Interfaz para programas de aplicación e Internet de las cosas

Fuente: gacetilla técnica de Opto 22, traducida especialmente por Sergio Roitman, de *Multiradio*,
sergio.roitman@multiradio.com.ar, *www.multiradio.com.ar*

Introducción

Todos sabemos acerca de la Internet de las cosas (IoT) y su objetivo: proveer datos útiles directamente a las personas que toman decisiones comerciales, y permitir que las máquinas se comuniquen entre sí para tomar decisiones útiles para optimizar las operaciones de la empresa. Pero, ¿cómo funciona realmente la Internet de las cosas? ¿Cuál es el camino, desde lo básico, para que todas estas máquinas puedan conectarse entre sí utilizando las tecnologías de la nube?

En el mundo de hoy, existen millones de sensores, máquinas, dispositivos y actuadores. Se monitorean, se los usa para controlar procesos y para obtener datos de ellos. Sin embargo, muy pocos de estos sensores y dispositivos tienen la capacidad incorporada para comunicarse de forma directa con sistemas informáticos. Muchos de ellos se conectan (PLC), controladores de automatización programables (PAC), o DCS. Pero esos sistemas fueron especialmente diseñados para otros fines, no para comunicarse en la Internet de las cosas.

Para obtener datos de estos controladores, los sistemas informáticos de la compañía, o mediante Internet de las cosas, se requiere una cadena compleja de hardware y software de conversión: PLC, drivers propietarios, conversores de protocolo, y más. Es una secuencia compleja de instalar y mantener que requiere tiempo, dinero y experiencia en todos los niveles. Incluso si está instalado, su gran complejidad hace que sea difícil establecer la seguridad necesaria y mantener la integridad de los datos.

Datos importantes en los sistemas de control

¿Por qué es tan importante obtener datos de estos sistemas? Estos datos son utilizados principalmente para monitorear y controlar procesos y máquinas en sus aplicaciones de automatización. Sin embargo, algunos también son de gran utilidad más allá del sistema de automatización. Por ejemplo, los siguientes:

- Los gerentes pueden necesitar ver cuántas unidades se produjeron en la última hora; comparar esa cifra con la del día previo, a la misma hora; monitorear el rendimiento para identificar problemas de calidad en la producción; identificar a quien acaba de acceder por la puerta de seguridad.
- Los gerentes de planta pueden necesitar: registrar las temperaturas de todas las unidades de refrigeración en múltiples ubicaciones; activar una bomba (así como también un enfriador, una luz o la línea de producción) o desactivarla; cambiar el ajuste de temperatura en una unidad de enfriamiento; prever un programa de mantenimiento basado en el tiempo de uso de una máquina, o el uso de energía eléctrica.
- El personal de administración y finanzas puede acceder a datos enviados a su base de datos de negocios, tales como: niveles de inventario; cuánta energía eléctrica fue utilizada por cada usuario en los edificios de la empresa; cuántos productos fueron enviados o recibidos; el costo o el tiempo necesarios para producir el producto A frente al producto B, a través de la línea de producción.

Los datos en los sistemas de control podrían ser útiles por estas y muchas otras necesidades, pero es difícil traspasar estos datos a los sistemas informáticos de la compañía para su análisis.

Las dificultades para acceder a los datos del controlador

Muchas veces los PAC y PLC supervisan procesos y equipos de control cuyo procesamiento no puede interrumpirse porque causaría pérdidas de producción, daños a las maquinas o peligro para la seguridad humana.

Debido a que sus funciones son tan críticas, las redes tradicionales de control industrial están protegidas contra el acceso no autorizado y la interrupción de la red, separándose físicamente de otras redes de la empresa, incluso cuando las redes de control utilizan Ethernet. Los ingenieros y técnicos de automatización, también llamados "personal de tecnología de operaciones" (OT), son renuentes a abrir las redes de control de la empresa a las redes de tecnología de la información (TI).

