3); la resolución de nombres de host, incluida en el servicio DNS; (c) la localización automática de servicios de red, tales como dispositivos de impresión. Este servicio no está incluido en ninguno de los servicios indicados anteriormente.

El servicio de configuración automática (3.6) utiliza el protocolo mDNS (*multicast Domain Name System*), funciona por multidifusión, y permite conocer los servicios ofertados por los dispositivos que están conectados en la red controlada. Además, el servicio de configuración automática (3.6) aporta a los usuarios con capacidad de administración un servicio REST (*REpresentation State Transfer*) mediante el que son informados desde cualquier punto de internet de los dispositivos conectados a una red controlada remota, que incluso puede ser móvil. El servicio de configuración automática (3.6) interactúa con el servicio de túneles para permitir el acceso a los dispositivos conectados en cualquier red controlada de forma totalmente transparente.

Finalmente, el módulo SCRA (3) ofrece un servicio de acceso a perfiles de uso (denominado DIGEXLAB). Este servicio cuenta con una interfaz de configuración mediante la cual el usuario administrador puede realizar, entre otras, las siguientes funciones: (a) monitoriza desde internet los accesos activos a los distintos dispositivos de la red controlada y verifica las comunicaciones; (b) controla la alimentación eléctrica de estos dispositivos; (c) para e inicia a voluntad el servicio de túneles y el servicio de configuración automática (3.6); (d) cuenta con una base de datos de perfiles de usuario que se gestiona mediante una interfaz de comunicación; (e) habilita los módulos IIMS (6) autorizados para la validación diferida de perfiles de usuario; (f) gestiona los canales de comunicaciones necesarios para hacer accesibles de forma remota desde internet los distintos conjuntos de dispositivos o plantas conectados a la red controlada; (g) configura los parámetros asociados al servidor que constituye el módulo SCRA (3), como la IP pública, el conjunto de IPs del lado de la red controlada y los ficheros de claves para la encriptación de las comunicaciones; (h) configura los parámetros asociados a DIGEXLAB, como, al menos, los puntos de acceso a los distintos

dispositivos conectados a la red controlada o el identificador del servidor del módulo SCRA (3); y (i) controla el acceso colaborativo a los dispositivos conectados a la red controlada, y en general todos los parámetros de configuración, funcionamiento y seguridad del módulo SCRA (3).

Módulo CPD (4)

El módulo CPD (4) consiste es un microcomputador con sistema operativo con las mismas funciones que el módulo SCRA (3), pero que no dispone de dirección válida en internet, sino que está conectado en una red interna que dispone de acceso a internet. Para hacer visibles los dispositivos conectados a esa red, convirtiéndola de esta forma en una red controlada, el módulo CPD (4) cuenta con un software cliente para su comunicación con el módulo CPS (5). Este cliente solicita la publicación en la nube de los accesos al servicio proxy y al servicio de túneles.

El funcionamiento del módulo CPD es igual que el del SCRA descrito en el apartado anterior, excepto las funciones relacionadas con la publicación de los accesos (funciones g, h e i). Estas funciones las realiza, para los accesos controlados por un módulo CPD, el módulo CPS y su funcionamiento es el mismo que el descrito para el módulo SCRA. Es decir, la combinación de los módulos CPD+DPS equivale a un módulo SCRA con una capacidad menor de número de dispositivos a implementar acceso.

Módulo CPS (5)

El módulo CPS (5) consiste en un servidor conectado a internet con una dirección pública válida, que se encarga de crear los puntos de acceso a los servicios proxy y de túneles solicitados por el módulo CPD (4). Su estructura es la misma que la de los módulos anteriores, sin algunas de sus funcionalidades como el servicio de localización automática (3.6) o el servicio REST, que ya incorpora el módulo CPS (5).

Módulo IRS

En este módulo están registradas las instituciones que usan la invención y los perfiles de administración de cada una de ellas. Se encarga por tanto de la gestión de licencias registradas de la presente invención. Hace posible además que los recursos conectados a las redes controladas por varios módulos SCRA (3) puedan ser compartidos entre ellos y con otras instituciones diferentes.

Módulo LSRAC

El módulo LSRAC es un módulo software necesario para superar las limitaciones de ejecución impuestas por los navegadores, que confinan las comunicaciones a su ámbito de ejecución. Para el uso de las aplicaciones propietarias es necesario crear un túnel de comunicaciones entre el equipo del usuario y el dispositivo situado en una red controlada. El punto de entrada a ese túnel no se puede crear desde el navegador porque no sería accesible desde la aplicación propietaria. Para resolver este problema, el módulo LSRAC crea un servicio que se inicia al encenderse el computador del usuario, ejecutándose en segundo plano, y que crea un socket por el que escucha las órdenes de establecimiento de túneles que parten del módulo UI (2), ejecutado en el navegador. Este servicio es el encargado de establecer los sockets de entrada a los túneles que sean necesarios para conectar las aplicaciones propietarias desde el equipo del usuario con el dispositivo conectado a la red controlada. El módulo LSRAC pone además en marcha un servicio local de configuración automática (3.6). Por tanto este módulo aporta dos funcionalidades: la de comunicaciones descrita arriba y el servicio local de configuración automática.

