# AUTOMATION 2023

VOLUME 5

## Cybersecurity & Connectivity

- Four Threats Facing Automated Factories
- ISA on Advancing Industrial Cybersecurity
- Empower Industrial Networks to Be Secure
- Security in Edge Controllers and I/O
- Ethernet Switches for Managing Network Security
- Get IIoT Networks Future Ready

AUTOMATION.COM | ISA A subsidiary of the International Society of Automation

# Table of Contents

AUTOMATION 2023 VOLUME 5
**CYBERSECURITY & CONNECTIVITY**


**Page 5**

## Empower Industrial Networks to Drive OT/ICS Cybersecurity

By Andrew McPhee, Cisco

Gain visibility at scale and enforce ISA/IEC62443 zones and conduits to find and contain threats.

**Page 17**

## Look for Cybersecurity Features in Edge Controllers, I/O

By Benson Hougland, Opto 22

Built-in security options help users build a more secure network for connected automation.

**Page 29**

## Managing Network Security

By Charlie Norz, WAGO Corp.

How choosing the right type of Ethernet switch can improve OT cybersecurity.

**Page 33**

## ISA on Advancing Industrial Cybersecurity

From the International Society of Automation

Helping policy makers and private-sector leaders protect critical infrastructure.

**Page 40**

## Mitigate Four Cyber Threats Facing Automated Factories

By Mars Cheng and YenTing Lee, TXOne Networks

As IT and OT systems converge, attackers have more factory OT network entry points.

**Page 47**

## Getting IIoT Networks Ready for the Future

By Roger Chen, Moxa

Three tips can enhance network preparedness and help secure IIoT networks.

**Page 51**

## What Is ETHOS, and Why Now?

By Danielle Jablanski, Nozomi Networks

How an open sharing platform is helping critical infrastructure.

**Page 55**

## Effectively Securing Operational Technology

By Richard Springer, Fortinet

By learning from the past, industrial firms can prepare to respond to threats.

# Introduction



SPONSORS

## The Unique Nature of Control System Security

Cybersecurity threats and vulnerabilities pose a clear and mounting danger to global industrial and infrastructure facilities that goes beyond financial loss or compromised information. Disruption of connected networks, equipment and processes can also threaten the safety and security of industrial personnel and the customers they serve. That's why the community of engineers and automation professionals working every day to keep facilities and communities safe and operations uninterrupted must understand how to keep their industrial networks and systems secure. At the core of this challenge is understanding the unique nature of control system equipment, how it is vulnerable, and how it can be secured. That's why this September edition of AUTOMATION 2023 covers topics including visibility at scale, enforcing ISA/IEC62443 zones, the security features to look for in Ethernet switches and edge controllers, and tips for securing OT and IIoT networks.

Get more essential insights about operating and securing industrial control systems and critical infrastructure in AUTOMATION 2023 and topical newsletters from Automation.com, a subsidiary of the International Society of Automation (ISA). The next issue of AUTOMATION 2023 comes out in November and will focus on IIoT and Industry 4.0 topics including smart sensors, intelligent instrumentation, digital transformation and more.

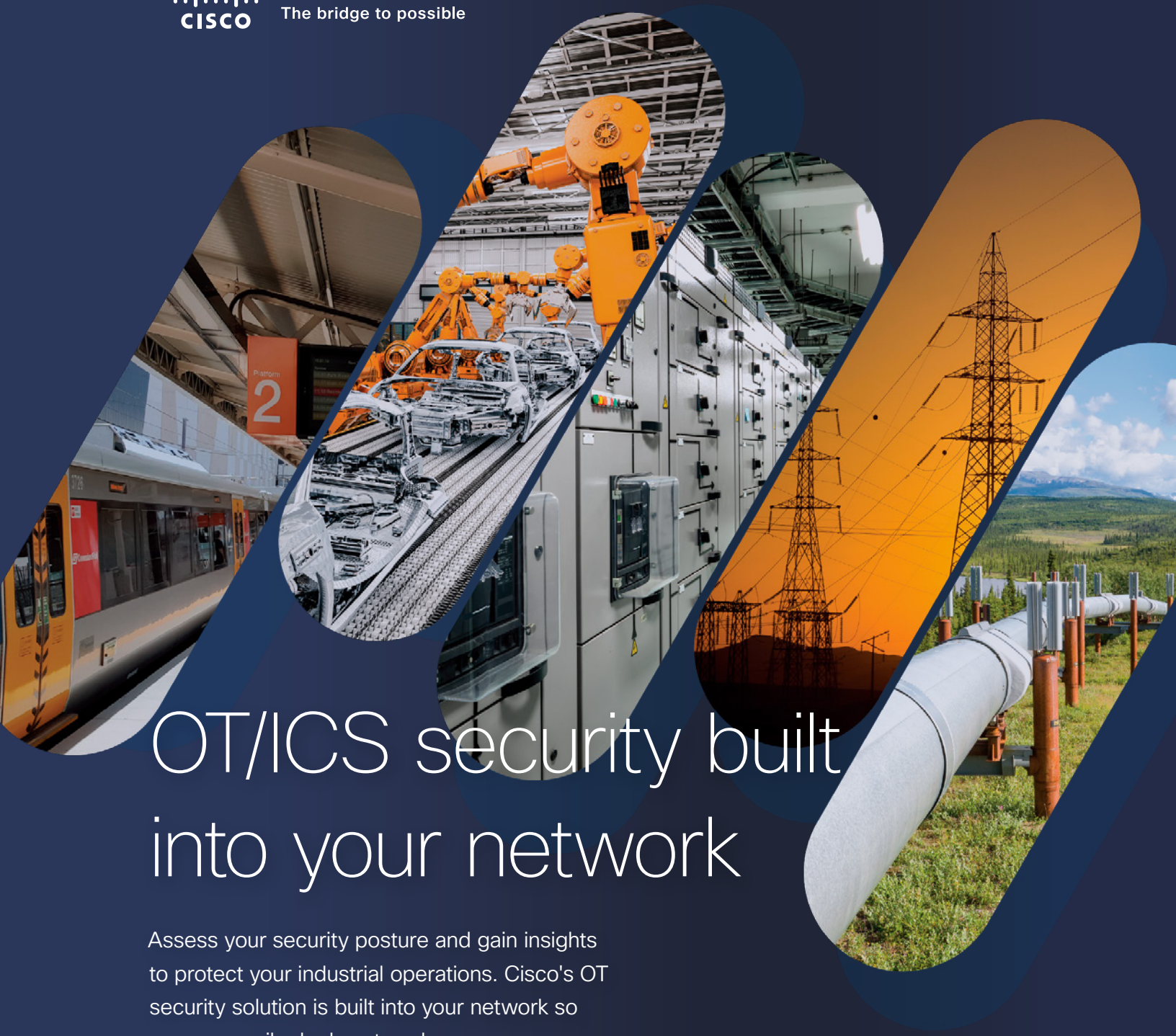
Renee Bassett
Chief Editor
rbassett@isa.org

**About AUTOMATION 2023**

The AUTOMATION 2023 ebook series covers Industry 4.0, smart manufacturing, IIoT, cybersecurity, connectivity, machine and process control and more for industrial automation, process control and instrumentation professionals. To subscribe to ebooks and newsletters, visit: www.automation.com/newslettersubscription.

AUTOMATION 2023 is published six times per year (January, March, May, July, September, and November) by Automation.com, a subsidiary of International Society of Automation (ISA). To advertise, visit: www.automation.com/en-us/advertise.

The bridge to possible



# OT/ICS security built into your network

Assess your security posture and gain insights to protect your industrial operations. Cisco's OT security solution is built into your network so you can easily deploy at scale.

cisco.com/go/iotsecurity

# Empower Industrial Networks to Drive OT/ICS Cybersecurity

## Gain visibility at scale and enforce ISA/IEC62443 zones and conduits to find and contain threats.

Deploying firewalls to build a demilitarized zone (DMZ) between operational technology (OT) and information technology (IT) domains is the mandatory first step to secure operations. But as users digitize their operational environment and deploy Industry 4.0 technologies, they are connecting more devices, enabling more remote access, and building new applications. Seamless communications between IT, cloud, and industrial networks are needed and the airgap approach to industrial security is falling short of being sufficient.

By Andrew McPhee, Cisco

Solutions designed to secure industrial networks typically monitor network traffic to gain visibility on assets, behaviors, malicious activities, and threats. They also rely on deploying rugged firewalls to segment industrial networks and build zones and conduits as recommended by the ISA/IEC62443 security standards.

The process of evaluating and testing these solutions initially tends to go well—after a successful proof of concept, industrial organizations begin to deploy at scale. That is where they begin to run into issues.

Often, it is cost prohibitive for organizations to buy the number of security appliances they need to cover their entire operational environment. Or the networking team does not have the resources to deploy, maintain, and manage a fleet of security appliances. The additional traffic created to gain visibility on a large scale would likely necessitate a separate network—which would also require the resources to deploy, maintain, and manage it.

Fortunately, there is a better approach to gaining visibility into the OT environment and segmenting the industrial network. This article explains how users can empower their industrial networks to gain visibility at scale, as well as to contain threats by enforcing ISA/IEC62443 zones and conduits.

**Embed DPI capabilities** into existing networking hardware to achieve full network visibility.

## Understanding the need for OT visibility

Operational environments are typically made of many industrial assets (valves, actuators, drives, robots, power breakers, etc.) managed by industrial control system (ICS) devices—programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), distributed control systems (DCS), etc.)—that are controlled by software orchestrating a process. These OT devices have been deployed over a period of many years—sometimes even decades—back when cybersecurity was not a concern. As a result, they lack strict security

policies. To further complicate matters, some devices can be deployed, managed, and decommissioned by third-party contractors.

When organizations attempt to secure their industrial networks, they encounter two primary issues:

1. **A lack of visibility.** As OT assets can be quite old, widely dispersed, and involve many contractors, operators often do not have an accurate inventory of what is on the network. Without this, they have limited ability to build a secure communications architecture.
2. **A lack of control.** A lack of visibility also means operators are often unaware of which devices are communicating to each other or even of communications reaching industrial devices from the outside. You cannot control what you do not know.

The first step to securing an industrial network is to obtain visibility. Users must understand what devices are on the network, what they are communicating, and where those communications are going.

**Per ISA/IEC62443**, segment the industrial network into zones and conduits to restrict communications between assets to prevent attacks from spreading.

## OT visibility: Beware of hidden costs

The technology to achieve network visibility is available today. Deep packet inspection (DPI) decodes all communication flows and extracts message contents and packet headers, providing the visibility to understand the OT security posture.

DPI allows users to gather device information such as the model, brand, part numbers, serial numbers, firmware and hardware versions, rack slot configurations, and more. It also allows identification of software vulnerabilities and an understanding of what is being communicated over the network. For example, users can see if someone is attempting to upload new firmware into a device or trying to change the variables used to run the industrial process.

When collecting network packets to perform DPI, security solution providers typically configure switch port analyzer (SPAN) ports (Figure 1) on network switches and send all traffic to a central server or dedicated appliances installed here and there in the network.

In an industrial network, most traffic occurs behind a switch at the cell layer because that is where the machine controllers are deployed. Very little traffic goes up to the central network. Gaining comprehensive visibility will require users to collect traffic from every switch in the network, and not just from a few aggregation switches.

Although this can be acceptable for a small industrial site, this cannot be seriously considered in highly automated industries generating a lot of ICS traffic (such as manufacturing), or when devices are widely spread in locations with no or poor network connectivity (oil and gas pipelines, water or power distribution, roadways, etc.).

