DISEÑO DE CIBERSEGURIDAD Y MEJORES PRÁCTICAS PARA EL SISTEMA DE *groov* EPIC

Cuando se junta, procesa, y comparte datos de equipos industriales en las instalaciones o en sitios remotos, la ciberseguridad es una gran preocupación. Los sistemas y equipos, y los datos que contienen, son esenciales y delicados, y requieren dispositivos para el internet industrial de las cosas (IIoT) y software que los protegen.

Para todos los sistemas digitales, la seguridad es un tema complejo con diferentes implicaciones según la organización y el sistema. Los requisitos de seguridad cambian constantemente según la evolución del sistema, y es clave integrar la seguridad en el diseño del sistema. Como escribió Bruce Schneier en 2000, "La seguridad es un proceso, no un producto."

Para abordar las complexidades cambiantes de la seguridad, se necesita comprender los riesgos de la seguridad, comprender el entorno, y comprender las herramientas de seguridad que hay disponibles. Los expertos en la seguridad reconocen los varios elementos de seguridad en los sistemas, incluso la seguridad física, las políticas y procedimientos, y la seguridad de la red.

"La seguridad es un proceso, no un producto."

- Bruce Schneier

El sistema *groov* EPIC® de Opto 22 ayuda a enfrentar los requisitos para la seguridad de la red. Diseñado desde cero para construir un sistema extensivo y seguro, *groov* EPIC brinda las herramientas y métodos necesarios para que el sistema sea lo más seguro posible desde el punto de vista de acceso a la red, y al mismo tiempo manteniendo la flexibilidad necesaria para la aplicación. De hecho, ningún otro controlador industrial en el mercado ofrece el mismo nivel de características y opciones de ciberseguridad.

Por supuesto, la seguridad resultante del sistema depende del desarrollador, pero *groov* EPIC está listo para ayudar. Esta nota técnica explica las características de ciberseguridad que están integradas en el *groov* EPIC, y sugiere las mejores prácticas para configurar un sistema seguro con *groov* EPIC.

Al aplicar estas características, puede ayudar cumplir con las pautas de seguridad tal como se señala en la especificación ISA/IEC 62443, que proporciona "una estructura flexible para abordar y mitigar las vulnerabilidades de seguridad actuales y futuras, en los sistemas de control y automatización industriales (IACSs)."[1]

Cómo Conseguir Ayuda

Como siempre, si está utilizando *groov* EPIC y no encuentra la ayuda que necesita en esta nota técnica o en el documento *groov EPIC User's Guide* (formulario 2267), comuníquese con el Apoyo Técnico de Opto 22. El apoyo técnico es gratuito.

Nota: Correos electrónicos y llamadas telefónicas al Apoyo Técnico de Opto 22 se contestan en la orden que se reciben.

Teléfono: 800-TEKOPTO (800-835-6786 llamada gratuita en los EE.UU. y Canada)
951-695-3080
Lunes a Viérnes, 7 AM a 5 PM, Tiempo del Pacífico

FAX: 951-695-3017

Email: support@opto22.com

Página Web: www.opto22.com

1. "New ISA/IEC 62443 standard specifies security capabilities for control system components," InTech online, https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

ENTENDIMIENTO DEL DISEÑO Y LA CONFIGURACIÓN POR DEFECTO DEL SISTEMA DE *groov* EPIC

Para ver cómo ayuda el *groov* EPIC con el diseño de un sistema seguro, se verá el diseño de seguridad y los valores por defecto del EPIC en las siguientes categorías:

- Sistema operativo
- Interfaces de red
- Herramientas de networking
- Cortafuegos (firewall)
- Cuentas
- Gestión de certificados de seguridad
- Opciones para comunicación de datos
- Diseño de seguridad adicional para desarrolladores

Sistema operativo

Diferente a los controladores y computadoras tradicionales que normalmente se utilizan en la automatización o en el internet industrial de las cosas (IIoT), los procesadores de *groov* EPIC se basan en una compilación a medida y específica del código abierto del sistema operativo de Linux®. Al contrario de lo que se piense, un sistema operativo de código abierto es, en muchos sentidos, más seguro que uno cerrado (especialmente un sistema operativo conocido y frecuentemente atacado como Microsoft® Windows®).

Primero, *groov* EPIC solo incluye lo necesario en el sistema operativo, el cual reduce ataques. Por ejemplo, se puede comparar esta vulnerabilidad limitada con Windows, el cual incluye componentes para todo tipo de propósitos. "La vulnerabilidad más fácil de enfrentar es la que no se incluye", indicó Ryan Ware, Arquitecto de Seguridad para Intel®, en 2017.

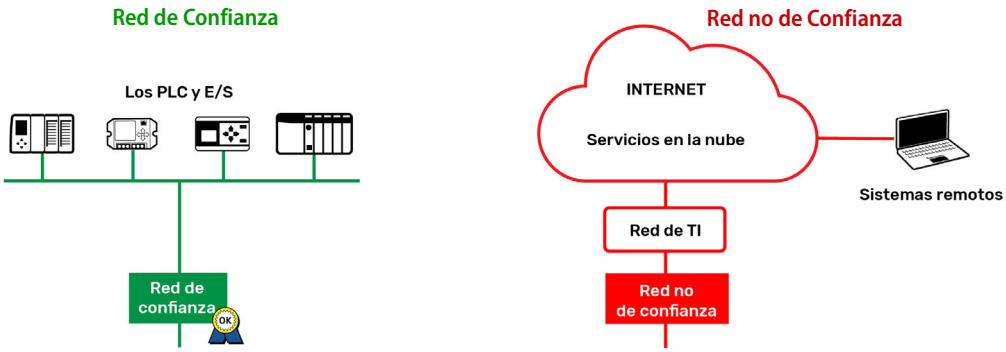
En segundo lugar, el código abierto significa una colaboración abierta. Debido a la cantidad de desarrolladores que trabajan con Linux, las vulnerabilidades tienden a corregirse rápidamente, mucho más rápido que en una sola empresa de software con un número limitado de desarrolladores.

En tercer lugar, y lo más importante, la compilación Yocto Opto 22 de EPIC Linux está **firmada criptográficamente** con la clave privada de Opto 22. Esto significa que cualquier firmware o paquete de software que un pirata informático pueda intentar cargar al procesador EPIC, no se aceptará; sólo firmware y paquetes firmados criptográficamente por Opto 22 se podrán cargar.

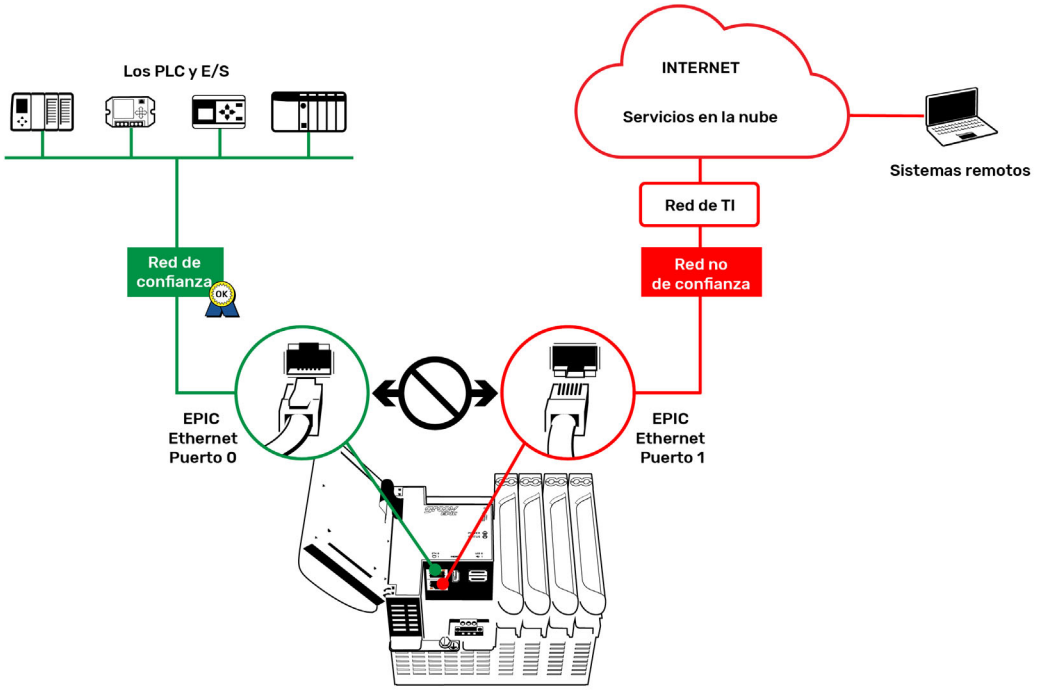
Interfaces de red

Un concepto clave en la especificación ISA/IEC 62443-3 acerca la ciberseguridad industrial es la zonificación: el mantenimiento de redes aisladas para evitar el acceso no autorizado a los datos. *groov* EPIC incluye dos interfaces independientes de Ethernet que aíslan la red confiable (en ETH0) de la red no confiable (en ETH1).

