groov PRODUCTS CYBERSECURITY DESIGN AND BEST PRACTICES

When you're gathering, processing, and sharing operational data from industrial equipment on premises or located remotely, cybersecurity is a big worry. Your systems and equipment—and the data in them—are essential and sensitive, and you need industrial internet of things (IIoT) devices and software that protect them.

For all digital systems, security is a complex issue with different implications depending on your organization and your system. Security requirements constantly change as your system evolves, and building security into your system design is key. As Bruce Schneier wrote back in 2000, "Security is a process, not a product."

To address security's complex, changing nature, you need to understand security risks, understand your environment, and understand the security tools you have to work with. Security experts recognize several elements of system security, including physical security, policies and procedures, and network security.

> **"Security is a process, not a product."**
>
> **- Bruce Schneier**

Opto 22's *groov* products—*groov* RIO edge I/O and the *groov* EPIC system—help you address network security requirements. Designed from the ground up to help you build a secure extended system, *groov* EPIC gives you the tools and methods necessary to make your system as secure as possible from a network access standpoint, while maintaining the flexibility you need for your implementation. In fact, no other industrial edge I/O or real-time controller currently on the market offers the same level of cybersecurity features and options.

Of course the ultimate security of your system depends on you, but *groov* products are here to help. This technical note describes the cybersecurity features built into *groov* RIO and *groov* EPIC and suggests best practices for setting up a secure system.

The application of these features can help you comply with security guidelines as outlined in the ISA/IEC 62443 specification, which provides "a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs)."[1]

For Help

As always, if you are using *groov* products and cannot find the help you need in this technical note or in the product user's guides (see list on page 2), contact Opto 22 Product Support. Product support is free.

Phone:	800-TEK-OPTO (800-835-6786 toll-free in the U.S. and Canada) 951-695-3080 Monday through Friday, 7 a.m. to 5 p.m. Pacific Time
Email:	support@opto22.com
Opto 22 website:	www.opto22.com

NOTE: Email messages and phone calls to Opto 22 Product Support are grouped together and answered in the order received.

[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

Related Documents

groov Product	Part number(s)	Document name	Form number
groov RIO Universal I/O	GRV-R7-MM1001-10 GRV-R7-MM2001-10	*groov* RIO Universal I/O User's Guide	2324
groov RIO EMU energy monitoring unit	GRV-R7-I1VAPM-3	*groov* RIO EMU User's Guide	2372
groov EPIC processor	GRV-EPIC-PR1 GRV-EPIC-PR2	*groov* EPIC User's Guide	2267

UNDERSTANDING *groov* PRODUCT DESIGN AND DEFAULT CONFIGURATION

To see how *groov* products can help you design a secure system, let's look at their security design and defaults in the following areas:

- Operating system
- Network interfaces
- Networking tools
- Firewalls
- Accounts
- Security certificate management
- Data communication options
- Additional security design for developers

Operating system

Unlike the traditional controllers, processors, and computers typically used in automation or industrial internet of things (IIoT) applications, the processors in *groov* products are built upon a custom, industry-specific build of the open-source Linux® operating system. Contrary to what you might think, an open-source OS is in many ways more secure than a closed one (especially a well-known and often-attacked OS such as Microsoft® Windows®).

First, a *groov* product includes only the operating system components necessary for its purpose, which reduces attack vectors. Contrast this limited vulnerability with Windows, for example, which includes components for all kinds of purposes. "The easiest vulnerability to address is the one you don't include," noted Ryan Ware, Security Architect at Intel®, in 2017.

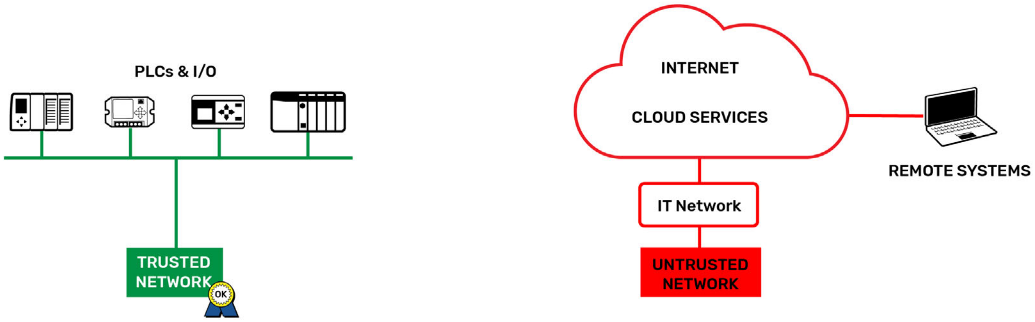
Second, open source means crowd sourced. Because of the number of developers working on Linux, vulnerabilities tend to be addressed very quickly—far more quickly than they can be at an individual software company with a limited number of developers.

Third, and most important, the Opto 22 Yocto build of Linux is **cryptographically signed** with the Opto 22 Private Key. That means that any firmware or software package a hacker might try to upload to the *groov* processor will not be accepted; only firmware and packages that are cryptographically signed by Opto 22 can be loaded.

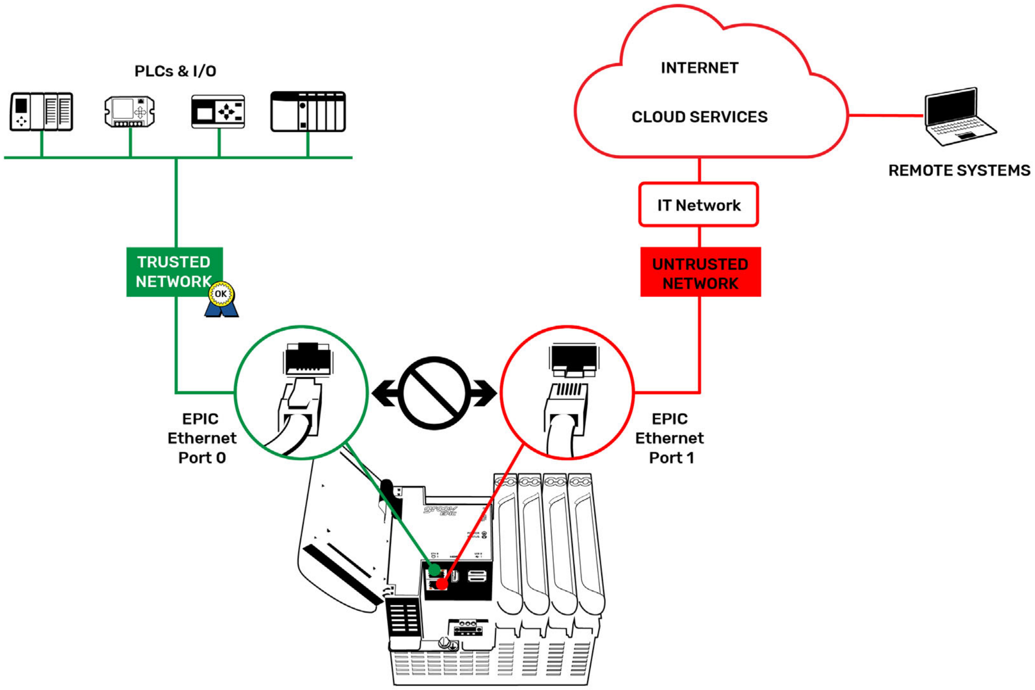
Network interfaces

A key concept in the ISA/IEC 62443-3 specification on Industrial Cybersecurity is *zoning*—keeping networks isolated to avoid unauthorized access to data. *groov* products include options for multiple network interfaces, to isolate trusted networks from untrusted networks.

- A **trusted network** is any network where you know exactly who has access to it, for example, your OT network where existing PLCs and I/O reside.
- An **untrusted network** is any network where you don't know who has access to it, like an IT network or the internet.



