(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 979 143**

(51) Int. Cl.:

G06F 9/48 (2006.01)
G06F 9/50 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.06.2017 PCT/EP2017/064149**

(87) Fecha y número de publicación internacional: **14.12.2017 WO17212036**

(96) Fecha de presentación y número de la solicitud europea: **09.06.2017 E 17729114 (3)**

(97) Fecha y número de publicación de la concesión europea: **28.02.2024 EP 3469482**

(54) Título: **Procedimiento y sistema para proporcionar un servicio proxy en un sistema industrial**

(30) Prioridad:

10.06.2016 US 201662348770 P
24.06.2016 US 201662354683 P
26.06.2016 US 201662354799 P
11.10.2016 US 201662406932 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.09.2024

(73) Titular/es:

SCHNEIDER ELECTRIC INDUSTRIES SAS (100.0%)
35, rue Joseph Monier
92500 Rueil-Malmaison, FR

(72) Inventor/es:

HARRIMAN, MERRILL y
MEHMEDAGIC, ALEN

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Procedimiento y sistema para proporcionar un servicio proxy en un sistema industrial

CAMPO TÉCNICO

La invención se refiere a un procedimiento para proporcionar un servicio proxy en un sistema industrial. También se refiere a un sistema de proveedor de servicios proxy.

ANTECEDENTES

La automatización es el uso de dispositivos de control automático y diversas tecnologías para automatizar la supervisión, el funcionamiento y el control de procedimientos e instalaciones sin intervención humana significativa para lograr un rendimiento superior al control manual. Los sistemas de automatización conocidos para supervisar y controlar procedimientos e instalaciones suelen comprender varios dispositivos de automatización, tal como dispositivos de control o controladores (p. ej., controladores lógicos programables (PLC), controladores de automatización programables (PAC)), dispositivos de entrada/salida (dispositivos de E/S), dispositivos de campo (p. ej., sensores y actuadores), ordenadores personales (PC), interfaces hombre-máquina (HMI). Los sistemas de automatización conocidos utilizan tecnologías de comunicación (por ejemplo, Ethernet) para comunicarse. Una arquitectura de automatización define la disposición y las relaciones entre los dispositivos de automatización para satisfacer determinadas restricciones y requisitos.

Los sistemas de control industrial se componen de dispositivos con capacidades de procesamiento nulas o limitadas, o con servicios básicos o inexistentes. Por ejemplo, algunos dispositivos sólo admiten protocolos nativos (Modbus TCP, EtherNet/IP). Es posible que otros dispositivos no sean capaces de ofrecer páginas web de gama alta.

Sustituir estos dispositivos por dispositivos inteligentes compatibles con protocolos/servicios web de alto nivel puede resultar prohibitivo y no necesariamente óptimo.

El documento WO 2015/084628 A1 describe la interacción basada en la web con la automatización de edificios.

El documento US 2013/0332938 A1 se refiere al check-pointing no periódico para el reintento granular fino del trabajo en un entorno informático distribuido.

SUMARIO DE LA INVENCIÓN

En un aspecto, se desvela un procedimiento de acuerdo con la reivindicación 1 para proporcionar un servicio proxy en un sistema industrial. Realizaciones preferentes se detallan en las reivindicaciones dependientes.

En otro aspecto, se desvela un sistema industrial de acuerdo con la reivindicación 7.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A modo de ejemplo únicamente, las realizaciones de la presente divulgación se describirán con referencia al dibujo adjunto, en el que:

La **Figura 1** es un diagrama que ilustra una arquitectura simplificada de un sistema SDA.

La **Figura 2** es un diagrama de bloques que ilustra subsistemas de un sistema SDA de acuerdo con algunas realizaciones.

La **Figura 3** es un diagrama de bloques que ilustra un ejemplo de sistema en el que puede implementarse un procedimiento para proporcionar servicios proxy.

La **Figura 4** es un diagrama de flujo que ilustra un ejemplo de un procedimiento para proporcionar servicios proxy en el sistema de la **FIG. 3.**

La **Figura 5** es un diagrama de flujo que ilustra el ejemplo **FIG.4** con más detalle.

La **Figura 6** es un diagrama de flujo que ilustra un ejemplo para descomponer una solicitud de servicio de acuerdo con el ejemplo de la **FIG.5.**

La **Figura 7** es un diagrama de bloques que ilustra un ejemplo de un sistema para actualizar un dispositivo heredado de acuerdo con algunas realizaciones.

La **Figura 8** es un diagrama de bloques que ilustra un ejemplo de un sistema para mejorar la funcionalidad básica de un dispositivo físico o virtual de acuerdo con algunas realizaciones.

La **Figura 9** es un diagrama de bloques que ilustra un ejemplo de un sistema para mejorar un dispositivo heredado con protocolo incompatible de acuerdo con algunas realizaciones.

La **Figura 10** es un diagrama de bloques que ilustra un ejemplo de un sistema para mejorar servicios soportados por un dispositivo heredado de acuerdo con algunas realizaciones.

La **Figura 11** es un diagrama de bloques que ilustra un ejemplo de un sistema en el que se puede implementar un procedimiento para configurar conmutadores SDN para proporcionar servicios proxy.

DESCRIPCIÓN DETALLADA

Existe la necesidad de permitir que dispositivos básicos de baja capacidad participen en la habilitación/prestación de tareas y servicios de alto nivel. Esto puede lograrse introduciendo servicios de representación. Sin embargo, un entorno industrial es un sistema centrado en IP, lo que significa que los protocolos de comunicación dependen para su direccionamiento de una dirección IP específica. Por lo tanto, no se puede confiar en las soluciones proxy anteriores que implementan servicios de resolución de nombres, como DNS y WINS. Dado que los protocolos de comunicación industriales no permiten desviar un paquete o una solicitud de servicio a una dirección distinta de la especificada explícitamente como dirección de destino.

Para superar las desventajas anteriores, la presente divulgación describe un sistema proveedor de servicios proxy operable en un entorno industrial, un sistema de Automatización Definida por Software (SDA) que incluye una Red Definida por Software (SDN) que tiene un controlador de red. La tecnología SDA proporciona una arquitectura de referencia para diseñar y mantener un sistema de automatización altamente disponible, escalable y flexible. La tecnología SDA permite que sistemas de control y el software asociado se ejecuten dentro de una plataforma de niebla o una nube privada. Se pueden encontrar sistemas de control de diversos grados de complejidad en instalaciones de fabricación tradicionales, refinerías, submarinos, vehículos, túneles, sistemas de manipulación de equipajes, sistemas de gestión de la energía, sistemas de gestión de edificios, sistemas de control de aguas de inundación, sistemas de control de la red eléctrica y similares. Al trasladar todos los sistemas de control, o al menos una porción de ellos, a una plataforma de niebla o a una nube privada, y proporcionar una interfaz de software a los elementos del sistema de control, la tecnología SDA permite realizar las tareas de ingeniería de todo el ciclo de vida de la ingeniería de automatización, como el diseño, la programación, la configuración, la instalación, la operación, el mantenimiento, la evolución y el apagado, de una forma más sencilla, eficiente y rentable. La tecnología SDN permite separar la lógica de control de una red del hardware o dispositivo de red subyacente (por ejemplo, conmutadores, enrutadores) y centralizar lógicamente el control de la red, lo que permite configurar y reconfigurar de forma más sencilla elementos o dispositivos de red que incluyen conmutadores y enrutadores, así como cualquier nodo que asuma una función similar, sin tener que acceder a cada dispositivo físico. Por ejemplo, el controlador SDN centralizado lógicamente puede acceder a cada dispositivo de red mediante un conjunto de protocolos.

En varias realizaciones del sistema proveedor de servicios proxy, el controlador de red está configurado para redirigir el flujo de comunicación en función de criterios que incluyen: una dirección IP, un tipo de protocolo, un tipo de solicitud de servicio, un tipo de fuente, subfunciones de un protocolo, tipo de comandos opcionales, MIB SNMP adicionales, páginas web alternativas o aumentadas, contenido de datos. De esta manera, un dispositivo proxy se establece / configura para manejar la comunicación en nombre de un dispositivo diana al que realmente se dirigió. Dicho dispositivo proxy se denominará nodo de servicio proxy. O, más en general, denominado motor de servicio proxy, que comprende uno o más nodos de servicio proxy, distribuidos por el sistema SDA.

La presente divulgación también describe un procedimiento para proporcionar servicios proxy en un sistema industrial que incluye una red definida por software (SDN) que tiene un controlador de red.

Un sistema SDA puede ser configurado y probado durante las fases de diseño y puesta en marcha. Un sistema SDA también puede reconfigurarse cuando está en funcionamiento. En cualquiera de estas fases, un portal de automatización permite a un operador u otro usuario interactuar con el sistema de automatización.

A través del portal de automatización, un usuario puede optar por configurar los servicios que deben ser prestados por el sistema. Por ejemplo, para el control de una estación de bombeo puede ser conveniente tener en cuenta las precipitaciones, lo que podría obligar a aumentar la actividad de bombeo. Por lo tanto, es útil un servicio que proporcionara un gráfico de predicción de precipitaciones junto con la velocidad de bombeo de una o varias bombas, u otros datos del proceso.

Tales servicios pueden ser diseñados por un usuario configurando el nodo de servicio proxy para recoger o agregar datos y hacerlos disponibles como una petición de servicio. El portal de automatización creará un conjunto o esquema de reglas para gestionar la solicitud de servicio recién creada. A continuación, el controlador de red SDN actualizará su conjunto de reglas y organizará y dirigirá el tráfico teniendo en cuenta el conjunto de reglas actualizado. Además, este conjunto de reglas puede actualizarse, modificarse o sustituirse dinámicamente con el tiempo.

El motor de servicio proxy gestionará el tráfico dirigido al mismo, por ejemplo, procesando una solicitud o datos, o respondiendo a una solicitud, etc. El motor de servicio proxy puede recopilar datos de dispositivos distribuidos, agregar información y presentarla como una única respuesta de servicio.

Esto libera al dispositivo básico de soportar los protocolos de gama alta, reduciendo así su huella de firmware y hardware, y por lo tanto su coste, manteniendo las capacidades requeridas. Los dispositivos heredados podrían

parecer dotados de la última tecnología en servicios web siempre actualizados. Esto también puede tener un impacto positivo significativo en el rendimiento y el determinismo para el protocolo nativo del dispositivo básico, ya que el dispositivo puede estar muy optimizado para la funcionalidad de su sistema de control. Además, el mantenimiento y la actualización podrían ser más eficientes si los complejos servicios de gama alta estuvieran en una ubicación central en lugar de distribuidos entre numerosos productos de la red del cliente.

El paradigma proxy es contrario a la incorporación de hasta la última capacidad en los dispositivos para hacerlos lo más inteligentes posible. Uno de los problemas de este enfoque basado en dispositivos inteligentes es que repercute negativamente en el coste y el rendimiento, ya que los dispositivos tienen que ser capaces de soportar no sólo su función principal, sino también una plétora de otros servicios. Al final, al cliente sólo le importa que el servicio se preste en el sistema. La técnica de servicio proxy desvelada no consiste en fabricar dispositivos más inteligentes, sino en fabricar dispositivos dedicados más eficientes y utilizar la solución del sistema para aportar capacidades mucho más allá de lo que un dispositivo inteligente podría llegar a ofrecer. Una vez distribuidos y virtualizados los servicios, podrían emplear conceptos de big data para ofrecer capacidades nunca vistas en un sistema de control industrial.

La FIG. **1** es un diagrama que ilustra una arquitectura simplificada de un sistema SDA de acuerdo con algunas realizaciones. La arquitectura representa un servidor de niebla 105 vinculado a un software de sistema 140, y dispositivos inteligentes conectados 115A, 115B que están acoplados de manera comunicativa al servidor de niebla 105 y al software de sistema 224 a través de una red troncal de comunicaciones 110. La arquitectura también representa que al menos algunos dispositivos inteligentes conectados 115B y el servidor de niebla 105 pueden estar acoplados de manera comunicativa a una nube 150.