- Una **red de confianza** es cualquier red en la que se sabe exactamente quién tiene acceso a ella, por ejemplo, la red de OT (tecnología operativa), donde se encuentran los PLC y las E/S existentes.
- Una **red que no es de confianza** es cualquier red en la que no se sabe quién tiene acceso a ella, como una red de TI o el Internet.



groov EPIC no es un router, el cual funciona para unir dos redes. Al contrario, la configuración por defecto de *groov* EPIC mantiene las redes confiables y las redes no confiables separadas en zonas distintas. Por defecto, esta configuración elimina la posibilidad de exponer dispositivos no seguros en la red a los demás.



Además, se pueden agregar interfaces de red adicionales, junto con las dos interfaces integradas de Gigabit Ethernet. Por ejemplo, se puede agregar una red WiFi (una WLAN) a *groov* EPIC utilizando un adaptador WiFi USB aprobado, conectado al puerto USB del procesador EPIC. (Para obtener más información sobre los adaptadores aprobados, consulte el *groov EPIC User's Guide*).

También puede agregar un túnel de red privada virtual de OpenVPN a través de una existente interfaz de red física (Ethernet o WiFi), para proporcionar acceso remoto al procesador *groov* EPIC con un conexión autenticada y encriptada. (Obtenga más información en "VPN (red privada virtual)" en la página 4.)

Ambas interfaces, tanto la red inalámbrica como el túnel VPN, son independientes entre sí y las interfaces de Ethernet, y por defecto, la configuración de EPIC las coloca en zonas separadas. Esta combinación de múltiples interfaces de red independientes, proporciona mucha versatilidad, y a la vez, proporciona muchas formas para aislar los dispositivos no seguros en la red, de las redes que no son de confianza.

Herramientas de networking

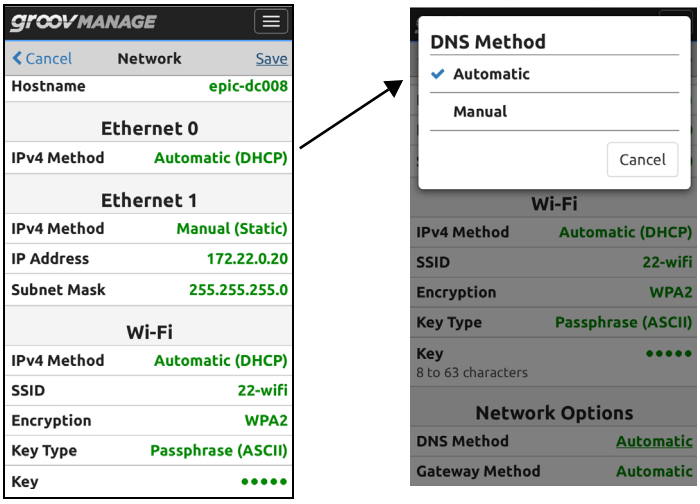
Para facilitar las comunicaciones de datos de *groov* EPIC y hacerlas más seguras, el software de configuración basado en web de *groov* Manage, proporciona herramientas de red configurables, incluso servicios de red estándar, redes privadas virtuales (VPNs), y una función de redireccionamiento de puertos para establecer conexiones de datos entre zonas.

Servicios de red estándar

En todas las interfaces de red, *groov* EPIC utiliza servicios de red estándar como DHCP y DNS.

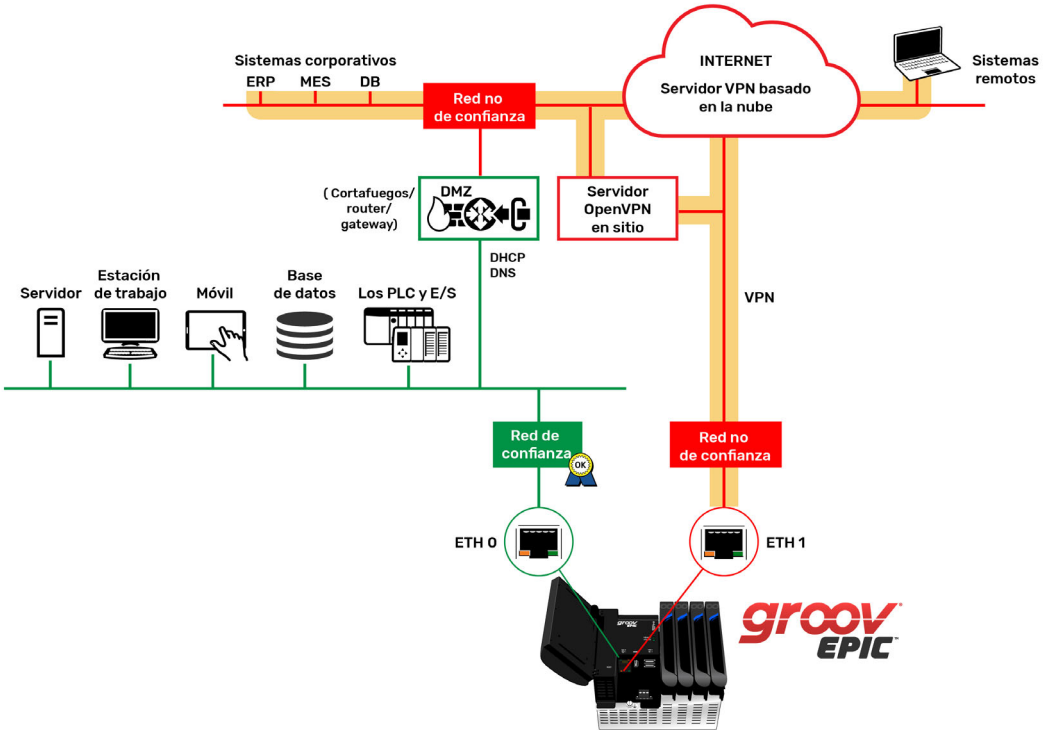
- **DHCP** (Dynamic Host Configuration Protocol) asigna de forma dinámica y automática, direcciones IP al procesador EPIC.
- Los servicios de **DNS** (Domain Naming System) facilita acceso al EPIC en la red porque permite usar un nombre de host en lugar de una dirección IP. (Es común usar DNS para llegar a sitios web como google.com con el nombre "google.com" en lugar de usar la dirección IP de los servidores de Google.)

Si es necesario, el *groov* EPIC se puede configurar con configuraciones opcionales de IP estáticas, pero el estándar es usar DHCP y DNS. Para la resolución de nombres y acceso a otras redes por medio de comunicaciones salientes originadas en el dispositivo, se puede utilizar *groov* Manage para elegir direcciones DNS y Gateway estándares, y la configuración automática o manual.