Además, las redes de control industrial suelen utilizar protocolos industriales, como Profinet, Ethernet/IP o Modbus, en lugar de los protocolos estándares TCP/IP que se utilizan en el mundo de la informática.

Sin embargo, para hacer realidad el objetivo de Internet de las cosas, los dos grupos, tecnología de operaciones y de la información, deben trabajar juntos para lograr dos objetivos: primero, cuidar la seguridad de las redes de control críticas, y segundo, proporcionar los datos necesarios donde y cuando se requieran.

Esto puede simplificarse y permitir alcanzar los objetivos de Internet de las cosas usando un controlador *Snap PAC* de *Opto 22*. Veamos por qué a continuación.

Snap PAC y los módulos de entrada/salida

Como todos los controladores industriales, los *Snap PAC* manejan y controlan muchos datos: de

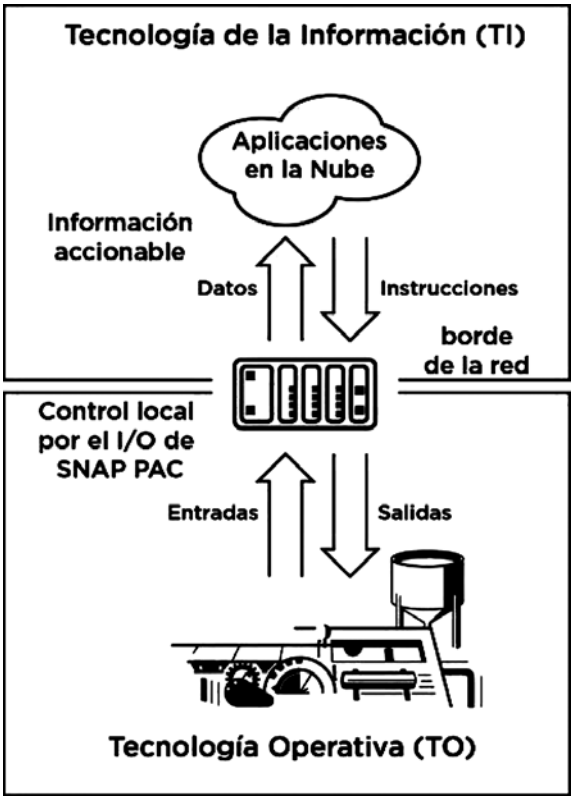

Figura 1

puntos de entrada/salida (E/S) conectados al PAC, y los datos de variables dentro de la lógica del controlador.

Estos son controladores de automatización programables (PAC) de tamaño reducido y robustos para ambiente industrial; que se utilizan en aplicaciones en todo el mundo. Sus módulos controlan entradas/salidas analógicas y digitales, con una amplia gama de señales de entrada y salidas, de uno a treinta y dos puntos.

Tanto en la automatización como en Internet de las cosas, los módulos E/S cumplen una función fundamental: son transductores entre el mundo físico y el digital. Como saben los ingenieros de automatización, los sensores y máquinas típicamente intercambian señales eléctricas como voltaje y corriente para comunicarse entre sí; en cambio, los PLC, PAC y DCS trabajan con información digital. La transducción se puede dar en ambos sentidos:

- Para el monitoreo, cada entrada lee las señales eléctricas de cosas físicas y las convierte a sistema binario de unos y ceros.
- Para el control, la salida convierte los ceros y unos a señales eléctricas que actúan sobre cosas físicas.

Eso, que funciona para la automatización, no es válido para la Internet de las cosas. El obstáculo esta en hacer llegar los datos al último nivel, ya sea sacarlos de la red de tecnología operacional e