***groov* EPIC processors** include two independent Gigabit Ethernet interfaces, each with its own IP address, that isolate trusted networks (on ETH0) from untrusted networks (on ETH1). EPIC is not a router, which functions to join two networks together. Instead, *groov* EPIC's default configuration keeps your trusted networks and your untrusted networks apart, separating them into zones. This default configuration eliminates any chance of unsecure devices on one network interface being exposed to the others.



In contrast, *groov* RIO's two built-in network interfaces are not independent; they are switched and use the same IP address.

However, **both *groov* RIO and *groov* EPIC** provide additional network interface options. For example, you can add a **WiFi** network (a WLAN) to *groov* RIO or *groov* EPIC using an approved USB WiFi adapter connected to the USB port. (For more information on approved adapters, see the product user's guide.)

You can also add an OpenVPN **virtual private network** tunnel over an existing physical network interface (Ethernet or WiFi) to provide remote access to the *groov* product over an authenticated and encrypted connection. (Learn more in "VPN (virtual private network)" on page 5.)

Both the wireless network interface and the VPN tunnel are independent of each other and the Ethernet interfaces, and the default configuration places network interfaces in separate zones. This combination of multiple, independent network interfaces provides significant versatility, while creating many ways to isolate unsecure network devices from untrusted networks.

Networking tools

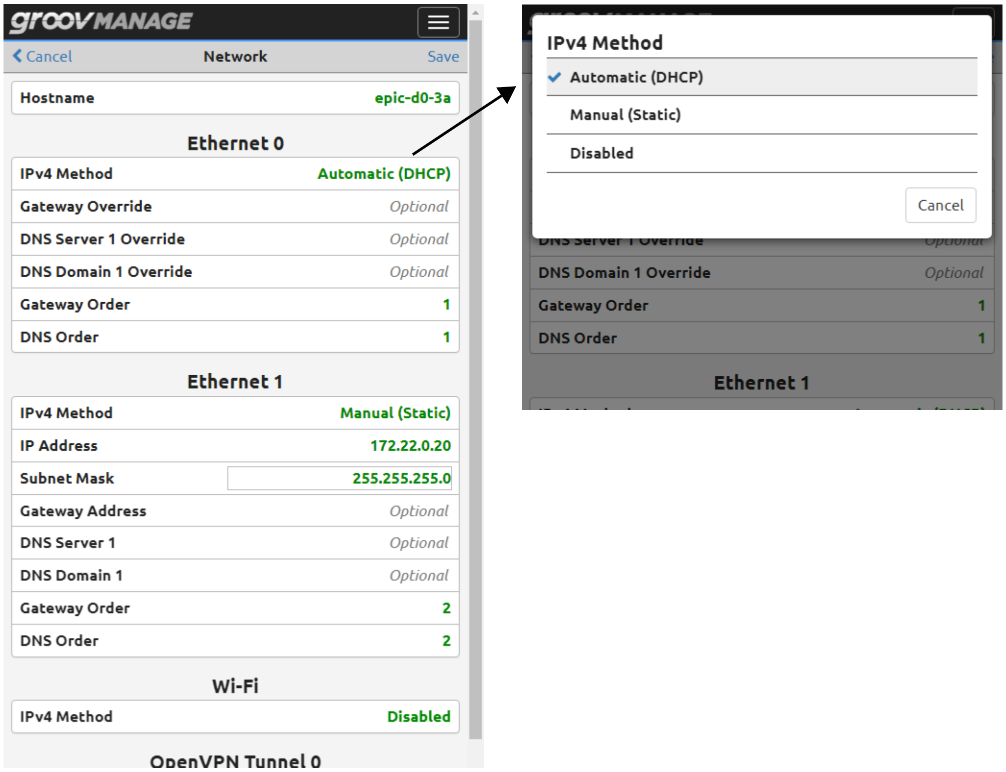
To make data communications easier and more secure, *groov* products' web-based configuration software, *groov* Manage, provides configurable networking tools, including standard network services, virtual private networks (VPNs), and a Port Redirect feature to establish data conduits between zones.

Standard network services

On all network interfaces, *groov* products use standard network services like DHCP and DNS.

- **DHCP** (Dynamic Host Configuration Protocol) dynamically and automatically assigns IP addresses to your *groov* RIO or EPIC.
- **DNS** (Domain Naming System) services make it easier to access your *groov* product on the network by letting you use a hostname rather than an IP address. (You use DNS every day to reach websites like google.com by typing in the name "google.com" rather than the IP address of Google's servers.)

If necessary, you can configure your *groov* device to use optional static IP configurations, but the default is DHCP and DNS. For name resolving and outbound, device-originating access to other networks, you can use *groov* Manage to choose standard DNS and Gateway addresses and automatic or manual configuration.



Hostname	epic-d0-3a

Ethernet 0

IPv4 Method	Automatic (DHCP)
Gateway Override	Optional
DNS Server 1 Override	Optional
DNS Domain 1 Override	Optional
Gateway Order	1
DNS Order	1

Ethernet 1

IPv4 Method	Manual (Static)
IP Address	172.22.0.20
Subnet Mask	255.255.255.0
Gateway Address	Optional
DNS Server 1	Optional
DNS Domain 1	Optional
Gateway Order	2
DNS Order	2

Wi-Fi

IPv4 Method	Disabled

OpenVPN Tunnel 0

IPv4 Method

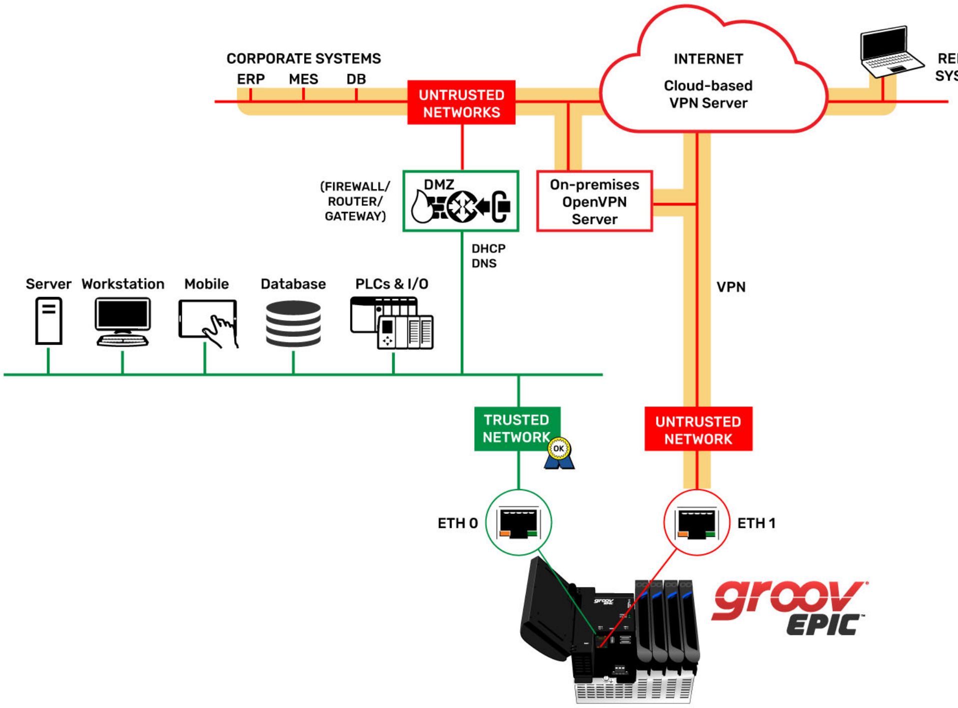
✓ Automatic (DHCP)
Manual (Static)
Disabled

DNS Domain 1 Override	Optional
Gateway Order	1
DNS Order	1

Ethernet 1

VPN (virtual private network)

For users who need to access *groov* RIO or EPIC from an untrusted network (for example, if they are offsite using the internet or on an IT LAN that is considered untrusted), you can use a VPN tunnel. VPNs are a secure, encrypted, device-originated data communication method to access your device from an untrusted network. An OpenVPN client is included in both *groov* RIO and *groov* EPIC.