Connecting security appliances to network switches addresses the issues associated with duplicating network traffic. The appliance collects and analyzes network traffic locally and only sends data

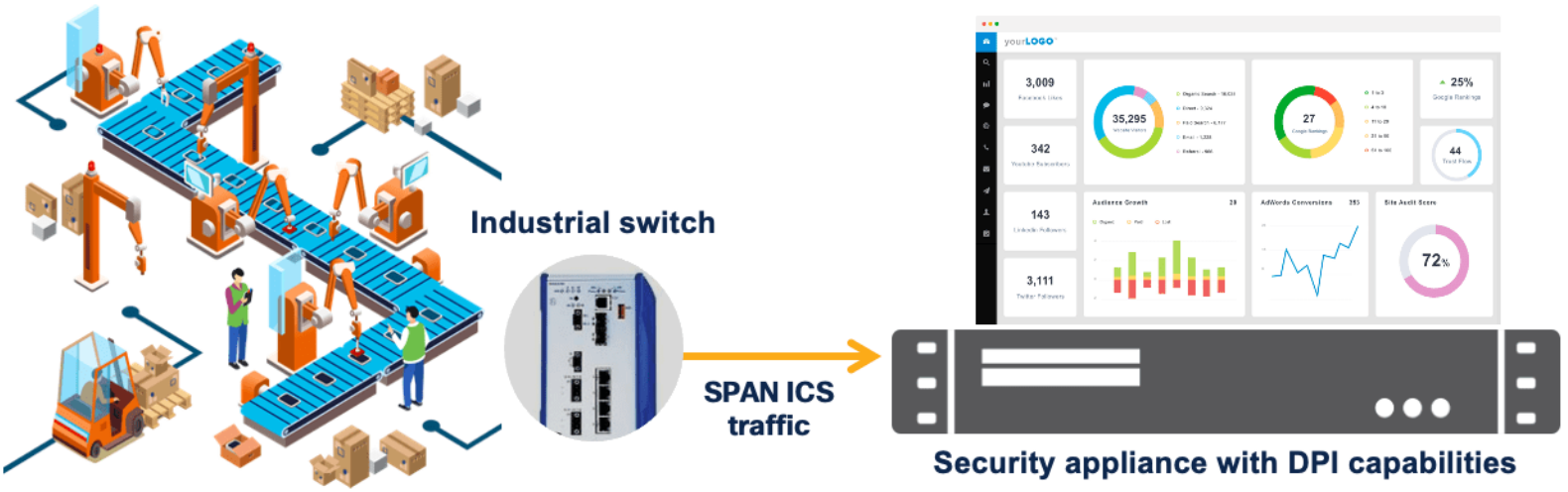



Figure 1. Typical ICS/OT visibility solutions depend on SPAN ports.

to a server for additional analysis. However, installing, managing, and maintaining dedicated hardware can quickly lead to space and operational issues. And because most industrial traffic is local, gaining full visibility will raise cost and complexity to intolerable levels (Figure 2).

## Empowering networks to gain scalable visibility

There is a better way to achieve full network visibility: embed DPI capabilities into existing networking hardware. An industrial-grade switch or router with native DPI capability eliminates the need to duplicate network flows and deploy additional appliances. Obtaining visibility is a matter of activating the sensor feature within the switch or router. Cost, traffic, and operational overhead are minimized.

A DPI-enabled switch or router decodes traffic locally to extract meaningful information. It only sends lightweight metadata to a central server, which runs the analytics and anomaly detection. That metadata represents about 3-to-5 percent of general traffic. The traffic is so

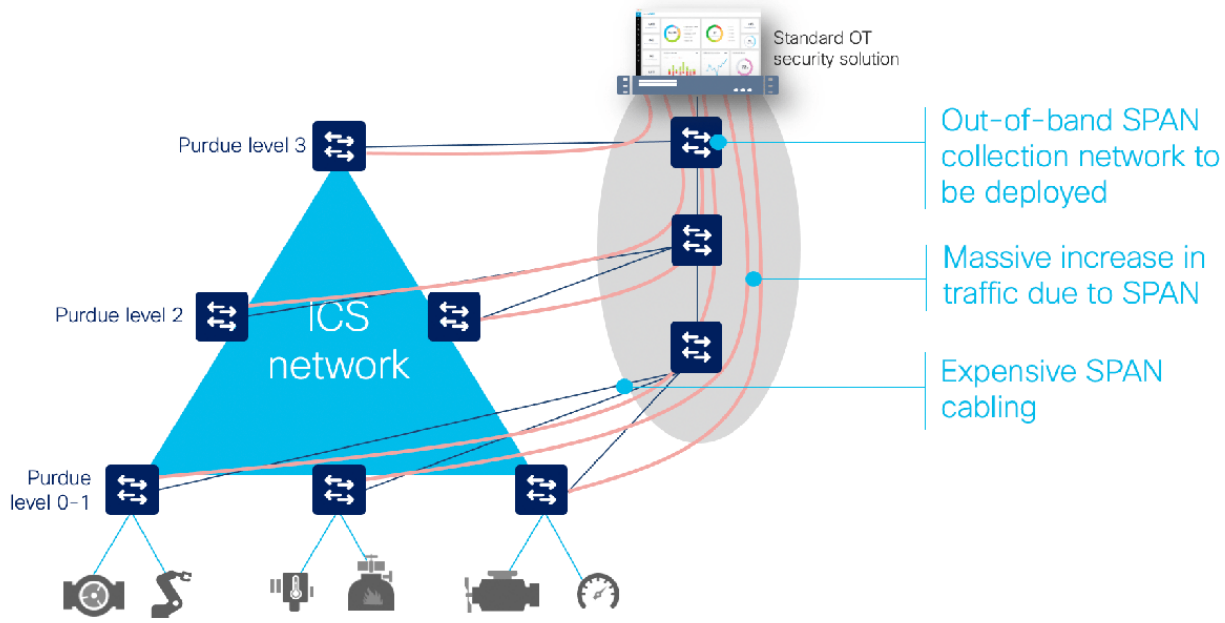



Figure 2. SPAN-based solutions incur huge additional hidden costs.

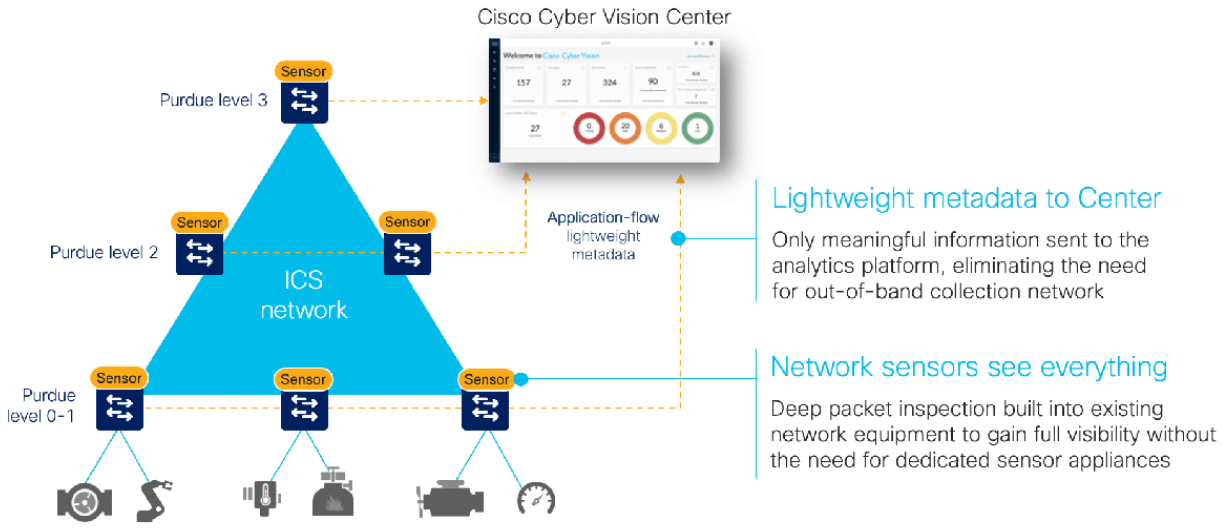



Figure 3. OT/ICS visibility built into networking equipment is more scalable and sees everything.

lightweight, it can be transferred over the industrial network without causing congestion or requiring extra bandwidth.

Embedding DPI in networking equipment affords both IT and OT unique benefits. IT teams can leverage the existing infrastructure to secure industrial operations without having to source, deploy, and manage additional hardware. Because these network elements see all industrial traffic, embedded sensors can provide insights into every component of the industrial control systems. As a result, OT teams can obtain visibility (Figure 3) into operations that they have never had before.

When evaluating OT security solutions, be aware of their architectural implications. Embedding security capabilities into industrial network equipment is the best option to simplify deployment and make it scalable. This requires computing capabilities. Look for DPI-enabled switches and routers designed for industrial networks.

Cisco has embraced this approach. Cyber Vision leverages a unique edge computing architecture that enables security

monitoring components to run within industrial network equipment but can also run using SPAN collection networks to analyze traffic coming from switches and routers that do not support this embedded DPI capability.

## Visibility helps to define zones and conduits

The ISA/IEC-62443 security standards require segmenting the industrial network into zones and conduits. The objective is to restrict communications between assets to prevent attacks from spreading and disrupting the entire production infrastructure.

A zone is a collection of assets that have common security requirements. For example, an automobile plant may have a production line for welding and another for painting. There is no reason equipment in welding would need to interact with that in the paint shop. Placing each in its own zone limits any damage if equipment in one zone gets infected.

Conduits support communication between zones. Under the least privilege principle, OT assets can only communicate with those in their zone. Security policies must be defined for assets to be allowed to communicate outside of their zones, and only through the communication conduit.

Implementing such an architecture will greatly improve security, as well as the overall network performance compared to a flat network where all devices share the same bandwidth. It requires, however, to have an accurate inventory of all connected assets and a perfect understanding of their roles and communication needs in the industrial process.

Visibility is foundational to building zones and conduits. It allows operations engineers to get a clear view of how their industrial network operates, better plan for safety and production continuity, and work together with IT teams to document critical business processes with their associated devices.

Next, IT and OT can work together to group assets into zones (Figure 4), decide how those zones should communicate with each other, and define their criticality to the organization to better understand risks, prioritize threat detection, and manage alarms.

IT personnel often lack an understanding of the OT environment and how it works. OT visibility solutions such as Cisco Cyber Vision enables operations teams to document their industrial process in a way that helps build a collaborative workflow with IT, giving the context it needs to build security policies that will drive segmentation.