VPN (red privada virtual)

Para los usuarios que necesitan acceso a *groov* EPIC desde una red que no es de confianza (por ejemplo, si están usando el internet fuera de las instalaciones o en una LAN de TI que no se considera confiable), pueden usar un túnel VPN. La VPN es una forma de comunicación de datos segura, encriptada, y originada en el dispositivo, que accede al EPIC desde una red que no es de confianza. Un cliente de OpenVPN está incluido en el *groov* EPIC.



Se puede utilizar *groov* Manage para configurar conexiones de VPN como interfaces de red adicionales en el EPIC. Estas interfaces adicionales se conectan a servidores configurados externamente y son compatibles con OpenVPN, lo cual permite que otros clientes se conecten al mismo servidor VPN para tener acceso a las aplicaciones de software en EPIC. Los servidores OpenVPN se pueden ubicar en las instalaciones, o en la nube con productos de servicios de VPN como OpenVPN Cloud.

Los túneles VPN requieren que exista una interfaz de red física, como una interfaz Ethernet o una interfaz opcional de WiFi, para que funcione. Cuando se configura la interfaz VPN, intenta conectarse al servidor VPN a través de una interfaz de red física existente. Es probable que también se requiera un gateway válido en esa interfaz para que EPIC pueda llegar al servidor VPN y establezca el túnel VPN.

Cualquier cliente (como una PC o dispositivo móvil) que esté configurado correctamente con un cliente apropiado de OpenVPN Connector, puede iniciar una sesión de forma segura en el servidor VPN utilizando una cuenta válida o un archivo de configuración de cliente OpenVPN (.ovpn). Una vez conectado, el cliente puede tener acceso a las aplicaciones de software en EPIC, como *groov* Manage o *groov* View.

Por defecto, el acceso VPN a un procesador de *groov* EPIC proporciona acceso solo al software que se ejecuta en ese EPIC, no a cualquier otro dispositivo conectado al EPIC a través de otras interfaces de red. Pero si se desea permitir el acceso a otros dispositivos, se puede configurar la función de redireccionamiento de puertos, Port Redirect, para crear un conducto entre varias interfaces de redes. (Ver "La función de redireccionamiento de puertos: creación de conductos entre zonas" en la página 6.)

MADE IN THE USA

El uso de un VPN para recibir apoyo para los productos

También se puede crear un túnel VPN seguro para recibir apoyo técnico de Opto 22.

Se supone que tiene problemas con el sistema *groov* EPIC y se comunica con el grupo de Apoyo Técnico para conseguir ayuda. Si sería provechoso, se puede abrir un túnel VPN con *groov* Manage para que el ingeniero de apoyo técnico pueda tener acceso temporalmente al dispositivo cuando le ayude a resolver el asunto. (Ver imagen a la derecha).

Se necesitará un gateway configurado correctamente para llegar a la Internet y poder conectar al servidor VPN de Apoyo Técnico de Opto 22.

La función de redireccionamiento de puertos: creación de conductos entre zonas

En algunos casos, es posible desear llegar a dispositivos que se encuentran en una zona de red aislada por el *groov* EPIC. Por ejemplo, quizá hay otro PLC o dispositivo en la red de confianza (la red OT), y desea llegar desde otra red confiable (como un VPN), u otra interfaz de red configurada. Posiblemente se necesita realizar cambios en ese PLC o dispositivo desde el software propietario de ese sistema (por ejemplo, conectar el software RSLinx de Rockwell Automation® a un PLC Allen-Bradley®). Normalmente, estas conexiones no son seguras.

Por diseño, la configuración estándar de EPIC no enruta tráfico entre sus interfaces de red. Sin embargo, hay una función avanzada en la versión de firmware *groov* EPIC 3.2 o superior, que permite designar un redireccionamiento de puerto para permitir el tráfico que viene de una red de interfaz que pase a una dirección IP o puerto de host en otra interfaz, para la creación de un conducto entre zonas.

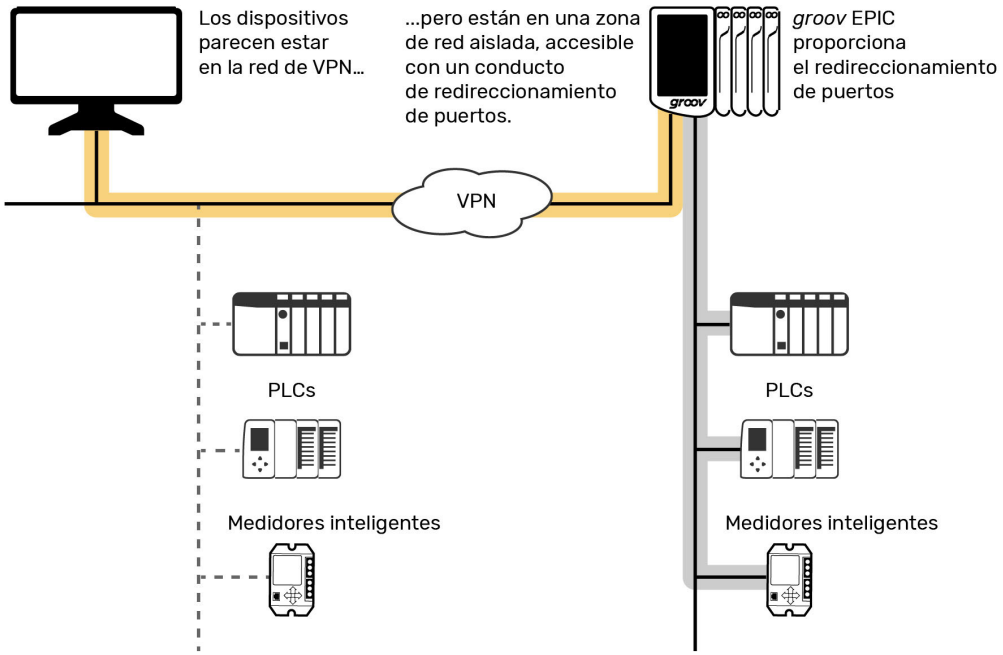
PRECAUCIÓN: *¡Tenga mucho cuidado para asegurar que no exista un puerto abierto en una interfaz de red que no sea de confianza!*

Como se discutió anteriormente, la mejor práctica es cerrar todos los puertos de red inseguros (como el puerto 502 de Modbus®/TCP) en interfaces de red que no son de confianza. Sin embargo, un túnel VPN creado en una interfaz de red que no es de confianza, solo permite comunicaciones de datos autenticadas y cifradas a través de esa interfaz, de modo que sólo los usuarios autorizados puedan acceder.

En este caso, se configura un redireccionamiento de puerto, o sea, un conducto, desde la interfaz del túnel VPN, para redirigir paquetes de la zona de red no confiable donde está establecido el túnel VPN, a la zona de red confiable, donde está el PLC inseguro. Idealmente, el conducto es activado solo por encargo y solo por un tiempo limitado. Se puede hacer de dos maneras:

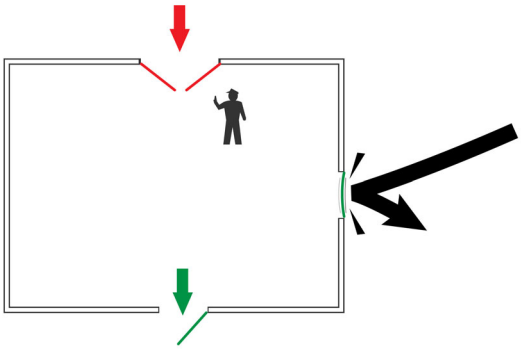
- Directamente en *groov* Manage con HTTPS seguro (puerto 443)
- Programáticamente con aplicaciones en el EPIC como Node-RED, Ignition Edge, PAC Control, u otro software que utiliza la API REST de EPIC para habilitar y deshabilitar la redirección del puerto

Este escenario ofrece un método temporal y totalmente seguro para acceder a dispositivos en una zona de red aislada desde cualquier sitio donde una conexión de cliente de VPN esté establecida. Estos dispositivos parecen estar en la red de VPN, pero en realidad están en otra zona de red que está conectada al *groov* EPIC.