El servidor de niebla 105 está compuesto por una colección de recursos de control y recursos informáticos que están interconectados para crear un sistema lógicamente centralizado pero potencialmente distribuido físicamente para alojar los sistemas de automatización de una empresa. El "servidor de niebla" o la "plataforma de niebla", tal y como se utiliza en la presente memoria es un sistema de gestión de la nube (o subsistema localizado o sistema localizado) que se ha localizado en uno o más nodos informáticos y/o control. En otras palabras, el servidor de niebla 105 es una tecnología en la nube que se ha bajado al terreno o instalación local (de ahí el término "niebla") en forma de uno o más nodos informáticos y/o control para gestionar todo el sistema de automatización o una parte del mismo. El servidor de niebla 105 permite la virtualización al proporcionar una infraestructura de virtualización en la que se puede ejecutar y/o gestionar el sistema o sistemas de automatización. La infraestructura de virtualización incluye nodos informáticos que ejecutan huéspedes tal como máquinas virtuales, recipientes y/o metales desnudos (o imágenes de metal desnudo). Los huéspedes propiamente dichos pueden ejecutar invitados que incluyen aplicaciones y/o implementaciones de software de componentes físicos o unidades funcionales y un portal de automatización o software de sistema 140. Tal y como se utiliza en la presente memoria, la virtualización es la creación de una versión virtual de algo. Por ejemplo, un componente virtual o un componente virtualizado (por ejemplo, un PLC virtual, un conmutador virtual, virtualización de funciones de red (NFV)) representa una función que se ejecuta en un huésped que se ejecuta en un nodo informático. No tiene una existencia física por sí misma. El servidor de niebla 105 no tiene por qué estar localizado en una sala de control centralizada; los controladores, dispositivos y/o servidores 135 cercanos a los sensores y accionadores (por ejemplo, dispositivo IO, dispositivo integrado) también pueden considerarse bajo la gestión del servidor de niebla 105. En algunas realizaciones, el servidor de niebla 105 también puede agregar, almacenar y/o analizar datos, y/o informar de los datos o análisis a la nube 150. La nube 150 puede ser una nube empresarial (es decir, una nube privada), una nube pública o una nube híbrida. El software del sistema 140 proporciona un único punto de entrada para que un usuario final defina (por ejemplo, diseñar, proveer, configurar, y similares) el sistema de automatización. Una forma de definir el sistema de automatización es gestionando la distribución de las aplicaciones/funciones de la aplicación donde los usuarios quieren que se ejecuten.

Los dispositivos conectados inteligentes 115A, 115B (también productos conectados inteligentes) supervisan y/o controlan dispositivos, sensores y/o accionadores cercanos a los equipos/materias primas/entorno mediante la ejecución de aplicaciones/funciones de aplicación. En varias realizaciones, un dispositivo inteligente conectado tiene las siguientes características: (1) los componentes físicos y eléctricos, (2) el firmware o una parte "inteligente" incorporada, y (3) la conectividad y la interoperabilidad. En algunas realizaciones, un dispositivo inteligente conectado puede tener también un componente de ciberseguridad que puede operarse de forma remota, o a bordo.

Algunos dispositivos inteligentes conectados 115A pueden ejecutar aplicaciones o funciones de aplicación ("aplicaciones") localmente (por ejemplo, el bucle de regulación de velocidad/par de un variador de velocidad) porque tienen la capacidad de procesamiento para hacerlo. Esto significa que no es necesario ejecutar esas aplicaciones en otro lugar (por ejemplo, en un PC conectado, en un servidor o en otros dispositivos informáticos) para obtener datos que permitan realizar sus funciones. Esto tiene la ventaja de un tiempo de respuesta más rápido (es decir, menos latencia) y un ahorro en el ancho de banda de la red. Otra ventaja de la ejecución local o a bordo de las aplicaciones es que mejora la consistencia de los datos y la robustez de la arquitectura, ya que el dispositivo puede seguir produciendo información (por ejemplo, alarmas) o registrando datos aunque la red esté caída.

En algunas realizaciones, los dispositivos inteligentes conectados 115B pueden ser ejecutados total o parcialmente en uno o más servidores (por ejemplo, el servidor 135, el servidor de niebla 105). Por ejemplo, un dispositivo inteligente conectado 115B puede responder a señales remotas (por ejemplo, llamadas a procedimientos remotos, interfaz de programación de aplicaciones o llamadas API) como si una aplicación se ejecutara localmente, cuando en realidad la

aplicación se ejecuta remotamente, por ejemplo en el servidor de niebla 105. En algunas realizaciones, los dispositivos inteligentes conectados pueden capturar datos en tiempo real sobre su propio estado y el estado de su entorno (por ejemplo, los dispositivos siendo supervisados) y enviar dichos datos al servidor de niebla 105 y/o a una nube remota 150. En algunas realizaciones, los dispositivos inteligentes conectados 115A, 115B pueden transformar los datos capturados en tiempo real en información (por ejemplo, alarmas), almacenarlos y realizar análisis operativos sobre ellos. Los dispositivos inteligentes conectados 115A, 115B pueden entonces combinar las funciones de supervisión y control descritas anteriormente para optimizar su propio comportamiento y estado.

La red troncal de comunicaciones 110 facilita la interacción entre el servidor de niebla 105, el software del sistema 140 y los dispositivos inteligentes conectados 115A, 115B. La red troncal de comunicaciones (o la red troncal del Internet de las Cosas (IoT)/Internet Industrial de las Cosas (IIoT)) abarca un conjunto de arquitecturas de red y ladrillos de red que permiten las conexiones físicas y lógicas de los dispositivos inteligentes conectados 115A, 115B, el servidor de niebla 105 y cualquier otro componente que forme parte de la arquitectura SDA. Por ejemplo, los distintos equipos de una planta pueden conectarse entre sí y con el sistema de la empresa (por ejemplo, MES o ERP) utilizando tecnologías basadas en diversos estándares tal como: Ethernet, TCP/IP, web y/o tecnologías de software. La red troncal de comunicaciones 226 en forma de red troncal global unificada de Ethernet Industrial puede proporcionar: un fácil acceso a los datos, desde la planta (OT) hasta las aplicaciones empresariales (IT), una forma flexible de definir diferentes tipos de arquitecturas de red (por ejemplo, estrellas, cadena tipo margarita, anillo) que se ajusten a las necesidades del cliente, una arquitectura robusta que pueda cumplir requisitos como la disponibilidad, la seguridad y el soporte de entornos difíciles y la información correcta a las personas adecuadas en el momento adecuado en un solo cable.

La red troncal de comunicaciones 110 incluye una infraestructura completa de Ethernet industrial que ofrece conmutadores, enrutadores y/o un sistema de cables para abordar las necesidades de todas las topologías. La red troncal de comunicación 110 también admite un conjunto de protocolos de conectividad basados en normas (por ejemplo, Modbus/TCP-IP, Ethernet IP, OPC UA, DHCP, FTP, SOAP, REST, etc.). La red troncal de comunicaciones 110 también puede soportar un conjunto de funciones web que ofrecen funciones como el diagnóstico, la supervisión y la configuración utilizando páginas web estándar y la arquitectura de referencia de integración de dispositivos que define los patrones, el ladrillo para integrar el grupo de dispositivos a los controladores a nivel de aplicación y a nivel de red para la configuración, el ajuste y el diagnóstico. En algunas realizaciones, los elementos de ciberseguridad pueden incorporarse a la arquitectura. La red troncal de comunicaciones 110 también se adhiere a un conjunto de reglas de arquitectura que estructuran la arquitectura a nivel de prestaciones (Calidad de Servicio o QoS), robustez (RSTP y PRP HSR para la redundancia) y seguridad (IEC61508). En algunas realizaciones, la red troncal de comunicaciones 110 también admite la integración de un conjunto de pasarelas para conectar a la red de equipos heredados (es decir, no Ethernet).

La red troncal de comunicaciones 110 puede utilizar múltiples protocolos para proporcionar múltiples servicios para satisfacer múltiples necesidades. En la tabla 1 se enumeran algunos ejemplos de necesidades de comunicación y protocolos adecuados.

Tabla 1 Servicios y Protocolos

Servicios	**Protocolo**
Dispositivo a dispositivo	Modbus/EtherNet/IP, DDS, OPC UA, pub/sub
Dispositivo a control	Modbus/Eip, NTP, DHCP, FTP
Dispositivo a control para tiempo real duro	SercosIII, Profinet IRT, EtherCat
Control entre pares	DDS, OPC UA, pub/sub
Control a sala de control	OPC, Modbus, TCP
A través de la arquitectura	Modbus/Eip, SNMP, SMTP, NTP, HTTP, FTP

Las redes de los sistemas existentes están muy segmentadas para permitir una comunicación garantizada o fiable. La red troncal de comunicaciones 110 en la arquitectura SDA puede superar los problemas de los sistemas existentes a través de las tecnologías de redes definidas por software (SDN) y/o redes sensibles al tiempo (TSN). La tecnología SDN puede aportar simplicidad y flexibilidad a estas redes, permitiendo la comunicación en y a través de diferentes capas dirigidas por políticas de red. La tecnología TSN añade un conjunto de capacidades a la Ethernet estándar para proporcionar capacidad en tiempo real e intercambios con garantía de tiempo en zonas o en toda la arquitectura. Además, la solución de ciberseguridad también puede integrarse y adaptarse a la arquitectura SDA.

Un sistema SDA comprende varios subsistemas que trabajan en conjunto para proporcionar una solución totalmente integrada para crear, gestionar y operar sistemas de automatización. La **Figura 2** es un diagrama de bloques que ilustra los subsistemas de un sistema SDA de acuerdo con algunas realizaciones. Un sistema SDA 100 en algunas realizaciones incluye un subsistema de servidor de niebla 205 ("servidor de niebla") que tiene un controlador de niebla o controladores de niebla redundantes 210, uno o más nodos informáticos 215 y almacenamiento 225. El sistema SDA 200 también incluye un subsistema de componentes de software 230. En otras realizaciones, el sistema SDA puede incluir además un subsistema de ciberseguridad ("CS") 250 que tiene un controlador de seguridad o controladores de seguridad redundantes 255, componentes de seguridad físicos y/o virtualizados 260 y un repositorio de políticas de seguridad que 265. En otras realizaciones, un sistema SDA 400 también puede incluir un subsistema de red 270 que tiene un controlador de red o controladores de red redundantes 290, una red física 280, componentes de red física 282, redes virtuales 220, componentes de red virtual 222 y un repositorio de políticas de red 285.

El servidor de niebla 205 proporciona un entorno de virtualización en el que se puede ejecutar y/o gestionar el sistema o sistemas de automatización. El servidor de niebla 205 comprende nodos informáticos 215 que proporcionan capacidades de procesamiento lógico y pueden alojar aplicaciones, bases de datos y similares con un alto nivel de elasticidad. Los ejemplos no limitantes de nodos informáticos incluyen: servidores, ordenadores personales, dispositivos de automatización incluyendo dispositivos inteligentes conectados y similares.