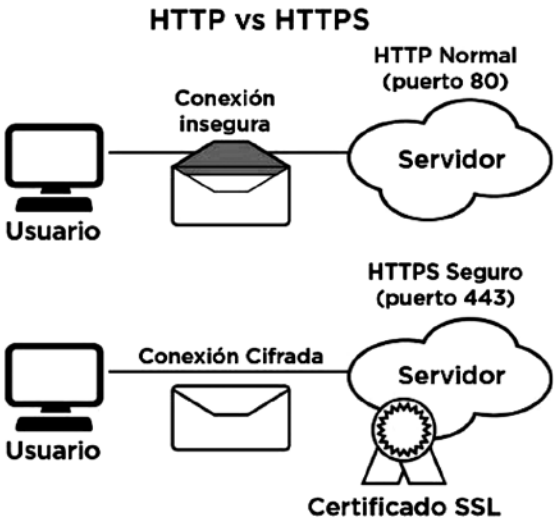

Figura 2. Snap Pac y E/S, de Opto 22

ingresarlos a la de información, o viceversa, debido a los distintos protocolos que usa cada una. Como hemos visto, se necesita una variedad de hardware y de software como convertidores de protocolo, middleware y drivers para traspasar los datos de los PLC, los PAC y de los DCS a los sistemas de tecnología de la información. Sin este último paso, Internet de las cosas es imposible.

Para los controladores de *Snap Pac* de la serie *S* y de la serie *R* de *Opto 22*, la clave está en que simplifica este último paso, reduciendo la brecha entre los sistemas de tecnología operacional y de la información.

Acceso a los datos

A continuación, se muestra cómo los *Snap Pac* reducen esta brecha. Primero, basan su funcionamiento en redes Ethernet estándar y se comunican a través del protocolo estándar de Internet, por lo que las redes y protocolos ya son naturalmente compatibles con las tecnologías de la información.

Y segundo, a partir de la versión de firmware R9.5a, los *Snap Pac* también incluyen dos bloques fundamentales de la Internet de las cosas:

- un servidor integrado de HTTP/HTTPS para comunicaciones;
- una RESTful API

Veamos lo que significan estos términos y las ventajas para el personal de la empresa que necesita datos que, hasta ahora, estaban confinados a los sistemas y equipos de control.

HTTP y HTTPS

El HTTP es el protocolo de aplicaciones sobre el que se basa de la comunicación de datos a través de la Internet. Sin embargo, HTTP por sí solo no proporciona una comunicación segura; todos los datos que transporta la red están abiertos a cualquier persona en la red.

El uso de HTTP combinado con TLS/SSL se convierte en HTTPS, que es una comunicación segura.

Lo que lo hace seguro es que HTTPS proporciona encriptado: todos los datos que pasan por la conexión están cifrados.

Encriptado vs. autenticación

Es fácil confundir el encriptado (cifrado) y la autenticación, pero son conceptos diferentes y es importante entenderlos y utilizarlos para la seguridad, ya sea en su red local o a través de la Internet.

'Encriptado' significa convertir los datos a texto sin sentido, que no significa nada a menos que se tenga de antemano la clave para descifrarlo. Los datos cifrados están protegidos, si son interceptados, son inútiles sin la clave. Hay varias maneras de cifrar y descifrar datos pero, fundamentalmente, el cifrado es una manera de hacer los datos comprensibles solo para las personas y los sistemas que deberían tener acceso a ellos.

La autenticación, por su parte, certifica que uno es quien dice ser en la red.

Las transacciones a través de HTTPS muchas veces son ciegas, y es importante para asegurarse de que la persona o sistema en el otro extremo sea "auténtica", no una "impostora". Muchas veces, solo un nombre de usuario y una contraseña son suficientes para establecer la autenticidad, pero algunos sistemas requieren más pruebas, como una ficha o una huella digital.

Frecuentemente, se añade la autenticación al cifrado (realizada a través de un canal cifrado), por lo que se tiene una conexión segura en la que también se tiene que comprobar identidad.

Por ejemplo, al comprar un libro en *Amazon*, se ve el HTTPS y su símbolo del candado en la barra de

URL (*Uniform Resource Locator*, 'localizador de recursos uniforme'). Pero también se debe ingresar un nombre de usuario y contraseña para que *Amazon* verifique que uno es uno y pueda procesar la venta.