Cortafuegos

Los cortafuegos son fundamentales para proteger las comunicaciones de datos. Un cortafuegos en una red o en un dispositivo (un host) funciona como las puertas de un edificio. Muchas veces, la puerta de la entrada principal de un edificio se abre hacia adentro para que se pueda entrar, y un guardia de seguridad o recepcionista verifica la identificación y se fija en quien va y viene. Las puertas de salida de emergencia se abren únicamente para afuera. Están cerradas por fuera para mantener la seguridad, pero la gente dentro del edificio pueden salir fácilmente si quieren.



Los cortafuegos bloquean el tráfico entrante que no es deseado, pero permiten el tráfico saliente según sea necesario.

En una red o dispositivo con un cortafuegos, las comunicaciones pueden salir a servidores o servicios externos, parecido a cómo salen las personas por medio de las puertas de salida de emergencia en un edificio. Pero las comunicaciones que llegan y tratan de entrar son rechazadas, como cuando las personas no pueden entrar por las salidas de emergencia cerradas. Estas comunicaciones entrantes se permiten sólo a través de un puerto de red específico que fue abierto para permitirlas, y solo con la encriptación y las credenciales correctas. Nuevamente, es como entrar a través de la puerta principal de un edificio, pero solo si tienen una identificación y una cita para visitar a alguien adentro.

El procesador de *groov* EPIC tiene un cortafuegos configurable que es fundamental para mantener la seguridad del sistema. Los cortafuegos del dispositivo proporciona seguridad al no permitir el tráfico no solicitado de llegar a las redes configuradas del EPIC, las aplicaciones de software, y los dispositivos conectados. Normalmente, el único tráfico que permite llegar son las respuestas al tráfico que se originó en el software de EPIC. Las conexiones originadas por dispositivos son clasificadas como confiables porque se conoce el origen.

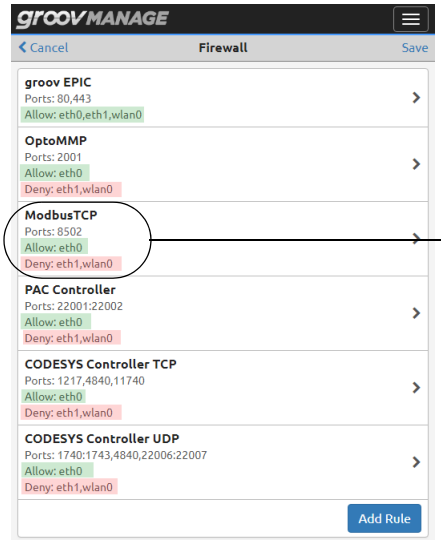
Cada interfaz de red en el EPIC, las dos interfaces Ethernet (ETH0 y ETH1), la interfaz opcional inalámbrica (WLAN0), y la interfaz opcional de VPN (TUN0), tiene su propia configuración de cortafuegos. Se puede establecer reglas de cortafuegos individuales para cada interfaz, para redes confiables (donde los puertos inseguros están abiertos) y redes no confiables (donde solo deben estar abiertos los puertos encriptados y autenticados). A continuación con la configuración por defecto del cortafuegos para las dos interfaces de Ethernet.

La configuración estándar del cortafuegos de EPIC

Por defecto, la configuración del **cortafuegos interno** del procesador EPIC asume que se utilizan las dos interfaces de red como fueron diseñadas: para aislar zonas de red confiables y no confiables:

- En la interfaz de red de **confianza** de Ethernet (**ETH0**), *groov* EPIC permite las comunicaciones de red a través de puertos necesarios para protocolo industrial, pero que son inseguros y abiertos. Estos puertos permiten comunicación con software y protocolos en el procesador EPIC, como por ejemplo:
  - PAC Control™ y CODESYS® (herramientas de desarrollo)
  - OptoMMP (protocolo utilizado por las E/S de EPIC)
  - Modbus/TCP (para comunicación con los PLCs y otros dispositivos)
- En la interfaz de red de Ethernet que **no es confiable** (**ETH1**), *groov* EPIC permite el tráfico solo por el puerto seguro de 443 y solo permite el acceso autenticado a través de conexiones seguras y encriptadas. Esta interfaz de red proporciona acceso encriptado y autenticado a *groov* Manage, *groov* View, Node-RED, y la API RESTful.
- Todos los demás puertos de entrada en la interfaz ETH1 de la red de Ethernet, están **bloqueados por defecto**.

En *groov* Manage, se presenta la configuración de cada interfaz para cada aplicación, así para ver claramente a cuáles aplicaciones se les permite acceso, y a cuáles bloquear:



La configuración por defecto, según la aplicación para las interfaces de red de confianza de Eth0, y no de confianza de Eth1.

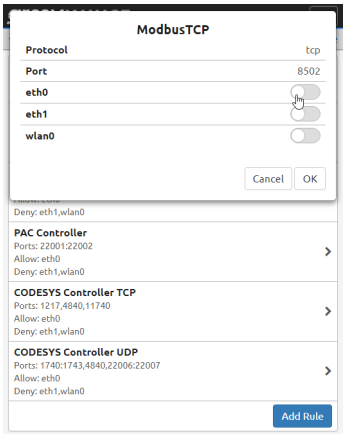
Nota: El puerto 80 está abierto, pero todo el tráfico se redirige automáticamente al puerto seguro de 443.

Por ejemplo, el protocolo de Modbus/TCP es permitido por defecto, en la interfaz de confianza, pero bloqueado en la interfaz no de confianza.

Recordar que la configuración por defecto asume que ETH0 está en una red confiable. Hay que verificar que la red en realidad es confiable.

Se puede configurar el cortafuegos de EPIC para cada interfaz y adaptarla a la aplicación. Por ejemplo, se puede cambiar la configuración estándar y cerrar los puertos para cualquiera de los servicios que no se

utilicen. En el ejemplo que sigue, si no se utiliza Modbus/TCP, hay que cerrar el puerto 8502 para no permitir tráfico, incluso en la interfaz de red de confianza:



Para mayor seguridad, se deben cerrar puertos que no se ocupan.

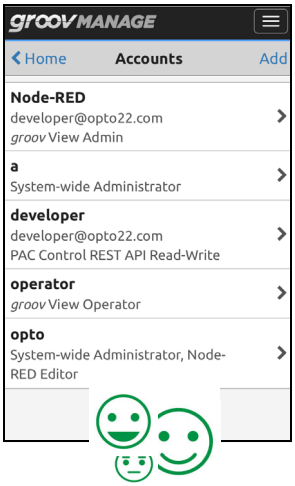
Clientes y servidores

Hay que tener en cuenta que *groov* EPIC puede ser ambos un cliente (un dispositivo que origina conexiones) y un servidor (un dispositivo que escucha las solicitudes de conexión). La configuración del cortafuegos varía según el uso de EPIC. Por ejemplo:

- MQTT, el cliente de OpenVPN, y los nodos de Node-RED, son clientes que originan comunicaciones e intentan comunicarse con otros servidores que corren en el EPIC. Por ejemplo, MQTT origina comunicaciones a un servidor de MQTT central, el broker. Los nodos de Node-RED originan comunicaciones a servidores SQL, servicios basados en la nube, y así por el estilo. No es necesario tener configuraciones de puertos entrantes en el cortafuegos para clientes que se ejecutan en el EPIC. Las comunicaciones son salientes y permitidas por defecto por el cortafuegos de EPIC. (Ver más sobre MQTT en la página 11.)
- El *groov* View que corre en el EPIC es un servidor que escucha las peticiones de las PC o dispositivos móviles que ejecutan navegadores. Por defecto, el cortafuegos de EPIC está configurado para abrir el puerto seguro de HTTPS (puerto 443), utilizado por *groov* View para permitir conexiones entrantes. Estas conexiones están encriptadas y requieren autenticación por los usuarios.

