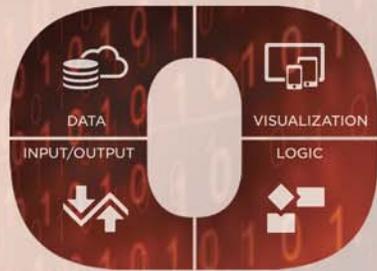


INTERNET



THINGS

La API de SNAP PAC REST y la Internet de las Cosas

*Para los Profesionales
de OT*

OPTO 22

www.opto22.com

Opto 22

43044 Business Park Drive • Temecula • CA 92590-3614

Phone: **800-321-6786** or **951-695-3000**

Pre-sales Engineering is free.

Product Support is free.

www.opto22.com

Form 2187S-161003

© 2016 Opto 22. All rights reserved. Dimensions and specifications are subject to change. Brand or product names used herein are trademarks or registered trademarks of their respective companies or organizations.

La API de SNAP PAC REST y la Internet de las Cosas

Para los Profesionales de OT

Introducción

Todos sabemos de la Internet de las Cosas (IoT, de las iniciales en inglés Internet of Things) 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 IoT? ¿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 a los controladores lógicos programables (PLCs), controladores de automatización programables (PACs), o sistemas de control distribuido (DCSs). Pero esos sistemas fueron especialmente diseñados para otros fines, no para comunicarse en la IoT.

Para obtener datos de estos controladores, los sistemas informáticos de la compañía, o mediante IoT, se requiere una cadena compleja de hardware y software de conversión: PLCs, 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

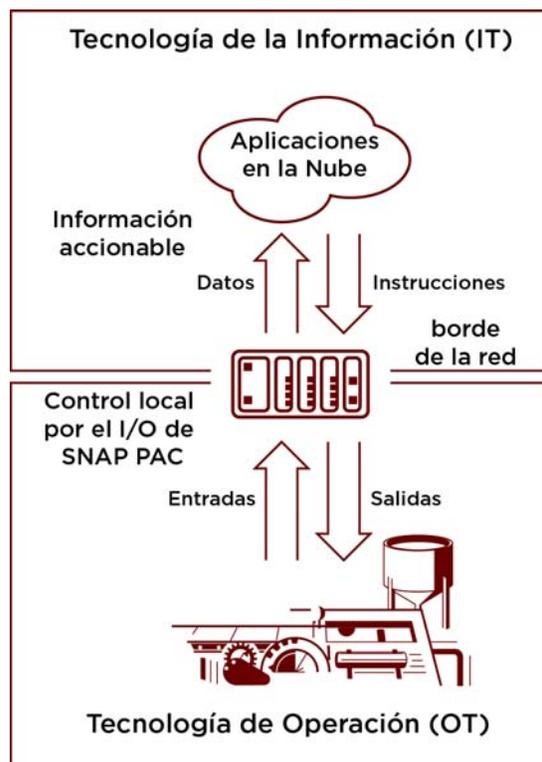
¿Por qué es tan importante obtener datos de estos sistemas? Estos datos son utilizados principalmente para monitorear y controlar procesos y máquinas en sus aplicaciones de automatización. Sin embargo, algunos también son de gran utilidad más allá del sistema de automatización. Por ejemplo:

Los gerentes pueden necesitar:

- Ver cuantas 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 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 set point de 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
- 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
- Cuánta energía eléctrica fue utilizada por cada usuario en los edificios de la empresa.

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 (IT) de la compañía para su análisis.

Las dificultades para acceder a los datos del controlador

Muchas veces los PACs y PLCs supervisan procesos y equipos de control cuyo procesamiento que no puede ser interrumpido 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, separandolas 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 reacios a abrir las redes de control de la empresa a las redes de Tecnología de la Información (IT).

Además, las redes de control industrial suelen utilizar protocolos propietarios 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, OT y IT, 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 IoT usando un controlador SNAP PAC de Opto 22 con características únicas. Veamos por qué a continuación.

SNAP PAC y I/O

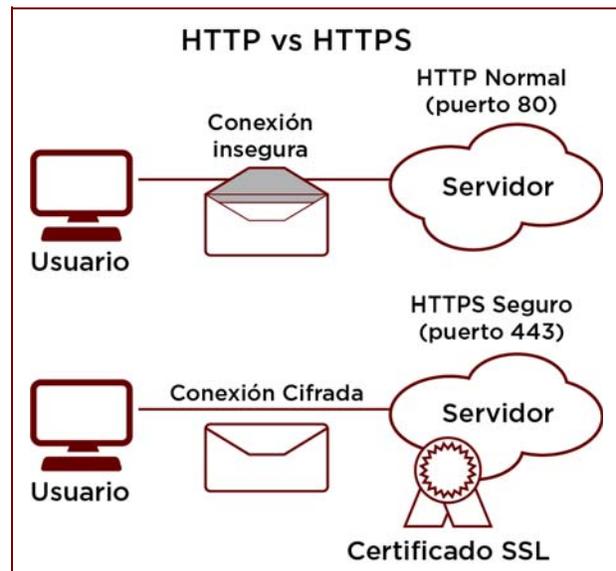
Como todos los controladores industriales, los SNAP PAC de Opto 22 manejan y controlan muchos datos: de puntos de I/O conectados al PAC, y los datos de variables dentro de la lógica del controlador.