You can use *groov* Manage to configure VPN clients as additional network interfaces on your *groov* RIO or EPIC. These additional client interfaces connect to externally configured OpenVPN-compatible servers, allowing other clients connected to the same VPN server to access your *groov* product's software applications. OpenVPN servers can be located on premises, or in the cloud with VPN-as-a-service products like OpenVPN Cloud.

VPN tunnels require an existing physical network interface—like one of your Ethernet interfaces or an optional WiFi interface—to work. When the VPN interface is set up, it attempts to connect to the VPN server over an existing physical network interface. A valid gateway on that interface will likely also be required so that the *groov* product can reach the VPN server and establish the VPN tunnel.

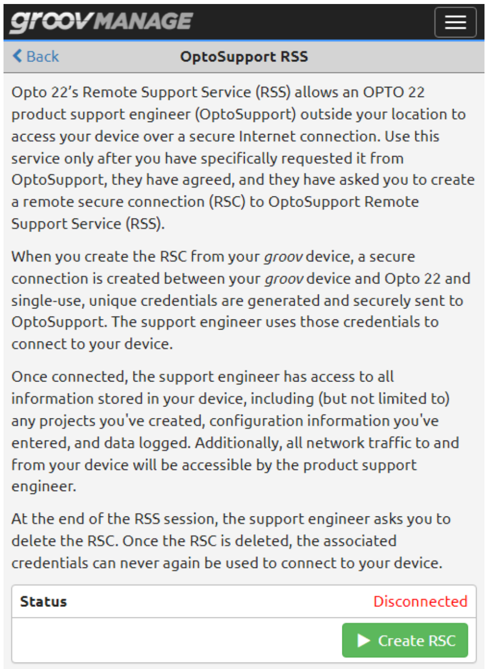
Any client (like your PC or mobile device) that is properly configured with an appropriate OpenVPN Client Connector can securely log into your VPN server using a valid account or OpenVPN client configuration file (.ovpn). Once connected, your client can reach your *groov* RIO or EPIC's software applications, like *groov* Manage or *groov* View.

By default, VPN access to a *groov* product provides access only to software running on that product, not to any other devices connected to it via other network interfaces. If you want to allow access to other devices, however, you can configure the Port Redirect feature to create a conduit between various network interfaces. (See "Port redirect feature: creating conduits between zones" on page 6.)

Using a VPN for product support

You can also create a secure VPN tunnel to Opto 22 Product Support.

Suppose you are having concerns about your *groov* product and contact Product Support for assistance. If you think it would be helpful, you can use *groov* Manage to open a VPN tunnel so that the Product Support Engineer can temporarily access your device and help resolve the issue. (See image at right.)



Opto 22's Remote Support Service (RSS) allows an OPTO 22 product support engineer (OptoSupport) outside your location to access your device over a secure Internet connection. Use this service only after you have specifically requested it from OptoSupport, they have agreed, and they have asked you to create a remote secure connection (RSC) to OptoSupport Remote Support Service (RSS).

When you create the RSC from your *groov* device, a secure connection is created between your *groov* device and Opto 22 and single-use, unique credentials are generated and securely sent to OptoSupport. The support engineer uses those credentials to connect to your device.

Once connected, the support engineer has access to all information stored in your device, including (but not limited to) any projects you've created, configuration information you've entered, and data logged. Additionally, all network traffic to and from your device will be accessible by the product support engineer.

At the end of the RSS session, the support engineer asks you to delete the RSC. Once the RSC is deleted, the associated credentials can never again be used to connect to your device.

Status: Disconnected

You will need a properly configured gateway to the internet in order to connect to Opto 22's Product Support VPN server.

Port redirect feature: creating conduits between zones

In some cases you may want to reach devices that are in a network zone isolated by your *groov* product. For example, perhaps you have another PLC or networked device on your trusted network (OT network) that you want to reach from another trusted network (like a VPN) or other configured network interface (see illustration on next page.) Maybe you need to make changes to that PLC or device from that system's own proprietary software (for example, RSLinx software from Rockwell Automation® connecting to an Allen-Bradley® PLC). Normally, such connections are not secure.

By design, a *groov* device's default configuration does not route traffic between network interfaces. However, an advanced feature available in *groov* EPIC firmware version 3.2 or higher and *groov* RIO firmware version 3.4 or higher lets you designate a port redirect to permit network traffic coming in on one interface's network port to pass through to an IP address or host's port on another interface, creating a conduit between zones.

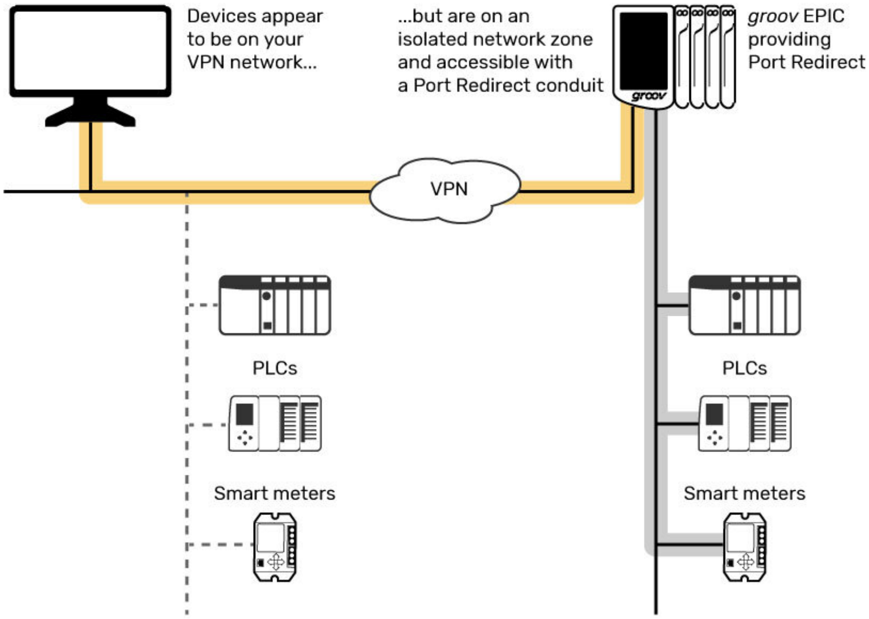
CAUTION: *Use extreme caution here to ensure that an unsecure open port does not exist on an untrusted network interface!*

As discussed in "Firewalls" on page 7, best practice is to block all unsecure network ports (like Modbus®/TCP port 502) on untrusted network interfaces. However, a VPN tunnel created on an untrusted network interface allows only authenticated, encrypted data communications over that interface, so only authorized users can gain access.

In this scenario, you configure a port redirect—a conduit—from the VPN tunnel interface from the untrusted network zone, where the VPN tunnel is established, to the trusted network zone, where the unsecure PLC is. Network packets are then redirected through this conduit. Ideally, you enable the conduit only on demand and for a limited time period. You can do so in either of two ways:

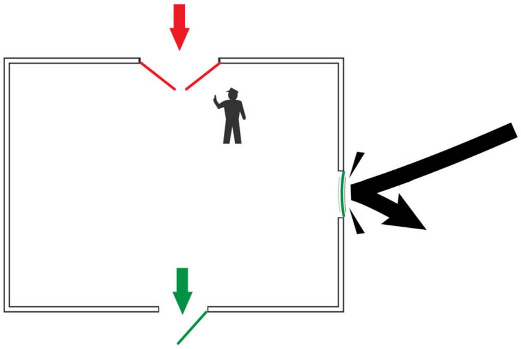
- Directly in *groov* Manage, which uses secure HTTPS (port 443)
- Programmatically in other applications on your *groov* product—Node-RED, Ignition Edge, PAC Control, or other software—using the REST API to enable and disable the port redirect

This scenario delivers a temporary and fully secure method for accessing devices on an isolated network zone from anywhere another client VPN connection is established. These devices appear to be on your VPN network, but in reality they are on a separate network zone attached to your *groov* RIO or EPIC.