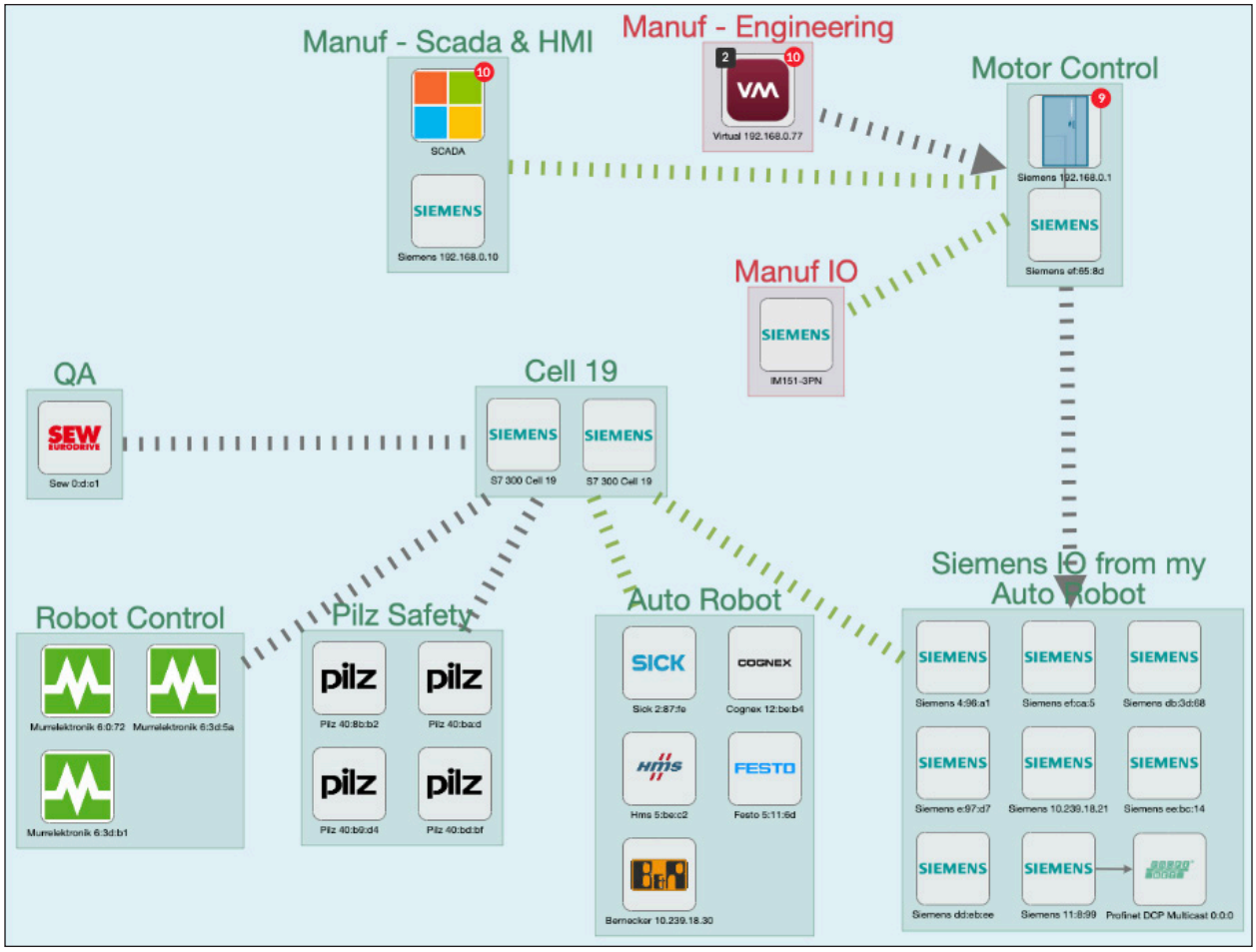



Figure 4. Grouping OT assets helps OT and IT teams work together to define zones and conduits.

## Make the network enforce segmentation policies

Now that the industrial network is well documented, IT can focus on segmenting the network to implement the zones and conduits defined with OT. To achieve this, many would recommend deploying firewalls controlling access to each zone. Although such an architecture has been widely used to segment IT networks, it will quickly prove to be impractical in OT/ICS environments.

Firewalls are perfect to build an industrial demilitarized zone (IDMZ) or secure remote site connectivity in an SD-WAN infrastructure. But using firewalls for zone segmentation in industrial plants leads to similar deployment issues to those IT is facing with visibility appliances. Not only can it be really expensive, but it also requires reconfiguring the industrial network: rewiring it and changing IP addresses of hundreds of OT assets. Operations will have to be halted to implement the changes and might not go back to normal as easily as expected. Chances are, the line of business will not be willing to take the risks and incur such revenue losses.

Maintaining these firewalls rules can become a challenge as OT often has to deploy new assets, move others, reconfigure zones, and more. Industrial networks are not as static as one would think. Operations generally do not have the skills required to configure firewall rules and cannot always depend on IT for every move, add, and change.

Fortunately, it is possible to logically segment industrial networks to enforce security policies without deploying and maintaining firewalls (Figure 5). Solutions such as Cisco Identity Services Engine (ISE), for example, work with network switches, routers, and wireless access points to restrict communications as per the zones and conduits that have been defined. It leverages groups defined in Cyber Vision to allow/deny communications for each asset. When a change is required, just move the asset to another group in Cyber Vision for ISE to automatically apply the corresponding security policy.

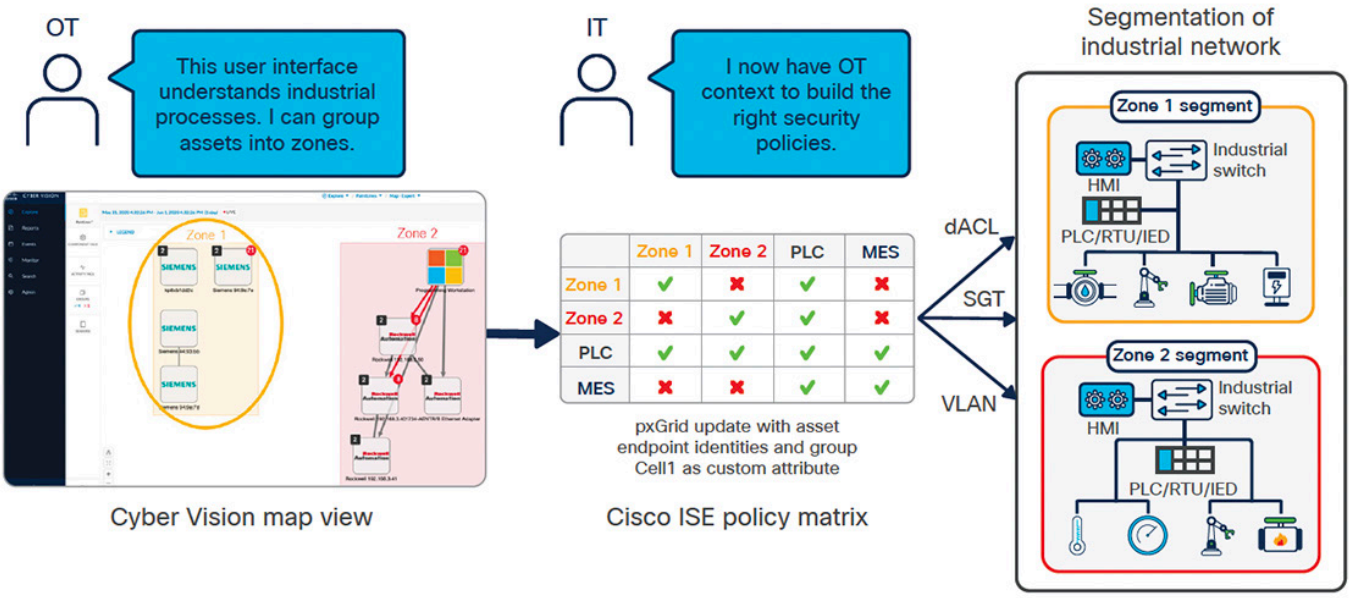



Figure 5. Cisco Cyber Vision and ISE enable a dynamic and automated approach to policy enforcement.

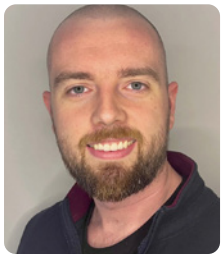
This software-based network segmentation, also called virtual segmentation or micro-segmentation, enables a dynamic and automated approach to policy enforcement that simplifies industrial security projects. It is easier to deploy, scale, and maintain than using zone-based firewalls. It also empowers the operations team to take an active role in defining and managing zones and conduits, helping IT and OT to work together in building and securing the industrial network.

## The network as sensor and enforcer

Industrial operations require advanced cybersecurity capabilities. The traditional approach consisting of deploying dedicated appliances for OT visibility, threat detection, and policy enforcement is proving to be too complex to deploy and too costly to scale. Modern industrial networking can benefit from the latest advances in IT networking, especially when these innovations are implemented with OT constraints in mind.

When working on an industrial cybersecurity project or thinking of expanding or refreshing the industrial network, look for industrial switches and routers that embed these visibility and enforcement capabilities. Avoiding to source, install, and manage additional appliances will have a positive impact on sustainability objectives. It will also allow scalability of industrial security projects while giving operations more flexibility to modify the industrial network without putting its security at risk or requiring extensive IT support when it can be difficult to hire skilled IT/OT networking professionals.

## ABOUT THE AUTHOR



**Andrew McPhee** is a solutions manager for Industrial Security at Cisco, responsible for security architectures across industrial verticals. Since joining Cisco in 2015, McPhee has held roles in the company as both engineer and architect. His roles span the Automotive Business Unit, the Security Business Group, and most recently the IoT BU. He has released Cisco Validated Designs for projects such as SASE, Zero Trust, and Breach Defense Technologies.


# Industrial Control with Remote I/O

**RIO MM1**
Universal I/O

**RIO MM2**
Universal I/O with Ignition
IgnitionEDGE

**RIO EMU**
Energy Monitoring

**10 Channels of software-configurable I/O:**

- Analog input sensing (V/mV/mA/Ohms)
- Temperature input sensing (ICTD/TC/thermistor)
- Simple discrete input sensing
- Powered switch discrete input sensing
- Analog output control (V/mA)
- Discrete output control, including 2 mechanical relays

***groov* RIO with CODESYS embedded** uniquely combines the power of an IEC-61131-3 programmable controller with 10 channels of universal, software-configurable I/O, plus state-of-the-art cybersecurity features, including account management, certificates, encryption, and network segmentation.

Learn more at www.opto22.com.

groov® RIO

now with

CODESYS

and

Sparkplug COMPATIBLE



OPTO 22
Your Edge in Automation.™

# Look for Cybersecurity Features in Edge Controllers, I/O

## Built-in security options help users build a more secure network for connected automation.

By Benson Hougland, Opto 22

Sharing operational data from industrial equipment can improve decision making from the shop floor to the executive suite. But cybersecurity is a constant worry. Industrial systems and data are essential, sensitive, and must be protected. How can newer industrial automation hardware help users protect their systems and still get important data to on-premises and cloud-based software and services?

For all computer networks, security is a complex issue that changes based on the organization and its system. As systems evolve, security requirements change and grow. Building flexible security into the system design is key.

To address security's complex, changing nature, users must understand security risks, environment, and the security tools at hand. Security experts recognize several elements of system security, including physical security, policies and procedures, and network security.

**Just like laptops or bank accounts**, edge controllers and edge I/O can require users to identify themselves using a unique username and password before they can do anything else.

For network security, newer industrial edge controllers and input/output (I/O), like Opto 22's *groov* EPIC and *groov* RIO, help users meet requirements in ways that used to be impossible in automation, except by using industrial computers (IPCs), servers, or security-specific network appliances. Designed from the ground up to help build distributed systems, edge controllers and edge I/O provide the tools and methods necessary to make systems as secure as possible from a network access standpoint, while maintaining the flexibility required for specific applications.

Key cybersecurity features that edge controllers and I/O are helping to popularize include user authentication, connection encryption, firewalls, network zoning, and outbound communications.

## User authentication

Controlling who can access a device and exactly what each user can do with it is a vital part of cybersecurity. Just like laptops or bank accounts, edge controllers and edge I/O can require users to identify themselves

using a unique username and password before they can do anything else (Figure 1). These devices typically provide services for creating and managing users as well as related parameters like session timeouts. Security-conscious edge devices avoid the use of a default username and password that someone might be able to guess or look up on the Internet.

Edge controllers may provide different access levels for administrators, developers, operators, API calls, and so on, then allow those user rights to be assigned to authorized people or software services. Authentication may happen through either a username/password combination or an API token.

When limiting access to the edge device in this way, consider it as part of a total security system that includes other best practices like requiring that authorized users change their passwords every three months or securing the control equipment in a locked cabinet with keys accessible to a limited number of personnel.

If a site manages user accounts through a lightweight directory access protocol (LDAP) service (for example, Microsoft Active Directory Service), users may be able to work with their IT department to configure edge devices to connect to the LDAP server, authenticate a user, and help determine which services a user can access. For simple setups, use the LDAP server to authenticate users and give them default local permissions.