El controlador del servidor de niebla 210 utiliza un software de gestión del servidor de niebla para realizar sus funciones. El software de gestión del servidor de niebla puede basarse en un software de gestión de la nube como OpenStack. El software de gestión de la nube, como OpenStack, en su forma estándar/listo para la venta, suele utilizarse en el mundo de las tecnologías de la información (TI) para la gestión de los centros de datos. Sin embargo, la gestión de los sistemas de automatización implica una serie de retos diferentes. Por ejemplo, algunos sistemas de automatización pueden ejecutar aplicaciones críticas para el tiempo y/o la seguridad que necesitan garantías deterministas con respecto al retraso, la fiabilidad y/u otros factores. La consideración de un sistema automatizado de corte de queso en el que un movimiento sincronizado de alta velocidad entre una hoja de cuchillo que corta un bloque de queso y el movimiento del bloque de queso es fundamental para producir rebanadas de queso de espesor uniforme. Si hay algún retraso en el procesamiento o en la red, puede dar lugar a que las rebanadas de queso tengan un espesor diferente, lo que supone un desperdicio y una pérdida de productividad.

El controlador del servidor de niebla 210 gestiona todos los aspectos del entorno de virtualización y el ciclo de vida completo de los nodos informáticos 215. Por ejemplo, el servidor de niebla 205 puede levantar y retirar huéspedes como máquinas virtuales, recipientes o metales desnudos en nodos informáticos, y crear y destruir componentes virtualizados 245 y redes virtuales 220. Un componente/elemento/instancia virtualizado 245, tal y como se utiliza en la presente memoria, es un equivalente lógico de un dispositivo físico o una parte del dispositivo físico que representa, implementado como una entidad de software para ejecutarse dentro del servidor de niebla 205. Los componentes virtualizados 245 también pueden incluir componentes de software tal como aplicaciones y/o funciones de aplicación en un huésped (por ejemplo, una máquina virtual configurada con una aplicación es un componente/elemento/instancia virtualizado).

El controlador del servidor de niebla 210 puede proporcionar alta disponibilidad (HA) a través de la redundancia del controlador y la gestión de los fallos de los nodos informáticos. El controlador también puede gestionar la puesta en marcha, el apagado y la aplicación de parches de los distintos nodos informáticos. En algunas realizaciones, la plataforma de servidor de niebla puede proporcionar soporte para la alta disponibilidad de los componentes virtualizados. En algunas realizaciones, el servidor de niebla 205 puede incluir un nodo de almacenamiento o almacén de datos 225. El almacenamiento 225 puede almacenar imágenes virtuales, volúmenes (es decir, el disco duro de una imagen instada), aplicaciones y procedimientos de datos, y similares.

El subsistema de componentes de software 230 puede incluir componentes virtualizados 245 que se alojan en el ecosistema de virtualización del servidor de niebla 205. El subsistema de componentes de software 230 también puede incluir instancias virtualizadas de software 235 que se ejecutan dentro del entorno de virtualización (por ejemplo, software de programación, configuración y/o gestión (por ejemplo, Unity, SoMachine, SCADA) que se utilizan para programar, configurar, gestionar o establecer una interfaz de otro modo con los dispositivos de automatización. En algunas realizaciones, el subsistema de componentes de software 230 también puede incluir un software de sistema 240 (también llamado portal de automatización) que proporciona una interfaz única para gestionar la topología, el inventario, la configuración, la programación, el control y/o el diagnóstico de los dispositivos de automatización y/o del sistema de automatización en su conjunto.

A través del software del sistema 240 los usuarios pueden acceder a varias aplicaciones para la definición y gestión del sistema en todas las fases del ciclo de vida. Por ejemplo, el software del sistema 240 puede ser utilizado para configurar y establecer parámetros en el equipo durante la fase de ingeniería y afinar, programar y/o diagnosticar el equipo durante la fase de mantenimiento. Algunas de las ventajas del software del sistema 240 incluyen la simplicidad y facilidad para los usuarios finales y la reducción de costes, dado que todos los aspectos de cualquier equipo de un sistema de automatización pueden gestionarse desde un único portal. Además de proporcionar un único punto de entrada a todo el sistema, el software del sistema 240 también presenta una interfaz de usuario consistente y una experiencia de usuario, que ayudan a reducir la inconsistencia y aumentar la eficiencia y la productividad.

El subsistema de Ciberseguridad (CS) 250 incluye un controlador CS asociado o controladores CS redundantes 255 y componentes de seguridad virtualizados y/o físicos 260. El subsistema de seguridad 250 proporciona una solución holística de ciberseguridad a través de políticas de seguridad y componentes de seguridad tal como sistemas de detección/protección de intrusos, cortafuegos virtualizados de nueva generación, sistemas de identificación y autoridad de certificados, y similares. El controlador CS 255 difunde las políticas de seguridad a los componentes virtualizados y/o físicos para garantizar que se establezcan las protecciones de seguridad necesarias. En algunas realizaciones, el subsistema CS también puede proporcionar servicios de política de seguridad y autenticación a otros componentes y subsistemas. Las políticas de seguridad del sistema CS 250 pueden almacenarse en un repositorio de políticas de seguridad 265 en algunas realizaciones.

El subsistema de red 270 incluye la infraestructura de red Ethernet para toda la solución del sistema SDA. El subsistema de red 270 es un subsistema de red SDN que tiene un controlador SDN o controladores SDN redundantes como el controlador de red 290. La red SDN proporciona la separación de la lógica de control de la red del hardware de red subyacente (por ejemplo, enrutadores, conmutadores) y la centralización lógica del control de la red a través del controlador SDN. Esto significa que el controlador SDN puede difundir políticas de red a través de la infraestructura de red (es decir, la red física 280 y los componentes de red física 282, así como las redes virtuales 220 y los componentes de red virtual 222) para controlar la conectividad, el ancho de banda y la latencia, los Acuerdos de Nivel de Servicio (SLA) (por ejemplo, con respecto a: tiempo de respuesta determinista/tiempo de transferencia), el control del flujo de tráfico, etc., y el hardware de red puede implementar esas políticas. Las políticas de red del subsistema de red 270 pueden almacenarse en un repositorio de políticas de red 285 en algunas realizaciones.

En algunas realizaciones, el subsistema de red 270 puede comprender una red de radio de malla. En una red de radio en malla, cada nodo puede conectarse con al menos otros dos nodos y los datos pasan de un nodo a otro en un procedimiento denominado "salto". Dado que los propios nodos hacen de enrutadores, las redes de malla de radio no suelen necesitar enrutadores designados. Sin embargo, algunas redes de radio de malla incluyen uno o más enrutadores de malla junto con los nodos de malla para retransmitir el tráfico en nombre de otros enrutadores de malla y/o nodos de malla. En algunas realizaciones, el subsistema de red 270 puede comprender circuitos virtuales en una red híbrida o de malla de radiofrecuencia (RF) de alta velocidad con comunicación facilitada únicamente por los transceptores de radio de los nodos, sin ningún dispositivo externo. Así, en algunas realizaciones, la configuración de los elementos de red del subsistema de red o de la infraestructura de red puede incluir la configuración de los nodos de malla y/o de los enrutadores de malla (por ejemplo, los enrutadores de malla habilitados para OpenFlow) en la red de radio de malla.

En algunos ejemplos no cubiertos por las reivindicaciones, el subsistema de red 270 puede ser un subsistema de Red Sensible al Tiempo (TSN) que tiene un controlador TSN como el controlador de red 290 y una infraestructura TSN. El subsistema de red TSN garantiza que los datos de misión crítica y sensibles al tiempo se transfieran/compartan de acuerdo con el tiempo máximo de transferencia determinista predefinido y con alta fiabilidad. Normalmente, la infraestructura TSN incluye componentes de red aptos para TSN. Cabe destacar que en algunas realizaciones, el subsistema de red 270 puede comprender redes SDN y TSN (y por tanto controladores SDN y TSN y componentes SDN y TSN). En varias realizaciones, el controlador de red 290 puede ser un controlador de red virtual de servidor de niebla nativo, un controlador de sistema de gestión de red tradicional, un controlador SDN, un controlador TSN, y/o cualquier combinación de los mismos. La invención define un sistema que comprende un controlador SDN. Las realizaciones que no incluyen un controlador SDN no entran en el ámbito de aplicación de las reivindicaciones.

Las funciones de los subsistemas de la solución SDA se complementan entre sí para proporcionar una solución totalmente integrada. Específicamente, el servidor de niebla 205 puede establecer una interfaz con cada uno de estos subsistemas a través del alojamiento de elementos virtualizados del subsistema y/o a través de las funciones de control del subsistema.

Refiriéndose a la FIG. 3, se muestra un ejemplo de sistema de acuerdo con algunas realizaciones. El sistema 300 incluye una herramienta de aplicación 302, una red definida por software (SDN) 304 que tiene un nodo controlador de red 390, un motor de servicio proxy 306 que comprende nodos de servicio proxy 306a - 306n, dispositivos físicos308a - 308m y dispositivos virtuales 312a - 312p.

La herramienta de aplicación 302 permite a un operador u otro usuario interactuar con el -sistema 300 y permite controlar y configurar el sistema 300. La herramienta de aplicación 302 puede formar parte o estar disponible a través de un portal de automatización o software de sistema 240. El nodo controlador de red 390 orquesta, configura y proporciona comunicación dentro del sistema 300 entre los diversos dispositivos y componentes a través de la Red Definida por Software 304.

Varios dispositivos físicos 308a - 308m pueden estar presentes en el sistema 300, dependiendo del tipo de máquina o planta que se automatice / opere. Del mismo modo, el sistema puede emplear varios dispositivos virtuales 312a - 312p que ejecutan una o más funciones de automatización en hosts que se ejecutan en nodos de computación en el servidor de niebla 305. El motor de servicio proxy 306 comprende uno o más nodos de servicio proxy 306a - 306n, de los cuales cada uno es direccionable por el nodo controlador de red 390. En varias realizaciones, el motor de servicio proxy 306 puede residir en el servidor de niebla 305. En otras realizaciones, puede residir en un recurso informático independiente, un nodo de computación, un PLC u otro dispositivo de control, o cualquier otro recurso que proporcione

capacidades de procesamiento. Además, el motor del servicio proxy puede estar distribuido en cualquiera de los elementos mencionados.

Refiriéndose a la FIG. 4, se ilustra un ejemplo de procedimiento para proporcionar un servicio proxy. El procedimiento se explicará haciendo referencia al ejemplo del sistema 300 de la FIG. 3. Desde la herramienta de aplicación 302 se solicita un servicio 402. El nodo controlador de red 390 dirige 404 la solicitud de servicio entrante a al menos un nodo de servicio proxy 306a - 306n. Este direccionamiento 404 de la solicitud de servicio se basa en un conjunto de reglas. El al menos un nodo de servicio proxy 306a - 306n procesa 406 la solicitud de servicio y entrega 408 el servicio solicitado (es decir, entrega respuesta a la solicitud de servicio).

Las reglas presentes en el conjunto de reglas pueden ser establecidas de antemano por la herramienta de aplicación y/o pueden ser reconfiguradas durante la operación. El conjunto de reglas incluye direcciones de destino para dispositivos de automatización físicos (por ejemplo, dispositivos físicos 308a-m), dispositivos de automatización virtuales (por ejemplo, dispositivo virtual 312a-p) y nodos de servicio proxy (por ejemplo, nodos de servicio proxy 306a-n). El conjunto de reglas incluye además asociaciones de criterios predeterminados y cada una de las direcciones de destino. Por lo tanto, un criterio o una combinación de varios criterios juntos puede asociarse a una dirección de destino particular. Los criterios predeterminados incluyen: una dirección IP, el contenido del paquete, el contenido del mensaje, un tipo de protocolo, un tipo de solicitud de servicio, un tipo de dispositivo, un tipo de fuente, subfunciones de un protocolo, tipo de comandos opcionales, MIB SNMP adicionales, páginas web alternativas o aumentadas y contenido de datos. Los comandos opcionales serían comandos disponibles, por ejemplo, dentro de un protocolo, pero no necesariamente compatibles con un dispositivo heredado.