Clientes y servidores

HTTP y HTTPS utilizan un método de comunicación sin estado (*stateless*) cliente-servidor, que consiste en pares de petición/respuesta individuales en una red. El cliente solicita los datos, el servidor responde.

- Un cliente solo puede hablar, nunca puede escuchar o responder. El cliente solicita o envía los datos a los intervalos que él mismo fija.
- Un servidor nunca puede iniciar una conversación. Está constantemente escuchando, pero no puede hablar; solo puede escuchar y responder. El servidor responde a las solicitudes de datos o reconoce los datos que se le envían.

El cliente debe ser capaz de contactar al servidor en una red TCP/IP. Se observa que este método de cliente-servidor es parecido al método de comunicación maestro-esclavo de Modbus:

- El cliente es el maestro Modbus: hace las solicitudes y envía datos.
- El servidor es el esclavo Modbus: escucha, envía los datos solicitados, y reconoce datos enviados a él.

Notese que el servidor de *Snap Pac HTTPS* provee datos almacenados en el PAC. El servidor HTTPS no puede "enviar" los datos a cualquier destinatario. Un cliente debe hacer una solicitud al PAC, y luego el PAC responderá. Recuerdese que un servidor no puede "hablar", sino que solo puede escuchar.

El cliente puede utilizar una instrucción estándar HTTP Get ('tomar, asir') para solicitar datos del PAC y otra HTTP Post ('enviar') para enviar datos al PAC. El formato de la petición se canaliza por la API REST del *Snap Pac*

La API REST de *Snap PAC*

Una API es una interfaz de usuario para programas de computadoras. Es un mecanismo por el cual un programa de computadora puede acceder a datos o recursos de otro programa. La API REST de *Snap Pac* utiliza el protocolo HTTPS. Hay otras API que utilizan otro protocolo como el MQTT, pero HTTPS es el más común hoy en día.

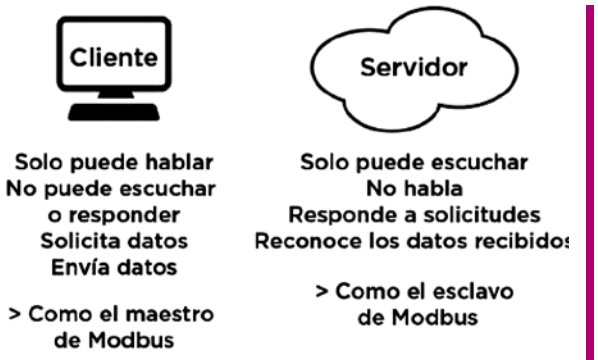

Figura 3. HTTP vs. HTTPS

Toda la API REST de *Snap Pac* está documentada en *developer.opto22.com*. Incluye todas las llamadas posibles que puede hacer para leer o escribir datos al PAC, utilizando un lenguaje de programación compatible con REST. Algunos de estos, todos conocidos por programadores web o de tecnologías de la información, son: *PHP, Python,.NET, JavaScript*, y otros.

La API muestra cómo acceder a los datos de puntos de E/S, así como a los datos numéricos y a las cadenas de variables en la lógica del PAC. Los datos son devueltos en JSON, un formato estándar de intercambio de datos que los humanos pueden interpretar (texto), y las computadoras pueden analizar y generar fácilmente.

¿Qué se necesita para acceder a los datos de Snap PAC?

No se necesitan convertidores de protocolo ni drivers de software. Ni siquiera necesita OPC. Todo lo que se necesita es un *Snap PAC* con firmware R9.5a o superior, y su E/S.

Se puede acceder a los datos del servidor de forma segura a través de HTTPS (con el cifrado y la autenticación) desde las redes estándar de tecnologías de la información, con protocolos y herramientas de programación habituales. Para empezar:

- Contar con alguien que conozca algún lenguaje de programación compatible con la API RESTful. O utilizar Node-RED;
- estar familiarizado con el formato JSON;
- asegurarse de que el cliente tiene acceso al PAC a través de una red TCP/IP por el puerto 443;
- decidir si el acceso a los datos será de solo lectura o de lectura-escritura.