Devices appear to be on your VPN network...
...but are on an isolated network zone and accessible with a Port Redirect conduit
groov EPIC providing Port Redirect
VPN
PLCs
Smart meters
PLCs
Smart meters

Firewalls

Firewalls are critical in securing data communications. A firewall on a network or on a device (a host) is kind of like the doors in a building. The door on a building's main entrance often swings in so you can enter, and a security guard or receptionist checks your ID and keeps an eye on who comes and goes. Emergency exit doors swing out only. They're locked from the outside for security, but people inside the building can easily get out if they need to.



Firewalls block unwanted incoming traffic but permit outgoing traffic as necessary.

With a firewalled network or device, communications can occur outbound to external servers or services, just like people can leave through the emergency exit doors of a building. But communications attempting to come in are rejected, just like people can't come in through the locked emergency exits. These inbound communications are permitted only through a specific network port that's been opened to allow them, and only with the right encryption and credentials—again, like entering through a building's main entrance door, but only if they have an ID and an appointment to visit someone inside.

groov RIO and *groov* EPIC have a configurable device firewall, which is critical in addressing security for the system. The device firewall helps provide security by stopping unsolicited traffic from accessing your *groov* product's configured networks, software applications, and connected devices. Typically the only traffic it allows back through is responses to traffic that originated from the *groov* device. Device-originated connections are considered trustworthy because their origin is known.

Each network interface on the *groov* RIO or EPIC—RIO's Ethernet interface (ETH0), EPIC's two Ethernet interfaces (ETH0 and ETH1), the optional wireless interface (WLAN0), and the optional VPN interface (TUN0)—has its own firewall settings. You can set specific firewall rules for each interface, for trusted networks (where unsecure ports are open) and untrusted networks (where only encrypted, authenticated ports should be open).

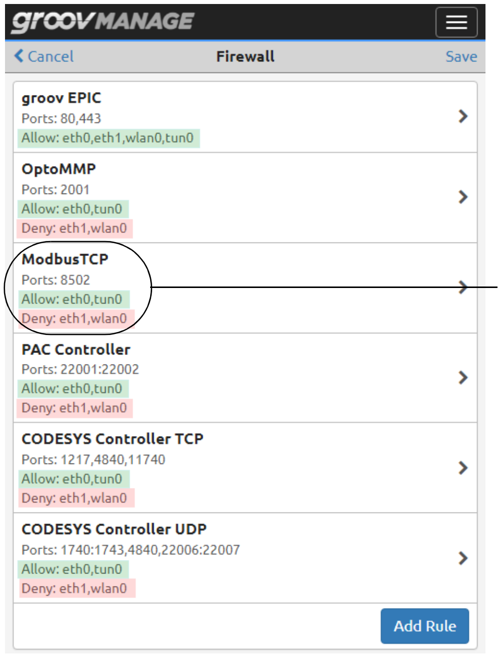
Default device firewall configuration

By default, the device firewall on *groov* products blocks unsolicited inbound traffic on all network interfaces, allowing only responses to device-originated connections to come through. For example, let's look at the default firewall configuration for the *groov* EPIC's Ethernet interfaces

The *groov* EPIC processor's internal firewall default configuration assumes that you are using the two wired network interfaces as designed to isolate trusted and untrusted network zones:

- On the Ethernet **trusted** network interface (**ETH0**), *groov* EPIC allows network communications through necessary but unsecure industrial protocol ports that are configured *open*. These ports allow communication with software and protocols in the *groov* EPIC processor, for example:
  - PAC Control™ and CODESYS® (development tools)
  - OptoMMP (protocol used by the EPIC's I/O)
  - Modbus/TCP (for communication with PLCs and other devices)
- On the Ethernet **untrusted** network interface (**ETH1**), *groov* EPIC allows traffic only on secure port 443 and permits only authenticated access over secure, encrypted connections. This network interface provides authenticated, encrypted access to *groov* Manage, *groov* View, Node-RED, and RESTful APIs.
- All other inbound connection ports on the ETH1 Ethernet network interface are **blocked by default**.

In *groov* Manage the configuration for each network interface is shown by application, so you can clearly see which applications are allowed access and which are denied:



groov EPIC
Ports: 80,443
Allow: eth0,eth1,wlan0,tun0

OptoMMP
Ports: 2001
Allow: eth0,tun0
Deny: eth1,wlan0

ModbusTCP
Ports: 8502
Allow: eth0,tun0
Deny: eth1,wlan0

PAC Controller
Ports: 22001:22002
Allow: eth0,tun0
Deny: eth1,wlan0

CODESYS Controller TCP
Ports: 1217,4840,11740
Allow: eth0,tun0
Deny: eth1,wlan0

CODESYS Controller UDP
Ports: 1740:1743,4840,22006:22007
Allow: eth0,tun0
Deny: eth1,wlan0

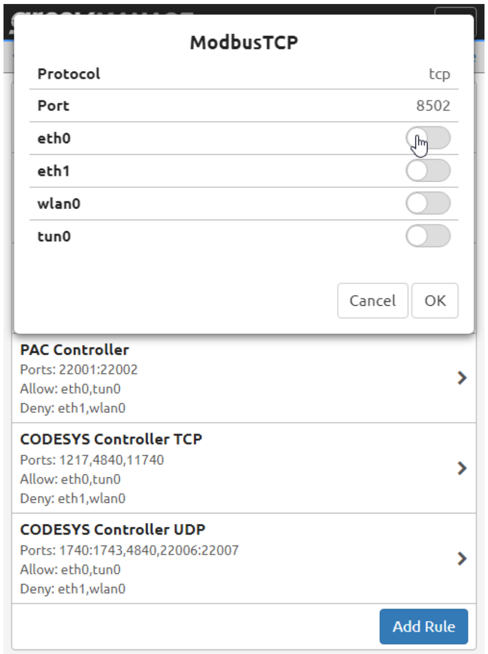
Default configuration by application for trusted Eth0 and untrusted Eth1 network interfaces

Note: Port 80 is open, but all traffic is automatically redirected to secure port 443.

For example, Modbus/TCP is allowed by default on trusted ETH0 but denied on untrusted interfaces.

Remember that the default configuration assumes that ETH0 is on a trusted network. Make sure that network actually is trusted.

You can configure the *groov* EPIC's firewall for each network interface to suit your application. For example, you can change the default configuration to close ports for any services that won't be used. In the example below, if you are not using Modbus/TCP, you should close port 8502 so it will not allow any traffic, even on the trusted network interface:



ModbusTCP

Protocol	tcp
Port	8502
eth0	○
eth1	○
wlan0	○
tun0	○

PAC Controller
Ports: 22001:22002
Allow: eth0,tun0
Deny: eth1,wlan0

CODESYS Controller TCP
Ports: 1217,4840,11740
Allow: eth0,tun0
Deny: eth1,wlan0

CODESYS Controller UDP
Ports: 1740:1743,4840,22006:22007
Allow: eth0,tun0
Deny: eth1,wlan0

You can (and should) close unused ports for greater security.

Optional WiFi and VPN interfaces have the same default firewall configuration, and for both *groov* RIO and *groov* EPIC, you can change them similarly in *groov* Manage.