De esta manera, la solicitud de servicio sigue siendo dirigida al dispositivo diana, pero el flujo de comunicación es redirigido (por ejemplo, por el controlador de red 390) basado en uno o más de los criterios predeterminados. Esto permite que la solicitud sea atendida en nombre del dispositivo diana. En consecuencia, podría crearse un motor de servicios proxy, es decir, una colección de proxies de servicios de gama alta centralizados lógicamente, para proporcionar capacidades en toda la red para diversos servicios.

Por referencia a la FIG. 5, el procedimiento de la FIG. 4 se ilustra con más detalle. En este caso, dirigir 402 la solicitud de servicio comprende determinar 504 una dirección de destino de acuerdo con el conjunto de reglas y enrutar 506 la solicitud de servicio a la dirección de destino determinada.

El procedimiento ilustrado en la FIG. 5 muestra con más detalle que el procesamiento 404 de la solicitud de servicio puede incluir la descomposición o deconstrucción 508 de la solicitud de servicio, la agregación 510 de los resultados necesarios para responder a la solicitud de servicio, y la compilación 512 de la respuesta de servicio solicitada. Como se muestra en la **FIG**. 6, descomponer 508 la solicitud de servicio puede incluir dividir 604 la solicitud de servicio en una o más subsolicitudes o tareas a ser manejadas por los nodos de servicio proxy, y/o uno o más dispositivos de automatización físicos, y/o uno o más dispositivos de automatización virtuales. La solicitud de servicio puede indicar la presencia de tareas que pueden tratarse por separado, por ejemplo, cuando éstas han sido seleccionadas por un operador a través de la herramienta de aplicación a partir de una lista de tareas disponibles en el sistema SDA para prestar un servicio combinado. Además, o cuando dicha indicación no está presente, el motor de servicio proxy puede estar configurado para identificar las tareas requeridas para el servicio solicitado. Para ello, la descomposición 508 de la solicitud de servicio puede incluir además la identificación 602 de las tareas enumeradas en un conjunto de configuración de servicio.

Con la solicitud de servicio dividida 604 en subsolicitudes o tareas, estas tareas pueden ser distribuidas 606 para su posterior procesamiento por dispositivos físicos y virtuales dedicados particulares o por el propio nodo de servicio proxy. Por distribución se entiende el proceso de asignar o atribuir cada tarea particular a su objetivo asociado para el procesamiento: dispositivo físico / virtual o nodo de servicio proxy. Si las tareas se distribuyen a dispositivos físicos o virtuales, el nodo de servicio proxy enrutará 608 estas tareas a los dispositivos de destino.

En algunas realizaciones, un conjunto de configuración de servicio puede listar tareas para procesar paquetes o más en el flujo de comunicación de procesamiento general, para agregar datos de diagnóstico, y / o para responder a la solicitud de servicios. Puede incluir además el reenvío de paquetes con dirección IP a un dispositivo de automatización de destino identificado por la dirección IP, para compilar una respuesta de servicio solicitada, para entregar resultados de un servicio compilado, y/o para rastrear una identidad u ontología del al menos un dispositivo de automatización. El conjunto de configuración del servicio puede ser almacenado y mantenido por el motor de servicio proxy 306 y accesible a través de la herramienta de aplicación 302. O puede almacenarse y mantenerse en cualquier otra ubicación adecuada, como la herramienta de aplicación 302 o el nodo controlador de red 390.

La herramienta de aplicación 302 puede tener un catálogo de servicios disponibles, o ser capaz de recuperar una lista de servicios disponibles. Un operador puede elegir servicios de una lista de servicios disponibles para crear servicios personalizados. Del mismo modo, la herramienta de aplicación 302 también puede acceder a un catálogo de tareas o subpeticiones disponibles a partir de las cuales un operador puede construir uno o más servicios personalizados. La Red Definida por Software 304, incluyendo el nodo controlador de red 390, orquestará entonces la configuración de los servicios personalizados.

Ejemplo 1 - Actualización de un dispositivo heredado con una función obsoleta

Como un ejemplo de aplicación del procedimiento descrito, un dispositivo heredado que requiera una actualización de firmware para, por ejemplo, abordar un riesgo de seguridad o cualquier otra funcionalidad, podría "actualizarse virtualmente". Por referencia a la FIG. 7, el nodo de servicio proxy 706 puede estar configurado para dirigir la actualización de firmware o el parche de software a un dispositivo virtual 712. El dispositivo virtual 712, que podría ejecutarse en un nodo de computación independiente en el servidor de niebla 705 o dentro del motor de servicio proxy 706, se instalaría entonces, en lugar del dispositivo heredado 708, con la actualización de firmware o el parche de software. Una vez instalado, todas las comunicaciones y/o solicitudes de servicio destinadas al dispositivo heredado 708 se dirigirían al dispositivo virtual 712. Esto permite actualizar virtualmente dispositivos heredados 708 que no serían capaces de ejecutar el firmware actualizado e incluso permitiría actualizar virtualmente dispositivos heredados que no fueron diseñados para obtener actualizaciones. Otro ejemplo de actualización funcional puede ampliarse a los servicios web, como el uso de un logotipo de empresa diferente en un sitio web presentado por el dispositivo heredado. Otros ejemplos de actualizaciones funcionales pueden incluir mejoras del aspecto de los servicios prestados por un dispositivo heredado, como por ejemplo una interfaz gráfica de usuario (GUI), la marca u otros elementos de interfaz presentados a un operador.

Ejemplo 2 - Mejora de un dispositivo físico o virtual básico

Como otro ejemplo de aplicación del procedimiento desvelado, puede parecer que las páginas web de gama alta son proporcionadas por el dispositivo físico o virtual más básico, mientras que en realidad la solicitud de servicio fue interceptada y redirigida por un controlador SDN a un servicio proxy virtual. El servicio proxy utilizaría los protocolos nativos del dispositivo diana real (Modbus TCP, EtherNet/IP, BacNet o similares) para recopilar datos del dispositivo con el fin de construir la respuesta del servicio web solicitado. Por ejemplo, por referencia a la FIG. 8, una estación de carga de baterías que carga una batería a través de un panel solar equipado con un medidor de energía básico 808, como un medidor de intensidad luminosa, sólo podría proporcionar el valor actual de la intensidad luminosa. A continuación, un nodo de servicio proxy 806 añade los datos de intensidad luminosa a lo largo del tiempo y un servicio web virtual 812 conectado a la nube 816 ofrece previsiones meteorológicas locales. Estos flujos de comunicación puede entonces combinarse para no sólo predecir cuándo la batería estará completamente cargada con base en el valor instantáneo de intensidad luminosa, sino tener en cuenta la previsión meteorológica para predecir el ritmo de carga y una predicción mejorada de cuándo la batería estará completamente cargada.

Por lo tanto, una petición de servicio de un cliente remoto 814 para una indicación detallada de capacidad completa será dirigida por el nodo controlador de red 890 al nodo de servicio proxy 806. El nodo de servicio proxy 806 dividirá la solicitud de servicio en subsolicitudes o tareas para recuperar los datos agregados del medidor de intensidad luminosa 808 y para recuperar la previsión meteorológica del servicio web 812. Las respuestas de estas tareas distribuidas se compilan y entregan como un único servicio o respuesta al solicitante del servicio.

Como otro ejemplo de mejora de un dispositivo físico básico, puede habilitarse el soporte de consultas de diagnóstico. Algunos dispositivos heredados no admiten un complemento completo de información de diagnóstico de red. Sin embargo, el controlador de red y/o los conmutadores SDN de la red pueden obtener gran parte de esta información observando el tráfico hacia y/o desde el dispositivo. Por ejemplo, dado que el controlador de red participaría en la creación y eliminación de conexiones de red, como una conexión Modbus TCP, a un dispositivo, el controlador de red puede rastrear la existencia de estas conexiones en nombre del dispositivo heredado. Entonces, un servicio proxy SNMP, u otro servicio de diagnóstico similar, podría responder, en nombre del dispositivo heredado, a las consultas de las conexiones Modbus TCP existentes recogiendo la información del controlador de red. Aunque al usuario le parezca que el dispositivo admite el listado de las conexiones Modbus TCP actuales, en realidad, el dispositivo físico no participaría en absoluto en la consulta. La consulta original del cliente de diagnóstico es dirigida por el controlador de red al servicio SNMP Proxy. El servicio SNMP Proxy interroga los datos de diagnóstico del controlador de red para obtener la lista de conexiones actuales al dispositivo heredado. A continuación, el servicio SNMP Proxy responde a la consulta con información detallada sobre la conexión. No es necesario que el dispositivo físico participe en modo alguno en la transacción de consulta de diagnóstico.

Ejemplo 3 - Direccionamiento de un dispositivo inexistente a través de su dirección IP

Ampliando aún más el concepto de virtualización distribuida, el dispositivo diana podría ser en realidad una distribución de servicios repartidos entre múltiples entidades virtuales; el dispositivo real no existe en un único lugar, sino en múltiples lugares dentro del sistema de virtualización (es decir, el servidor de niebla) y/o la nube. En efecto, lo que desde un punto de vista externo parece un dispositivo con un determinado conjunto de capacidades es en realidad un enigma. Los servicios del "dispositivo diana" son una colección abstracta de servicios independientes que, en conjunto, presentan un determinado comportamiento deseado. Por ejemplo, un servicio SysLog que registre eventos como el inicio/cierre de sesión, cambios en el procesamiento operativo, cambios de estado como alta/baja velocidad, apagado, errores, etc. Además, podrían utilizarse técnicas de enjambre para dirigir el comportamiento de la colección de servicios independientes con el fin de proporcionar una capacidad única. Por ejemplo, se puede ofrecer un servicio de gestión de la energía que permita apagar las funciones no críticas.

Ejemplo 4 - Mejora de un dispositivo heredado con un protocolo incompatible

Refiriéndose a la FIG. 9, se representa un sistema de ejemplo que incluye la herramienta de aplicación 914, el nodo controlador de red 990, el nodo de servicio proxy 906 y un dispositivo industrial heredado (por ejemplo, PLC) 912. El dispositivo PLC 912 sólo está equipado con una pila de protocolos para ModBus y no soporta IP / Ethernet. Para mejorar la comunicación con el dispositivo PLC 912, el nodo de servicio proxy 906 está configurado para incluir un registro ModBus. El nodo de servicio proxy 906 es ahora capaz de traducir cualquier entidad de dispositivo ModBus en una dirección de red IP / Ether, muy parecido a un servidor DNS regular para Ethernet /IP. De esta manera, la funcionalidad inherente del dispositivo PLC 912 se extiende más allá de sus capacidades básicas.

Ejemplo 5 - Rampa del motor

Como ejemplo de un servicio personalizado, un motor de accionamiento sólo capaz de ser operado de una manera particular, tal como el modo encendido/apagado, puede ser provisto de modos expandidos tal como, por ejemplo, rampa, mediante la construcción de un servicio personalizado basado en la funcionalidad básica. Esto puede lograrse, por ejemplo, diseñando un servicio que permita configurar un patrón de conmutación que encienda/apague el accionamiento del motor de tal manera que el accionamiento pueda acelerar o desacelerar de forma más controlada. Por lo tanto, mientras que el dispositivo heredado sólo soporta su modo de funcionamiento básico, el uso del servicio de nodo proxy permitiría añadir modos de funcionamiento adicionales al accionamiento del motor.