El servicio de configuración automática

Como se ha descrito anteriormente, el servicio de configuración automática está incluido dentro del módulo SCRA (3), el módulo CPD (4) y el módulo LSRAC. Este servicio informa de los dispositivos que hay conectados a una red controlada y de los servicios de comunicaciones que oferta cada uno. Para que todos los dispositivos respondan al servicio de configuración automática, es necesario instalar un módulo LSRAC en el módulo CDAS (1) de cada dispositivo. Los equipos convergentes con software propietario, que no incluyen módulo CDAS (1), se dan de alta en el módulo SCRA (3) responsable de la red controlada a la que están conectados. Los usuarios administradores pueden configurar el servicio de configuración automática (Discovery) de una red controlada para que pueda ser consultado de forma remota. Eso se consigue mediante el cliente local de configuración automática.

Cliente local de configuración automática

El objetivo del servicio cliente local de configuración automática es facilitar la administración y el mantenimiento de una red controlada. Este servicio se instala en los módulos CDAS (1) de los distintos dispositivos conectados a la red y en los computadores de administración del sistema. La aplicación cliente de configuración automática, al ser activada, abre un interfaz de examinador de red. En ella se presenta una lista de todos los dispositivos o conjuntos de dispositivos que han respondido a la consulta de configuración automática en la red controlada del equipo que hace la consulta.

Los equipos que responden directamente son los que tienen instalados el servicio de configuración automática incluido en el módulo LSRAC, en el CPD (4) y en el CDAS (1). Para dar de alta en la red controlada a los equipos convergentes con software propietario, se utiliza la interfaz del módulo SCRA (3).

La interfaz del examinador de red dispone además de la posibilidad de realizar una consulta de configuración automática de forma remota mediante una petición al servicio REST. Para ello es necesario identificar el usuario y el perfil de uso que realiza la consulta. Desde esta interfaz se puede realizar una consulta remota a cualquier módulo SCRA (3) o CPD (4) en los que el usuario disponga de cuenta. Así, una vez configurado y seleccionado un módulo SCRA (3) o CPD (4) específico, se realiza la petición al servidor de configuración automática.

Así pues, accediendo a un dispositivo concreto se habilitarán los servicios de comunicaciones ofertados por el mismo, y accediendo sobre uno de ellos en concreto, el examinador de red solicitará la creación de los túneles necesarios para acceder al dispositivo de la red controlada y activar la aplicación asociada al servicio solicitado. Así por ejemplo si se accede a un dispositivo ModBus (que en ese caso estará habilitado), se accede al dispositivo a través de un monitor ModBus. De la misma forma, si el dispositivo seleccionado es una cámara IP se ejecuta un navegador a través del túnel correspondiente y se conecta con la cámara de la red controlada desde internet.

Gracias al sistema descrito, es posible proporcionar acceso SCOC desde internet a datos y dispositivos para su monitorización, control y configuración frente al acceso VPN a datos y frente al control remoto de encendido y apagado de dispositivos de los controladores IP. Los dispositivos a los que se accede pueden ser ya convergentes mediante aplicaciones suministradas por sus fabricantes o mediante módulos UI (2) desarrolladas con software libre y plataformas abiertas. En todo caso, la invención también hace convergentes los que no lo son mediante su módulo CDAS (1).

La invención configura el acceso desde internet a dispositivos individuales o a conjuntos de equipos como líneas de producción, plantas, etc. Además, la invención es escalable porque al servicio en la nube que se desarrolle se puede unir un número creciente de dispositivos e incluso puede proporcionar varios servicios en la nube. Esta nube puede ser privada de la empresa, un servicio IaaS (Infrastructure As A Service) como el ofertado por empresas como Amazon u otras públicas. Incluso la empresa se puede constituir como proveedor IaaS.

Finalmente, la invención permite la integración del acceso conjunto a todos los sistemas y dispositivos de una empresa o grupo de empresas en sus módulos IIMS (6). Del mismo modo, la invención permite registrar todas las instituciones que usan el sistema y los perfiles de administración de cada una de ellas. Este módulo hace posible que los recursos conectados a las redes controladas por varios módulos SCRA (3) puedan ser compartidos entre ellos y con otras instituciones diferentes.