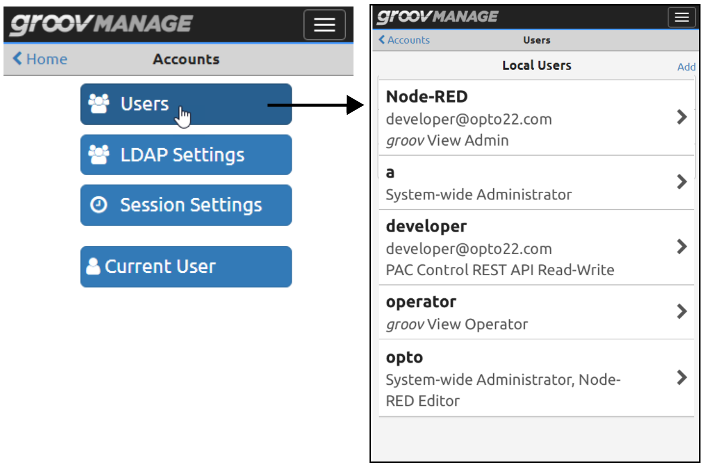
Clients and servers

Note that a *groov* product can act as both a client (a device that originates connections) and a server (a device that listens for requests to connect). Firewall configuration varies based on how it acts. For example:

- MQTT, the OpenVPN client, and Node-RED nodes attempting communications to other servers are clients that originate communications. For example, MQTT originates communications to MQTT brokers, and Node-RED nodes originate communications to SQL servers, cloud-based services, and so on. No incoming firewall port configurations are needed for these client applications running on your *groov* product. Their communications are outbound and by default are allowed by the device firewall. (See more about MQTT on page 11.)
- *groov* View running on *groov* EPIC, and the internal OPC UA server in *groov* RIO and *groov* EPIC (firmware version 3.4 or higher required) are servers that listen for connection requests. In the case of *groov* View, requests come from PCs and mobile devices running browsers. For the OPC UA server, requests come from an OPC UA client. By default, the device firewall is configured to open the HTTPS secure port (port 443) for *groov* View clients, to allow incoming connections. The OPC UA servers available in *groov* devices (native server and servers through Ignition, CODESYS, or SSH) also use secure connections; ports used by clients vary depending on the server. These connections are encrypted and must be authenticated by users.

Whether *groov* RIO or *groov* EPIC acts as a client or a server, once communications are established, data can flow in both directions as long as the connection is active.

Accounts



Node-RED
developer@opto22.com
groov View Admin

a
System-wide Administrator

developer
developer@opto22.com
PAC Control REST API Read-Write

operator
groov View Operator

opto
System-wide Administrator, Node-RED Editor

Controlling who can access your data and exactly what each user can do with it is a vital part of cybersecurity.

When you first start *groov* RIO or *groov* EPIC, you must create a local administrator account with your own username and password before you can do anything else. *groov* products do not have a default username or password that someone might be able to guess.

For security, the administrator account credentials you create are *not recoverable*.

groov products provide **user account management** through *groov* Manage. You can create administrator, developer, operator, REST API, and other accounts, and then assign permissions to authorized people or software services. Authentication (over an encrypted connection) is by either username/password or API token.

All users can create long, complex passwords consisting of numbers, capitalization, punctuation, spaces, phrases and words in any language, and even emoticons.

As an administrator, you can also set user session timeouts globally, adjusting the timeout for individual users as needed. You can set user sessions to never expire or to run from 30 minutes to two weeks.

LDAP (lightweight directory access protocol)

If your site manages user accounts through an LDAP service (for example, Microsoft Active Directory Service), you can work with your IT department to configure your *groov* product in *groov* Manage to **connect to the LDAP server**, authenticate a user, and help determine which services a user can access. For simple setups you can use the LDAP server to authenticate users and give them default local permissions. For systems with a larger number of users or more complex user management, you can use *groov* Manage to map an LDAP group to a specific set of permissions.

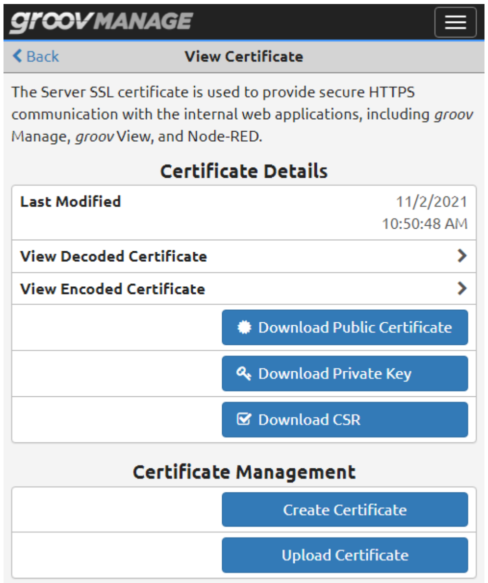
NOTE: Your original administrator account for groov RIO or groov EPIC gives you direct, local access to your device and is ***not*** *managed by your LDAP service.*

Details on how permissions work and how to assign them are in your *groov* product's user's guide (see page 2).

Security certificate management

Security certificates are a way that clients can verify servers, so that when one tries to connect, it can be assured it's communicating with the correct server and not an impostor. *groov* products provide built-in **certificate management** in *groov* Manage.

groov RIO and *groov* EPIC support X.509 PKI standard certified client connections to secure servers (Client SSL) and from clients to the *groov* device's secure server (Server SSL) using TLS/SSL certificates, which can be device generated, self-signed, or registered publicly through a Certificate Authority (CA). For more information on certificates, see your *groov* product user's guide, our videos on security certificates, and examples on developer.opto22.com.



The Server SSL certificate is used to provide secure HTTPS communication with the internal web applications, including *groov* Manage, *groov* View, and Node-RED.

Certificate Details

Last Modified	11/2/2021 10:50:48 AM
View Decoded Certificate	>
View Encoded Certificate	>

Certificate Management

Data communication options for better security

As we saw in the Firewalls section, a device is inherently more secure and requires less security configuration when it **initiates data communication** (as a client to a server) over an outbound network port, rather than having to open a port to receive connection requests.

Publish/subscribe (pub/sub) is a communication method that takes advantage of this greater security by using device-originated communications only. *groov* RIO and *groov* EPIC can use MQTT, a pub/sub protocol, to report status (authenticated and encrypted) to a central broker. Once connected to the broker, the connection persists, so the *groov* RIO or EPIC can also receive any new commands for it or to status messages from other devices, thereby providing bi-directional communication.

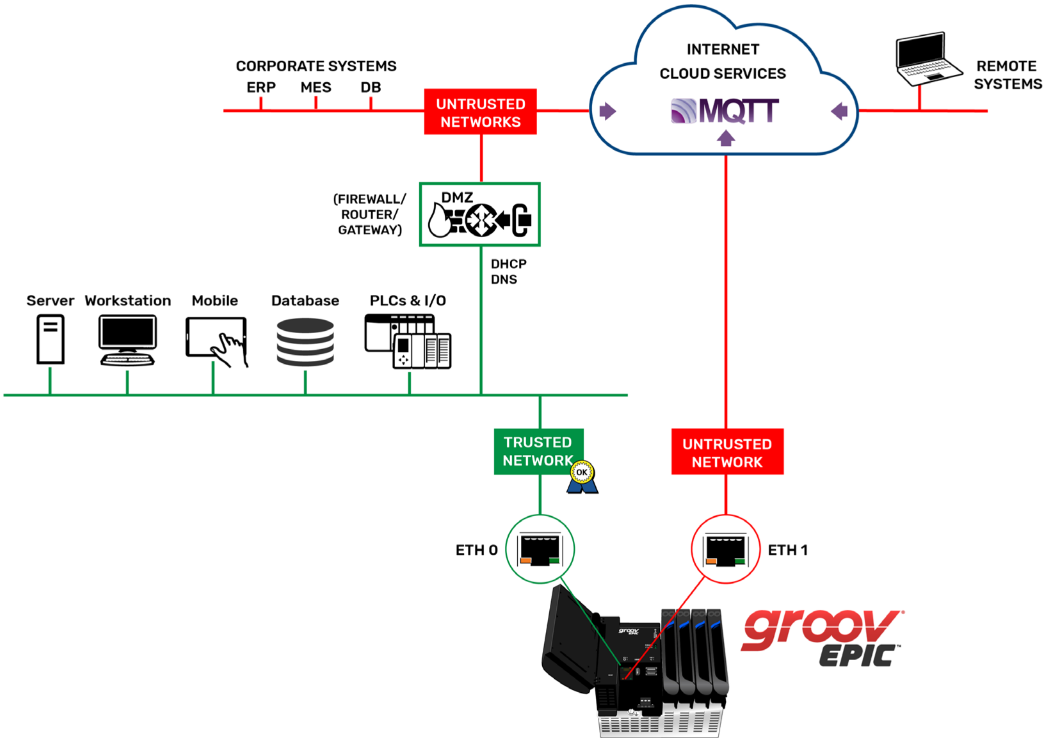
Because MQTT data flow is device originating, the firewall allows the data out, keeps track of the session status, and allows any packets coming back from the broker to pass through.