Refiriéndose a la FIG. 10, un PLC 1014 está dispuesto para controlar un accionamiento de motor heredado 1008. El accionamiento del motor 1008 puede controlarse mediante comandos para las siguientes funciones soportadas RUN, STOP y SET SPEED. Por lo tanto, el PLC 1014 puede solicitar (etapa 1) cualquiera de estas funciones básicas al accionamiento del motor 1008. Un controlador de red 1090, como parte de una SDN, dirigirá la solicitud (etapa 2) al accionamiento del motor 1008. Además, el PLC puede solicitar funciones mejoradas (etapa 3), que no son soportadas directamente por el accionamiento del motor 1008. Para ello, el controlador de red 1090 dirige (etapa 4) la solicitud de servicio mejorado a un motor de servicio Proxy 1006 que está configurado para proporcionar uno o más perfiles de accionamiento mejorados 1006c. El perfil de accionamiento mejorado 1006c está dispuesto para soportar un perfil de accionamiento particular que se construye mediante el uso del accionamiento de motor heredado 1008 soportado por los servicios RUN / STOP / SET SPEED. El perfil de accionamiento mejorado puede ser un perfil de accionamiento de velocidad de rampa, como una velocidad linealmente creciente o decreciente o una velocidad no linealmente creciente o decreciente, como por ejemplo una curva escalonada o conectada a trozos, o podría incluir cualquier otro perfil de accionamiento compuesto. El motor de servicio Proxy 1006 facilita la comunicación (etapa 5) entre el perfil de accionamiento mejorado 1006c y el accionamiento del motor 1008. Por lo tanto, la solicitud de servicio del PLC se dirige a través del controlador de red 1090 al motor de servicio proxy 1006 para permitir el soporte de servicios mejorados.

Aún por referencia a la FIG. 10, el motor de servicio proxy 1006 incluye como servicios proxy adicionales un Nuevo servidor web 1006a, un SysLog 1006b, y un Nodo de servicio proxy 1006N. El servicio proxy SysLog 1006b permite registrar los eventos que se producen en el motor de servicio proxy 1006 y en el accionamiento del motor 1008. El accionamiento a motor 1008a incluye un antiguo servidor web, que en este ejemplo sólo es capaz de mostrar el estado actual del accionamiento a motor: en marcha, parado o a la velocidad establecida. El nuevo servidor web 1006a permite aumentar el antiguo servidor web 1008a con, por ejemplo, el estado del accionamiento del motor de acuerdo con el perfil de accionamiento mejorado. Como por ejemplo, la instancia actual en el perfil de accionamiento, el progreso del perfil de accionamiento y una trayectoria de la velocidad pasada y futura del accionamiento del motor.

Ejemplo 6 - Configuración de dispositivos SDN para dirigir solicitudes de servicio

Refiriéndose a la FIG. 11, se muestra un ejemplo de sistema no incluido en el ámbito de las reivindicaciones, en el que puede implementarse otro ejemplo de procedimiento para prestar servicios de proxy. En este ejemplo, se explica con más detalle la forma en que el controlador de red organiza la dirección de las solicitudes de servicio. El sistema incluye un dispositivo de control o interfaz 1114, como una aplicación, cliente o PLC que puede estar dispuesto para controlar y/o interactuar con uno o más dispositivos (no mostrados) similar al ejemplo de la FIG. 10. El sistema incluye además un motor de servicio proxy 1106 que tiene nodos de servicio proxy 1106a-N dispuestos de manera similar al ejemplo de la FIG. 10. El controlador de red 1190 controla una serie de dispositivos SDN 1191 - 1195, como conmutadores, enrutadores, puertas de enlace, dentro de la Red Definida por Software 1104.

En este sistema, una solicitud de servicio es inicialmente enviada al controlador de red 1190. El controlador de red dirige la solicitud determinando el dispositivo diana y enruta la solicitud al dispositivo diana, por ejemplo, el Nuevo servidor web 1106a. Con el dispositivo diana y el enrutamiento hacia el mismo determinado para una solicitud en particular, el controlador de red puede actualizar el conjunto de reglas y configurar y/o programar uno o más de los dispositivos SDN para aplicar esa regla. En consecuencia, cuando se envía una nueva solicitud destinada al mismo dispositivo diana, la solicitud no necesita ser reenviada al controlador de red, sino que puede ser reenviada por los dispositivos SDN 1191 - 1195 al dispositivo diana directamente. Por lo tanto, un procedimiento para implementar servicios proxy puede incluir un controlador de red que configure dispositivos SDN para enrutar solicitudes de servicio.

Aunque la presente invención se ha descrito anteriormente con referencia a realizaciones específicas, no pretende limitarse a la forma específica expuesta en la presente memoria. Más bien, la invención está limitada únicamente por las reivindicaciones adjuntas y, otras realizaciones que las específicas anteriores son igualmente posibles dentro del ámbito de estas reivindicaciones adjuntas.

Además, aunque las realizaciones ejemplares se han descrito anteriormente en alguna combinación ejemplar de componentes y/o funciones, se debe apreciar que, las realizaciones alternativas pueden ser proporcionadas por diferentes combinaciones de miembros y/o funciones sin apartarse del ámbito de la presente divulgación. Además, se contempla específicamente que una característica particular descrita, ya sea individualmente o como parte de una realización, puede combinarse con otras características descritas individualmente, o partes de otras realizaciones.

REIVINDICACIONES

1. Procedimiento para proporcionar un servicio proxy en un sistema industrial (200) que comprende una red definida por software, SDN, (304) con un nodo controlador SDN (390), comprendiendo el procedimiento:

- proporcionar un motor de servicio proxy (306) que comprenda al menos un nodo de servicio proxy (306a), residiendo el motor de servicio proxy (306) en un entorno de virtualización (305) que se ejecuta en nodos de computación distribuidos (215);

- interceptar y redirigir, por el nodo controlador SDN (390), una solicitud de servicio entrante destinada a un dispositivo de automatización de destino (308a) al al menos un nodo de servicio proxy (306a) con base en un conjunto de reglas, la redirección implica la determinación de una dirección de destino de acuerdo con el conjunto de reglas y el enrutamiento de la solicitud de servicio a la dirección de destino determinada;

- procesar la solicitud de servicio por el al menos un nodo de servicio proxy (306a); y

- prestar el servicio solicitado;

en el que el conjunto de reglas comprende:

- direcciones diana para dispositivos de automatización físicos (308a), dispositivos de automatización virtuales (312a) y nodos de servicio proxy (306a); y

- asociaciones de criterios predeterminados y cada una de las direcciones de destino; y en las que los criterios predeterminados incluyen: una dirección IP, un tipo de protocolo, un tipo de solicitud de servicio, un tipo de fuente, subfunciones de un protocolo, tipo de comandos opcionales, MIB SNMP adicionales, páginas web alternativas o aumentadas y contenido de datos.

2. Procedimiento de acuerdo con la reivindicación 1, en el que el procesamiento de la solicitud de servicio incluye:

- descomponer la solicitud de servicio;

- agregar los resultados necesarios para la solicitud de servicios; y

- compilar el servicio solicitado.

3. Procedimiento de acuerdo con la reivindicación 2, en el que la descomposición de la solicitud de servicio comprende:

- dividir la solicitud de servicio en una o varias tareas parciales que serán gestionadas por:

el nodo de servicio proxy (306a); y/o

uno o varios dispositivos físicos de automatización (308a); y/o

uno o más dispositivos virtuales (312a).

4. Procedimiento de acuerdo con la reivindicación 2 o 3, en el que la descomposición de la solicitud de servicio comprende: identificar tareas parciales enumeradas en un conjunto de configuración de servicio.

5. Procedimiento de acuerdo con la reivindicación 4, en el que el conjunto de configuración de servicio comprende tareas parciales para al menos una de:

procesar flujo de comunicación;

agregar datos de diagnóstico;

responder a la solicitud de servicios;

reenviar el flujo de comunicación con dirección IP a un dispositivo de automatización de destino (308a) identificado por la dirección IP;

compilar un servicio solicitado;

entregar resultados de un servicio compilado;

rastrear identidad y/u ontología de un dispositivo de automatización (308a).

6. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además: el nodo controlador SDN (390) configurando uno o más dispositivos SDN (1191) para aplicar el conjunto de reglas.

7. Un sistema industrial (200), que comprende:

- una Red Definida por Software (304) con un nodo controlador SDN (390); y

- un motor de servicio proxy (306) que tiene al menos un nodo de servicio proxy (306a),

en el que el al menos un nodo de servicio proxy (306a) está dispuesto para ejecutar un procedimiento de prestación de un servicio proxy de acuerdo con una cualquiera de las reivindicaciones precedentes.

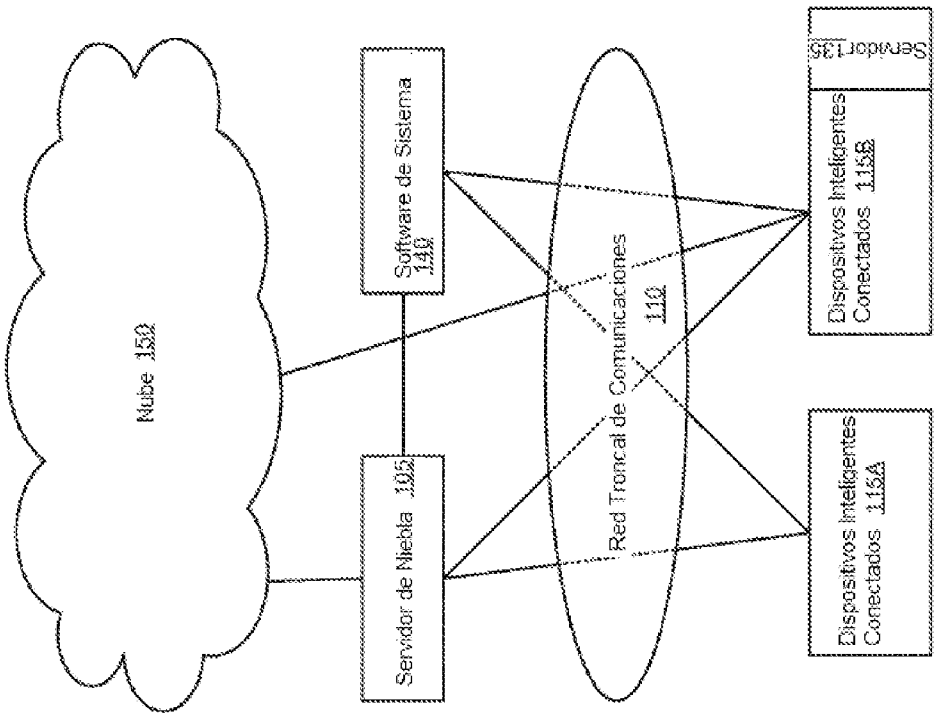
Nube 150
Software de Sistema 140
Servidor de Niebla 105
Red Troncal de Comunicaciones 110
Dispositivos Inteligentes Conectados 115B
Servidor 135
Dispositivos Inteligentes Conectados 115A