Ya sea si EPIC responde como un cliente o un servidor, al establecer las comunicaciones, los datos pueden fluir en ambas direcciones, con tal que la conexión esté activa.

Cuentas



El control de quién tiene acceso a datos y qué exactamente puede hacer cada usuario con ellos es una parte esencial de la ciberseguridad. Cuando arranca *groov* EPIC por primera vez, se requiere una cuenta de administrador local con nombre de usuario y contraseña antes de poder seguir adelante. El procesador EPIC no tiene un nombre de usuario ni contraseña por defecto que alguien pueda adivinar. Las credenciales de la cuenta del administrador no son recuperables por razones de seguridad.

groov EPIC proporciona **administración de cuentas de usuario** a través de *groov* Manage. Se pueden crear cuentas de administrador, desarrollador, operador, API REST y más, y luego se pueden asignar esos derechos de usuario a personas autorizadas o a servicios de software. La autenticación (a través de una conexión encriptada) se realiza mediante el nombre de usuario/contraseña o token de API.

Todos los usuarios pueden crear contraseñas largas y complejas que incluyen números, mayúsculas, puntuación, espacios, frases, y palabras en cualquier idioma, e incluso emoticonos.

LDAP (protocolo ligero para acceso a directorios)

Si la instalación maneja cuentas de usuario a través de un servicio LDAP (por ejemplo, Microsoft Active Directory Service), se puede trabajar con el departamento de TI para configurar el *groov* EPIC usando *groov* Manage, y **conectarlo al servidor LDAP**, autenticar a un usuario, y determinar cuáles servicios un usuario puede acceder. Para configuraciones sencillas, se puede utilizar el servidor LDAP para autenticar a los usuarios y darles permisos predeterminados. Para sistemas con un mayor número de usuarios o una gestión de usuarios más compleja, se puede utilizar *groov* Manage para asignar un grupo de LDAP a un conjunto de permisos específicos.

*NOTA: La cuenta de administrador original para groov EPIC provee acceso directo y local al EPIC y **no** está administrado por el servicio LDAP.*

Los detalles sobre cómo funcionan los permisos y cómo asignarlos se encuentran en el Capítulo 6 del documento *groov EPIC User's Guide*.

Gestión de certificados de seguridad

Los certificados de seguridad son una forma que permite a los clientes verificar los servidores, de modo que cuando uno intenta conectarse, se puede asegurar que está comunicando con el servidor correcto y no con uno malicioso. *groov* EPIC proporciona **gestión de certificados** integrada con *groov* Manage.

El sistema EPIC admite conexiones de clientes certificados por el estándar PKI X.509 a servidores seguros (Cliente SSL), y de los clientes al servidor seguro de EPIC (servidor SSL) utilizando certificados TLS/SSL, los cuales pueden ser generados por el dispositivo, autofirmado, o registrado públicamente a través de una autoridad de certificación (CA). Para obtener más información sobre certificados, consulte el *groov EPIC User's Guide* y los ejemplos en developer.opto22.com.

Opciones de comunicación de datos para mayor seguridad

Como fue explicado en la sección de "Cortafuegos,", un dispositivo es más seguro y requiere menos configuración de seguridad cuando **inicia la comunicación de datos** a través de un puerto de red saliente en lugar de tener que abrir un puerto para recibir peticiones de conexión.

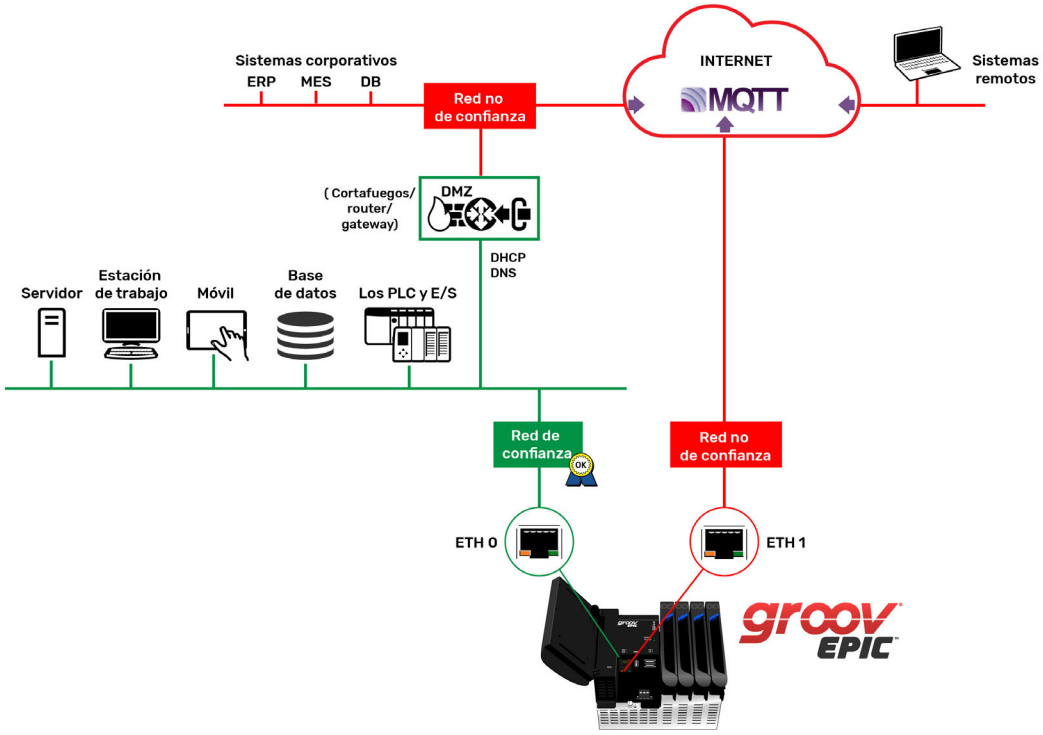
La publicación/suscripción (pub/sub) es una forma de comunicación que aprovecha esta mayor seguridad al utilizar únicamente comunicaciones originadas desde el dispositivo. *groov* EPIC usa MQTT, un protocolo pub/sub, para reportar el estado (autenticado y encriptado) a un broker central. Al conectar al broker, la conexión es persistente y el EPIC se puede suscribir a cualquier instrucción nueva o a mensajes de estado de otros dispositivos, y así, proporcionar comunicación bidireccional.

Como el flujo de datos MQTT origina en el dispositivo, el cortafuegos permite la salida de datos, mantiene seguimiento del estado de la sesión, y permite pasar los paquetes que regresan del broker.

La conexión persistente de MQTT es el mecanismo crítico que usa el broker para determinar el estado de las conexiones de los clientes a todos tiempos. En un modelo pub/sub para SCADA (control de supervisión y adquisición de datos) o comunicaciones industriales, siempre se quiere asegurar que los clientes están conectados. Si la conexión persistente de un publicador de datos está interrumpida, el broker notifica esto a todos los clientes suscritos para que todos sepan el estado del sistema.

Por el contrario, en las comunicaciones de solicitud/respuesta, las conexiones no persisten si los clientes no las mantienen. Por ejemplo, si Node-RED (un cliente) se conecta a un servidor SQL, cuando los datos se envían desde el cliente al servidor y el servidor responde, la conexión se cierra. Las transferencias de datos que siguen, tienen que ser iniciadas cada vez por el cliente. En el ejemplo de *groov* View, el cliente (el navegador web) mantiene la conexión abierta al servidor (*groov* View) mientras la sesión web del cliente esté activa.