REIVINDICACIONES

1.- Un sistema para el acceso a redes de datos seguras que siendo modular y escalable, es conectable con al menos una red segura conectada con una pluralidad de equipos físicos o plantas accesibles en red y una red pública no segura accesible a través de un módulo UI (2) ejecutable en un navegador web y que se **caracteriza** por que comprende, al menos, un módulo SCRA (3) configurado para controlar el acceso a una red segura con varios conjuntos de equipos físicos o plantas, todos ellos accesibles en red; que también puede sustituir un módulo SCRA (3) por un módulo CPD (4) conectado a una red segura con acceso a equipos físicos convergentes que constituyan un conjunto o planta; y configurado para solicitar la publicación en un módulo CPS (5) configurado para hacer visible desde la red pública no segura las solicitudes de publicación realizadas por el módulo o por los módulos CPD (4).

2.- El sistema de acuerdo con la reivindicación 1 que comprende al menos un módulo CDAS (1) configurado para hacer accesible en red los datos de un dispositivo físico.

3.- El sistema de acuerdo con una de las reivindicaciones 1 o 2 que comprende un módulo IIMS (6) para integrar el acceso a los dispositivos físicos o conjuntos de dispositivos en un gestor de contenidos externo.

4.- El sistema de acuerdo con la reivindicación 3 que comprende un módulo IRS que tiene almacenados todos los módulos IIMS (6) licenciados para su uso.

5.- El sistema de acuerdo con una cualquiera de las reivindicaciones anteriores que comprende un módulo LSRAC que es un módulo programable e instalado en un computador de usuario que elimina las limitaciones de comunicación impuestas por los navegadores.

6.- El sistema de acuerdo con una cualquiera de las reivindicaciones 2 a 5 donde el módulo CDAS (1) comprende: (a) una primera capa interfaz de red (1.1) que puede ser de tipo Ethernet o inalámbrica, mediante la cual el módulo CDAS (1) se conectará a la red; (b) una segunda capa de procesamiento y computación de datos (1.2) que aporta la torre de protocolos TCP/IP la capacidad de procesamiento necesaria para el mantenimiento de las comunicaciones por la red y las necesidades de procesamiento de datos; (c) una tercera capa de adquisición de datos (1.3) que proporciona la interfaz necesaria para que la capa de procesamiento y computación (1.2) reciba y envíe información; y (d) una cuarta capa de

adaptación de niveles (1.4) que ajusta los rangos de tensiones de las señales eléctricas de los sensores y actuadores a valores óptimos de entrada en la capa de adquisición (1.3).

7.- El sistema de acuerdo con una cualquiera de las reivindicaciones anteriores, donde el módulo SCRA (3) comprende un conjunto de funcionalidades de comunicación (3.1) que controlan el acceso con dos estrategias distintas; donde los accesos con protocolos derivados de HTTP se gestionan por un servidor proxy transparente para estos protocolos (3.2); y donde los accesos a los equipos físicos accesibles en red que utilicen protocolos propietarios se gestionan mediante un servidor de túneles que permite utilizar el software propietario para la visualización, configuración y programación de los dispositivos (3.3).

8.- El sistema de acuerdo con una cualquiera de las reivindicaciones anteriores donde el módulo SCRA (3) incluye un servicio de configuración automática de los equipos que se conectan a la red controlada (3.6); y donde el servicio de configuración automática (3.6) comprende: (a) la asignación automática de direcciones IP, que puede ser realizada por el servicio DHCP, incluido en el módulo SCRA (3); la resolución de nombres de host, incluida en el servicio DNS; y (c) la localización automática de servicios de red.

9.- El sistema de acuerdo con una cualquiera de las reivindicaciones anteriores, donde el módulo CPD (4) publicado en un módulo CPS (5) aporta un conjunto de funcionalidades de comunicación idénticas a las funcionalidades de comunicación (3.1) del módulo SCRA (3) que controlan el acceso con dos estrategias distintas; donde los accesos con protocolos derivados de HTTP se gestionan por un servidor proxy transparente para estos protocolos; y donde los accesos a los equipos físicos accesibles en red que utilicen protocolos propietarios se gestionan mediante un servidor de túneles que permite utilizar el software propietario para la visualización, configuración y programación de los dispositivos.

10.- El sistema de acuerdo con la reivindicación 7 y 8 donde el servicio de localización automática (3.6) utiliza el protocolo mDNS y funciona por multidifusión y aporta a los usuarios con capacidad de administración un servicio REST mediante el que son informados desde cualquier punto red pública no segura de los dispositivos conectados a una red segura; y donde el servicio de localización automática (3.6) interactúa con el servicio de túneles para permitir el acceso a los dispositivos conectados en cualquier red segura de forma totalmente transparente.

11.- El sistema de acuerdo con una cualquiera de las reivindicaciones anteriores donde

el servicio de localización automática está incluido dentro del módulo SCRA (3), el módulo CPD (4) y el módulo LSRAC.