Los controladores de SNAP PAC de Opto 22 son controladores de automatización programables (PACs) de tamaño reducido y robustos para ambiente industrial, y se utilizan en aplicaciones en todo el mundo. Los módulos de SNAP PAC controlan entradas/salidas analógicas y digitales, con una amplia gama de señales de entrada y salidas, de 1 a 32 puntos.

Tanto en la automatización como en Internet de las Cosas, los módulos de I/O 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 si; en cambio los PLCs, PACs y DCS trabajan con información digital. La transducción se puede dar en ambos sentidos:

- **Para el monitoreo**, cada modulo de I/O (entrada) lee las señales eléctricas de cosas físicas y las convierte a unos y ceros habituales en el mundo digital.
- **Para el control**, el modulo de I/O (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 IoT. El obstáculo es en hacer llegar los datos al último



nivel, ya sea sacarlos de la red OT e ingresarlos a la IT o viceversa, debido a los distintos protocolos que usan OT e IT respectivamente. 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 PLCs, los PACs y de los DCS a los sistemas de TI. 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 OT e IT.

Acceso a los datos de SNAP PAC

A continuación se muestra como los SNAP PAC reducen esta brecha. Primero, basan su funcionamiento en **redes Ethernet estándar** y se comunican a través del **protocolo estándar de Internet (IP)**, por lo que las redes y protocolos ya son naturalmente compatibles con las tecnologías de TI.

Y segundo, a partir de la versión de firmware R9.5a, los SNAP PAC también incluyen dos bloques fundamentales de la IoT:

- un **servidor integrado de HTTP/HTTPS** para comunicaciones
- una **RESTful API** (interfaz constituida por un programa de aplicación basado en la arquitectura REST, la cual tiene un formato estándar para desarrollar programas).

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* (Hypertext Transfer Protocol) 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 (del inglés Transport Layer Security y el previo Secure Sockets Layer)

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 la convertir los datos a texto sin sentido, que no significan nada a menos que se tenga la clave correcta, la cual fue establecida de antemano, 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 sólo por las personas y los sistemas que deberían tener acceso a los mismos.

Autenticación certifica que usted 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 es "auténtico", no un "impostor". Muchas veces, sólo un nombre de usuario y una contraseña son suficientes para establecer la autenticidad, pero algunos sistemas requieren más pruebas de autenticidad, 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.

Pero también tiene que ingresar su nombre de usuario y contraseña, para que Amazon confirme que realmente es usted y que se puede 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* sólo 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; sólo 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 (volveremos sobre esto más adelante).

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.

Note 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. Recuerde que un servidor no puede hablar; sino que sólo puede escuchar.

El cliente puede utilizar una instrucción estándar HTTP GET para solicitar datos del PAC y otra HTTP POST 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 HTTP/S. Hay otras APIs que utilizan otro protocolo como el MQTT, pero HTTP/S es el más común hoy en día.

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 IT son: PHP, Python, .NET, JavaScript y otros.

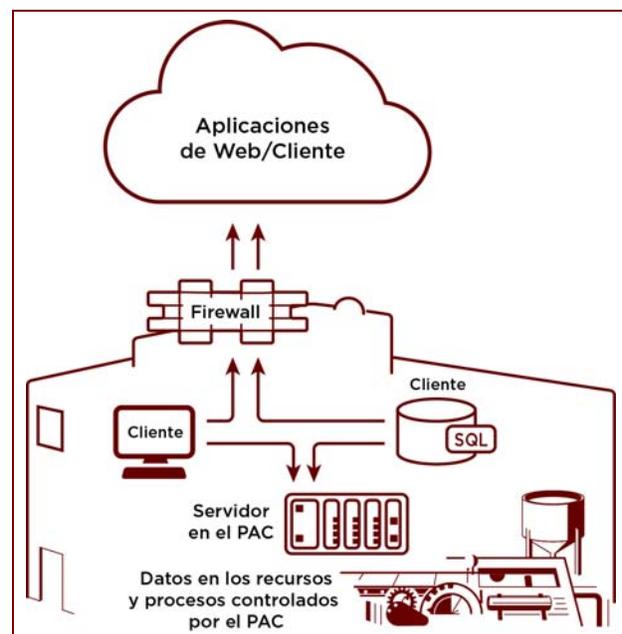
La API muestra cómo acceder a los datos de puntos de I/O, así como a los datos numéricos y a las cadenas de variables en la lógica del PAC.