FIG. 1

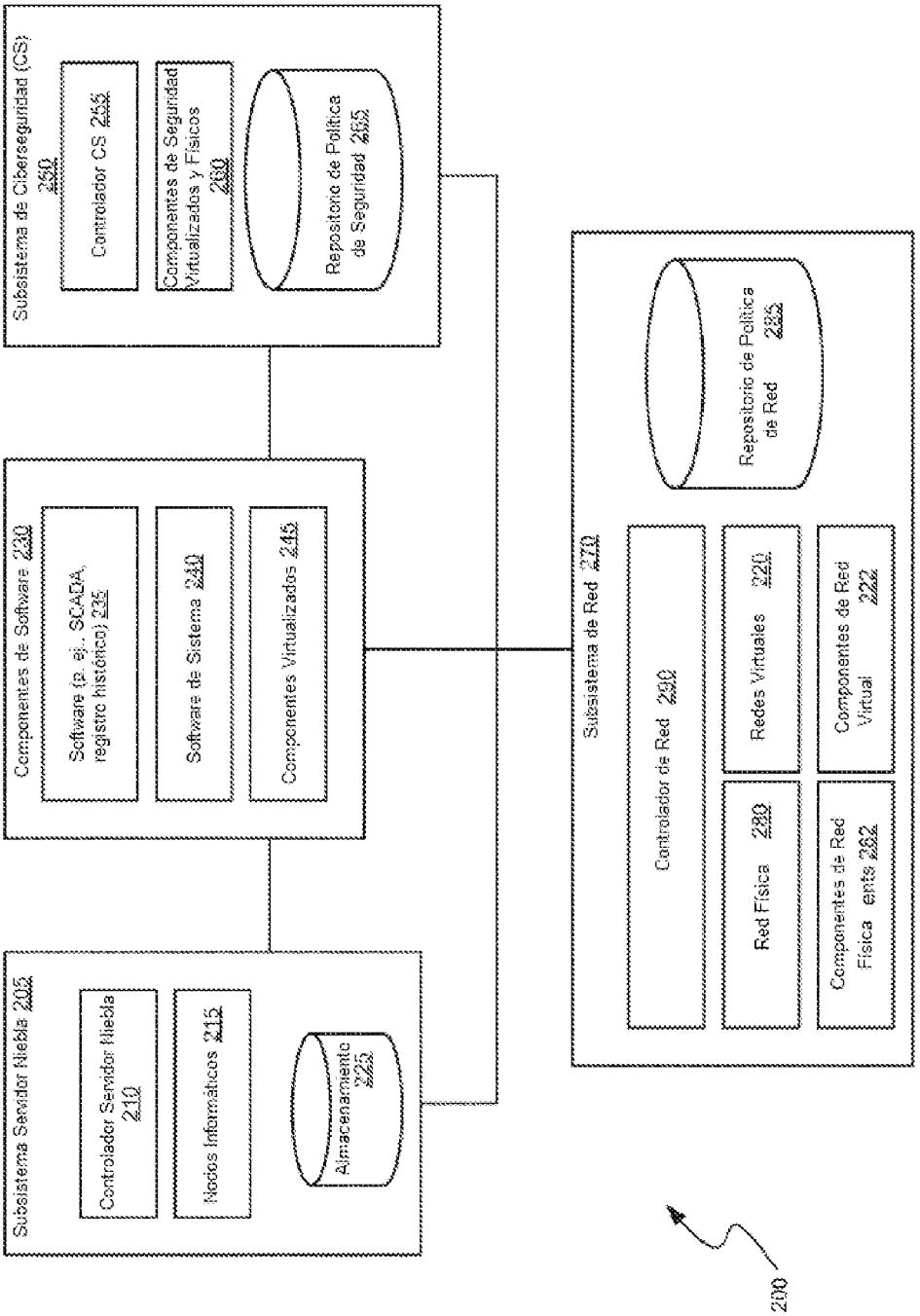
Subsistema de Ciberseguridad (CS) 250
Controlador CS 255
Componentes de Seguridad Virtualizados y Físicos 260
Repositorio de Política de Seguridad 265
Componentes de Software 230
Software (p. ej., SCADA, registro histórico) 235
Software de Sistema 240
Componentes Virtualizados 245
Subsistema Servidor Niebla 205
Controlador Servidor Niebla 210
Nodos Informáticos 215
Almacenamiento 225
Subsistema de Red 270
Repositorio de Política de Red 285
Controlador de Red 290
Redes Virtuales 220
Componentes de Red Virtual 222
Red Física 280
Componentes de Red Física ents 282
200

FIG. 2

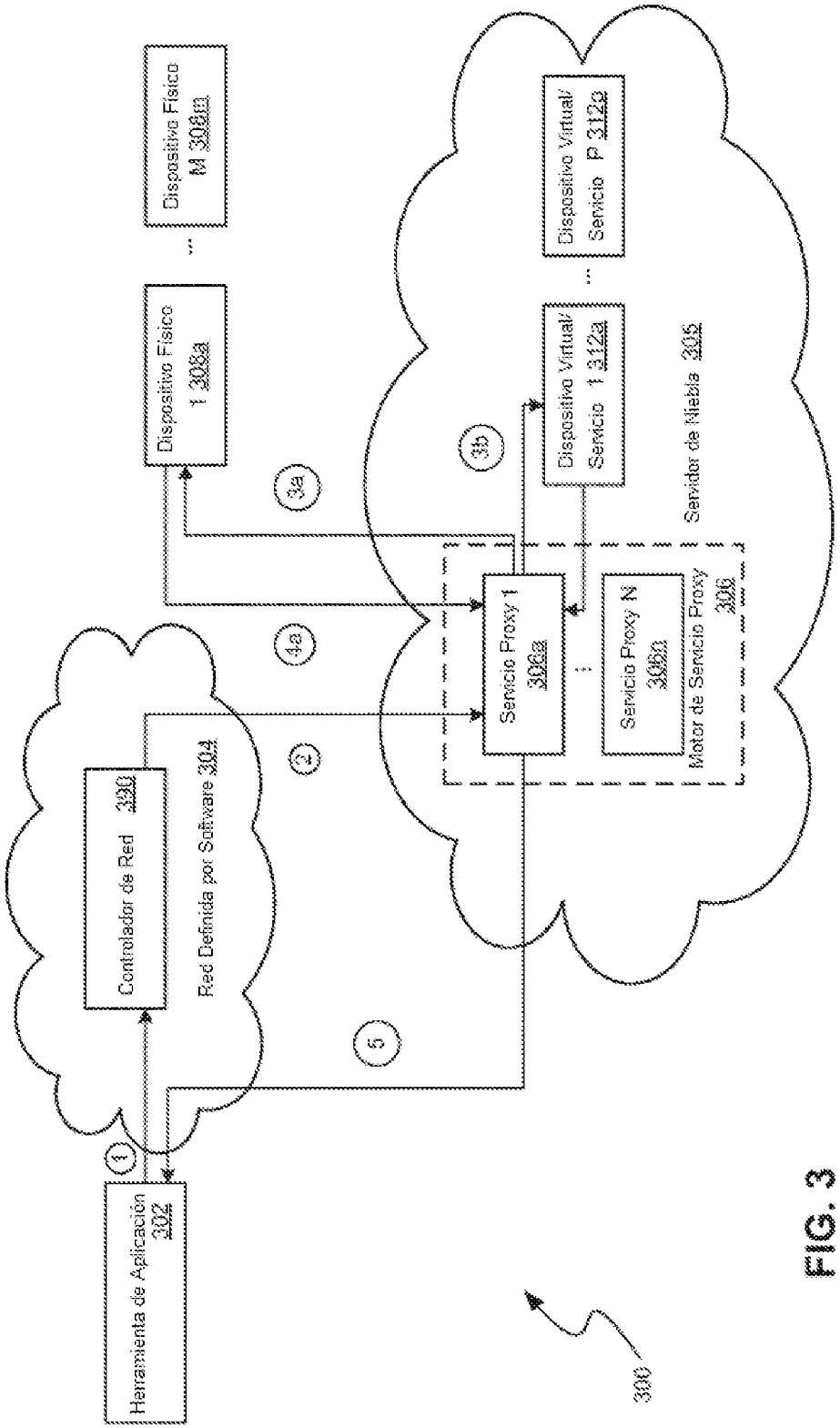
Herramienta de Aplicación 302
Controlador de Red 320
Red Definida por Software 304
Dispositivo Físico 1 308a
Dispositivo Físico M 308m
Servidor de Niebla 305
Servicio Proxy 1 306a
Servicio Proxy N 306n
Motor de Servicio Proxy 306
Dispositivo Virtual/ Servicio 1 312a
Dispositivo Virtual/ Servicio P 312p
1
2
3a
3b
4a
5
300

FIG. 3

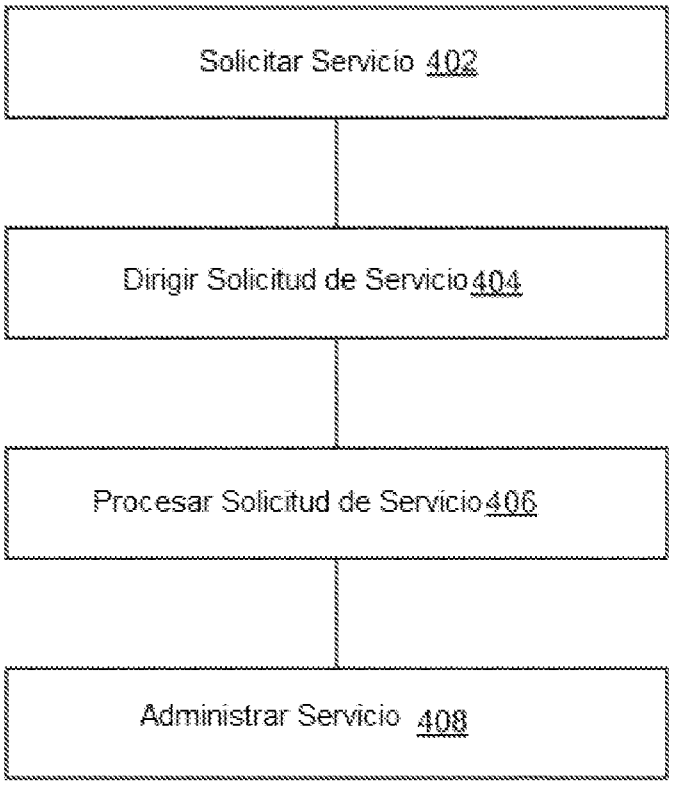
Solicitar Servicio 402
Dirigir Solicitud de Servicio 404
Procesar Solicitud de Servicio 406
Administrar Servicio 408

FIG. 4

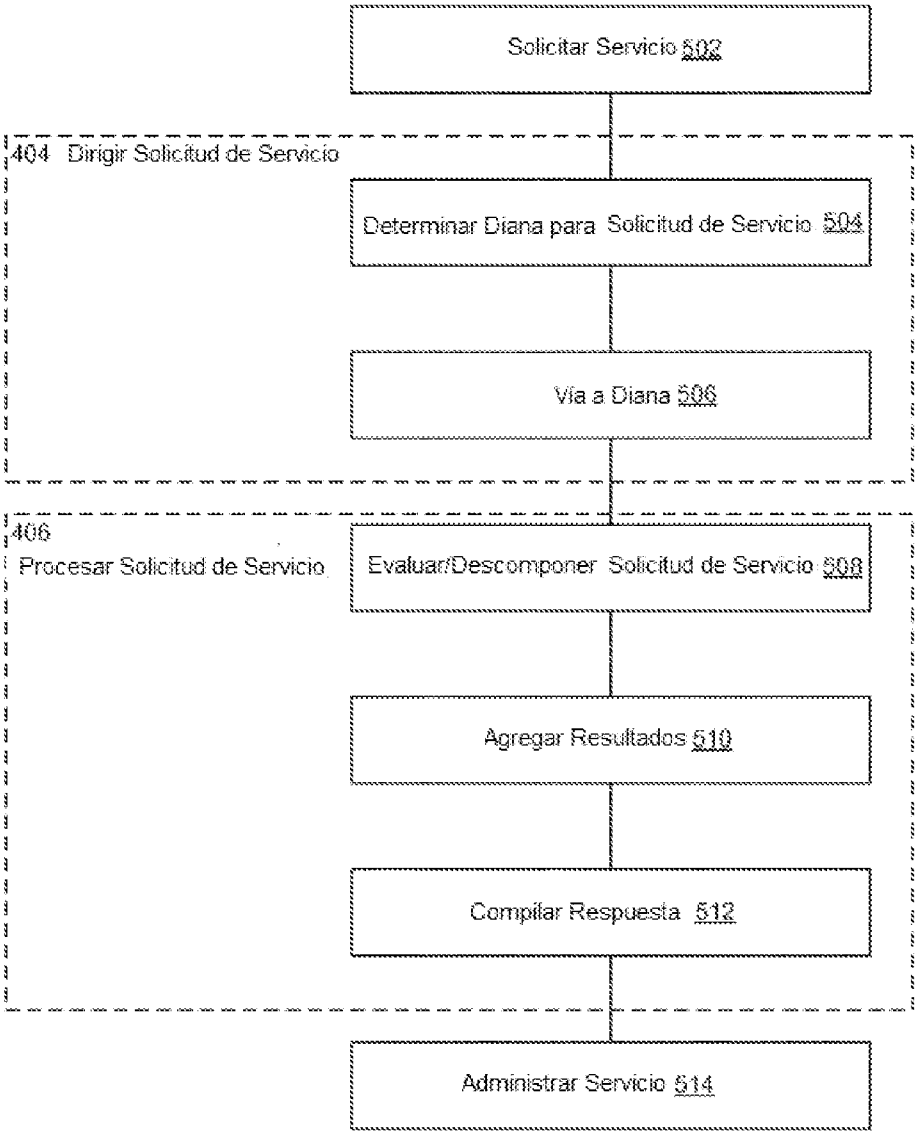
Solicitar Servicio 502
404 Dirigir Solicitud de Servicio
Determinar Diana para Solicitud de Servicio 504
Vía a Diana 506
406
Procesar Solicitud de Servicio
Evaluar/Descomponer Solicitud de Servicio 508
Agregar Resultados 510
Compilar Respuesta 512
Administrar Servicio 514