With MQTT, this persistent connection is the critical mechanism for the MQTT broker to determine the state of client connections at all times. In a pub/sub model for SCADA (supervisory control and data acquisition) or industrial communications, you always want to be sure that clients are still connected. If a data publisher's persistent connection is broken, the broker notifies all subscribers about the disconnect so that the state of the system is known to all.

In contrast, in request/response communication, connections do not persist unless the client maintains them. For example, if Node-RED (a client) connects to a SQL server, once data is sent from the client to the server and the server responds, the connection is closed. Subsequent data transfers must be initiated by the client each time. In the example of *groov* View, the client (your browser) keeps the connection open to the server (*groov* View) only as long as the client browser session is active.

Device-originated communication is sometimes called *using an outbound port*. In contrast, when the device has to have a configured port opened in order to receive communications originated from outside, it can be called *using an inbound port*. Through outbound, device-originating data communications such as MQTT, *groov* products offer a secure option that requires far less configuration. For more information on using MQTT, see MQTT Resources on our website.

The following diagram illustrates how MQTT works with *groov* EPIC.



MADE IN THE USA

PUTTING IT ALL TOGETHER

Your industrial network may have a number of requirements, including:

- Realtime I/O sensing and control
- Multi-vendor network integration
- Data acquisition from field devices

And the data in your control systems and field devices may be required for use by:

- Software and services that are on premises and in the cloud
- Applications that use MQTT communications, like Canary's Historian
- Remote PCs that need VPN access to industrial data or that must establish a conduit to legacy PLCs
- SCADA systems and HMIs that use industrial data for monitoring, control, and collection, like Inductive Automation's Ignition

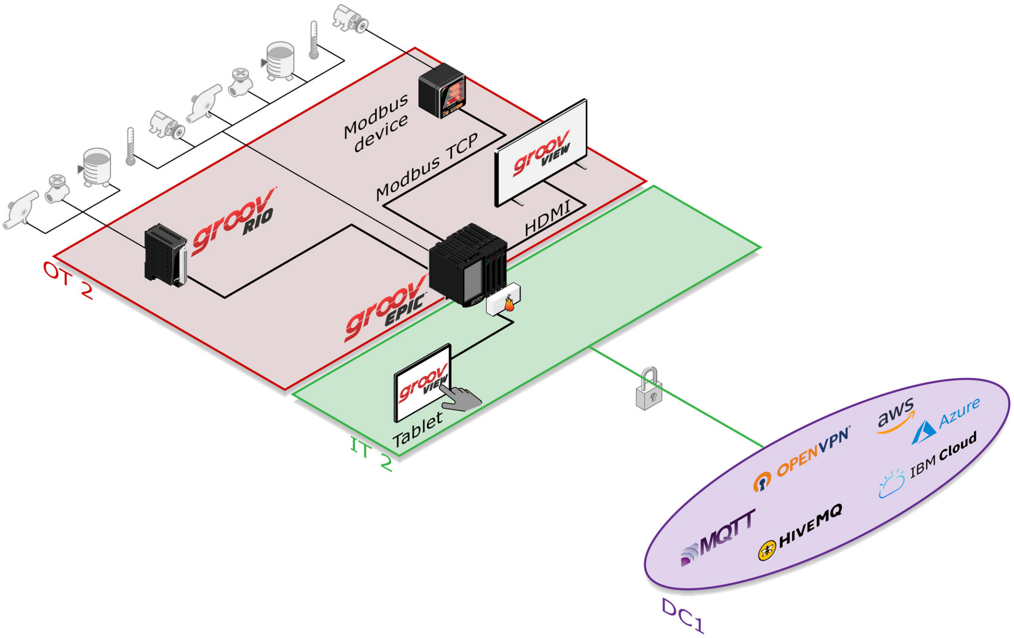
Which of these requirements do you have, and how can these pieces all fit together? Let's take a look at how *groov* products help secure this complex infrastructure and connect data from various endpoints in a complete system architecture.

Realtime I/O sensing and control

We'll start with a real-time I/O sensing and control application, shown in the image below, potentially operating in a hazardous area. Traditional field assets like sensors and switches are wired directly to the *groov* EPIC's I/O modules or to *groov* RIO modules acting as remote I/O. These *groov* devices can also communicate with Modbus devices over Modbus/TCP. As shown, *groov* EPIC also provides a local operator interface using *groov* View and a connected HDMI monitor.

Using its device firewall and independent network interfaces, the *groov* EPIC delineates two security zones: a trusted network for the local control system (OT2) and an untrusted network for external clients (IT2).

The *groov* EPIC serves up data through encrypted connections to PCs and mobile devices in IT2 or, through it, to applications on premises and in the cloud.



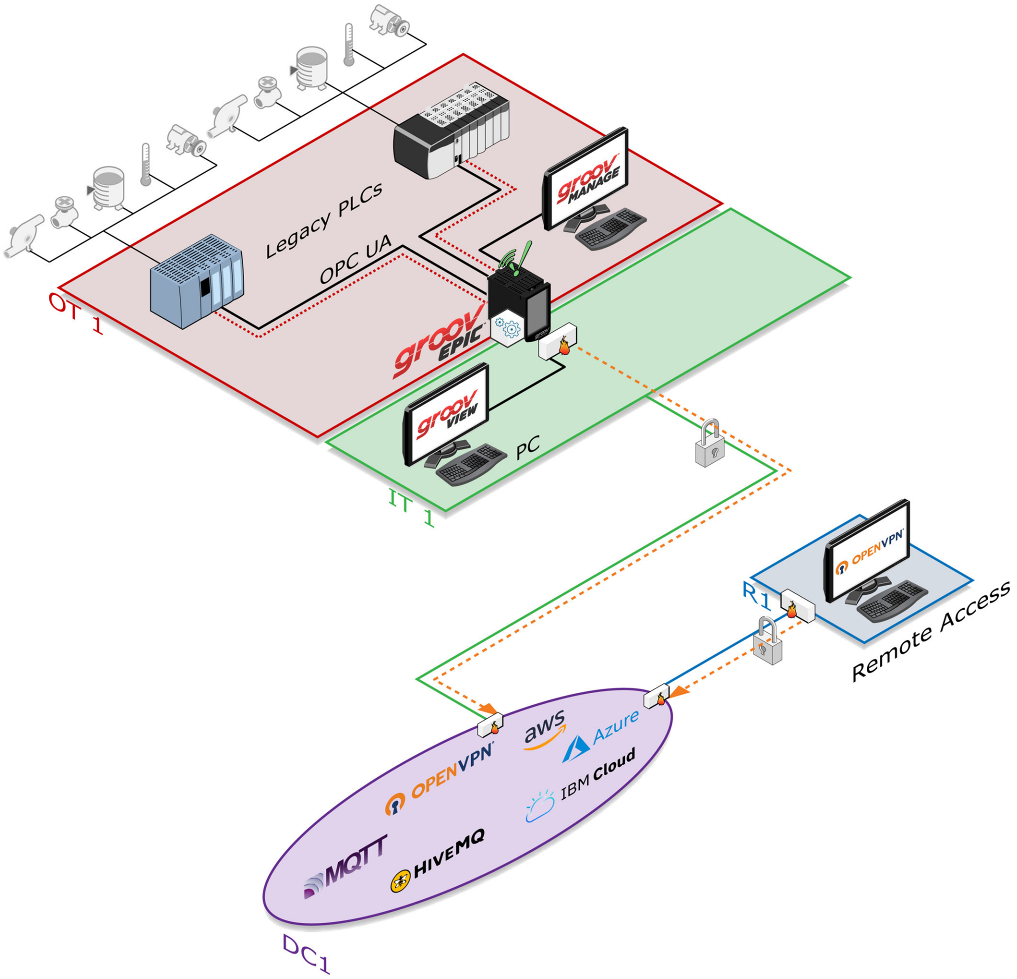
Multi-vendor network integration

What if you have an existing system, but you need to get the data that's locked in legacy PLCs? Here you're using a *groov* device for its port redirect capabilities. All *groov* EPIC processors and *groov* RIO model GRV-R7-MM2001-10 run Ignition from Inductive Automation. These *groov* products can connect to legacy PLCs via Ignition's built-in native drivers and communicate PLC data via OPC UA.