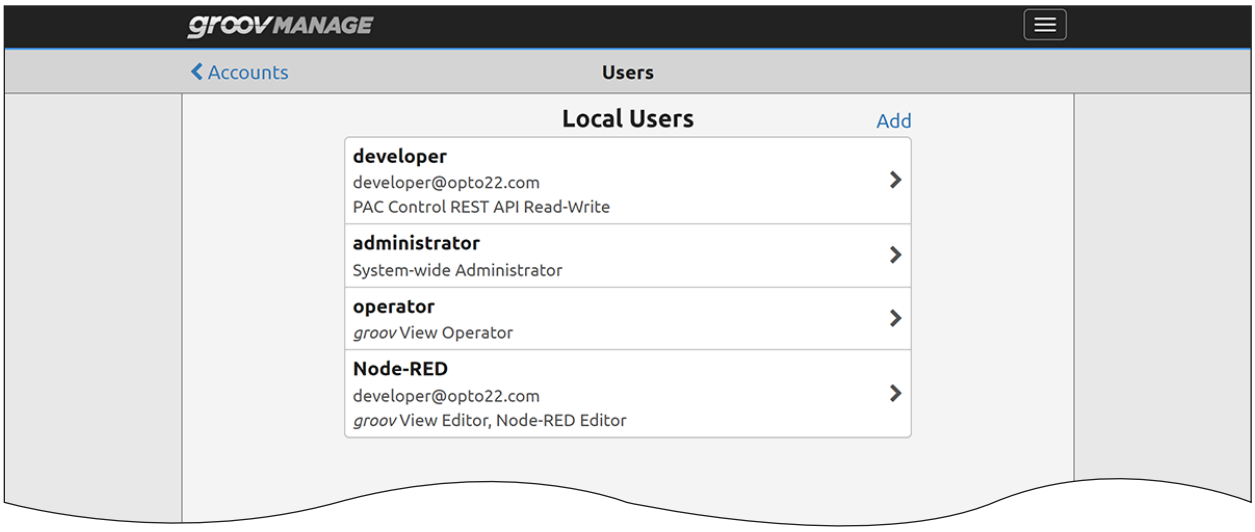



Figure 1. Opto 22's *groov* EPIC and *groov* RIO provide granular user and software client access control.

For systems with a larger number of users or more complex user management, just map an LDAP group to a specific set of permissions.

## Connection encryption

Authentication services tell a server that a user or piece of software is authorized to access the server's resources. Encryption—another important security feature—protects data so that it is unreadable by anyone who does not have the decryption keys. SSL/TLS [Secure Sockets Layer and its newer version, Transport Layer Security] use security certificates consisting of a private key and a public key to encrypt the traffic between the client and the server.

Security certificates are also a way that clients can verify a server's identity so that when a client tries to connect, it can be assured it is communicating with the correct server and not an impostor (Figure 2).

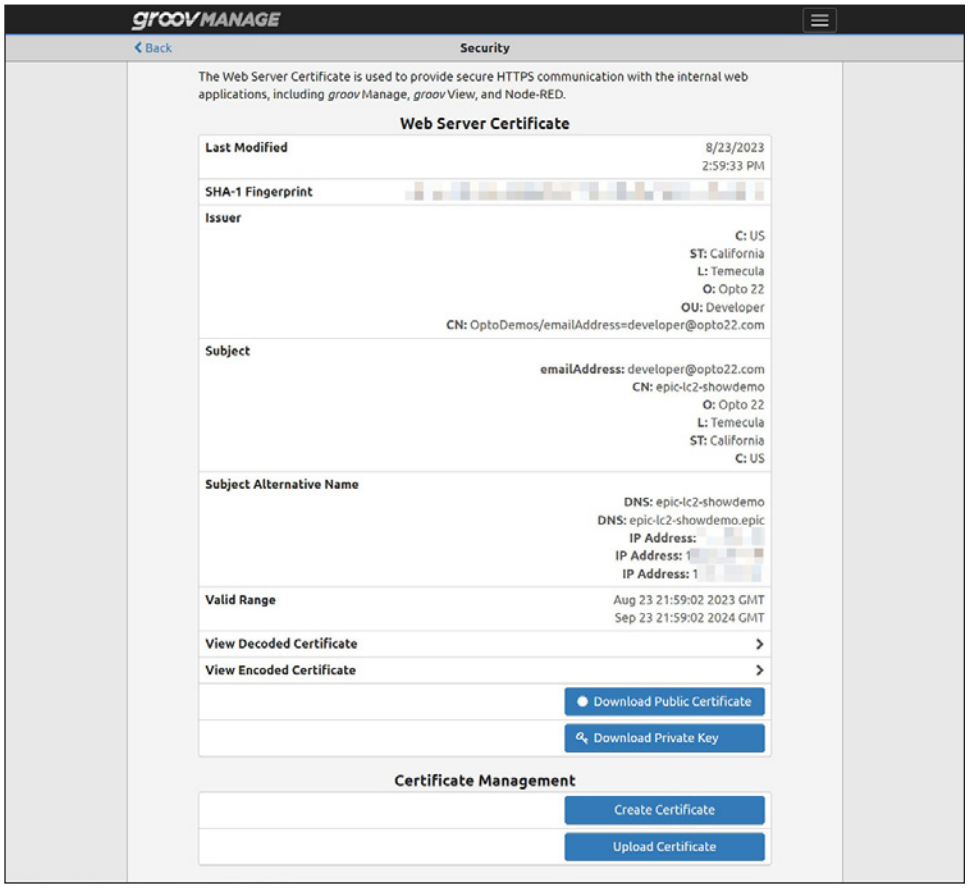



Figure 2. The *groov* EPIC system supports X.509 PKI standard certified client connections.

Industrial edge controllers can use this infrastructure to prevent incoming and outgoing data from being observed by unknown third parties—what is called a man-in-the-middle attack.

X.509 is a standard format for public key certificates and can be used by edge controllers and edge I/O to secure client connections to servers (client SSL) and from clients to the device's secure server (server SSL). SSL/TLS certificates can be device-generated, self-signed, or registered publicly through a Certificate Authority (CA).

For example, each *groov* EPIC processor and each *groov* RIO module comes with a unique certificate (called a self-signed server SSL certificate) to enable encrypted communication between its internal web applications and web browsers on computers and mobile devices. However, users might want to use a certificate signed by a third-party CA for any of the following situations:

- To allow access to the edge device by many more users and through many devices (like computers, smartphones, and tablets).
- To allow remote access to the edge device via REST API calls, OPC UA clients, or other inbound communications.
- To allow communication to travel through the Internet.

**Security certificates** are also a way that clients can verify a server's identity.

A Certificate Authority is a trusted organization that vouches for a server's identity on users' behalf. CA-signed certificates relieve users of the work of installing certificates on all the clients connected to an edge device.

When a server certificate is installed on the edge device and a client device attempts to connect, a certificate exchange validates the connection between them. So long as the client stays connected directly to the controller on a secure connection (using https, for example), the data they share is protected from a man-in-the-middle attack.

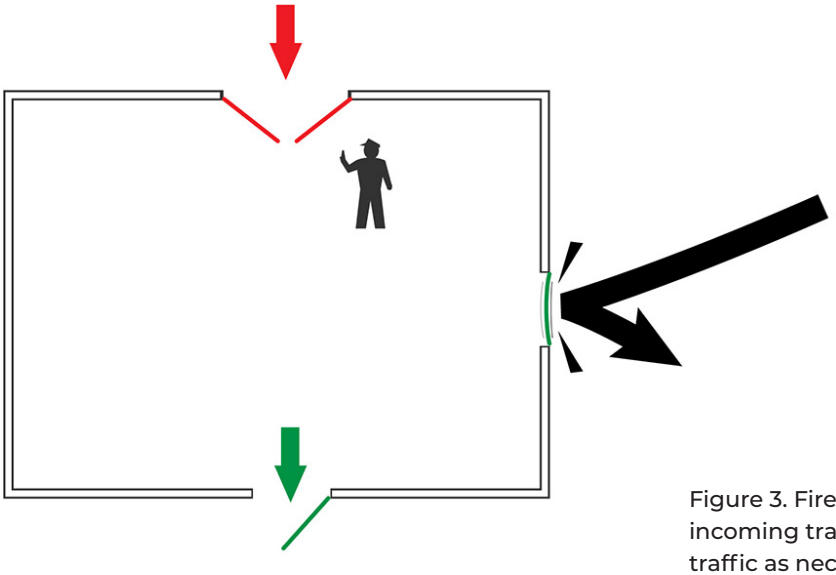


Figure 3. Firewalls block unwanted incoming traffic but permit outgoing traffic as necessary.

## Firewalls

Firewalls are critical in securing data communications, and since edge controllers and I/O are designed for distributed communication, embedded firewalls are becoming a required feature (Figure 3).

A firewall on a network or a device acts like the doors in a building. The door on a building's main entrance often swings in to allow entry, and a security guard or receptionist checks IDs and regulates who is allowed to enter. 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.

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.

Edge controllers and edge I/O with a device firewall help provide security by stopping unsolicited traffic from accessing automation networks, software applications, and connected devices. Typically, the only traffic the edge device should allow back through is responses to traffic that originated from the controller's software. Device-originated connections are considered trustworthy because their origin is known.

However, a device firewall typically provides configurable security options. For example, each network interface on *groov* EPIC—the two Ethernet interfaces, the wireless interface, and the virtual private network (VPN) interface—has its own firewall settings. Users can set specific firewall rules for each interface, for trusted networks (where unsecured ports are open), and untrusted networks (where only encrypted, authenticated ports should be open).

**Typically, the only traffic the edge device** should allow back through is responses to traffic that originated from the controller's software.

## Network zoning

A key concept in the ISA/IEC 62443-3 specification on industrial cybersecurity is zoning—keeping networks isolated to prevent unauthorized access to data. Industrial edge devices can help by providing independent interfaces that isolate trusted networks from untrusted networks.

- A trusted network is any network where users know exactly who has access to it, for example, the OT network where existing programmable logic controllers (PLCs) and I/O reside.
- An untrusted network is any network where users don't know who has access to it, like an IT network or the Internet.

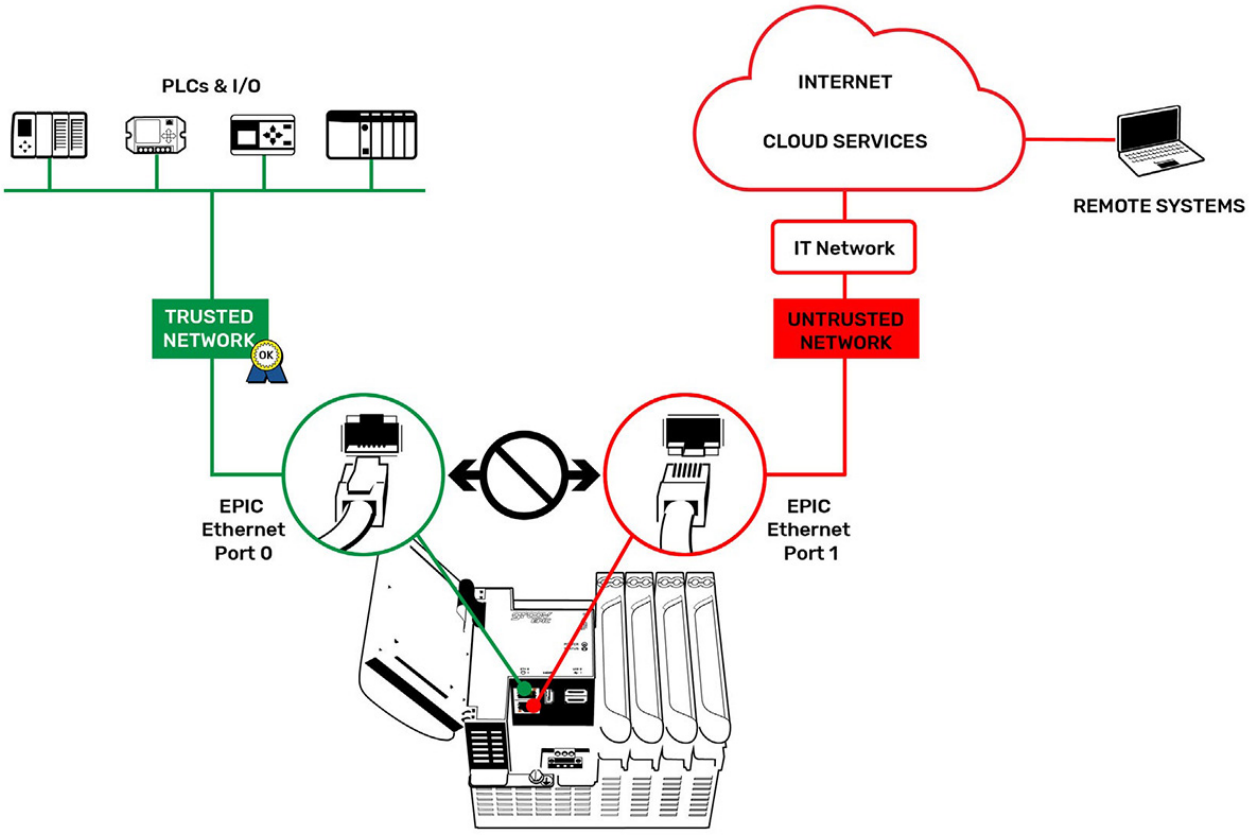



Figure 4. The *groov* EPIC's default configuration segments network traffic into trusted and untrusted security zones.