FIG. 5

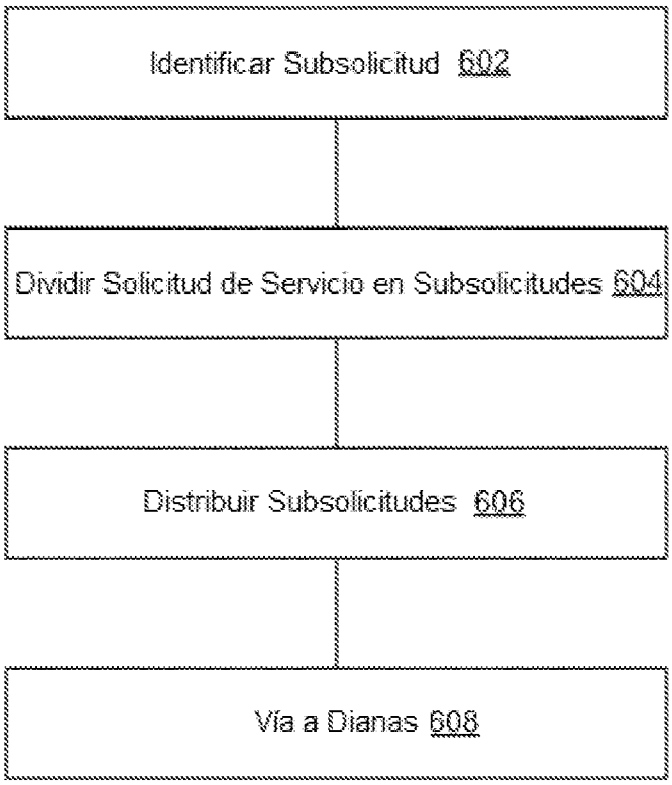
Identificar Subsolicitud 602
Dividir Solicitud de Servicio en Subsolicitudes 604
Distribuir Subsolicitudes 606
Vía a Dianas 608

FIG. 6

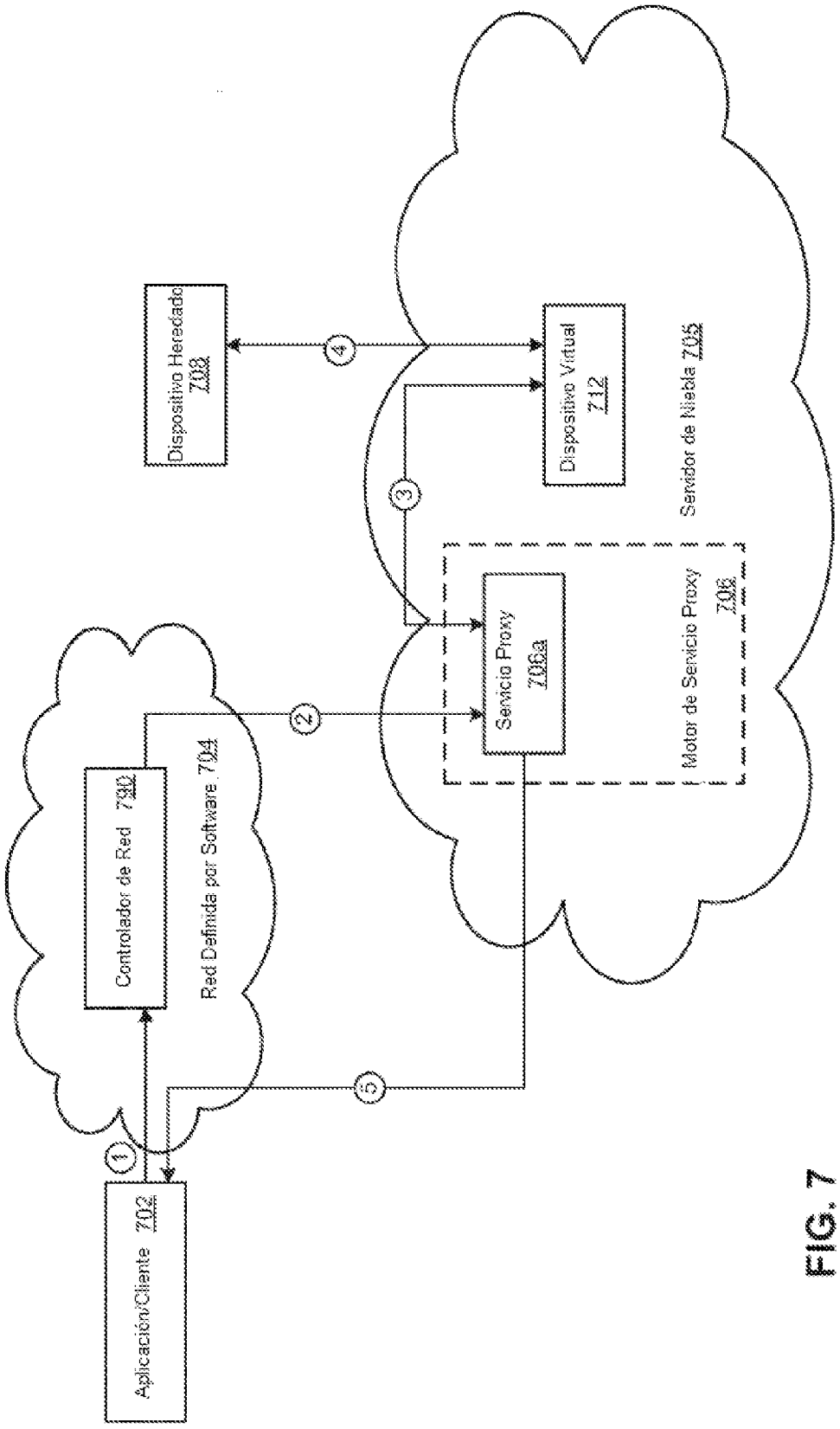
Aplicación/Cliente 702
Red Definida por Software 704
Controlador de Red 710
Servidor de Niebla 705
Motor de Servicio Proxy 706
Servicio Proxy 706a
Dispositivo Virtual 712
Dispositivo Heredado 708
1
2
3
4
5

FIG. 7

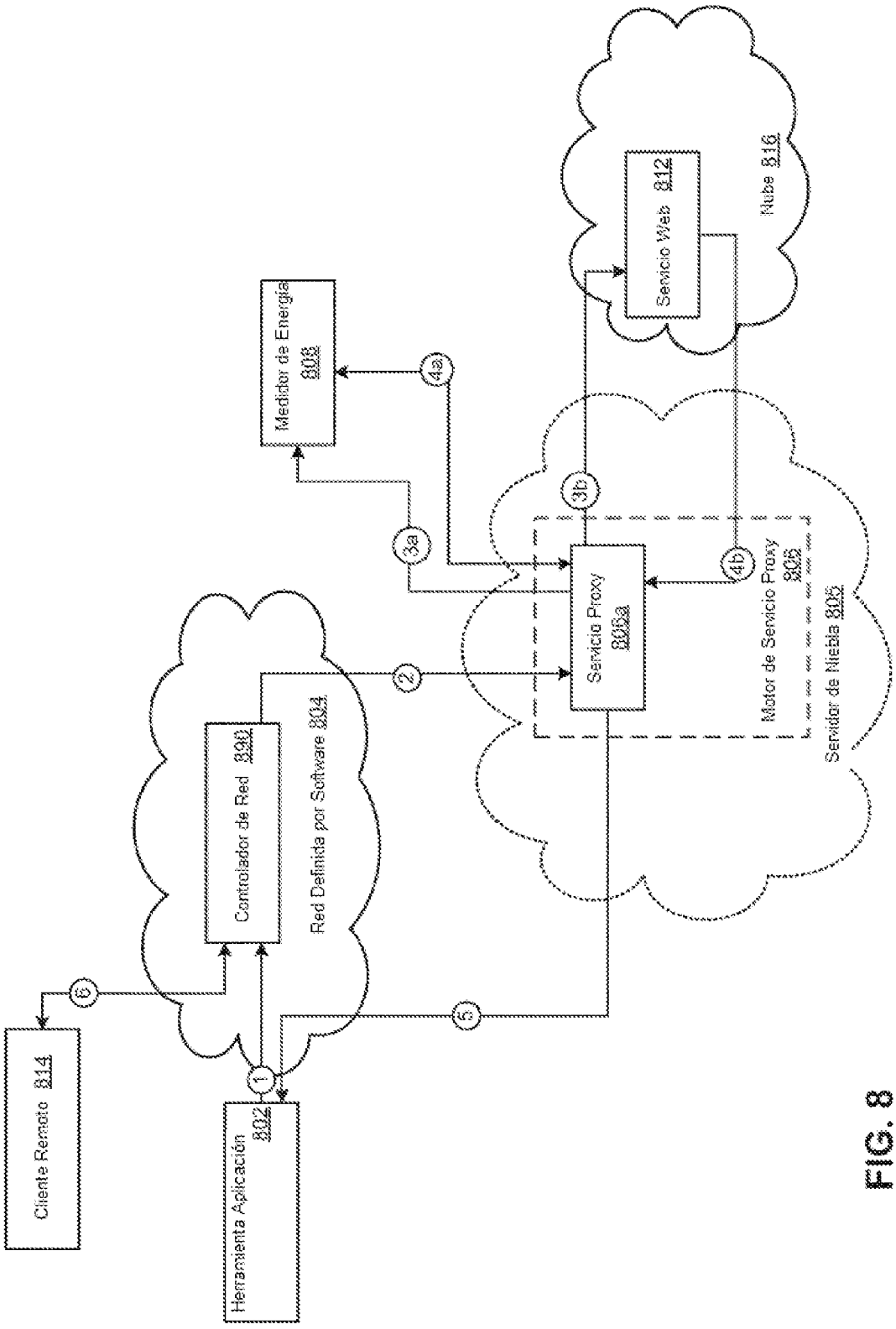
Cliente Remoto 814
Herramienta Aplicación 802
Controlador de Red 808
Red Definida por Software 804
Medidor de Energía 808
Servicio Web 812
Nube 816
Servicio Proxy 806a
Motor de Servicio Proxy 806
Servidor de Niebla 806
1
2
3a
3b
4a
4b
5
6