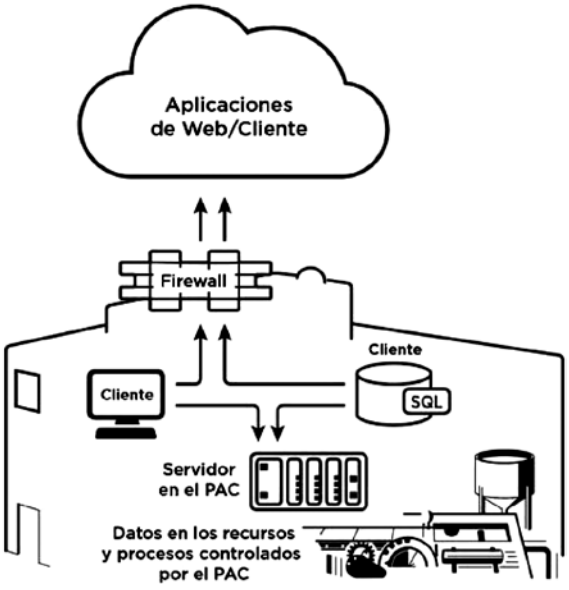

Figura 4.

Muchas veces, debido a la naturaleza crítica de los datos en un *Snap PAC*, el acceso de lectura-escritura debe ser cuidadosamente planificado. Considere todas las consecuencias posibles antes de conceder acceso de lectura-escritura a cualquier cliente, persona o sistema.

Consideraciones para las redes

Recomendamos nunca poner un controlador de *Snap PAC* directamente conectado a Internet. El PAC debería estar ubicado detrás de un firewall y, en la mayoría de los casos, la red de control debe estar separada de la red informática de la empresa, para cumplir los requisitos de la seguridad. Para esto, se podrían utilizar las dos interfaces independientes de red de Ethernet provistas.

Debido a que el equipo funciona como un servidor HTTPS para los datos en Internet de las cosas, el PAC debe ser accesible por el cliente a través de una red TCP/IP.

Un cliente podría ser una computadora que muestra los datos del PAC, una base de datos u otro sistema, un teléfono inteligente en la red inalámbrica que usa los datos en una aplicación, u otros servicios web o aplicaciones.

¿Qué pasaría si quisiéramos tener acceso a los datos del PAC desde otro lugar, como en un teléfono fuera del edificio o desde una ubicación remota? Solo se necesita configurar un cliente que tenga acceso a los datos PAC, y que este luego los envíe a través del firewall.

Node-RED

Para quienes no están habituados a programar del lado cliente usando uno de los lenguajes compatibles con la API REST, se puede tener acceso a los datos del PAC mediante el uso de la aplicación *Node-RED*.

Node-RED fue creado por *IBM* y es una herramienta visual gratuita, basada en la web. Se puede utilizar para conectar entre si dispositivos de hardware, API y otros servicios conectados en línea.

Por ejemplo, se podría utilizar *Node-RED* para proporcionarle, a un gerente de planta, un mapa que muestre las temperaturas, los tiempos de encendido/apagado de los enfriadores, y el consumo de energía eléctrica de cada edificio. Más aún, se podrían combinar datos de un PAC con los de un sitio web de clima como *Weather Underground*, o con *Google Maps*. Hay dos nodos disponibles para los Snap PAC, uno para lectura y otro para escritura.

(Nota del autor: *Node-RED* está basado en Node.js, pero no se necesita conocer este último para usarlo. Si se conoce *JavaScript*, se pueden añadir funciones con el editor de *Node-RED*, pero no es necesario). ❖

Figura 5

Nota del editor: *Opto 22* es una empresa estadounidense con más de cuarenta años de experiencia en la automatización, hoy fabrica controladores, relés de estado sólido, y módulos de E/S. Todos los productos están disponibles en todo el mundo gracias a una amplia red de distribuidores; en Argentina, a través de *Multiradio*.

Las siglas están desglosadas en página 5.