12.- El sistema de acuerdo con la reivindicación 10 donde para que todos los dispositivos respondan al servicio de localización automática, es necesario instalar un módulo LSRAC en el módulo CDAS (1) de cada dispositivo.

13.- El sistema de acuerdo con la reivindicación 10 donde los equipos accesibles en red que no incluyen módulo CDAS (1) porque tienen un programa propietario, se dan de alta en el módulo SCRA (3) responsable de la red controlada a la que están conectados.

14.- El sistema de acuerdo con una cualquiera de las reivindicaciones anteriores que comprende un cliente local de localización automática para facilitar la administración y el mantenimiento de una red segura; y donde este servicio se instala en los módulos CDAS (1) de los distintos dispositivos conectados a la red y en los computadores de administración del sistema, de tal forma que la aplicación cliente de localización automática, al ser activada, abre una interfaz de examinador de red donde se presenta una lista de todos los dispositivos o conjuntos de dispositivos que han respondido a la consulta de localización automática en la red segura del equipo que hace la consulta.

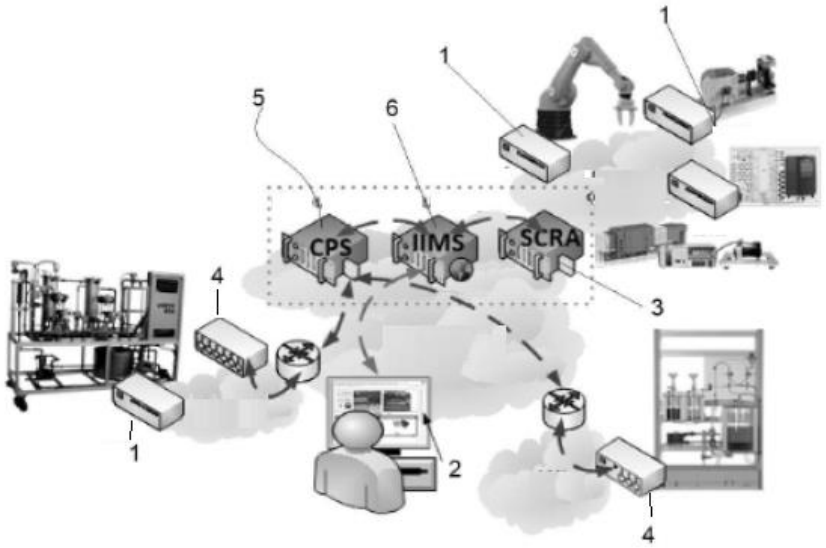

FIG.1

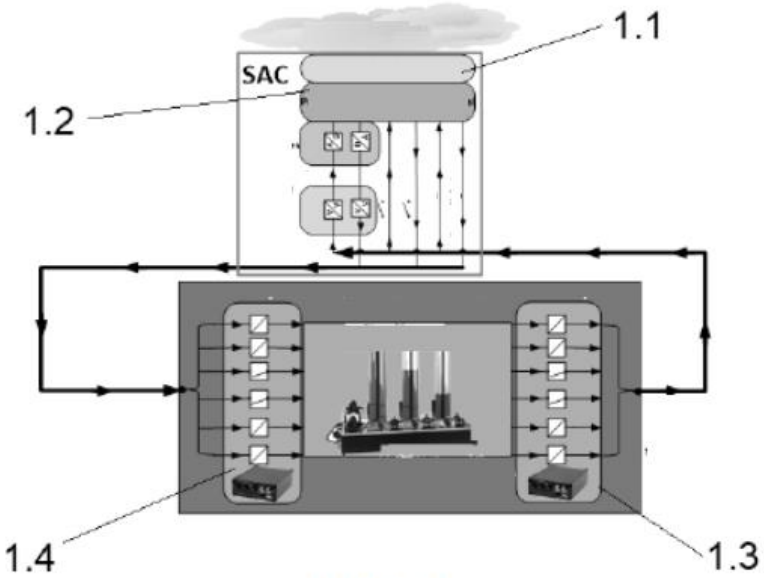

FIG.2

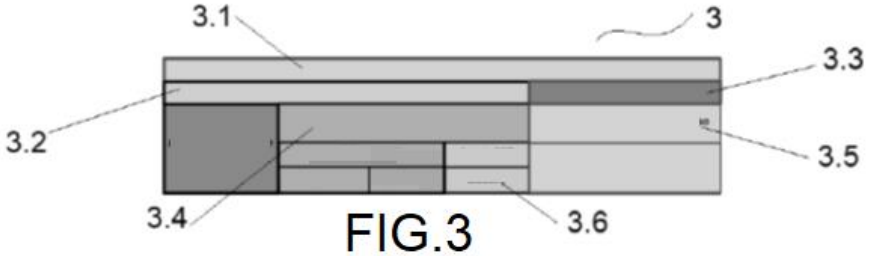

FIG.3