La comunicación originada desde el dispositivo a veces se llama por medio de un puerto saliente. Al contrario, cuando el dispositivo tiene que tener configurado un puerto abierto para poder recibir comunicaciones originadas desde el exterior, puede ser llamado con un puerto entrante. Por medio de comunicaciones de datos salientes que se originan en el dispositivo, como MQTT, *groov* EPIC ofrece una opción segura que requiere mucho menos configuración. Para obtener más información sobre el uso de MQTT, consulte el documento técnico: *White Paper: Industrial-strength MQTT/Sparkplug B* (formulario 2357, en la página web) y *Getting Started with MQTT in groov Products* (formulario 2350)



COMBINANDOLO TODO

Las redes industriales modernas muchas veces tienen muchos requisitos, incluso:

- Detección y control de E/S en tiempo real
- Integración de red de varios proveedores
- Adquisición de datos de dispositivos en campo

Y los datos de los sistemas de control y los dispositivos en campo pueden ser utilizados por:

- Software y servicios locales y en la nube
- Aplicaciones que utilizan comunicaciones MQTT, como el Historiador de Canary
- PCs remotas que necesitan acceso VPN a datos industriales o que requieren establecer un conducto a PLCs viejos
- Sistemas SCADA y HMI que utilizan datos industriales para monitoreo, control y recolección.

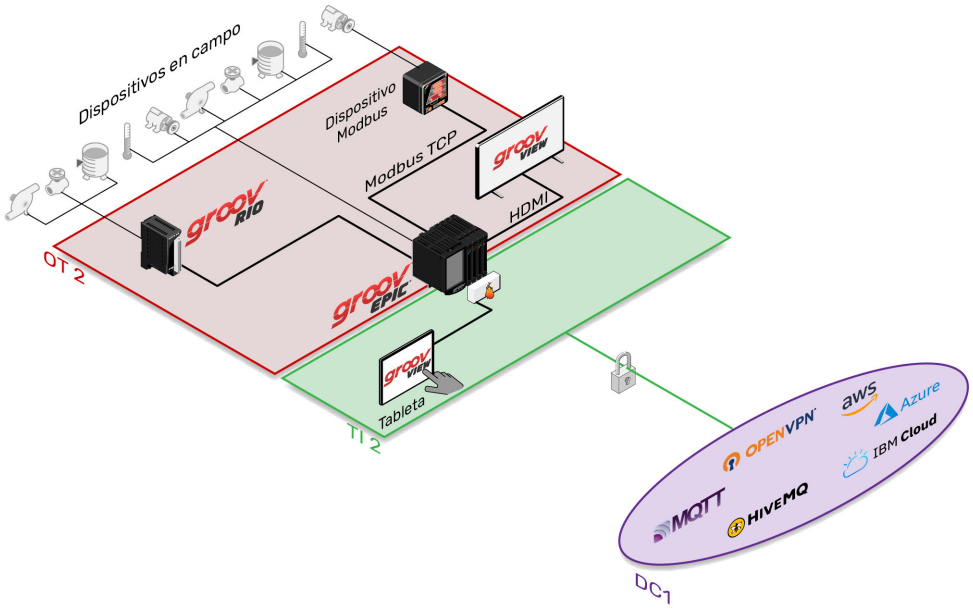
¿Cuáles de los requisitos se necesitan, y cómo interconectar estas opciones? A continuación para ver cómo ayuda el *groov* EPIC a proteger esta infraestructura compleja y conectar datos desde varios puntos enuna arquitectura completa del sistema.

Detección y control de E/S en tiempo real

Se comenzará con una aplicación de control en tiempo real, posiblemente operando en un zona peligrosa. Los activos tradicionales en campo como sensores e interruptores están conectados directamente a los módulos de E/S de *groov* EPIC o a los módulos remotos de *groov* RIO. El EPIC también comunica con dispositivos Modbus a través de Modbus/TCP y proporciona una interfaz de operador local mediante *groov* View y una pantalla conectada al puerto HDMI.

Con los cortafuegos e interfaces de red independientes, el EPIC delinea dos zonas de seguridad: una red para el sistema de control local (OT2) y otra red no confiable para clientes externos (TI2).

El EPIC envía datos a través de conexiones cifradas a varios PC y a dispositivos móviles en TI2 o por medio de aplicaciones locales y en la nube.



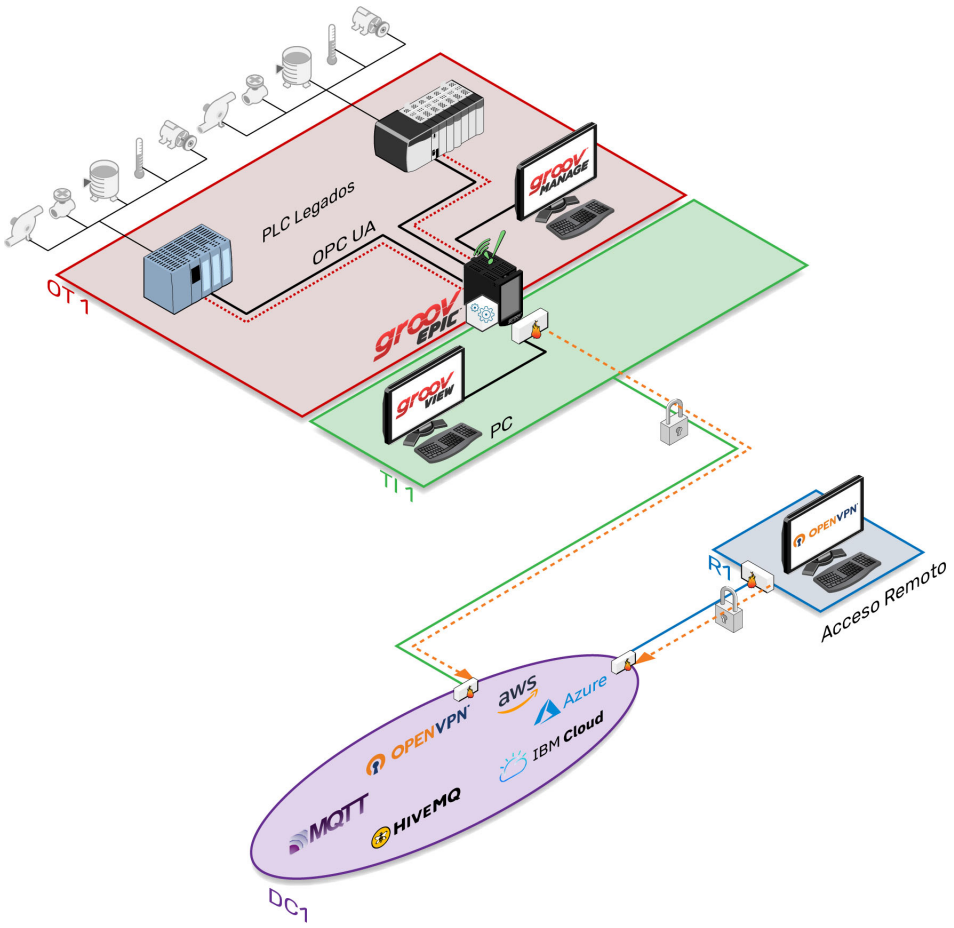
Integración de red con activos de varios vendedores

¿Qué sucede si hay un sistema existente, pero se necesita obtener los datos que están bloqueados en los PLC heredados? En este ejemplo, el *groov* EPIC se utiliza por las capacidades de enrutamiento/IIoT. Si no se necesitan E/S, se puede ocupar solo el procesador en un chasis para cero módulos (GRV-EPIC-CHS0).

Debido a que EPIC corre Ignition de Inductive Automation, se puede conectar a los PLC heredados a través de OPC UA y comunicar los datos del PLC. Y aquí nuevamente, el EPIC separa las redes de OT y TI entre dos zonas para mantener la seguridad.

Todos los datos necesarios de los sistemas heredados se pueden usar de la misma manera, en el HMI *groov* View (localmente y en dispositivos móviles), y en el software y los servicios de las instalaciones o en la nube (DC1), incluso túneles VPN (línea de puntos anaranjada).