For example, *groov* EPIC is not a router, which functions to join two networks together. Instead, it keeps trusted networks and untrusted networks apart, separating them into zones (Figure 4). This default configuration eliminates any chance of unsecured devices on one network interface being exposed to the others.

However, for users who need to access an edge controller or edge I/O from an untrusted network (for example, if they are using the Internet or a corporate LAN), edge devices can also support VPN tunneling, which allows disparate networks to be bridged through secure connections to a shared VPN server.

An industrial edge device with built-in VPN support (Figure 5) can connect to VPN servers as a client on an outbound, device-originated connection (so no open inbound ports on the device are required). Additionally, by configuring the edge device as a host, it can provide remote access to its own software services. Then, any other VPN client (like a PC or mobile device) can securely log into the VPN server using a valid account or client configuration file. Once connected, the client can reach the edge device's software applications.

By default, VPN access to an edge controller or I/O provides access only to software running on that device, not to any other devices connected to the controller via other network interfaces. However, if

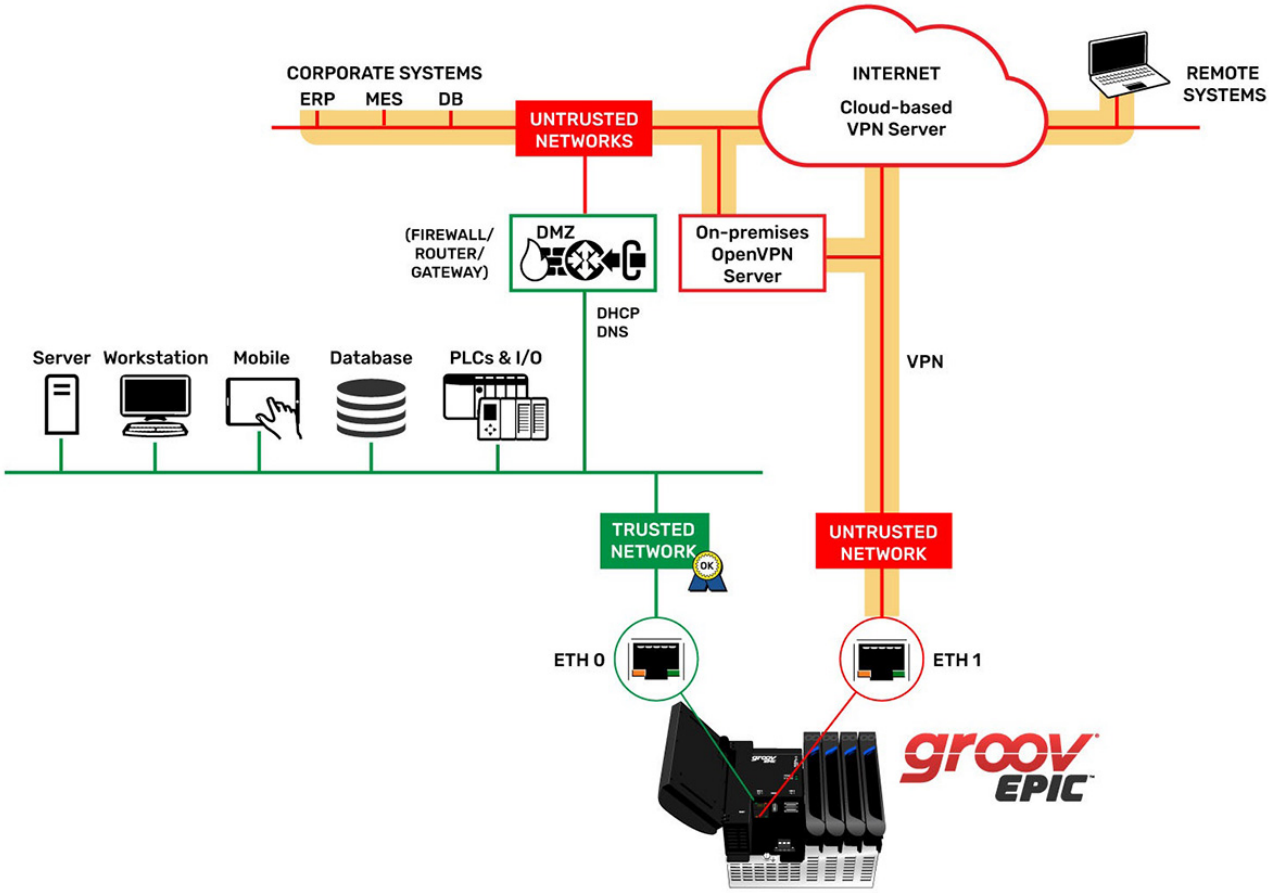



Figure 5. An edge-oriented virtual private network (VPN) using *groov* EPIC's embedded OpenVPN client.

users want to allow access to devices in another network zone, some edge controllers allow the use of port redirection (Figure 6) to create temporary conduits between various network interfaces.

For example, perhaps there is a PLC on a trusted OT network that must be reached from another network to make changes using the PLC's own proprietary software (for example, Logix software from Rockwell Automation connecting to an Allen-Bradley PLC). With port redirection, users can designate a specific port on one network interface to permit traffic to pass through to an IP address and port on the network interface connected to the PLC.

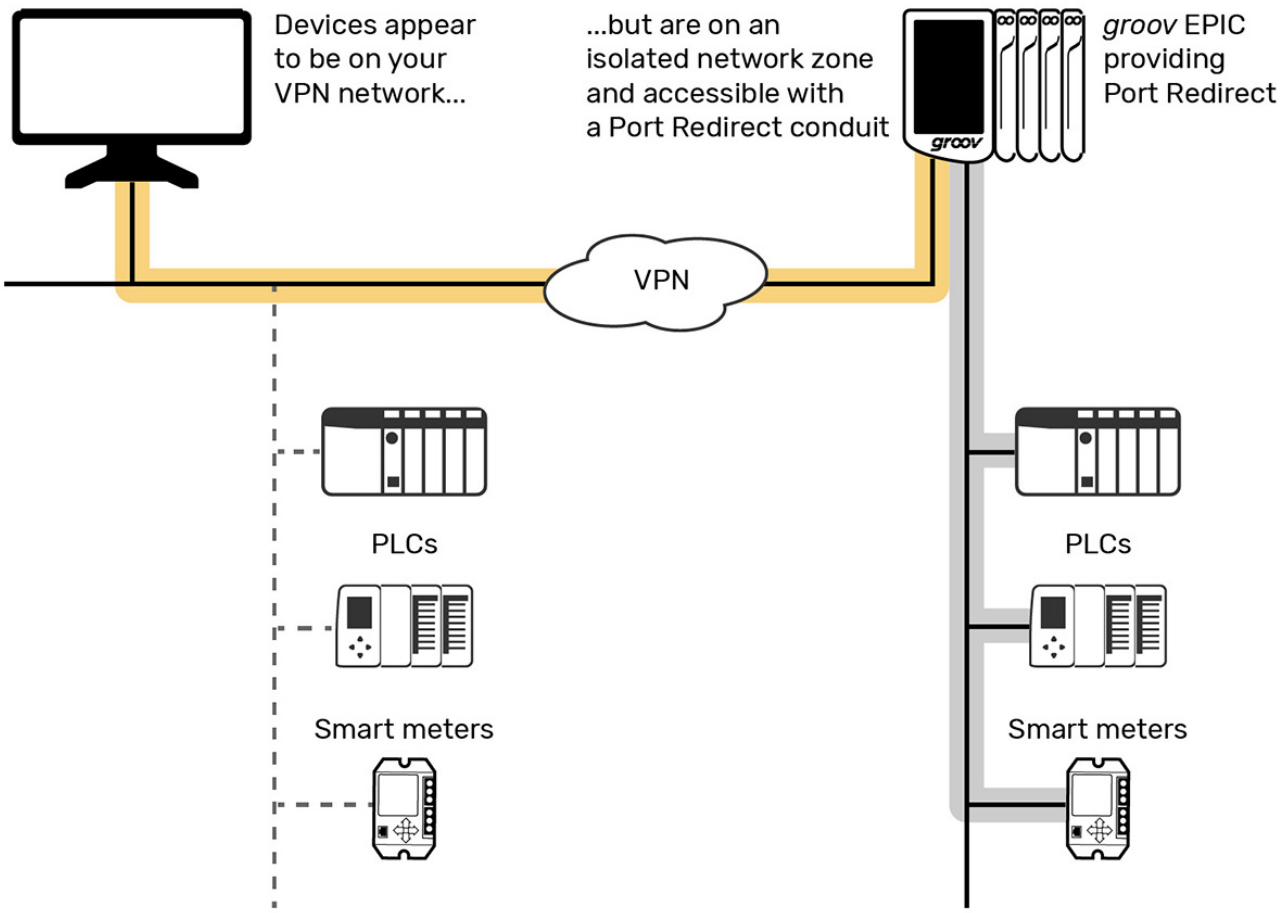



Figure 6. With *groov* EPIC's port redirect feature, a remote PC can securely update a protected PLC's software over a VPN connection.

Best practice is to block all unsecured 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, just configure a port redirect—a conduit—from the VPN tunnel interface established on the untrusted network zone to the trusted network zone, where the unsecured PLC is. This conduit should be enabled only on demand and for a limited time period.

## Outbound communications

As mentioned, an edge device is inherently more secure and requires less configuration when it uses outbound data communications, rather than having to open ports to receive connection requests. Should a malicious actor (human or software) obtain enough information to send a connection request to the device, it could exploit an open port in the firewall to grant itself control or read sensitive information. Restricting communications to outbound services means the firewall can be buttoned up tight, eliminating this vulnerability completely.

VPN, already explored here, is one example of device-originating, outbound communication that an industrial edge device might provide, but there are many others. Traditional automation activities like talking to remote I/O or polling Modbus/TCP devices require only outbound connections. More exciting still, RESTful calls to web services, posting data to SQL databases, and performing publish-subscribe communications over MQTT are also outbound communications that an industrial edge device can provide.

Note that protocols like MQTT and VPN provide the option to persist these outbound connections so that bidirectional communication is still possible within this security framework.

## New strategies, new options

Traditional approaches to securing automation networks like air

gapping, VLANs, or IP filtering naturally complicate efforts to build connected systems and democratize operational data. By contrast, industrial edge controllers and edge I/O offer a granular approach that embeds essential security functions directly into a user's process, maintaining a defense-in-depth strategy without restricting communication options or scalability.

This article is not intended to be a comprehensive guide to ICS security. However, when used in combination and as part of a larger security strategy, the functions outlined here—user authentication, connection encryption, firewalls, network zoning, and outbound communications—can significantly restrict access to critical control functions and sensitive data.

Importantly, these security functions now available in industrial edge devices are already prevalent throughout IT network infrastructure, making them highly compatible with existing security elements and helping to bridge the gap between IT and OT systems.