All the data you need from legacy systems can be used in the same ways, in software and services on your premises or in the cloud (DC1), including VPN tunnels (orange dotted).

And here's an added bonus: securely accessing your PLCs. For example, suppose you need to update a PLC's program from your PC at another site (R1). Using a VPN and *groov* RIO's or EPIC's port redirect feature, you can establish a conduit (red dotted) to securely access your PLC and make the change.

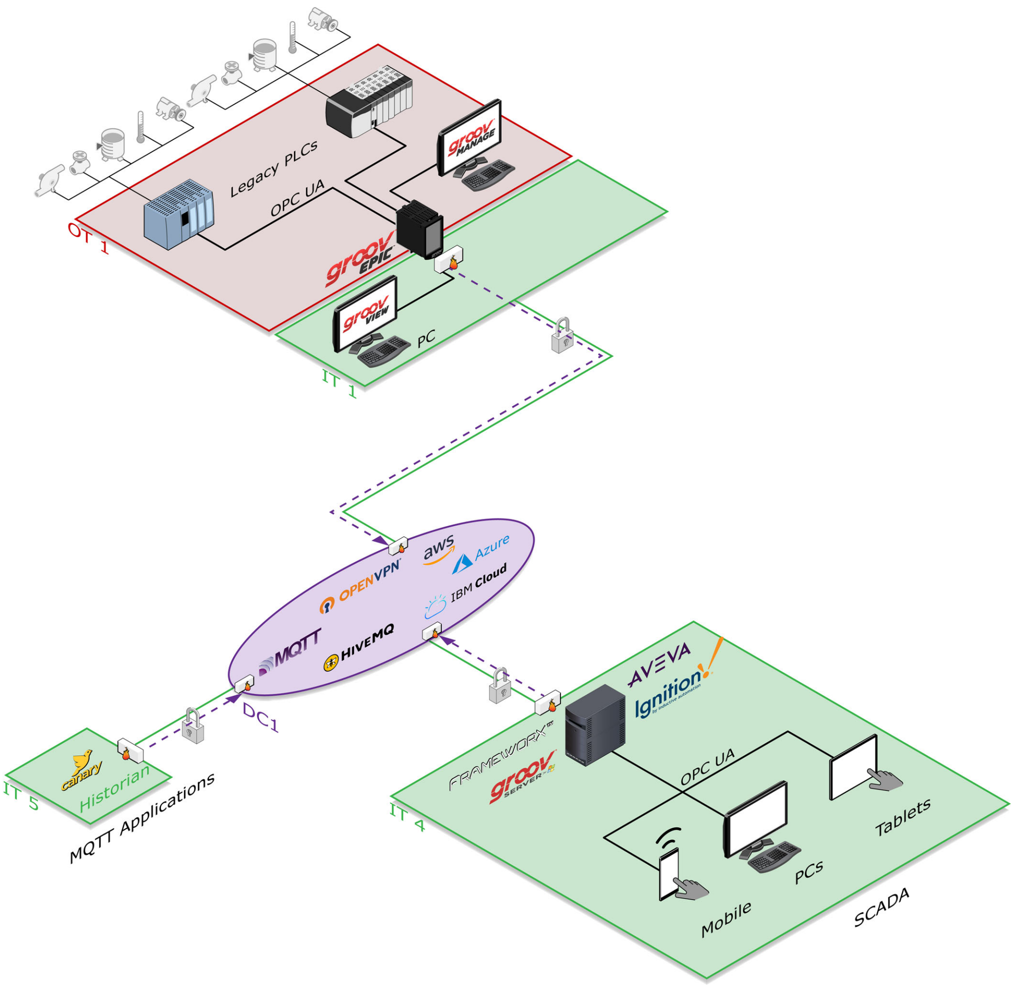
The diagram below shows a *groov* EPIC processor as an example. With *groov* EPIC, you can also separate OT and IT networks into two zones for security and use legacy PLC data in your *groov* View HMI (locally and on mobile).



MQTT/Sparkplug B for multi-vendor integration

Using MQTT/Sparkplug B adds efficiency, scalability, and interoperability to data communications and expands the applications you can integrate with *groov* RIO and *groov* EPIC. With MQTT, data from devices and systems wired to your *groov* product, as well as legacy PLC data, are communicated via an outgoing connection—which, once established, allows data to flow in both directions while requiring no open firewall ports (see "Data communication options for better security" on page 11).

Here we see how data moves through MQTT/Sparkplug B connections (purple dash). MQTT applications like Canary's Historian can easily exchange data with field devices and systems, as can SCADA systems.



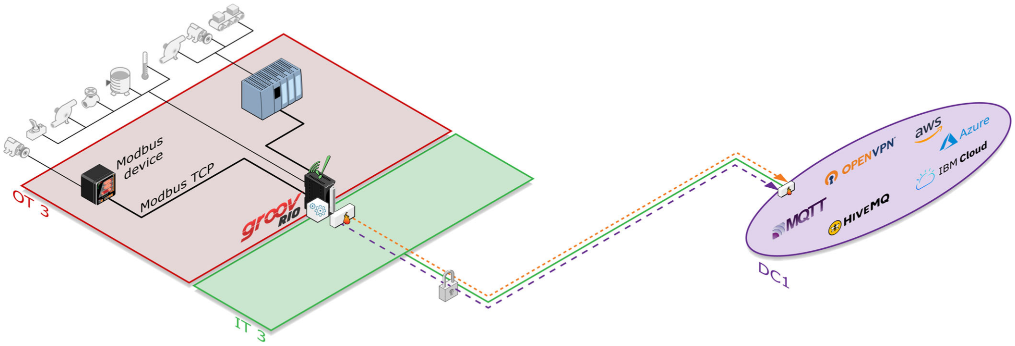
Data acquisition from field devices

Suppose you don't need real-time control capability, but you still need data from field devices. Here's where *groov* RIO shines. For example:

- The *groov* RIO EMU energy monitoring unit wires directly to 3-phase power loads and sends 64 channels of power and energy data (some measured, some calculated) wherever it is needed for tracking and analysis.
- The *groov* RIO MM2 universal I/O module (shown in the diagram below) talks to Modbus devices, connects directly to field devices, and runs Ignition Edge with its PLC drivers, acquiring data from everything at the site.

Like EPIC, *groov* RIO can share acquired data with other devices and software on premises and in the cloud using MQTT/Sparkplug B, Node-RED, and a VPN.

groov RIO's device firewall and encryption help secure this site. Although *groov* RIO does not have two independent physical Ethernet network interfaces like EPIC, it does have up to three network interfaces (Ethernet, WiFi, and VPN) that can separate networks into zones.