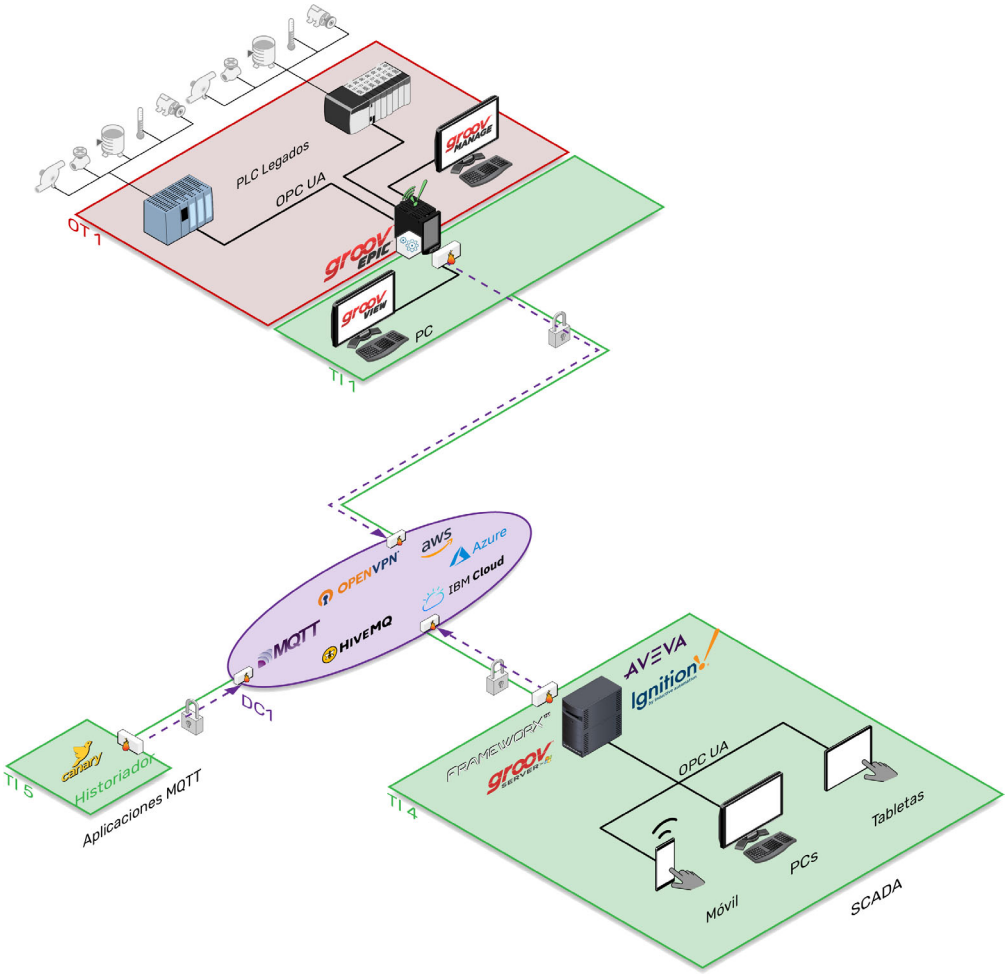
Y otra ventaja: acceso a los PLC de forma segura. Por ejemplo, se supone que se necesita actualizar el programa de un PLC desde una PC en otro sitio (R1). Con un VPN y la función de redireccionamiento de puertos en el EPIC, se puede establecer un conducto (línea de puntos roja) para acceder al PLC de forma segura y realizar el cambio.



MQTT/Sparkplug B para la integración de varios vendedores

El uso de MQTT/Sparkplug B agrega eficiencia, escalabilidad, e interoperabilidad a las comunicaciones de datos y amplía las aplicaciones que se pueden integrar con *groov* EPIC. Con MQTT, datos de dispositivos y sistemas controlados por el EPIC, como los datos de PLC heredados, se comunican a través de una conexión saliente, que, una vez establecida, permite que los datos fluyan en ambas direcciones sin requerir puertos abiertos de cortafuegos (ver "Opciones de comunicación de datos para mayor seguridad" en la página 11).

Este diagrama muestra cómo se mueven los datos a través de las conexiones MQTT/Sparkplug B (línea de puntos morada). Aplicaciones MQTT como el Historiador de Canary pueden intercambiar datos fácilmente con dispositivos y sistemas en campo, al igual que los sistemas de SCADA.



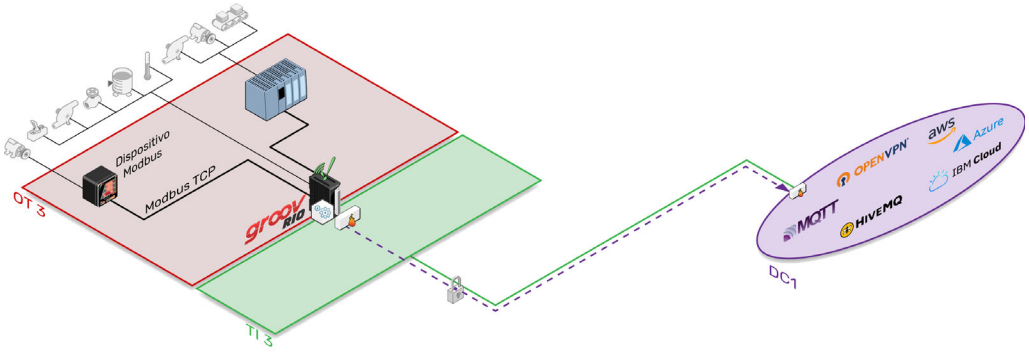
MADE IN THE USA

Adquisición de datos de dispositivos en campo

Se supone que no se necesita la capacidad de control en tiempo real, pero aún se necesitan datos de los dispositivos en campo. Aquí está donde el módulo de E/S edge de *groov* RIO MM2 es destacado. Se comunica usando el protocolo Modbus a dispositivos de Modbus, se conecta directamente a dispositivos en campo y corre Ignition Edge con drivers de software para los PLC, para adquirir datos de todo el sitio.

Igual a EPIC, *groov* RIO puede compartir los datos adquiridos con otros dispositivos y software en las instalaciones y en la nube utilizando MQTT/Sparkplug B y/o un VPN.

El cortafuegos y la encriptación del dispositivo de *groov* RIO ayudan a proteger este sitio. Aunque *groov* RIO no tiene dos interfaces de red Ethernet físicas como el EPIC, tiene hasta tres interfaces de red (Ethernet, WLAN, y VPN) que separan las redes entre zonas.