For more information, explore the full "*groov* Products Cybersecurity Design and Best Practices Technical Note" from Opto 22.

## ABOUT THE AUTHOR

**Benson Hougland** is vice president of marketing and product strategy at Opto 22. With 30 years of experience in information technology and industrial automation, Hougland drives product strategy for Opto 22 automation and control systems, which connect and secure the real world of OT with the systems and networks of IT and cloud. He speaks at trade shows and conferences, including IBM Think, ARC Forum, and ISA. His 2014 TEDx Talk introduces non-technical people to the IoT.

# MANAGING NETWORK SECURITY

## A simple approach to cybersecurity can be as simple as which Ethernet switch you use.

By Charlie Norz, WAGO Corp.

There is no doubt that network security for manufacturers is a top priority now more than ever. Controls engineers are constantly looking for ways to stave off cyberattacks and put action programs in place to help reduce security risks. The risks at the operational technology (OT) level are continually changing and keeping up with protecting a company's operational technical infrastructure may seem time-consuming and costly. However, there are ways to ensure the safety of a company's products, property, and processes in a concise and cost-effective way.

### Use proper Ethernet switches

On the most basic level, one of the ways to ensure security against outside hackers is to use the proper industrial Ethernet switches.

Some companies are happy with just the essential levels of networking, settling for low-cost options. This will get them the bare necessities to run their plant floor operations, usually in the form of an industrial unmanaged switch. These switches are an excellent option for networks with a control panel used for a plug-and-play option that has a fixed configuration. This keeps the information technology (IT) personnel from having to set up encryptions, prioritize channels, or create segregated devices to manage traffic and data. The downside of unmanaged switches is that they do not provide security functions.

Companies that have large networks may seek to have more than the basic functions of an unmanaged switch. With a slight increase in cost, the effectiveness of a lean managed switch can give controls engineers on the plant floor the peace of mind they need when running their systems. Lean managed switches can be configured to a company's specifications, can monitor settings, turn off unused ports, set up and manage encryptions, as well as help protect the network and data from active threats. Virtual Local Area Networks (VLANs) can also be installed that reduce security risks and help increase network performance.

WAGO's family of industrial Ethernet lean managed switches are designed to meet security and redundancy requirements and can be easily maintained by plant floor technicians. Emphasis has been placed on creating an intuitive and easy-to-use interface. The diagnostic dashboard allows quick system troubleshooting, even if users have no IT knowledge. With each port configured for specific connections, not only can transmission errors be detected, but improper connection or active threats can be revealed as well. Depending on the network size, switches come with either eight or 16 ports with two extra small form-factor pluggable (SFP) slots for connecting fiber optic cable for longer connections.

## Looking ahead

Having a safe and secure network to help protect plant floor data and information should be paramount to ensuring a company's ability to thrive in today's digital age. While you may want or need to take more high-end security measures, simply making the change from an unmanaged to a lean managed industrial switch could save you from the major headache caused by a cyberattack.

### ABOUT THE AUTHOR

**Charlie Norz** (Charlie.Norz@wago.com) is the senior product manager for automation at WAGO Corp. located in Germantown, Wis. WAGO's parent company in Minden, Germany pioneered CAGE CLAMP spring pressure connection technology and uses it in its interconnect, interface, and automation solutions.

# Connect The Dots With Ignition!

## The Unlimited Platform for Total System Integration

ALL YOUR DATA

ALL YOUR DEVICES

ALL YOUR OPERATIONS

ALL YOUR PEOPLE

ALL YOUR LOCATIONS

**ONE PLATFORM TO CONNECT ALL YOUR PROCESSES, PEOPLE & PROGRAMS**

Learn more about Ignition: ia.io/platform

inductive automation

# Advancing Industrial Cybersecurity

Helping policy makers and private-sector leaders protect critical infrastructure.

From the International Society of Automation

Cybersecurity threats and vulnerabilities pose a clear and present danger to our facilities, our processes, and the safety of our communities. But when most people think about cybersecurity, they focus on what are commonly considered information technology (IT) challenges impacting individual equipment or networks. While these are valid concerns, the impact on the facility or its operation from equipment or network compromise is much more concerning.

This position paper aims to address how policy makers and private-sector leaders can be best equipped to address the urgent need for improved critical infrastructure cybersecurity through globally relevant standards and conformance programs, as well as strong support for the community of engineers and automation professionals working every day to keep our facilities, processes, and communities safe.

**ISA's standards, training, conformance programs, and guidance** can help reduce the likelihood and consequence of a cybersecurity incident in an industrial automation and control system environment.

## Harm to critical infrastructure

The impacts of cyber intrusions on banking, business, and government networks, as well as databases have been widely publicized and are well known to the general public. Much less publicized and understood are the devastating impacts to public safety and welfare that could result from cyber-attacks on the networks and technology that underlie the vast critical infrastructure and manufacturing sectors on which all modern economies depend.

While certain high-profile incidents have made international news (e.g., TRISIS, NotPetya, and STUXNET), in fact, control system cyber incidents have been more numerous and more impactful than most people have been aware. At the core of this challenge is identifying control system events and reportable cyber incidents. Understanding the unique nature of control system equipment—and the impact of a compromise of that equipment on physical processes—requires specialist training for the engineering and automation community. Such training is available from the International Society of Automation (ISA); however, a major concern is that not enough engineers are equipped for the unique and growing challenges of the industrial cybersecurity environment.

Training is just one need among many. In reality, what a lot of organizations require is a cultural shift that prioritizes cybersecurity alongside functionality, efficiency, and safety as one of the fundamental workplace tenets. Until organizations prioritize cybersecurity at this level, even the best equipped and most trained engineers will be challenged to fully protect their industrial or infrastructure environment.

## Government directives

The U.S. National Cybersecurity Strategy and its Implementation Plan address these dangers by explicitly calling for:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety, and harmonizing regulations to reduce the burden of compliance.
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services.

However, the National Cybersecurity Strategy does not address the need for the engineering community to be involved, nor is the focus on control systems and processes. Further, the strategy does not specifically mention the leading consensus standards and conformance programs for industrial cybersecurity.

The European Union (EU)'s second iteration of the Network and Information Systems (NIS) Directive, NIS2, contains stricter rules and applies to a broader set of industries. Together with the EU's Critical Entities Resilience directive, this will see member states incorporating key provisions on cybersecurity into their national law. These are just two examples of countries and regions around the world that are taking such a stance and recognizing the threat to their critical infrastructure.

## Why ISA?

The International Society of Automation (ISA), a member association of automation professionals from across the globe, believes that protecting critical infrastructure against cyber-attacks is essential to national security, public and employee safety, and the economy. To help

address the challenge of protecting critical infrastructure, ISA produces a series of international consensus standards addressing the security of industrial automation and control systems. The ISA/IEC 62443 series of standards provides other guidance that presents a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in those systems.

This series of standards meets the World Trade Organization's criteria for international standards. The International Electrotechnical Commission (IEC), one of three United Nations sanctioned standards developers, has adopted the series, and designated them as having "horizontal" status, establishing primacy across the entirety of the vast range of IEC technical committees and subcommittees on matters pertaining to cybersecurity in industrial, critical infrastructure, and related applications. The United Nations Economic Commission for Europe has integrated the series into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe.

ISA created the ISA Global Cybersecurity Alliance (ISAGCA) to advance cybersecurity readiness and awareness in manufacturing, and critical infrastructure facilities and processes. The Alliance brings end-user companies, automation and control systems providers, IT infrastructure providers, services providers, system integrators, and other cybersecurity stakeholder organizations together to proactively address growing threats. ISA also offers the leading conformity assessment program for industrial cybersecurity products and systems, ISASecure, which certifies against the ISA/IEC 62443 series of standards.

ISA's positions, standards, training, conformance programs, and guidance can help reduce the likelihood and consequence of a cybersecurity incident in an industrial automation and control system environment.

### ISA takes the positions that:

- Mandating cybersecurity measures with prescriptive regulations is undesirable. Instead, regulations should support the use of risk-based approaches based on published consensus-based technical standards and conformance measures.
- Specific standards that take account of the unique characteristics of industrial automation and control systems should be used in preference to more general information technology standards.

### ISA recommends that:

Governments looking to secure their critical infrastructure should:

- Adopt by reference the ISA/IEC 62443 series of consensus standards addressing the security of industrial automation and control systems.
- Direct their regulations toward ensuring that critical infrastructure owner-operators apply a formal risk-based approach to cybersecurity management.
- Organizations looking to secure their critical infrastructure should:
    - Support their front-line engineers by fostering a cybersecurity culture within their organization, which prioritizes cybersecurity alongside other fundamental workplace tenets like efficiency and safety.
    - Provide ample opportunities for engineers to be trained and certified on the specific requirements of cybersecurity of industrial automation and control systems.

### ISA commits to:

- Developing and maintaining consensus-based standards, conformance programs, and guidance that secure industrial automation and control systems using a flexible risk-based approach that ensures any size organization in any sector can use appropriately and efficiently.

- Providing training resources to advance the understanding and application of the standards.
- Promoting the adoption of standards and providing vendor- and sector-agnostic guidance on how to apply these standards.
- Working with governments around the world to adopt standards and guidance to secure critical infrastructure.

An industrial automation and control system (IACS) is so much more than its hardware. It also includes the people and work processes needed to ensure the safety, integrity, reliability, and security of the control system. Policy makers and private-sector organizations alike must strongly consider the need for compliance to global consensus standards for IACS cybersecurity and must also create a culture of support and continuous training for the engineers who keep control systems operating at their best.

## ABOUT ISA

The International Society of Automation (ISA) is a non-profit professional association founded in 1945 to create a better world through automation. ISA empowers the global automation community through standards and knowledge sharing, driving the advancement of individual careers and the overall profession. ISA develops widely used global standards, certifies professionals, provides education and training, publishes books and technical articles, hosts conferences and exhibits, and provides networking and career development programs for its members and customers around the world.


txOne networks

Keep the Operation Running

# OT Cybersecurity. Simplified.

See why TXOne's solution was cited as a Top 2023 Innovator in Westlands Advisory's Industrial Cybersecurity Outlook 2023-2030 report

Download your free report

# Mitigate Four Cyber Threats Facing Automated Factories

As IT and OT systems converge, attackers have more factory OT network entry points.

Automated manufacturing is growing fast. Along with greater efficiency comes greater risk. Four automated factory technologies in particular warrant focused cybersecurity attention: the Industrial Internet of Things (IIoT), industrial robots, augmented reality (AR) devices, and additive manufacturing (AM).

By Mars Cheng and YenTing Lee, TXOne Networks

What these four technology areas have in common is the need to process large amounts of data, forcing more interaction and integration between information technology (IT) and operational technology (OT) networks. As IT and OT continue to converge, attackers have more factory OT network entry points, which means more vulnerabilities of concern.

According to the Trend Micro Security Predictions For 2023 report in collaboration with TXOne Networks, the authors foresee an upward trend in IT-based cyberattacks inadvertently affecting OT systems that are connected to IT networks—and worse, revealing OT systems as an underutilized attack vector through which malicious actors can move laterally between OT and IT environments.

In 2021, Trend Micro also revealed that 61 percent of automated manufacturers have experienced cybersecurity incidents, many causing downtime. To protect automated manufacturers, TXOne Networks analyzes the global trend of automated factories to identify the following potential threats and to propose an adaptive cybersecurity solution for shop floor industrial control systems (ICS).

IIoT, industrial robots, augmented reality, and additive manufacturing pose real threats to automated factories.

**What these four technology areas** have in common is the need to process large amounts of data, forcing more interaction and integration between IT and OT networks.

## 1. The Industrial Internet of Things

As large numbers of machines are introduced to the network in this era of digital transformation, factory environments can be vulnerable to initial access cyberattack techniques. Fully entrenched in the realities of Industry 4.0, smart manufacturing is deploying IIoT technologies to improve operational efficiency and reduce operating costs. The

adoption of IIoT technologies was expedited during the pandemic to keep operators safe while maintaining production. However, this brings the potential to expose vulnerabilities—especially in OT environments—that were once truly air gapped.