Los datos son devueltos en **JSON** (JavaScript Object Notation), un formato estándar de intercambio de datos que los humanos pueden interpretar (texto), y las computadoras pueden analizar y generar fácilmente.

¿Qué necesita para tener acceso a los datos de SNAP PAC?

No se necesitan convertidores de protocolo ni drivers de software. Ni siquiera necesita OPC (OLE for Process Control). Todo lo que se necesita es un SNAP PAC con firmware R9.5a o superior, y su I/O.

Se puede acceder a los datos del servidor del SNAP PAC de forma segura a través de HTTPS (con el cifrado y la



autenticación) desde las redes de IT standard, 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](#) (más adelante se trata este tema).
- Estar familiarizado con el formato [JSON](#) (JavaScript Object Notation)
- 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 sólo lectura o de lectura/escritura

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 en el SNAP PAC (consultar la guía de usuario del controlador para pasos de configuración).

Debido a que el SNAP PAC funciona como un servidor HTTPS para los datos en IoT, 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
- Otros servicios web o aplicaciones

¿Qué pasaría si quisiéramos tener acceso a los datos del PAC desde otro lugar, como en su teléfono fuera del edificio o desde una ubicación remota? Solo se necesita configurar un cliente que tenga acceso a los datos PAC, y éste 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 sí dispositivos de hardware, APIs y otros servicios online.

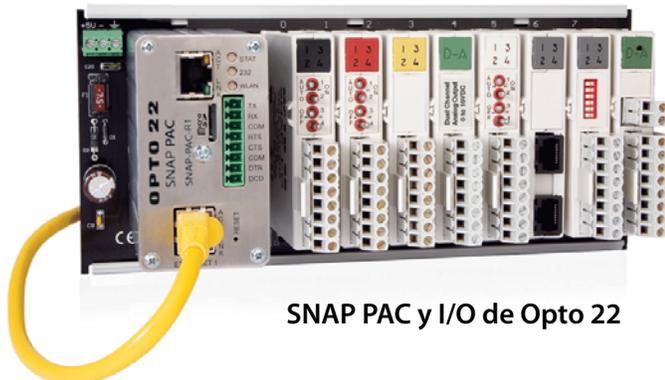
Por ejemplo, se podría utilizar Node-RED para proporcionar a un gerente de planta, un mapa que muestre las temperaturas, los tiempos que están encendidos/apagados los enfriadores, y el consumo de energía eléctrica de cada edificio. Más aún, se podrían combinar datos de un PAC, con los de un sitio web de clima como Weather Underground, y de Google Maps.

Hay dos nodos disponibles para los SNAP PAC, uno para lectura y otro para escritura. Para más información e instrucciones visitar [developer.opto22.com](#).

(Node-RED está basado en Node.js, pero no se necesita saber Node.js para usarlo. Si conoce JavaScript, tiene la opción de poder añadir funciones con el editor de Node-RED, pero no es necesario.)

¿Porque Usar Opto 22?

Hay tres razones: la experiencia, confiabilidad, y la atención personalizada. Opto 22 fue fundada en 1974, cuando su fundador, el ingeniero Bob Engman, diseñó un relé de estado sólido (SSR). Con más de 40 años de experiencia en la automatización, hoy fabrica controladores, relés de



SNAP PAC y I/O de Opto 22

estado sólido, y módulos de I/O reconocidos en todo el mundo por su confiabilidad, además de proveer software que es fácil de usar para el desarrollo de programas de control, visualización de datos en cualquier dispositivo, y la integración de sistemas de automatización redes de computadoras.

Todos los productos de Opto 22 están basados en estándares abiertos. Todos los productos son diseñados, fabricados, y con soporte en la sede en Temecula, California, EE.UU.



La mayoría de los relés de estado sólido y los módulos de I/O tienen garantía de por vida. El soporte técnico telefónico de fábrica es gratuito. La ingeniería de pre-venta también es gratuita, por lo que se puede contactar por cualquier consulta acerca de las aplicaciones.

Para Empezar

Ver developer.opto22.com para la API REST y los nodos Node-RED para los controladores de SNAP PAC.

Si ya se tiene un controlador de SNAP PAC serie-S o serie-R y sus módulos de I/O, confirmar que tiene la [versión de firmware R9.5a](#) o más nueva en el PAC. Se podría actualizar en caso de ser una versión previa.

Para ver información técnica de PAC y I/O, puede ver en nuestro sitio web, www.opto22.com:

- Controladores independientes de la [serie-S de SNAP PAC](#)
- Controladores para montaje en rack de la [serie-R de SNAP PAC](#)
- [SNAP I/O](#)

Todos los productos de Opto 22 están disponibles a través de distribuidores por todo el mundo.

¿Preguntas?

Póngase en contacto con su distribuidor local e Ingeniería Pre-venta de Opto 22 para cualquier pregunta acerca de los productos, la arquitectura del sistema, o el I/O.

Teléfono: **+1-951-695-3000**

O [envíe una pregunta a un ingeniero](#).