FIG. 8

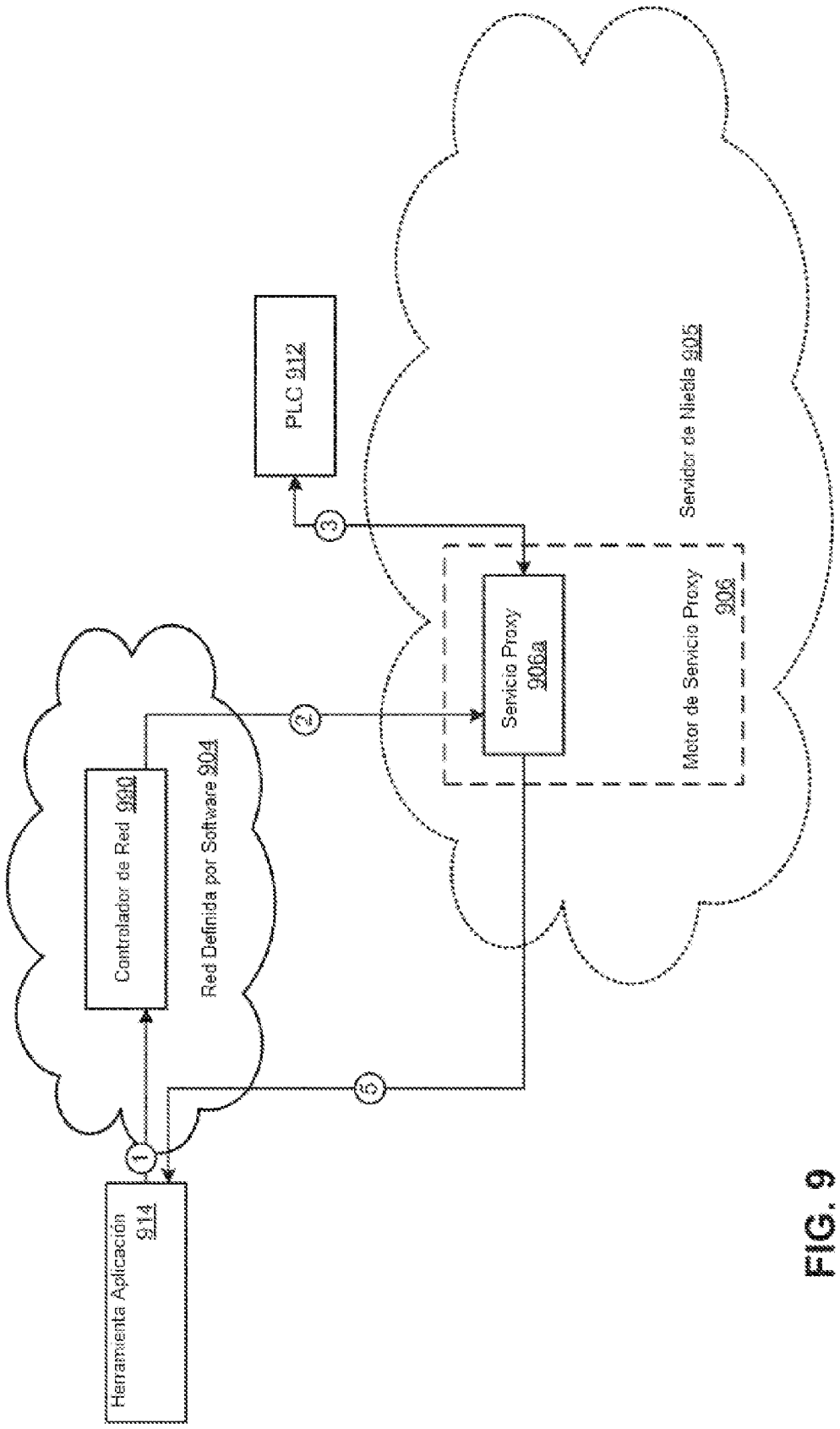
Herramienta Aplicación 914
Red Definida por Software 904
Controlador de Red 910
Servidor de Niebla 905
Motor de Servicio Proxy 906
Servicio Proxy 906a
PLC 912
1
2
3
5

FIG. 9

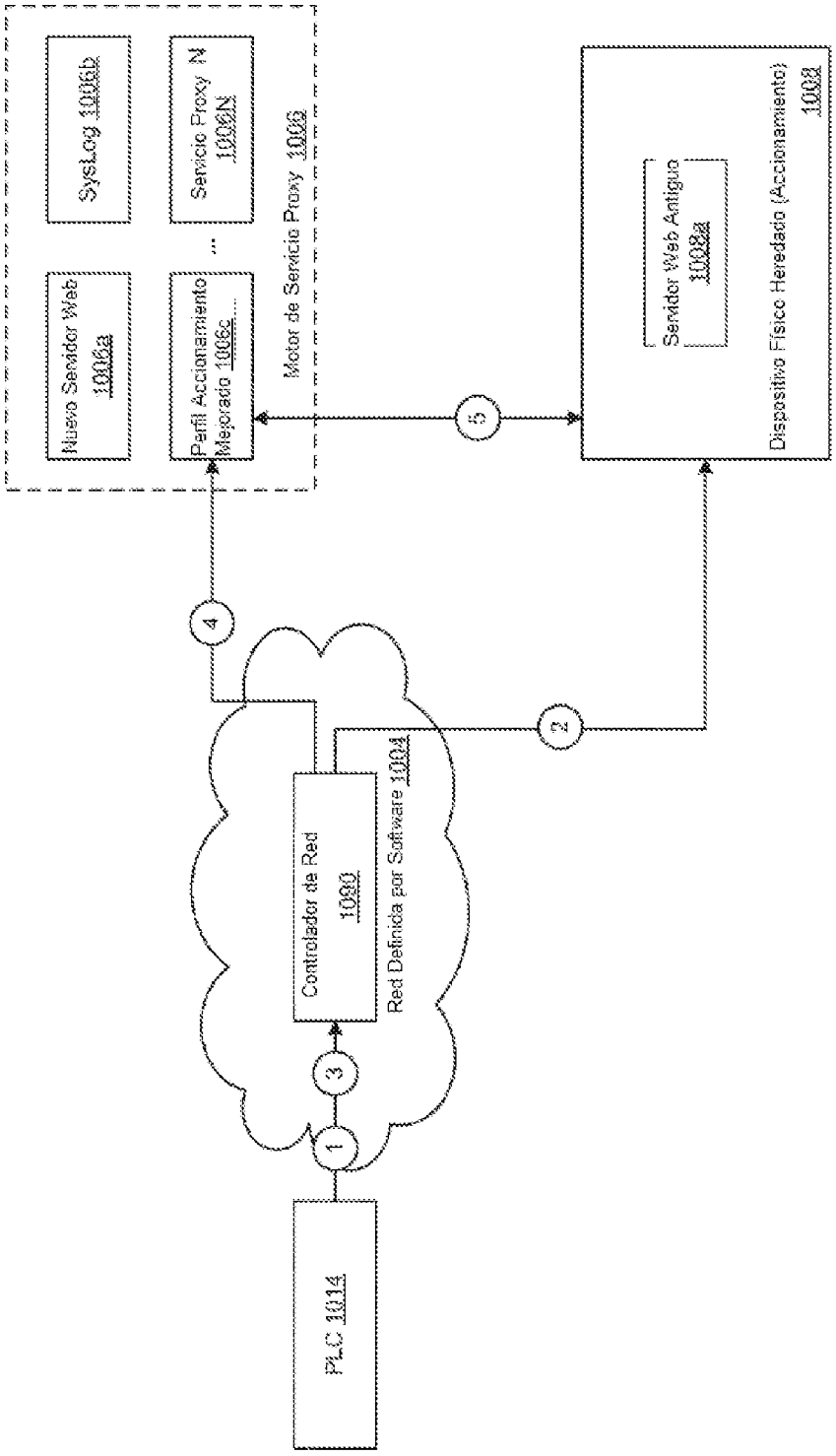
Nuevo Servidor Web 1016a
SysLog 1016b
Perfil Accionamiento Mejorado 1016c
...
Servicio Proxy N 1016N
Motor de Servicio Proxy 1016
Servidor Web Antiguo 1028a
Dispositivo Físico Heredado (Accionamiento) 1028
5
4
2
Controlador de Red 1030
Red Definida por Software 1034
3
1
PLC 1014

FIG. 10

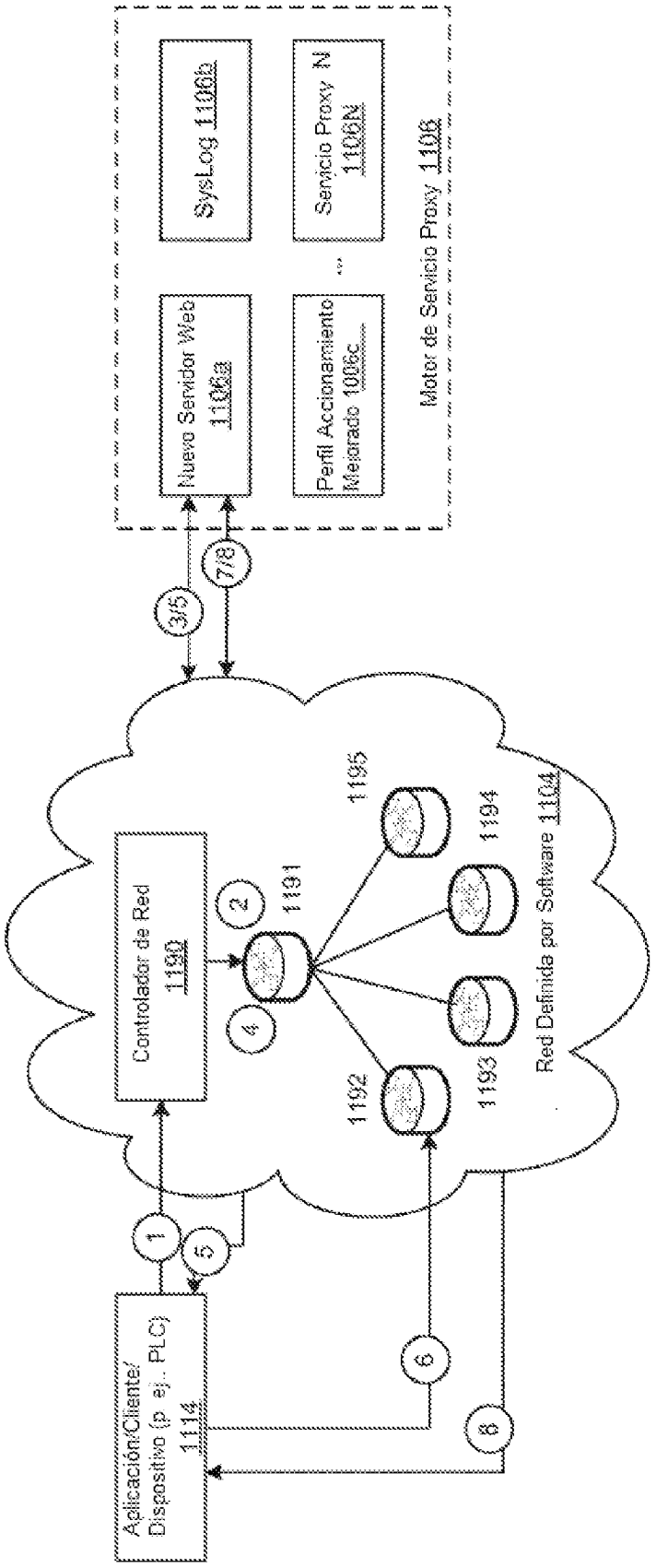
Aplicación/Cliente/
Dispositivo (p. ej., PLC)
1114
Controlador de Red
1190
Red Definida por Software 1104
1191
1192
1193
1194
1195
Motor de Servicio Proxy 1106
Nuevo Servidor Web
1106a
SysLog 1106b
Perfil Accionamiento
Mejorado 106c
Servicio Proxy N
1106N
1
2
3/5
4
5
6
7/8
8

FIG. 11