Commonly used IIoT protocols can provide more attack vectors to connected devices. Wireless is also a problem, as endpoint devices use *Wireless*HART or BLE to upload endpoint information to the cloud via a network gateway, creating entry points.

Protection requires network defenses to limit trusted data sources supported by a visualization solution to manage the server. Network defense solutions can learn the trusted behavior of each piece of equipment. When users know the trusted behaviors of each device, they can prevent attackers from carrying out further attacks.

## 2. Industrial robots

Malware can be introduced to the development environment of industrial robots, enabling highly privileged workstations to execute malicious behaviors.

Industrial robots (Figure 1) are autonomous and mobile, collaborating with each other to perform physical operations in

Figure 1. Industrial robots generally consist of a controller, robot, and workpiece.

many large-scale manufacturing factories. These industrial robots generally consist of a controller, robot, and workpiece. Engineers often upload or download extension kits from an app store-like service. If the content is not inspected, the engineer may unintentionally download infected kits, execute them, and threaten the factory network.

Some industrial robots don't authenticate the access control by default. If the equipment is exposed to the public network, attackers can exploit vulnerable but common network protocols. In some cases, public downloadable off-line programming (OLP) software can modify controller parameters, production logic, or robot status to tamper with factory production outcomes. To understand the potential for danger, in 2021 a cyber intruder penetrated a Florida water treatment facility twice in one day and was attempting to poison the supply when detected.

## 3. Augmented reality

Improperly stored augmented reality (AR) devices may allow the theft of factory data and the destruction of cloud data.

Wearable or handheld devices with AR technology are used to enhance the interaction between engineers and machines and access cloud data. When suppliers or technicians are required to enter the factory area, any AR devices that are not adequately protected by physical security can be and have been stolen, along with confidential factory information.

Information may include anything from production processes to pharmaceutical or food ingredients. AR devices used by engineers are considered trusted sources. In the wrong hands, they can be used to access enterprise cloud data and expand the impact throughout the factories.

## 4. Additive manufacturing

If the configuration files in additive manufacturing (AM) equipment are tampered with, the equipment can overheat, leading to large-scale disasters.

Many manufacturing plants are introducing additive manufacturing (AM) technology to manage supply chain issues, particularly in automated factories related to aerospace, automotive, or medical industries. In essence, AM technology is a computer-controlled process of creating a three-dimensional object by depositing materials one layer at a time. SANS researchers have found that thousands of insecure AM devices are exposed to the public network and the devices can be controlled without authorization.

When most AM devices used unencrypted files (G-code format) to control printing, attackers have the opportunity to steal confidential product information. Certain malicious firmware can make the device persistent, where excessive heating can cause large-scale disasters in factories.

## Four pillars of OT zero trust

TXOne Networks believes that effective cybersecurity solutions that ensure the operation reliability and digital safety of ICS and OT environments are best achieved through the OT zero trust methodology and its four pillars:

- **Inspect**: Conducting a security inspection before any new equipment enters the shop floor is necessary to prevent insiders from intentionally or unintentionally bringing malware into the factory environment.
- **Lock down**: Stop malicious behavior and unintended operation by implementing OT protocol command-specific allow lists at both the endpoint (machine) and OT network level.

- **Segment**: Network segmentation is vital. By arranging enterprise assets into isolated groups based on their purpose, users sharply limit options for attack, and restrict those attacks to a specific area to contain the damage.
- **Reinforce**: Virtual patching is strongly recommended to block loopholes on the manufacturing execution system (MES) and shield vulnerabilities of legacy or unpatchable systems protecting sensitive, critical assets.

To learn more about effectively protecting automated factories across the entire lifecycle of factory machines, download TXOne Networks' "OT Zero Trust Handbook."

## ABOUT THE AUTHORS

**Mars Cheng** is threat research manager and **YenTing Lee** is a threat researcher within PSIRT and Threat Research at TXOne Networks. TXOne Network's Threat Research Team performs a variety of vulnerability research on industrial control system (ICS) devices and protocols, as well as analyzes potential threats, malware and ransomware related to OT environments. Mars Cheng and YenTing Lee share the team's findings at top security conferences around the world including Black Hat, DEFCON, RSA Conference, and FIRST.

Enjoy **1 Year**
**Additional Warranty**
And 5 Year
Standard
Warranty

Special promotion:
Now until Dec 31, 2023

# EDS-2000/G2000-EL/ELP Series

## Industrial Unmanaged Ethernet Switches

**Scan the QR code to learn more**

- 5 or 8 Ethernet port options
- SC/ST fiber models are available for the EDS-2008-EL Series
- Full Gigabit ports for the EDS-G2000-EL/ELP Series
- Supports 12/24/48 VDC input
- Microsecond-level latency
- High EMC resistance
- QoS and BSP* DIP switch configuration

*Quality of Service (QoS) and Broadcast Storm Protection (BSP) can be configured via DIP switches.

# Getting IIoT Networks Ready for the Future

## Three tips can enhance network preparedness and help secure IIoT networks.

By Roger Chen, Moxa

When an Industrial IoT network is finally up and running, it may be tempting to rest on your laurels. Nonetheless, change remains the only real constant in the world of industrial networking. An IIoT network may be sufficient for your current needs. It may even be ready for foreseeable application requirements over the next several years. But what about the next decade? Change is always in the air, and you need to be prepared.

Since the early days of industrial automation, manufacturers have adopted a variety of purpose-built protocols and systems for highly specialized control applications instead of using standard Ethernet technologies. However, as IIoT continues to expand, industrial networks in the future will be required to transmit much larger volumes of data

between interconnected devices and to collect information from remote devices for both OT and IT engineers to access (Figure 1). With these growing demands on the horizon, network preparedness may determine an enterprise's success.

Consider these three tips to help prepare the IIoT network for the future.

## 1 Achieve greater integration with unified infrastructure

Over the years, various devices using different protocols have been deployed on industrial networks to provide diverse services. Under these circumstances, network integration usually costs more than expected or becomes more difficult to achieve. Manufacturers can either choose the status quo, that is, maintain their pre-existing isolated automation networks with numerous purpose-built protocols of the past, or seek solutions to deterministic services that can integrate these "islands of automation" into one unified network.

If the goal is to be ready for future demands, the choice is obviously the latter. The rule of thumb is to take potential industrial protocols into consideration and ensure you can redesign networks in case any new demands arise in the market. One approach is time-sensitive networking (TSN), a set of new standards introduced by the IEEE 802.1 TSN Task Group as an advanced toolbox. With TSN, users can build open, unified networks with standard Ethernet technologies that reserve flexibility for the future.

Figure 1. Industrial networks in the future will be required to transmit much larger volumes of data between interconnected devices and to collect information from remote devices for both OT and IT engineers to access.

## 2 Enable anywhere access with hassle-free cloud services

Cloud-based remote access offers many benefits to IIoT users such as reducing the travel time and expenses of sending maintenance engineers to multiple remote sites (Figure 2). Furthermore, cloud-based secure remote access can offer flexible and scalable connections to meet dynamic, fast-changing requirements. However, operational technology (OT) engineers may find it cumbersome to set up and maintain their own cloud servers for new services and applications. There is considerable effort associated with setting up new infrastructure, even in the cloud. Fortunately, original equipment manufacturers (OEMs) and machine builders can now deliver secure cloud-based services and remote access to their customers, therefore eliminating the need to maintain in-house cloud servers.

A key issue that demands scrutiny is the cloud server license scheme. Often, upfront costs may seem low for limited server hosts. Yet these apparent cost savings on server hosts may actually make a project uneconomical due to the limited scale of connections. Second, you may also need to consider central management capabilities to flexibly expand remote connections as your needs change. With this said, carefully weigh the costs and benefits of incorporating secure remote access to industrial networks. Always select solutions that minimize hassles and will help deliver more value to customers.

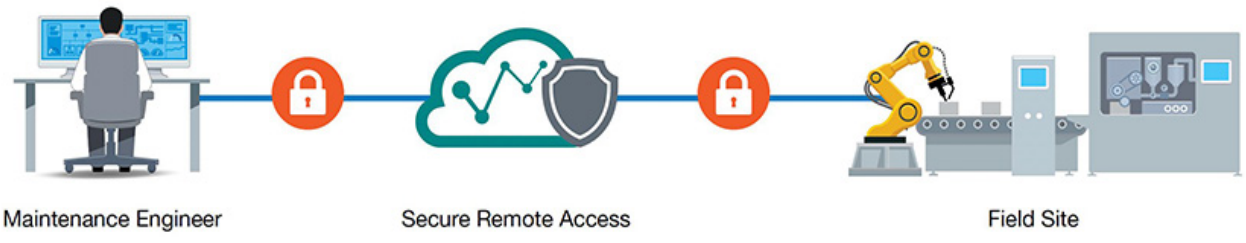



Figure 2. Cloud-based secure remote access can provide flexible and scalable connections to meet the dynamic, changing requirements of the future.

## 3 Use management software for better network status visibility

When complexity increases due to greater connectivity on industrial networks, it can become difficult to identify the root cause of problems and maintain sufficient network visibility. Control engineers often have to revert to trial and error to get the system back to normal, which is time-consuming and troublesome.

To facilitate and manage growing industrial networks, network operators need integrated network management software to make informed decisions throughout network deployment, maintenance, and diagnostics. In addition, as systems continue to grow, it is important to pay attention to a number of network integration concerns. First, only managing industrial networks in local control centers may not be feasible three or five years from now, especially when existing systems need to be integrated with new ones. It is therefore important to use network management software with integration interfaces such as OPC DA tags for supervisory control and data acquisition (SCADA) system integration or RESTful APIs for external web services. Furthermore, an interface to facilitate third-party software integration is also a key criterion for ensuring future flexibility.

For many industries, the IIoT presents as many challenges as opportunities. Nonetheless, this new frontier where traditional OT and IT silos converge is clearly the way of the future. Successfully deploying an IIoT application requires careful planning and attention to detail from the moment you decide to begin the journey. As a pioneering expert in industrial networking, Moxa provides a number of innovative technologies and solutions to help speed up network readiness for future IIoT applications.

### ABOUT THE AUTHOR

**Roger Chen** is manager of Cybersecurity Market Development at Moxa, Inc. Moxa's connectivity technology helps to make ideas real. We develop reliable network solutions that enable devices to connect, communicate, and collaborate with systems, processes, and people.

# What Is ETHOS, and Why Now?

## How an open sharing platform is helping critical infrastructure.

By Danielle Jablanski, Nozomi Networks

A group of cybersecurity companies that specializes in industrial control systems (ICS) and operational technology (OT) security recently launched ETHOS, the Emerging Threat Open Sharing platform. The platform is meant for sharing early warning signs across critical infrastructure owners and operators monitoring their OT networks and activity. ETHOS is a GitHub community project. The founding members aim to make the platform fully open source after an initial beta test of their proof of concept.

Founding members include 1898 & Co., ABS Group, Claroty, Dragos, Forescout, NetRise, Network Perception, Nozomi Networks, Schneider Electric, Tenable, and Waterfall Security. Any security vendor can build an

integration for an ETHOS server, and any organization, group, or company can develop and host its own ETHOS server.

The platform is being built to correlate security events across any number of end users, regardless of the security solutions they use, and requires integration with security vendor technologies to send and receive correlated notifications. ETHOS currently has a beta API that provides data-sharing functionality, and an initial server is in development. Shared information for ETHOS signs includes MITRE TTPs, IP addresses, hashes, and domains.

**The GitHub community project** is being built to correlate security events across end users, regardless of the security solutions they use.