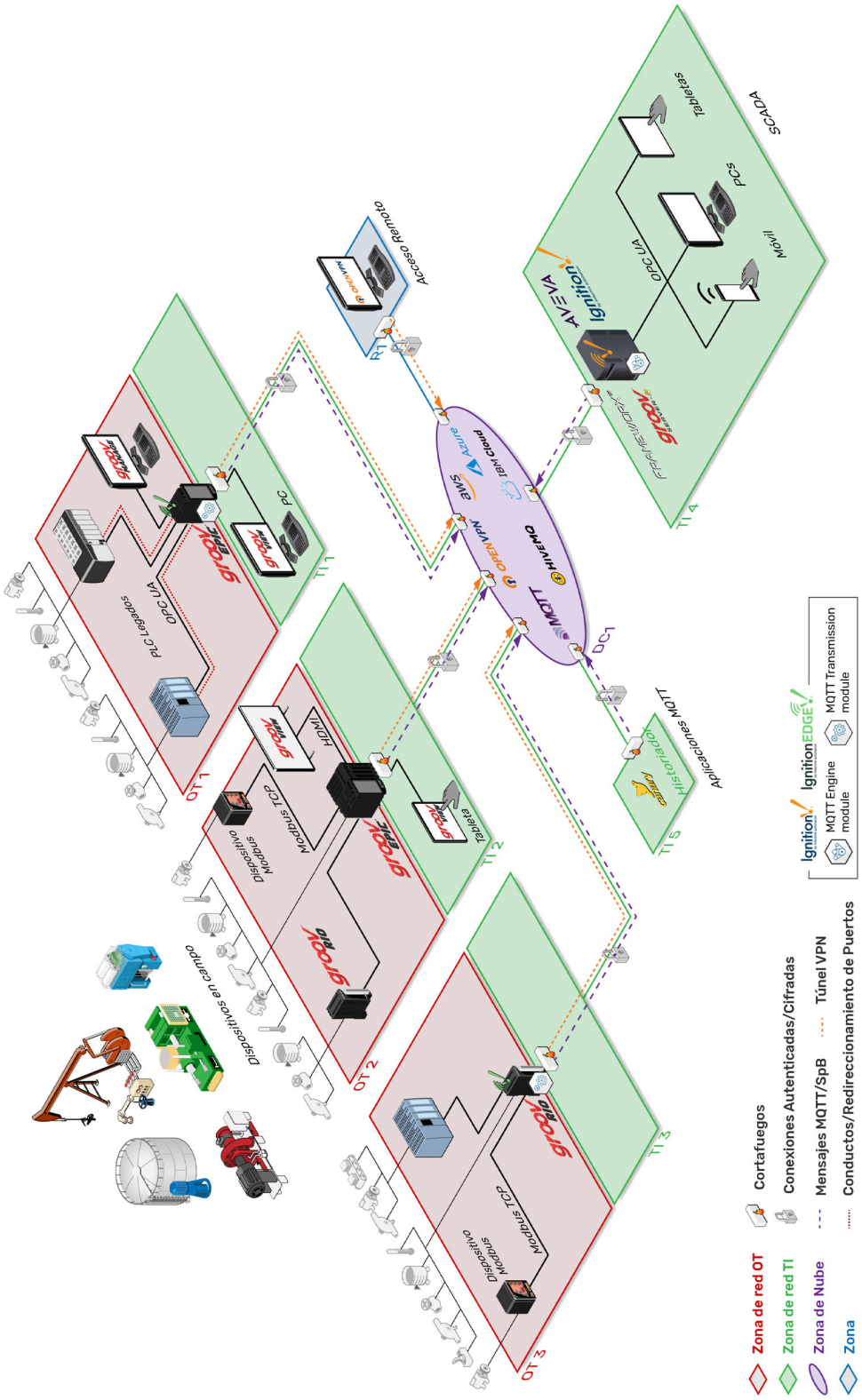


Escalabilidad fácil

Aquí está donde la arquitectura de *groov* EPIC/*groov* RIO realmente muestra su escalabilidad. Se puede construir fácilmente la infraestructura que ya se ha establecido (con o sin *groov* EPIC). Simplemente se agregan más módulos de *groov* RIO para integrar más dispositivos y adquirir datos de dispositivos en campo de otros sitios.

La arquitectura completa del sistema *groov* EPIC

En total, se ve una arquitectura de sistema que es flexible y escalable, y que puede ayudar a construir un sistema seguro para cumplir con los requisitos de proyectos. Revisar el diagrama que sigue y después las "Buenas Prácticas De Seguridad Para el groov EPIC" en la página 18



MADE IN THE USA

BUENAS PRÁCTICAS DE SEGURIDAD PARA EL *groov* EPIC

Cada situación es diferente y el profesional es el que sabe mejor qué acceso necesitará la aplicación y la arquitectura de red que utilizará. Sin embargo, como mencionado de principio a fín en esta nota técnica, *groov* EPIC fue diseñado para ayudar a crear un sistema seguro y ayudar abordar las pautas de seguridad que se indican en la norma ISA/IEC 62443. Según el diseño de EPIC, se recomienda ampliamente las siguientes mejores prácticas. Hay que tener en cuenta estas prácticas cuando se desarrollan las aplicaciones e implementan los proyectos.

Redes

- Colocar dispositivos no seguros (como los PLC o dispositivos heredados) solo en la zona de red confiable.
- Permitir sólo conexiones seguras, encriptadas y autenticadas en cualquier zona de red que no sea de confianza.
- Configurar el *groov* EPIC para utilizar la interfaz de red Ethernet ETH0 en la red de confianza.
- Utilizar ETH1 para cualquier red que no sea de confianza. Configurar excepciones en el cortafuegos del sistema solo si es necesario para la aplicación.
- Configurar el cortafuegos del sistema con *groov* Manage para cerrar todos los puertos en la red no utilizados en todas las interfaces de red.

Cuentas

- Exigir que todos los usuarios crean contraseñas largas y difíciles y que no las escriban en ninguna parte. Utilizar un administrador de contraseñas cuando corresponda.
- Trabajar con el departamento de TI para incluir *groov* EPIC si el sitio utiliza un servicio LDAP para la administración de usuarios.
- Utilizar una red VPN si se requiere acceso remoto y cifrado al EPIC a través de una red que no sea de confianza.
- Siempre cerrar la sesión de cualquier cuenta con privilegios de administrador para evitar el acceso no autorizado al procesador *groov* EPIC.
- Si el HMI *groov* View se corre en un monitor externo, siempre correrlo en modo quiosco o limitarlo para que solo pueda acceder a *groov* View.

Otras buenas prácticas

- Si se requiere un sistema completamente cerrado (por ejemplo, un OEM que utiliza *groov* EPIC en una máquina), después de terminar el desarrollo, hay que desactivar todos los puertos en el cortafuegos y desconectar todos los cables de Ethernet.

  Si alguien conecta un cable de Ethernet al EPIC para intentar acceso al sistema desde una computadora, los puertos estarán cerrados y el acceso a la red será denegado. Solo un usuario autorizado con privilegios de administrador puede acceder a *groov* Manage por medio de la pantalla integrada para reabrir los puertos necesarios para acceder a la red.
- Cuando sea posible, utilizar métodos de conexión originada por el dispositivo, saliente, autenticada y cifrada. Por ejemplo, utilizar MQTT para publicar datos a un broker MQTT. Métodos de comunicación de datos originada desde el dispositivo ayudan a:
  - Reducir los puertos abiertos entrantes en la red
  - Eliminar riesgos de intermediarios
  - No exponer credenciales confidenciales a través de la red

Para consideraciones adicionales durante el desarrollo de las aplicaciones, pasar a la siguiente página, "Diseño De Seguridad Adicional Para Los Desarrolladores."

DISEÑO DE SEGURIDAD ADICIONAL PARA LOS DESARROLLADORES

El diseño del sistema de *groov* EPIC proporciona acceso opcional al **Secure Shell (SSH)** para el desarrollo de aplicaciones, y a la vez, manteniendo la seguridad. De nuevo, hay herramientas en *groov* EPIC para ayudar en el diseño de un sistema seguro.

Se requiere una licencia para activar el acceso de Secure Shell (GROOV-LIC-SHELL). Esta licencia es gratuita. Al conseguir la licencia, se puede:

- Administrar el acceso al SSH y limitar el uso solo a la red de confianza.
- Configurar puertos específicos en el cortafuegos de *groov* EPIC según los parámetros de la aplicación.
- Instalar paquetes firmados criptográficamente desde el repositorio git de Opto 22.
- Compilar aplicaciones, supervisar los archivos de registro del servidor, iniciar y parar aplicaciones o servicios, y facilitar la transferencia de archivos.
- Hay que tener en cuenta que el apoyo técnico para sistemas que utilizan SSH es limitado.

Buenas prácticas adicionales para los desarrolladores

Además de las buenas prácticas recomendadas que comienzan en la página 18, los desarrolladores que usan SSH también deben hacer lo siguiente:

- Configurar acceso a SSH con un nombre de usuario y contraseña único y difícil, diferente al de *groov* Manage, *groov* View, o cualquier otro software que corre en *groov* EPIC.
- Habilitar acceso a shell solo para la configuración y programación del dispositivo. Al estar el sistema en servicio, hay que deshabilitar acceso a shell en *groov* Manage para prohibir acceso. Nunca hay que dejar acceso habilitado al SSH cuando el sistema está en producción.
- Nunca permitir acceso a SSH en una red que no sea de confianza.