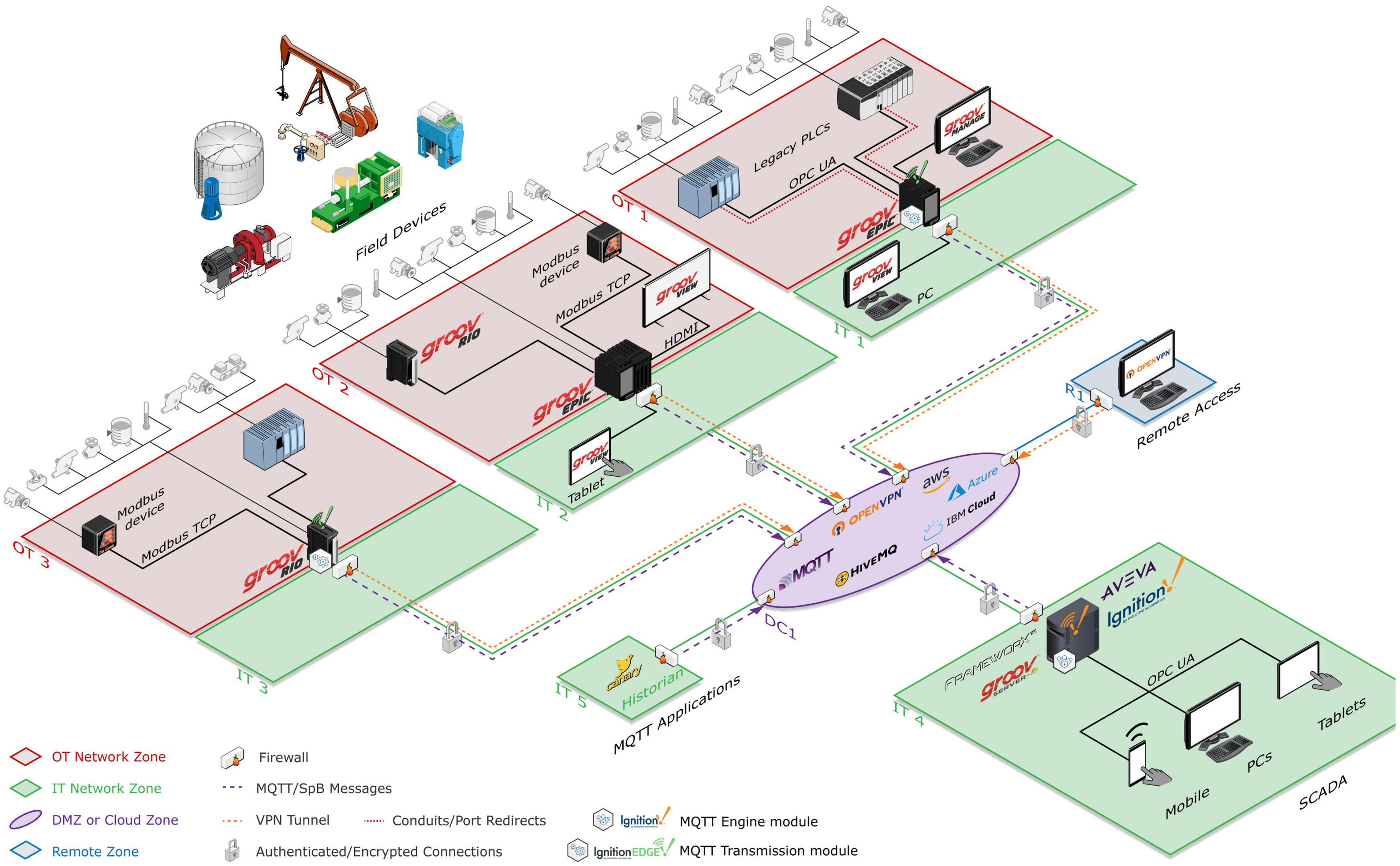


Easy scalability

Maybe you start with just one *groov* RIO EMU, monitoring power for machine health and predictive maintenance, and then you need additional monitoring or control. With the *groov* RIO/*groov* EPIC architecture, you can easily scale up by building on the infrastructure you've already established. Simply add more *groov* RIO modules and *groov* EPICs as needed to integrate additional devices and acquire data from field devices in more locations.

Complete *groov* EPIC System architecture

Putting it all together, you can see a flexible, scalable system architecture that can help you build a secure system to meet your individual project requirements. Take a look at the diagram below, and then review "groov Products Best Practices for Cybersecurity" on page 18.



MADE IN THE USA

groov PRODUCTS BEST PRACTICES FOR CYBERSECURITY

Every situation is different, and as a practitioner, you know best what access your application will need and what network architecture you'll use. As you work on your system, remember that *groov* products were designed to help you create a secure system and address security guidelines as described in the ISA/IEC 62443 standard. Based on the design of *groov* RIO and *groov* EPIC, we strongly recommend the following best practices. Keep these practices in mind as you develop your applications and deploy your projects.

Networks

- Be sure to place unsecure devices (like legacy PLCs or devices) only in the trusted network zone.
- In any untrusted network zones, permit only secure, encrypted, and authenticated connections.
- Configure your *groov* EPIC to use the ETH0 Ethernet network interface for your trusted network. Use ETH1 for any untrusted network. Configure exceptions in the system's firewall only if required for your application.
- Use WiFi or VPN network interfaces on both *groov* RIO and *groov* EPIC for zoning.
- Configure the system's firewall in *groov* Manage to close all unneeded network ports on all network interfaces.

Accounts

- Have all your users create long and difficult passwords, and don't write them down anywhere. Consider using a password manager where appropriate.
- If your site uses an LDAP service to manage user IDs, work with your IT department to include *groov* products.
- Use a VPN if you need remote, encrypted access to your *groov* product over an untrusted network.
- To prevent unauthorized access to the *groov* RIO or EPIC, always log out of any account that has administrator privileges.
- For *groov* EPIC, if you are running your *groov* View HMI on an external monitor, always put it in Kiosk mode or limit it so that only *groov* View is accessible.

Other best practices

- If you need a completely closed system (for example, if you are an OEM using *groov* EPIC in your machine), after you have finished development, disable all ports in the firewall and unplug any Ethernet cables.

  If someone attempts to connect an Ethernet cable to the *groov* EPIC processor to try to access the system from their computer, the ports will be closed and network access will be denied. Only an authorized user with administrator privileges can access *groov* Manage through *groov* EPIC's built-in display to reopen needed ports and gain network access.
- Whenever possible, use authenticated and encrypted outbound, device-originated data connection methods. For example, use MQTT to publish data to an MQTT broker. Device-originated data communication methods help you:
  - Reduce open inbound network ports
  - Eliminate man-in-the-middle exploits
  - Prevent exposing sensitive credentials over the network

If you're a developer, be sure to see "Additional security design for developers" on the following page.

ADDITIONAL SECURITY DESIGN FOR DEVELOPERS

The *groov* RIO and *groov* EPIC Linux OS gives developers optional **Secure Shell access** (SSH) for developing custom applications, while maintaining security. Again, you have tools in *groov* products to help you design a secure system.

A license is required to activate Secure Shell access (Opto 22 part number GROOV-LIC-SHELL). This license is free of charge. Once you have the license, you can:

- Manage SSH access and restrict it to the trusted network only.
- Configure specific network interface ports on the *groov* device firewall as required for your custom applications.
- Install cryptographically signed packages from Opto 22's git repository.
- Compile applications, monitor server log files, start and stop applications or services, and facilitate file transfers.

Note that product support for systems using SSH is limited.

Additional best practices for developers

In addition to the recommended best practices starting on page 18, developers using SSH should also do the following:

- Configure SSH access with a unique and difficult username and password, different from *groov* Manage, *groov* View, or any other software running on your *groov* product.
- Enable shell access only to configure and program the unit. Once the system is commissioned, disable shell access in *groov* Manage so that no one else can get in. Never leave SSH access enabled once the system is in production.
- Never allow SSH access on an untrusted network.