## Information-Sharing Trends

There are IT attacks that can cause process shutdowns out of caution, IT attacks that can impact OT systems directly as collateral damage, and OT- or ICS-specific attacks that exploit IT components as access points. Whether asset owners and sectors are preparing for the worst possible targeted attack or the perfect storm of an accident, defenders are left feeling as though they're searching for a needle in many haystacks. Four key trends have emerged for information sharing across critical infrastructure sectors:

- There has been broad realization that operations that tolerate little to no physical downtime are lucrative targets, with seemingly no sector that is off limits—food, hospitals, transportation—and tailored attacks are increasing.
- There are two different types of information sharing: known detections or "fully baked" intelligence based on something seen before and early warning indicators for novel attacks.
- Silos exist that are sector specific, within the private sector, and across government and international agencies, creating single sources of intelligence without due diligence and corroboration to indicate the significance of shared intelligence.
- Single points of dependence and failure exist across equipment, cybersecurity, and businesses/operations involving people, processes, and technology alike.

## Information-Sharing Challenges

Given the trends in information sharing, it is becoming more difficult for security teams to utilize available threat intelligence and understand how to reduce the severity of potential vulnerabilities in OT and ICS. Four key challenges have emerged for information sharing across critical infrastructure sectors:

- A key takeaway from much of the Cyber Solarium Commission's work is that industry is reluctant to aggregate information without a trusted third-party mechanism.
- No vendor-agnostic mechanism or platform exists for real-time sharing of early warning data.
- Despite commonalities, no two attacks on OT/ICS are ever exactly the same, and it is nearly impossible to fully automate remediation in process control systems and networks.
- Millions of potential targets with cyber-physical components and operations exist. Energy, manufacturing, water and wastewater, and food and agriculture facilities alone represent more than 8 million facilities and locations globally.

## Benefits of the ETHOS Platform

Threats to critical infrastructure can be adversarial or accidental, structural, and/or environmental. Increased digitization continues to expand the attack surface and propels technology interdependence. The OT cybersecurity industry is working to include real-world impact analysis into their products and solutions. Still, information sharing and prioritization across multiple sectors that deploy similar technologies in a multitude of purpose-built ways remains increasingly difficult.

There are many hypothetical scenarios and possibilities for OT/ICS cyber incidents, but less shared evidence and indicators for real-world cascading impacts. Lab experimentation and research is more useful than hyperbolic fearmongering. With widespread future adoption of the ETHOS platform and multiple interoperable servers, the open source platform has potential to deliver four key benefits to critical infrastructure:

- Correlation of early warning data has the potential to reduce dwell times for malicious threat actors doing reconnaissance in critical infrastructure networks and environments.
- Early warning and reduced dwell time has the potential to reduce the severity of fully completed threat actor campaigns, exploitation capacity, delivered payloads, downtime, and physical impacts.
- Like vulnerability researchers deploy reverse engineering to understand the exploitation and payloads crafted by threat actors, ETHOS participants can begin to do reverse reconnaissance analysis.
- This analysis can assist global threat research teams with selecting particular systems and technologies to research for CVE disclosures and global cyber threat intelligence teams with enhanced understanding of frequently deployed TTPs in early phases of the cyber kill chain in critical infrastructure.

ETHOS is not a shared proprietary threat intelligence feed with signatures, detections, and alerts from competitive monitoring tools and solutions. ETHOS is also not a replacement for STIX/TAXII and is complementary to STIX/TAXII information sharing. The ETHOS platform is run by an independent mutual benefit corporation with an open-source GitHub community. No central authority retains ownership of its intellectual property. Governance is structured by community members and licensed users, and membership applications will be available in June 2023.

## ABOUT THE AUTHOR

Danielle Jablanski is an OT Cybersecurity Strategist at Nozomi Networks. She is responsible for researching global cybersecurity topics, and promoting OT and ICS cybersecurity awareness throughout the industry.

# Effectively Securing Operational Technology

In 2023, three-fourths of operational technology (OT) organizations reported at least one intrusion in the previous year. Nearly one-third reported being victims of a ransomware attack (unchanged from 2022), but intrusions from malware and phishing increased 12% and 9%, respectively.

The frequency of attacks against industrial production systems has increased for several reasons, including the converging of OT systems with information technology (IT) systems, the emergence of cybercrime-as-a-service, the greater availability of attack kits on the dark web, and the increased vulnerability to interruption of high-value

By Richard Springer, Fortinet

> By learning from the past, industrial firms can prepare to respond to threats.

production systems and critical infrastructure. At the same time, the range of targets that represent OT and cyber-physical systems has increased as well.

Critical infrastructure assets related to water and electricity are increasingly targeted, and it's critical that they be safeguarded. When considering the dangers associated with these threats, it's vital to remember that many OT subsectors continue to depend on legacy hardware and software. Additionally, manufacturing continues to grow as a target. In recent industrial events, the adversaries have monetized production loss as part of their ransomware target selection.

Today, leading-edge cybersecurity strategies and solutions are essential. For many OT organizations, safety, dependability, and uptime are their top priorities, so it's more difficult than it might seem to manage OT cybersecurity risks. By learning from the past and taking proactive measures, industrial firms can negotiate the current OT environment while keeping security in mind.

**Cybersecurity knowledge** is significantly higher than it has ever been, but a network breach isn't just a possibility—it's an inevitability.

## Learning from the past

When it comes to OT security, cybersecurity knowledge is significantly higher than it has ever been. The C-suite and boards across industries are seeking information and doing their own research. With that said, a network breach isn't just a possibility—it's an inevitability.

Every organization should have an incident response plan and playbooks in place to prepare for the inevitable. Executives also require a communications plan and an understanding of their responsibilities. When an event occurs, everyone should be aware of any regulatory reporting obligations and put plans into practice rather than merely relying on theory. Assessments are part of the planning process. Assess the technology, be forthright about what you can do, and make sure to cover any gaps.

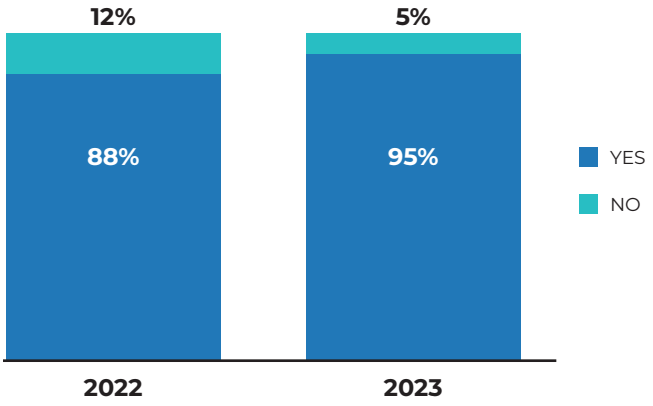



Figure 1. The proportion of OT professionals who thought OT cybersecurity would be moved to be under the chief information security officer (CISO) in the next 12 months. *Source: Fortinet State of Operational Technology and Cybersecurity Report*

Maintaining OT security is the responsibility of managers and directors in a range of roles, including plant operations. An important finding from the *2022 State of Operational Technology and Cybersecurity Report* was that organizational leaders are concerned about OT security, but the function is still managed by people in relatively low-ranking positions; however, 88% of respondents said they planned to place the responsibility for cybersecurity under a chief information security officer (CISO) in the next 12 months (Figure 1). A follow-up study in 2023 found that 95% of organizations said they planned to shift cybersecurity responsibility to the CISO. This increase indicates that the C-suite is taking OT security more seriously, but further action is needed.

## Getting a better handle on OT security

The damage from a network breach is considerably more expensive than the capital outlay for security and proactive incident response planning. In business environments, a data breach typically costs more than $4 million, but in OT environments, the costs can be much higher because of production and supply chain concerns. To keep OT systems secure, organizations should:

- employ network segmentation to shrink the threat landscape
- adopt a zero-trust methodology

- implement network access control (NAC) technology
- develop a vendor and OT cybersecurity platform strategy
- incorporate cybersecurity awareness training for all employees.

Let's dig deeper into the first two recommendations.

## Network segmentation

Industrial organizations can use network segmentation to stop unauthorized users from accessing their most important industrial assets, including programmable logic controllers (PLCs), industrial controls systems, and human-machine interfaces (HMIs).

Network segmentation enhances security by keeping attacks from propagating throughout a network and attacking vulnerable devices. It also lessens congestion, which frequently causes a decrease in performance. Network efficiency is crucial for resource-intensive services like those provided by factories, power plants, water treatment facilities, and oil rigs.

Network segmentation can be particularly challenging in an OT context because of the possibility of unintentionally affecting production during the segmentation process. The difficulties may be compounded when trying to segment an environment with devices from many providers. But with the right tools and processes in place, it is possible to successfully segment the network and even divide it further to take advantage of microsegmentation.

With microsegmentation, security architects can further segment an environment to provide lateral views of all assets in the same broadcast domain. Logically segmenting the network environment into unique security areas all the way down to the level of a single task achieves granularity. Because policies are applied to specific workloads, microsegmentation increases attack resistance by inhibiting a hacker's ability to migrate between compromised applications in the event of a breach.

## Adopting zero trust

Zero-trust approaches are similar between IT and OT, but the risk mitigation strategies are quite different. In IT, the major worry is someone hacking into systems and taking data. But in an OT environment if a key piece of equipment or system fails, millions of dollars could be at stake. An organization should have a risk mitigation plan that fits its requirements and allocate its resources accordingly.

Supporting a zero-trust approach requires building a strong asset management program. Industrial organizations are aware of the difficulty involved in creating an asset list and a configuration management database (CMDB). In some cases, multiple department-specific views of what an asset is may exist, and teams should have visibility into all of them. Consequently, the IT team may be able to view the environment differently with the use of tools and cabling capabilities that enable them to manage IT and OT assets more effectively.

The zero-trust security model involves more than just technology. Although the planned technologies should be evaluated, organizations also need to determine who is in charge of asset management and understand the data inventory. How is data stored and what databases are used? Where in the environment is that data going? To increase the effectiveness of technology, it's important to consider all of the people and processes involved.

Because all teams have a part to play, roles and relationships within the organization also must be defined. Most teams are likely to have some level of operational responsibility. For example, cybersecurity teams need visibility. Data needs to be accurate, timely, and of high quality. Yet the cybersecurity team does not own the data all the time. Asset management and even access management are foundational to the security team's function and essential to solving some problems, but that team doesn't ultimately own them. Larger organizations with many functions also generally have an internal audit function, and it's important to ensure that the assets are tracked and that the policies and procedures are being followed.

## Fail fast and partner often

Technology advances like the Industrial Internet of Things (IIoT) and 5G are affecting OT architecture, but it's important to be proactive and consider the security measures required for new technology.

To deal with advanced persistent threats, manufacturers also need to employ behavioral-based detection that incorporates the most recent, real-time threat intelligence. Threat actors are concentrating on reconnaissance, looking for ways to transform new technologies into weapons, and bypass security roadblocks, so it's important to have machine learning and artificial intelligence (AI)-based behavioral defense.

Even though no one can accurately forecast the future of OT cybersecurity, it's a good idea to embrace resilience and include partners in the equation. Adopt the "Fail fast, partner often" strategy. Without partners, scaling at the breadth and speed necessary today is impossible.

## Navigating the complex, converged OT cyber landscapes

Escalating cyber threats to critical infrastructure and lessons from past breaches underscore the inevitability of attacks. Collaborative C-suite leadership, proactive planning, and the right technology are pivotal. To secure OT networks, it's important to take advantage of network segmentation strategies and zero-trust approaches along with resilience and adaptability. Securing today's networks requires integrated solutions, robust partnerships, and unwavering CISO-led commitment. Because to succeed against relentless cyber adversaries, organizations must be both prepared and agile to present a united front.

### ABOUT THE AUTHOR

**Rich Springer** is the marketing director of OT Solutions at Fortinet. In this role, he works alongside regional marketing teams, OT product management, and OT threat researchers to promote the Fortinet Fabric of OT Solutions including network security, zero-trust, security operations, and AI-powered threat intelligence for IT/OT converged and OT market segments. Springer has a BS in mechanical engineering from Oregon State University.